



Una Entidad de Referencia de Portabilidad Numérica (ERPN) para Costa Rica

Respuesta Técnica

Jueves 28 de mayo de 2026

TRANSACTION NETWORK SERVICES, INC. CONFIDENCIAL – ACCESO RESTRINGIDO

Este documento y la información confidencial que contiene serán usados por la Superintendencia de Telecomunicaciones (Sutel) solo para considerar un posible acuerdo comercial con Transaction Network Services, Inc. y para ningún otro fin; y serán distribuidos, enviados o puestos a disposición solamente de las personas autorizadas que deban tomar conocimiento dentro de la Sutel, pero no de terceros, salvo con el consentimiento previo por escrito de Transaction Network Services, Inc.

©2026 Transaction Network Services, Inc. - Todos los derechos reservados

Tabla de Contenidos

| | | |
|----------|---|-----------|
| 1 | Resumen Ejecutivo | 1 |
| 1.1 | Propuesta de TNS para la Entidad de Referencia de Portabilidad Numérica (ERPN) de Costa Rica | 1 |
| 1.2 | Una solución de ERPN integral y probada para Costa Rica | 3 |
| 1.3 | Liderazgo en el Mercado Global – Implementación de Soluciones de Portabilidad Numérica en 13 Países | 5 |
| 1.4 | Diseño y desempeño adaptable y flexible | 7 |
| 1.5 | Capacidades de desarrollo y entrega de software | 8 |
| 1.6 | Solución ERPN de Extremo a Extremo con Arquitectura Escalable y Preparada para el Futuro | 10 |
| 1.7 | Por qué TNS | 11 |
| 1.8 | Contactos | 11 |
| 2 | Descripción general de la solución | 12 |
| 2.1 | | 12 |
| 2.2 | | 25 |
| 2.3 | | 27 |
| 2.4 | | 34 |
| 2.5 | | 35 |
| 2.6 | | 36 |
| 2.7 | | 36 |
| 2.8 | | 37 |
| 2.9 | | 38 |
| 2.10 | | 41 |
| 2.11 | | 42 |
| 2.12 | | 45 |
| 2.13 | | 46 |
| 2.14 | | 47 |
| 2.15 | | 50 |
| 2.16 | | 51 |
| 2.17 | | 51 |
| 2.18 | | 59 |
| 2.19 | | 64 |
| 2.20 | | 65 |
| 2.21 | | 66 |
| 2.22 | | 74 |
| 2.23 | | 75 |
| 2.24 | | 78 |
| 2.25 | | 80 |

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

| | |
|--|------------|
| 2.26..... | 83 |
| 2.27..... | 83 |
| 2.28..... | 84 |
| 2.29..... | 85 |
| 2.30..... | 86 |
| 2.31..... | 87 |
| 2.32..... | 88 |
| 2.33..... | 89 |
| 2.34..... | 90 |
| 2.35..... | 91 |
| 2.36..... | 94 |
| 2.37..... | 97 |
| 2.38..... | 98 |
| 3 Principales procesos de operación..... | 99 |
| 3.1..... | 99 |
| 3.2..... | 100 |
| 3.3..... | 100 |
| 3.4..... | 101 |
| 3.5..... | 104 |
| 3.6..... | 104 |
| 3.7..... | 105 |
| 3.8..... | 106 |
| 3.9..... | 106 |
| 3.10..... | 107 |
| 3.11..... | 107 |
| 3.12..... | 108 |
| 3.13..... | 109 |
| 3.14..... | 109 |
| 3.15..... | 110 |
| 3.16..... | 110 |
| 3.17..... | 111 |
| 3.18..... | 111 |
| 4 Implementación, continuidad y mejora innovadora del SIPN..... | 113 |
| 4.1..... | 113 |
| 4.2..... | 119 |
| 4.3..... | 120 |
| 4.4..... | 124 |
| 5 Sistema para interposición de tickets para consultas, incidencias y solicitudes de servicio entre operadores/proveedores, la Sutel y/o la ERP. | 126 |

| | |
|--|------------|
| 5.1..... | 126 |
| 5.2..... | 131 |
| 5.3..... | 131 |
| 5.4..... | 132 |
| 5.5..... | 133 |
| 5.6..... | 134 |
| 5.7..... | 135 |
| 5.8..... | 136 |
| 5.9..... | 137 |
| 5.10..... | 137 |
| 5.11..... | 138 |
| 6 Acuerdos de nivel de servicio mensuales (SLA) | 141 |
| 6.1..... | 145 |
| 6.2..... | 149 |
| 6.3..... | 150 |
| 6.4..... | 151 |
| 6.5..... | 152 |
| 6.6..... | 153 |
| 6.7..... | 155 |
| 7 Causales de resolución contractual | 157 |
| 7.1..... | 157 |
| 7.2..... | 157 |
| 7.3..... | 157 |
| 7.4..... | 157 |
| 7.5..... | 158 |
| 7.6..... | 158 |
| 7.7..... | 158 |
| 7.8..... | 158 |
| 7.9..... | 159 |
| 7.10..... | 159 |
| 8 Validación biométrica con prueba de vida (OPCIONAL) | 160 |
| 8.1..... | 160 |
| 8.2..... | 167 |
| 8.3..... | 168 |
| 8.4..... | 169 |
| 8.5..... | 170 |
| 8.6..... | 171 |
| 8.7..... | 171 |
| 9 Requisitos de admisibilidad de la oferta | 183 |

| | | |
|-----------|---|------------|
| 10 | Notificaciones | 192 |
| 11 | Marcas Registradas | 193 |
| 12 | Anexos | 194 |
| | Anexo 1 – Caso de Estudio : <i>Implementación de la Portabilidad Numérica Móvil y Fija en Perú</i> | 195 |
| | Anexo 2 – <i>Cartas de Referencias de Operacion</i> | 200 |
| | Anexo 3 – <i>Cartas de Referencia de Migración</i> | 208 |
| | Anexo 4 – <i>Declaración jurada de que el oferente no tiene vínculos económicos, propiedad o control por parte de algún operador/proveedor de telecomunicaciones de Costa Rica.</i> | 213 |

1 Resumen Ejecutivo

1.1 Propuesta de TNS para la Entidad de Referencia de Portabilidad Numérica (ERPN) de Costa Rica

Propuesta de valor de TNS: Menor Riesgo, Mayor Valor y Total Cumplimiento a los requisitos de la RFP de SUTEL.

Transaction Network Services, Inc. (TNS) se complace en presentar esta respuesta formal a la Solicitud de Propuesta (RFP) emitida por la Superintendencia de Telecomunicaciones (SUTEL) para la implementación, operación y evolución de la Entidad de Referencia de Portabilidad Numérica (ERPN) en Costa Rica..

En 2025, Koch Equity Development (KED) completó la adquisición de iconectiv, consolidando capacidades líderes globales en numeración y portabilidad dentro de su portafolio. KED es también propietario de TNS, adquirida en 2021, lo que permite integrar fortalezas complementarias en infraestructura, software y operación de redes críticas.

A partir del 1 de enero de 2026, las plataformas **TruNumber**, **TruOps** y **TruReach** fueron incorporadas al portafolio de TNS, reforzando su posicionamiento como proveedor integral de soluciones de telecomunicaciones y portabilidad numérica a nivel global.

Dentro de este portafolio, **TruNumber Portability Clearinghouse (TNPC)** constituye la plataforma central para la implementación de soluciones de **Entidad de Referencia de Portabilidad Numérica (ERPN)**. TNPC ha sido diseñada específicamente para:

- Facilitar a los reguladores la implementación eficiente de la portabilidad numérica
- Permitir que los operadores cumplan de manera ágil y confiable con los mandatos regulatorios
- Proveer una infraestructura centralizada, segura y escalable para la gestión de portaciones

Apalancando la experiencia técnica acumulada de iconectiv y las capacidades operativas de TNS, esta solución ofrece un modelo probado, flexible y adaptable a las necesidades regulatorias y de mercado de cualquier país.

TNS es un líder global en software y servicios de telecomunicaciones, ofreciendo soluciones abiertas, flexibles y configurables que soportan redes IP, fijas, móviles y de cable a nivel mundial. En el ámbito de portabilidad numérica, TNS proporciona soluciones completas de ERPN, incluyendo plataformas centralizadas, servicios administrados y soluciones de gateway de portabilidad tanto para operadores como para entidades regulatorias.

Actualmente, estas soluciones se encuentran implementadas en **13 países**, incluyendo múltiples despliegues basados en TNPC, lo que demuestra su madurez, escalabilidad y confiabilidad en entornos regulatorios diversos.

Para el soporte de estas soluciones, contamos con entidades en diferentes regiones y países, como pueden ver en la siguiente tabla:

| Entidades Globales TNS-iconectiv | | |
|-------------------------------------|---------------------------------------|--|
| Región | País | Nombre Legal Corporativo Oficial |
| Norteamérica | Estados Unidos | iconectiv, LLC (antes Telcordia Technologies, Inc.) |
| Latinoamérica | Argentina | Administradora de la Portabilidad Argentina S.A. (APA) |
| | México | iconectiv México, S. de R.L. de C.V. |
| | Chile | Telcordia Technologies Chile Limitada |
| Asia-Pacífico | India | MNP Interconnection Telecom Solutions India Pvt. Ltd. (MITS) |
| | Mercados de Asia / Pacífico (General) | Telcordia Technologies, Inc. (Sucursales Locales / Alianzas) |
| Medio Oriente y África | Medio Oriente / Arabia Saudita | Telcordia Technologies, Inc. (Sucursal de Arabia Saudita) / Alianzas de Operadores Locales |
| | Sudáfrica | Telcordia Technologies, Inc. (Sucursal de Sudáfrica) |
| Europa (Entidad Adicional) | Unión Europea (Registrada en Irlanda) | iconectiv Europe Limited |

Como resultado, la SUTEL podrá beneficiarse de:

- **Capacidades avanzadas de desarrollo de software**, que permiten evolución continua y rápida adaptación regulatoria
- **Experiencia probada en la entrega de proyectos a escala nacional**, en entornos complejos y multioperador
- **Profundo conocimiento de las operaciones e interdependencias de redes de telecomunicaciones**
- **Reputación de ser una compañía confiable, neutral y estable** desde el punto de vista financiero
- **Una trayectoria comprobada de colaboración con reguladores, gobiernos y operadores** en múltiples implementaciones de portabilidad numérica a nivel global

Soluciones probadas de TNS: Desde 1990, TNS se ha consolidado como un proveedor de confianza en servicios de redes y datos integrados, soportando a organizaciones líderes en pagos globales y comunidades financieras, así como a operadores de telecomunicaciones a nivel mundial. Esta trayectoria posiciona a TNS como un socio estratégico para la provisión de infraestructura crítica, segura y de alta disponibilidad.

TNS opera algunas de las redes de comunicaciones de datos en tiempo real más extensas del mundo, permitiendo a los participantes de distintas industrias interactuar y realizar transacciones de manera eficiente, segura y confiable. Estas capacidades habilitan el acceso a datos y aplicaciones críticas mediante plataformas de comunicaciones administradas, diseñadas para altos niveles de desempeño y resiliencia.

La infraestructura global de TNS soporta millones de conexiones activas y acceso a bases de datos críticas, integrando de forma segura redes públicas y privadas. Este modelo permite a los clientes operar bajo

esquemas de conectividad “uno a muchos” y “muchos a muchos” mediante una única interfaz, simplificando la operación y garantizando eficiencia a escala global.

A partir del 1 de enero de 2026, la incorporación de las plataformas **TruNumber, TruOps y TruReach** al portafolio de TNS fortalece significativamente sus capacidades tecnológicas y operativas. Esta integración permite a TNS ofrecer una propuesta aún más robusta y diferenciada, basada en:

- **Un portafolio ampliado de productos**, que incluye soluciones avanzadas de voz, mensajería, mitigación de fraude e inteligencia de redes
- **Un mayor acceso a talento especializado y experiencia de la industria**, que acelera la capacidad de innovación y adaptación a nuevas demandas del mercado
- **Una integración operativa sin fricciones**, que garantiza continuidad de servicio y altos estándares de seguridad y desempeño

Desde su creación, TNS ha acompañado a sus clientes en la transición desde tecnologías legadas hacia plataformas de última generación, facilitando la evolución tecnológica del ecosistema de telecomunicaciones. Actualmente, la compañía ofrece un amplio portafolio que abarca desde soluciones de conectividad dedicada hasta servicios gestionados de redes IP, con soporte local y alcance global para empresas y operadores de todos los tamaños.

Adicionalmente, TNS incorpora la experiencia y legado de iconectiv, que cuenta con más de 30 años de contribución a la industria de telecomunicaciones. Esta trayectoria incluye su evolución desde Bell Communications Research (“Bellcore”), posteriormente Telcordia, hasta su consolidación como iconectiv, participando en el desarrollo de algunos de los sistemas de telecomunicaciones más avanzados del mundo.

Este legado refuerza la capacidad de TNS para diseñar, implementar y operar soluciones críticas a nivel nacional, incluyendo sistemas fundamentales para la operación eficiente y segura de la portabilidad numérica.



1.2 Una solución de ERPN integral y probada para Costa Rica

La solución de ERPN de TNS consta de destacados Servicios de Configuración, Servicios Administrados y Servicios de Gestión de Programas.

TNS comprende plenamente los requerimientos establecidos por la SUTEL y presenta una **propuesta integral para la implementación y operación de la Entidad de Referencia de Portabilidad Numérica (ERPN)** en Costa Rica.

Nuestra solución abarca de manera completa el **establecimiento, diseño, implementación, administración, operación, mantenimiento y evolución** del sistema de portabilidad numérica, incluyendo la gestión de la base de datos central de numeración.

La propuesta de TNS consiste en una solución **centralizada, probada y de alta confiabilidad**, complementada por servicios profesionales especializados que garantizan su correcta implementación y operación a lo largo de todo el ciclo de vida del proyecto.

La solución de ERP se fundamenta en la plataforma **TruNumber Portability Clearinghouse (TNPC)**, que integra un motor avanzado de gestión de portaciones junto con una base de datos de referencia centralizada, permitiendo la portabilidad eficiente de números móviles y fijos entre operadores.

En este contexto, TNPC proporcionará las siguientes capacidades clave:

- **Gestión automatizada de portaciones:** permitirá a los operadores procesar, validar, activar y gestionar de forma automática las solicitudes de portabilidad de sus suscriptores, reduciendo tiempos operativos y errores manuales
- **Enrutamiento eficiente mediante ACQ:** garantizará que todos los operadores en Costa Rica accedan a información actualizada de enrutamiento, facilitando la correcta terminación de llamadas y el envío de SMS/MMS hacia números portados mediante el esquema *All Call Query (ACQ)*
- **Soporte integral a múltiples bases de datos:** incluirá repositorios especializados que soportan distintos tipos de portabilidad (móvil, fija, geográfica e intermodal), así como bases complementarias críticas, tales como la base de datos de equipos bloqueados y la base nacional de números de emergencia
- **Acceso regulatorio y analítica:** proporcionará a la SUTEL y a las entidades autorizadas acceso seguro a datos, reportes y herramientas analíticas relacionadas con el proceso de portabilidad, facilitando la supervisión, control y toma de decisiones regulatorias

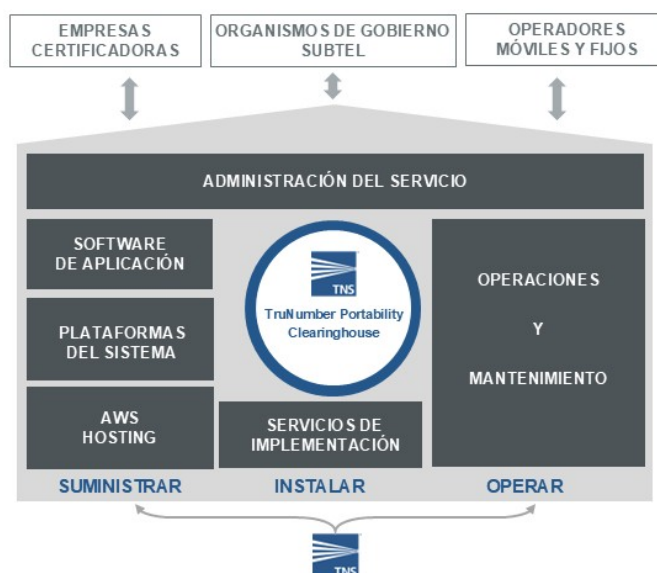


Figura 1 – Componentes de TNPC de TNS para Costa Rica

TNS proporcionará una solución integral que combina tecnología probada, servicios especializados y operación continua, abarcando todos los componentes necesarios para garantizar el funcionamiento eficiente y seguro del sistema.

En particular, TNS ofrecerá:

- **Software licenciado:**
Suministro de la plataforma **TruNumber Portability Clearinghouse (TNPC)**, incluyendo su configuración inicial, localización conforme a los requerimientos de Costa Rica y documentación completa de soporte técnico y funcional.
- **Servicios de implementación:**
Instalación y configuración del sistema, ejecución de pruebas de aceptación, habilitación de accesos para operadores, coordinación y ejecución de pruebas de industria, capacitación a usuarios clave, entrega de documentación y puesta en operación en ambiente productivo.

- **Gestión del programa:**
Dirección integral del proyecto mediante la planificación, organización y coordinación de todas las actividades requeridas para asegurar una implementación exitosa y el cumplimiento del cronograma establecido.
- **Servicios administrados:**
Soporte técnico continuo para la plataforma TNPC, incluyendo la atención de incidentes, resolución de problemas, gestión de versiones y parches, así como la administración de la infraestructura y operación del sistema en la nube.
- **Infraestructura de cómputo segura:**
Provisión y operación de la infraestructura tecnológica en la nube (AWS), soportando los ambientes de **producción, recuperación ante desastres (DRP) y pruebas**, bajo estándares de alta disponibilidad, seguridad y resiliencia.
- **Operación y mantenimiento:**
Servicios operativos integrales que incluyen mesa de ayuda, administración del sistema y de la base de datos, monitoreo continuo, respaldo y restauración de información, así como mantenimiento preventivo y correctivo de la plataforma e infraestructura.
- **Administración del servicio:**
Gestión formal del servicio mediante procesos estructurados de operación, incluyendo administración de servicios, soporte de ingeniería de sistemas y gestión de facturación asociada.

1.3 Liderazgo en el Mercado Global – Implementación de Soluciones de Portabilidad Numérica en 13 Países

TNS cuenta con una trayectoria comprobada en la operación de Entidades de Referencia de Portabilidad Numérica, respaldada por un equipo de expertos de tiempo completo con amplia experiencia en implementaciones a escala nacional.

Experiencia y Trayectoria: TNS cuenta con una trayectoria comprobada como proveedor líder de soluciones de **portabilidad numérica y plataformas de ERPNI**, soportando más de **2 mil millones de suscriptores en 13 países**, incluyendo Vietnam, Argentina, Túnez, Estados Unidos, Canadá, Chile, México, Grecia, India, Malasia, Emiratos Árabes Unidos y Sudáfrica.

La plataforma **TruNumber Portability Clearinghouse (TNPC)** se encuentra actualmente implementada en múltiples mercados internacionales, lo que demuestra su madurez, escalabilidad y confiabilidad en entornos regulatorios diversos.

TNS se distingue por su capacidad de diseñar e implementar soluciones de portabilidad numérica en **entornos geopolíticos, operativos y técnicos complejos**, adaptándose a marcos regulatorios específicos y a escenarios multioperador de alta exigencia.

Asimismo, TNS actúa como **Entidad de Referencia de Portabilidad Numérica (ERPNI)** en diversos países, proporcionando un modelo de operación **neutral, seguro y confiable**, alineado con las mejores prácticas internacionales.

Un elemento diferenciador clave es la capacidad de TNS para **facilitar la coordinación y el consenso entre los distintos actores del ecosistema** —regulador, operadores y otras entidades—, especialmente durante las fases críticas de diseño e implementación previa al lanzamiento de la portabilidad numérica.

entrega de software a tiempo

100% de entrega de software a tiempo



Figura 2 – Presencia Global de la Portabilidad Numérica de TNS

Experiencia operativa consolidada: Los ocho sistemas **TruNumber Portability Clearinghouse (TNPC)** actualmente en producción a nivel global acumulan **más de 100 años de operación combinada**, lo que constituye una trayectoria altamente significativa y comprobada en entornos reales.

Este desempeño se sustenta en décadas de experiencia en el diseño, implementación y operación de soluciones alojadas para la industria de telecomunicaciones en América del Norte desde 1984, lo que ha permitido a TNS desarrollar metodologías, arquitecturas y prácticas operativas ampliamente probadas.

Al seleccionar a TNS, Costa Rica contará con una solución de **Entidad de Referencia de Portabilidad Numérica (ERPN)** basada en componentes y procesos ya validados en múltiples implementaciones, lo que se traduce en **menor riesgo de implementación**, mayor estabilidad operativa y tiempos de despliegue optimizados.

Equipo de expertos de clase mundial: TNS dispone de un equipo de profesionales altamente calificados y de dedicación completa, con experiencia en planificación, diseño, desarrollo de software, pruebas, ingeniería y gestión de proyectos de portabilidad numérica.

Un factor diferenciador clave es la **continuidad del equipo técnico**, ya que el núcleo del grupo responsable del desarrollo de TNPC ha participado desde su primera implementación en Grecia en 2004. Esta continuidad garantiza:

- Profundo conocimiento práctico de los procesos de portabilidad numérica
- Madurez técnica en la evolución del producto
- Capacidad probada para anticipar y mitigar riesgos en implementación

En conjunto, la combinación de tecnología probada y un equipo altamente especializado permite a TNS ofrecer una solución ERPN robusta, confiable y alineada con las mejores prácticas internacionales.

TNS posee un conocimiento integral de los entornos de los operadores y una experiencia comprobada en la integración eficiente de sistemas back-end y flujos de trabajo con plataformas de ERP.

El entendimiento integral de TNS de los procesos de negocio y flujos operativos de los operadores ha permitido la integración exitosa de sus soluciones en múltiples entornos a nivel internacional.

Sumado a su experiencia en portabilidad numérica, TNS cuenta con la capacidad de analizar el impacto de estas soluciones sobre el negocio, las infraestructuras y la operación de red de los operadores, para **definir e implementar enfoques óptimos tanto a nivel de ingeniería como comercial**

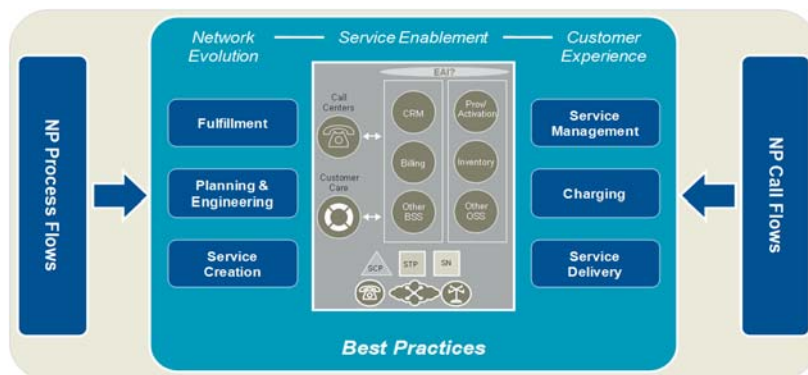


Figura 4 – Impacto de la Portabilidad Numérica en los Sistemas, Procesos y Redes de los Operadores

En particular, el entendimiento detallado de TNS de los procesos de negocio y flujos de trabajo de portabilidad numérica ha sido un factor clave para la integración exitosa de las soluciones TNPC y los gateways de TNS con los sistemas de negocio y las redes de los operadores.

Esta capacidad permite soportar de manera eficiente tanto el procesamiento de portaciones como el enrutamiento de llamadas, asegurando interoperabilidad y continuidad operativa en entornos multioperador.

TNS proporciona soluciones de **ERP** y **gateways de portabilidad numérica** en 13 países, incluyendo Vietnam, Túnez, Argentina, Estados Unidos, Reino Unido, Chile, Emiratos Árabes Unidos, India, Malasia, Sudáfrica, Grecia, México y Canadá, lo que demuestra su capacidad para operar en entornos regulatorios y tecnológicos diversos.

1.4 Diseño y desempeño adaptable y flexible

La plataforma de TNS incorpora de manera comprobada la mayoría de las funcionalidades de portabilidad numérica establecidas en la RFP

En la actualidad, TNS soporta la mayoría de los mensajes y funcionalidades de portabilidad numérica requeridos para Costa Rica.

Gracias a su arquitectura flexible, la plataforma **TruNumber Portability Clearinghouse (TNPC)** es capaz de gestionar múltiples conjuntos de procesos y modelos de mensajería, permitiendo su adaptación a distintos esquemas regulatorios y operativos.

Asimismo, TNPC permite la incorporación de nuevos procesos y mensajes mediante configuración, sin necesidad de realizar modificaciones en el código de la aplicación, lo que reduce significativamente tiempos de implementación y riesgos asociados a cambios.

El sistema es altamente configurable y puede ajustarse de manera ágil tanto durante la fase de implementación como en operación, facilitando la adaptación continua a la evolución de los procesos de portabilidad y a los requerimientos específicos de Costa Rica.

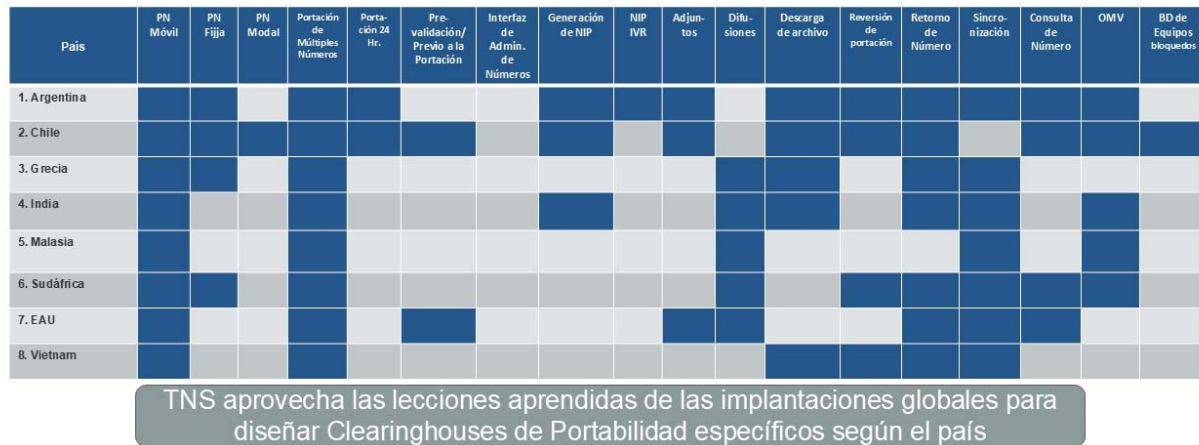


Figura 5 – Prestaciones y Capacidades Clave

TNS ha diseñado y dimensionado la solución de ERP para soportar los volúmenes de portación proyectados, asegurando escalabilidad, alto desempeño y continuidad del servicio..

La solución de **ERP** propuesta por TNS ha sido diseñada para soportar de manera eficiente los volúmenes de portación actuales de Costa Rica, y está preparada para escalar conforme crezcan las demandas de transacciones en el futuro.

La plataforma **TruNumber Portability Clearinghouse (TNPC)** se basa en una arquitectura modular orientada a componentes, lo que le permite ofrecer altos niveles de **escalabilidad, flexibilidad y disponibilidad**, adaptándose de manera ágil a nuevas necesidades de capacidad y desempeño.

El sistema soporta tanto **escalabilidad vertical como horizontal**, permitiendo absorber incrementos en el volumen de transacciones sin afectar la calidad del servicio. Esta arquitectura garantiza la continuidad operativa y el desempeño sostenido, tanto en escenarios actuales como futuros, **sin interrupciones para los operadores participantes**, independientemente de su rol en el proceso de portación.

1.5 Capacidades de desarrollo y entrega de software

TNS desarrolla internamente su software de Portabilidad Numérica y mantiene al equipo clave que lo diseñó, lo que garantiza control total sobre la evolución del producto, continuidad técnica y rápida capacidad de respuesta ante cambios regulatorios.

Un elemento diferenciador clave de TNS es su **capacidad interna de desarrollo de software de nivel empresarial**, orientada a la creación de soluciones robustas, seguras y de grado productivo.

TNS aplica metodologías de desarrollo enfocadas en la mejora continua de procesos, lo que permite garantizar calidad, trazabilidad y control en cada etapa del ciclo de vida del software.

Esta capacidad se traduce en beneficios directos para la SUTEL, ya que ante la necesidad de cambios regulatorios o funcionales en portabilidad numérica, TNS cuenta con la capacidad de:

- Evaluar rápidamente los impactos técnicos y operativos
- Proponer alternativas óptimas cuando sea necesario

- Implementar y entregar actualizaciones de manera oportuna y consistente

Este enfoque reduce significativamente los riesgos de interpretación, retrabajo y retrasos, facilitando una interacción eficiente sin necesidad de intermediación adicional.

Equipo especializado y experiencia comprobada. **TNS dispone de un equipo altamente calificado de especialistas de tiempo completo, con experiencia complementaria en portabilidad numérica, desarrollo de software, ingeniería, pruebas y gestión de proyectos.**

Este equipo acumula una amplia experiencia combinada en la implementación de soluciones de portabilidad numérica, respaldada por:

- Procesos rigurosos de pruebas funcionales y de desempeño
- Ejecución de pruebas de carga bajo distintos escenarios operativos
- Prácticas consolidadas de aseguramiento de calidad

Un diferenciador clave es la **profunda especialización acumulada en la plataforma TNPC**, que permite minimizar el tiempo de adopción, reducir curvas de aprendizaje y acelerar la ejecución del proyecto.

Además, la reutilización de componentes y lógica probada permite implementar nuevas funcionalidades mediante configuración o adaptación controlada, lo que contribuye directamente a:

- Reducción del riesgo de implementación
- Mayor estabilidad operativa
- Optimización de tiempos de despliegue

Como resultado, la solución propuesta para la ERPN se basa en elementos previamente validados en múltiples entornos, garantizando consistencia y confiabilidad.

Evolución continua del producto. **TNS mantiene un enfoque activo de evolución tecnológica de su plataforma, asegurando su alineación con las condiciones cambiantes del mercado y los requerimientos regulatorios.**

El equipo de gestión de producto define y actualiza continuamente la hoja de ruta de la solución, garantizando:

- Mejora continua de funcionalidades
- Adaptación a nuevas necesidades regulatorias
- Sostenibilidad tecnológica a largo plazo

TNS cuenta con un historial comprobado de cumplimiento en la entrega de software conforme a los cronogramas contractuales, alcanzando un 100% de entregas a tiempo en todas las implementaciones de TNPC.

TNS cuenta con una metodología consolidada para asegurar la **entrega oportuna de software de alta calidad**, basada en prácticas probadas de gestión y control de proyectos a lo largo de todo el ciclo de vida del desarrollo.

En particular, esta capacidad se sustenta en:

- **Alineación temprana y validación continua de requerimientos**, asegurando consenso entre las partes desde el inicio del proyecto
- **Gestión rigurosa de cambios**, incluyendo análisis de impacto, seguimiento estructurado y comunicación precisa de ajustes en los entregables
- **Monitoreo integral del ciclo de vida del proyecto**, con capacidades de análisis y seguimiento continuo del avance, desempeño y riesgos

- **Evaluación permanente del desempeño**, tanto del proceso como del proyecto, permitiendo la implementación de mejoras continuas

Apoyado en esta metodología, así como en su amplia experiencia y conocimiento técnico, TNS garantiza la capacidad de entregar la solución de **ERPN** conforme a los plazos establecidos, respaldado por una trayectoria comprobada en implementaciones similares.

El equipo de gestión de programas de TNS asume la responsabilidad integral del proyecto, abarcando desde el desarrollo hasta la implantación, integración y ejecución de pruebas, asegurando coordinación efectiva entre todos los componentes técnicos y operativos.

Como resultado, TNS mantiene un historial consistente de cumplimiento de cronogramas, basado en prácticas de gestión estructuradas y una ejecución disciplinada en cada fase del proyecto.

1.6 Solución ERPN de Extremo a Extremo con Arquitectura Escalable y Preparada para el Futuro

La solución de portabilidad numérica de extremo a extremo de TNS es el resultado de décadas de experiencia y conocimiento técnico acumulado en la implementación de plataformas críticas a nivel global..

TNS ofrece una solución de **portabilidad numérica de extremo a extremo**, respaldada por una trayectoria global y una experiencia técnica ampliamente reconocida en la industria.

A lo largo de los años, **más de 100 países** han recibido capacitación y consultoría de TNS en temas de numeración y portabilidad numérica, lo que refleja su rol activo en el desarrollo de capacidades regulatorias y operativas a nivel internacional.

TNS ha contribuido significativamente al desarrollo de estándares de portabilidad numérica desde sus inicios en América del Norte en la década de 1990, participando en su evolución y fortalecimiento en distintos foros internacionales. Esta experiencia ha permitido consolidar **mejores prácticas aplicables a reguladores y operadores** en múltiples entornos.

Además de su solución de **Entidad de Referencia de Portabilidad Numérica (ERPN)**, TNS proporciona servicios y plataformas de **gateway de portabilidad numérica**, incluyendo implementaciones pioneras como la primera portación en vivo en Estados Unidos al inicio de la portabilidad fija en 1997. Esta trayectoria se complementa con un sólido historial de implementaciones internacionales en entornos diversos.

Innovación y evolución de la solución. **La trayectoria y la innovación continua de TNS en numeración y portabilidad numérica permiten ofrecer soluciones preparadas para la evolución del sector de telecomunicaciones en Costa Rica.**

La arquitectura de la solución ERPN basada en **TNPC** está concebida como una plataforma extensible y flexible, capaz de soportar nuevos casos de uso y requerimientos regulatorios. En este contexto, TNS podrá habilitar, según los intereses de la SUTEL, el análisis y eventual incorporación de soluciones complementarias como:

- **Registro de identidad de dispositivos móviles**
- **Registro de tarjetas SIM prepagas**
- **Registro de información de suscriptores**

Estas capacidades permiten aprovechar la infraestructura existente para fortalecer iniciativas regulatorias relacionadas con seguridad, trazabilidad y protección contra fraude.

Valor para la evolución del ecosistema en Costa Rica. **La experiencia acumulada de TNS en portabilidad numérica y numeración, junto con su enfoque de innovación continua, posiciona a la compañía como**

un socio estratégico para acompañar a la SUTEL y a los operadores en la evolución del ecosistema de telecomunicaciones en Costa Rica.

1.7 Por qué TNS

TNS ofrecerá a la SUTEL una solución de ERP respaldada por experiencia comprobada, orientada a minimizar el riesgo de implementación y maximizar el valor a largo plazo.

TNS se encuentra altamente capacitada para proporcionar la solución de **Entidad de Referencia de Portabilidad Numérica (ERP)** para Costa Rica, respaldada por una combinación única de experiencia, capacidades técnicas y trayectoria comprobada.

En particular, TNS ofrece:

- **Experiencia internacional comprobada**, con implementación y operación exitosa de soluciones de ERP en múltiples países
- **Una solución técnica probada y en cumplimiento con estándares regulatorios**, que asegura escalabilidad, confiabilidad y eficiencia operativa
- **Amplio conocimiento de procesos y prácticas de portabilidad numérica**, tanto a nivel nacional como internacional, que sustentan un diseño flexible y adaptable
- **Experiencia en integración de sistemas y operaciones de telecomunicaciones**, permitiendo la interoperabilidad eficiente entre la ERP y los entornos de los operadores
- **Solidez financiera y trayectoria estable**, garantizando la continuidad del servicio durante todo el ciclo de vida del proyecto
- **Capacidades avanzadas de desarrollo de software**, que permiten una rápida adaptación a cambios regulatorios y evolución continua de la solución
- **Un equipo de expertos altamente especializado**, con capacidad de respuesta ágil y soporte oportuno
- **Capacidad de coordinación y facilitación entre actores del ecosistema**, actuando como un tercero neutral y confiable entre reguladores, operadores y otras partes interesadas

Como resultado, TNS ofrece a la SUTEL una solución de ERP que combina **alta calidad, bajo riesgo de implementación y valor sostenido a largo plazo**, alineada con las necesidades actuales y futuras del entorno de telecomunicaciones en Costa Rica

1.8 Contactos

TNS espera contar con la oportunidad de analizar los contenidos y detalles de esta respuesta en mayor profundidad. Si tiene alguna pregunta sobre esta propuesta, por favor contacte a:

Ejecutivo de Cuenta

Sergio Trevino

TNS Inc.

10740 Parkridge Blvd, Suite 100

Reston, VA 20191, EE.UU.

Teléfono: +1 510-964-6049

correo electrónico: strevino@tnsi.com

Líder Técnico

Shanmugavel Krishnan

TNS Inc.

100 Somerset Corporate Blvd.

Bridgewater, NJ 08807, EE.UU.

Teléfono: +1 732-236-0930

correo electrónico: skrishnan2@tnsi.com

2 Descripción general de la solución

- 2.1** *Implementar el Sistema Integral de Portabilidad Numérica (SIPN) en Costa Rica en cumplimiento de las resoluciones RCS-319-2014 (Anexo 5), RCS- 027-2021 (Anexo 6) y los acuerdos 029-017-2024 (Anexo 7), 021-067-2024 (Anexo 8) del Consejo de Sutel garantizando la continuidad del servicio de portabilidad las cuales se anexan en el pliego de condiciones. El oferente deberá describir detalladamente la arquitectura de la solución propuesta, incluyendo diagramas de alto nivel, indicando si la infraestructura es dedicada, compartida o híbrida.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Cumplimiento con RCS-319-2014 (Anexo 5):

TruNumber Portability Clearinghouse (TNPC) de TNS fue desarrollado con el propósito de operar dentro de marcos de portabilidad numérica tales como los definidos por SUTEL conforme a RCS-319-2014. La solución implementa totalmente el **modelo de enrutamiento All Call Query (ACQ)** respaldado por una Base de Datos Administrativa Central (NPCDB), que garantiza que todos los números portados sean administrados por un solo repositorio autorizado. Esta **NPCDB** de TNPC **mantiene los números de enrutamiento (RN), estado de portabilidad e histórico completo de transacciones**, que permite a los operadores consultar y enrutar el tráfico conforme a las normas ITU-T E.164. En línea con el modelo regulatorio de Costa Rica, TNPC no solo gestiona la base de datos centralizada, sino que también soporta la **autonomía del operador a través de copias locales de enrutamiento**, ofreciendo robustos mecanismos de sincronización que incluyen **archivos diarios de difusión/actualización de enrutamiento y actualizaciones de bases de datos completas e incrementales**. Esto garantiza que todos los operadores mantengan tablas de enrutamiento precisas y actualizadas, a la vez que preserva la resiliencia e independencia operativa de la red a lo largo del ecosistema.

TNPC cumple totalmente con los flujos de trabajo de portabilidad punta a punta, definidos en el Anexo 5 que incluyen **generación de NIP, prevalidación, validación del donante, programación y activación dentro de los tiempos regulados**. TNPC aplica todas las limitaciones de tiempos obligatorias a través del flujo de trabajo y los motores de temporizadores del Manejador de Mensajes embebido, que incluye ventanas de respuesta del donante, programación dentro de las 48 horas (o menos, cuando corresponda) y la ejecución dentro de una ventana de cambio de una hora con mínima interrupción del servicio. TNPC incluye un **Sistema Automático de Verificación (SAV)**, que garantiza el **manejo seguro de NIP** mediante entrega de SMS y ofrece respaldo (*fallback*) sin inconvenientes a través de un **mecanismo de IVR**, que permite a los usuarios recuperar su NIP en forma audible cuando falla la entrega del SMS. Esta capacidad de IVR detecta el número originador, lo valida contra NPCDB y entrega el NIP en forma segura, lo que garantiza la continuidad del proceso de portabilidad y el cumplimiento total con los requerimientos de accesibilidad regulatoria.

TNPC también admite los escenarios de transacciones avanzadas requeridos conforme al Anexo 5 que incluyen **portabilidad de múltiples números usando la funcionalidad de NIP grupal**. Para solicitudes masivas, el sistema genera NIP individuales y NIP grupales que permiten la autenticación eficiente, a la vez que mantiene la validación y auditoría por número. Cada número de un grupo se procesa en forma independiente, lo cual garantiza que los rechazos individuales no invaliden toda la solicitud. Además, TNPC implementa una lógica de prevalidación integral, que admite tanto validaciones automáticas (por ej., solicitudes duplicadas, titularidad de numeración, estado activo) como validaciones asistidas por el donante (por ej., verificaciones de identidad, estado del pago, condiciones de subsidios); todo ello dentro de los estrictos tiempos de respuestas de los SLA. La plataforma también aplica salvaguardas regulatorias tales como evitar solicitudes de portabilidad simultáneas, validar motivos de rechazo centralmente para evitar usos indebidos y garantizar que los operadores donantes no puedan bloquear o demorar procesos fuera de las reglas definidas.

TNPC asegura la precisión y sincronización continuas a lo largo de todas las redes al generar **archivos diarios de difusión/actualización de enrutamiento y actualizaciones de enrutamiento en tiempo real**,

que son distribuidos a todos los operadores durante la ventana de cambio. Esto garantiza la consistencia inmediata de la información de enrutamiento y elimina las demoras de propagación. Los requerimientos de seguridad e integridad de datos se cumplen de forma integral a través de **encriptación punta a punta, control de acceso basado en roles, registros inmutables de auditoría y aplicación de estricta titularidad de datos**, que asegura que todos los datos de portabilidad se encuentren bajo control solo de SUTEL y los operadores autorizados.

TNPC no solo cumple con todas las disposiciones del Anexo 5, sino que además las mejora a través de una **arquitectura probada, escalable y altamente resiliente** que se ha implementado con éxito en 17 países y múltiples entornos de portabilidad a nivel internacional.

Cumplimiento con RCS-027-2021 (Anexo 6):

La solución de TNPC se alinea completamente con los detalles regulatorios introducidos conforme a RCS-027-2021, que mejoran el marco de portabilidad original al aclarar las condiciones de rechazo, limitar la excesiva actividad de portación y consolidar el control de cancelación. TNPC implementa estos requerimientos a través de un motor de reglas de negocio centralizado y configurable que asegura que todas las condiciones de rechazo, tal como numeración inválida (número inválido o número no pertenece al donante de la solicitud de portabilidad), solicitudes duplicadas o supera la cantidad máxima de portaciones permitidas, sean aplicadas en forma consistente a lo largo de todos los operadores. TNPC mantiene un histórico completo de transacciones por suscriptor de NPCDB, que permite la validación en tiempo real de los límites de portación anuales y el rechazo automático de solicitudes que no cumplen.

TNPC ofrece soporte total de los procesos de cancelación de portación mejorados definidos en el Anexo 6, incluyendo las cancelaciones indicadas por el operador o accionadas por SUTEL vía la interfaz SOAP o REST. TNPC aplica estrictos controles de acceso basado en roles para garantizar que se apliquen los privilegios de cancelación solo bajo las condiciones autorizadas, tal como intervención por SUTEL para el interés público o demoras operativas justificadas por el operador receptor. Todas las solicitudes de cancelación son validadas, enrutadas a través de TNPC y procesadas dentro de los marcos de tiempo definidos con trazabilidad completa a través de registros de auditoría e histórico de transacciones inmutables en NPCDB.

Al embeber estas capacidades dentro de la capa de orquestación de flujos de trabajo, TNPC asegura no solo el cumplimiento sino también la ejecución de las condiciones regulatorias actualizadas con consistencia, transparencia y eficiencia operativa.

Cumplimiento con 029-017-2023 (Anexo 7):

La plataforma de TNPC cumple totalmente e implementa automáticamente el proceso de repatriación/retorno de número definido en el Anexo 7, lo que garantiza la gestión eficiente del ciclo de vida de los recursos de numeración de Costa Rica. De acuerdo con la regulación, al recibir una Solicitud de Retorno de Número del operador actual, TNPC valida que el número sea elegible para el retorno, identifica el operador asignatario original y actualiza la NPCDB centralizada conforme a ello. Este proceso garantiza el retorno de los recursos numéricos dentro del marco de tiempo regulatorio definido y los pone a disposición para reasignación de manera controlada y trazable.

TNPC integra el proceso de repatriación/retorno de número sin inconvenientes con sus mecanismos de difusión/**actualización de enrutamiento** y sincronización. Una vez que se retorna un número, TNPC genera y distribuye automáticamente la información actualizada de enrutamiento a todos los operadores a través del mecanismo de difusión diaria, que garantiza la consistencia inmediata a lo largo de todo el ecosistema. TNPC incluye los números retornados dentro de los **archivos de difusión estándar/actualización de enrutamiento generados en cada ventana de cambio**, donde se consolidan todas las actualizaciones de enrutamiento y se distribuyen simultáneamente a todos los operadores participantes. Estos archivos de difusión contienen el estado actualizado de cada número afectado, que incluye el retiro del estado de portación y la reasignación al operador original, lo cual permite a los operadores actualizar sus bases de datos locales de enrutamiento en tiempo real o tiempo casi real. Además de la difusión programada/**actualización de enrutamiento**, TNPC soporta descargas completas e incrementales a demanda, que permite a los operadores conciliar sus bases de datos en cualquier momento, si fuese requerido, para los números retornados. El número retornado se actualiza simultáneamente en NPCDB para

reflejar su estado de no portación, lo cual evita cualquier inconsistencia de enrutamiento y garantiza que todas las consultas y decisiones de enrutamiento posteriores estén alineadas en todo el ecosistema de redes.

Al embeber la repatriación dentro de motor de flujos de trabajo centralizado, TNPC garantiza la ejecución del proceso sin intervención manual, totalmente auditable y alineada con las expectativas regulatorias, soportando así la utilización eficiente de la asignación de numeración y manteniendo la integridad del plan de numeración nacional.

Cumplimiento del Acuerdo 021-067-2024 (Anexo 8):

La solución de TNPC soporta completamente la mejora operativa introducida por el Anexo 8, que permite que las transacciones de portabilidad numérica sean ejecutadas en feriados oficiales, a la vez que conserva la restricción existente de que las ventanas de cambio no se ejecutan los domingos, salvo sea de otro modo indicado por SUTEL, mejorando así la flexibilidad y experiencia del usuario. La arquitectura de TNPC está inherentemente diseñada para operación continua 24x7x365, aprovechando la infraestructura nativa en la nube de AWS, los flujos de trabajo automáticos y las capacidades de monitoreo en tiempo real. Como tal, el sistema puede procesar transacciones de portabilidad sin inconvenientes cualquier día, incluso feriados, sin requerir cambios estructurales ni intervención manual. La capacidad de programación de TNPC a través del motor del Manejador de Mensajes permite la configuración de las ventanas de cambio conforme a los requerimientos regulatorios, lo cual garantiza que las operaciones de portación no sean interrumpidas a la vez que se mantiene un estricto cumplimiento de la calidad de servicio y limitaciones de tiempo.

TNPC adapta los matices del procesamiento de feriados al posibilitar el manejo diferenciado de actividades administrativas y técnicas, tal como definen SUTEL y CTPN-M. Si bien el procesamiento de transacciones sigue siendo totalmente automático y continuo, TNPC admite flujos de trabajo configurables para manejo y escalamiento de incidencias, lo cual garantiza alinear las responsabilidades operativas con los niveles de servicio acordados durante las horas no hábiles.

TNPC ofrece capacidades integrales de monitoreo y alertas, que aseguran la detección y respuesta inmediata ante anomalías durante las operaciones en días feriados. Este enfoque garantiza que la mayor flexibilidad introducida por el Anexo 8 no comprometa la estabilidad del sistema, cumplimiento regulatorio ni integridad total del proceso de portabilidad numérica.

Consultar la sección 2.3 para los procesos más detallados admitidos por TNPC para Costa Rica.

Arquitectura de TNPC

La solución de TNPC propuesta está construida sobre una arquitectura de hardware y software que cumple con todos los requerimientos establecidos en los documentos de los anexos 2 al 8.

Arquitectura del Software de TNPC

La solución de TNPC de TNS, denominada la solución de ERPN, está diseñada para alta disponibilidad, escalabilidad, confiabilidad, seguridad y rendimiento.

La siguiente figura ilustra la Arquitectura del Software de TNPC.

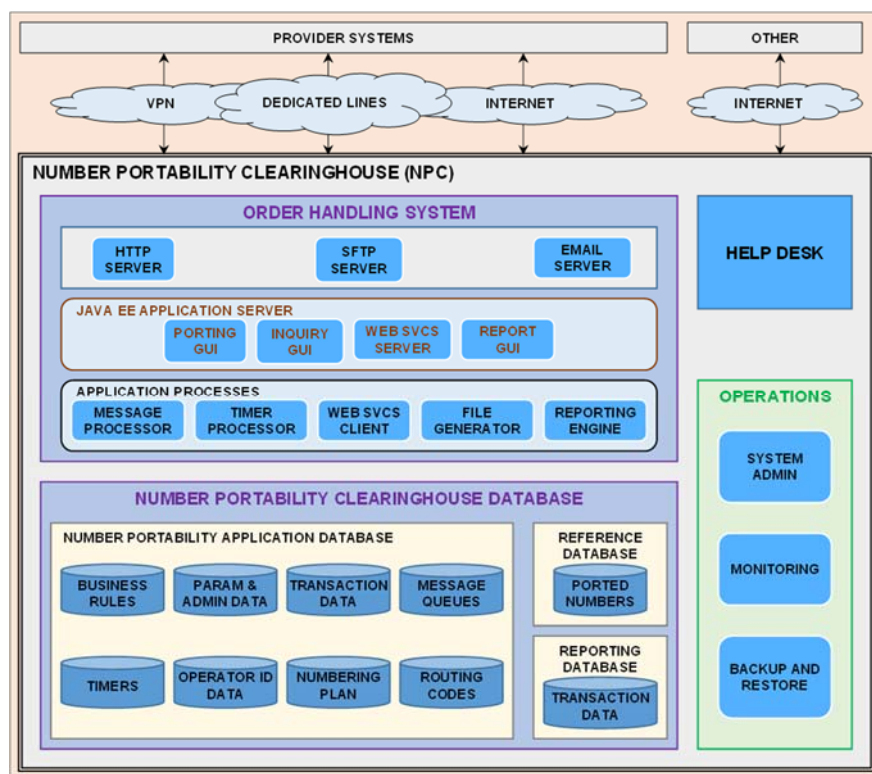


Figura 6 – Arquitectura del Software de TNPC

Conectividad con los operadores: Tal como se ilustra en el diagrama, el sistema soporta tres opciones de conectividad para los operadores que utilizarán el sistema para portar números. Las opciones recomendadas son Líneas Dedicadas o una VPN. También se soporta el acceso a través de Internet utilizando HTTPS. Además, el acceso puede estar a disposición de otras entidades que así lo requieran, por ejemplo, operadores que no portarán números, pero que necesitarán obtener los datos de enrutamiento para realizar All Call Query (ACQ). Para esas organizaciones, el acceso a Internet utilizando HTTPS puede ser suficiente.

TNPC consta de lo siguiente:

1. La Base de Datos Administrativa Central contiene la Base de Datos de Referencia de Números Portados, así como también todos los datos necesarios para la aplicación de la portabilidad numérica.
2. El Sistema de Intercambio de Información implementa los procesos de portación que brindan las interfaces para que los operadores accedan al sistema.
3. La Base de Datos de Consulta Pública de Números consta de una copia de la Base de Datos de Referencia de Números Portados, que se utiliza para consultar el estado de un número.

4. El Gateway de SMS (SMSG) acepta las solicitudes del Sistema de Intercambio de Información para enviar un NIP al suscriptor vía el protocolo SMPP.
5. El Sistema de Verificación Automática se implementa a lo largo del Sistema de Intercambio de Información y el SMSG.
6. El sistema de Respuesta Interactiva de Voz (IVR) notifica los NIP a los usuarios finales/suscriptores, en caso de falla en la entrega del NIP por SMS al suscriptor.

TNPC se implementa utilizando los productos de software estándar de terceros, por ej., el Servidor Apache HTTP y el Servidor Jboss Java EE Application, así como también componentes de software de aplicaciones desarrollados por TNS. El software desarrollado por TNS consta de componentes Java EE, que se ejecutan en el Servidor de Aplicaciones Java EE y procesos Java, que se ejecutan en la Capa de Aplicaciones fuera del Servidor de Aplicaciones Java EE.

TNPC utiliza el siguiente software de terceros:

1. Una capa de proxy inverso / acceso web como el Servidor Apache HTTP, que reside en la Capa Web acepta las solicitudes entrantes y las reenvía al Servidor de Aplicaciones JBoss.
2. El Servidor SFTP y el Servidor de Correo Electrónico, que también residen en la Capa Web, forman parte del Sistema Operativo Linux. El Servidor SFTP se usa para que los operadores accedan a los archivos.
3. El Servidor de Aplicaciones JBoss Java EE, que reside en la Capa de Aplicaciones, proporciona los Contenedores Servlet y EJB necesarios para los componentes del software de aplicaciones.
4. AWS Aurora/MySQL implementa la Base de Datos de Portabilidad Numérica y la base de datos SMSG.

El siguiente diagrama ilustra la interacción entre los módulos del software de TNPC dentro del Sistema de Intercambio de Información.

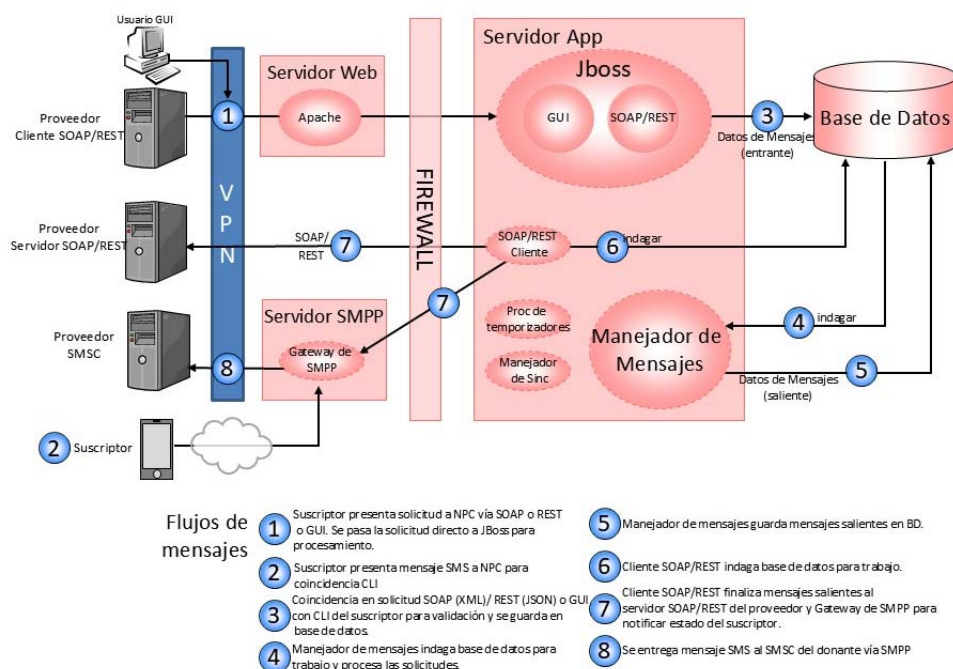


Figura 7 – Interacción de los componentes de software en el Sistema de Intercambio de Información

La plataforma de TNPC se implementa en una infraestructura **AWS EC2**, seleccionada por su **rendimiento, confiabilidad, alta disponibilidad y escalabilidad**.

Todo el software de la aplicación está codificado en lenguaje de programación Java, ya sea como procesos Java o como componentes de Java Enterprise Edition (Java EE) ejecutables dentro de un Servidor de Aplicaciones Java EE. Se eligió Java por su conjunto enriquecido de prestaciones orientadas a objetos, la amplia cantidad de funcionalidades disponibles en los diversos paquetes y la portabilidad hacia múltiples plataformas. Java EE ofrece enfoques basados en los estándares de la industria para construir aplicaciones escalables, mediante la integración de los componentes de terceros; y para flexibilidad en la implementación y monitoreo de la aplicación. La integración de terceros, como el agregado de nuevas fuentes de datos, se hace más fácil al utilizar una arquitectura de bus y plugs-in. Las soluciones de clustering listas para usar ofrecen **alta disponibilidad y también escalabilidad**. Una vez más la implementación y el monitoreo de las aplicaciones JAVA EE son facilitadas por herramientas estándar desarrolladas en torno a la administración de los servidores de la aplicación.

El servicio de base de datos propuesto por la solución de TNPC es **Amazon Aurora Serverless v2**, que ofrece escalabilidad elástica, alta disponibilidad, copias de resguardo automáticas y operaciones de bases de datos resilientes en múltiples zonas de disponibilidad. AWS Aurora tiene una configuración de escalamiento automático, a demanda para Amazon Aurora. **Incrementa o reduce automáticamente la capacidad**, según las necesidades de la aplicación. Utiliza almacenamiento distribuido con tolerancia a fallas y autorrecuperación, con replicación de 6 vías, que aumentará automáticamente a medida que se agreguen más datos. Los datos se replican en múltiples zonas de disponibilidad dentro de una sola región y esto permite ofrecer **alta disponibilidad** en caso de fallas en una AZ (Zona de Disponibilidad). Amazon Aurora Serverless v2 también ofrece toda la variedad de las capacidades de Amazon Aurora, incluyendo soporte multi-AZ, Base de Datos Global y réplicas de lectura.

TNPC incluye los siguientes componentes de software de las aplicaciones desarrolladas por TNS:

1. Base de Datos Administrativa Central

La Base de Datos Administrativa Central incluye la Base de Datos de Referencia de Números Portados, así como también Datos de Aplicaciones utilizados para implementar los procesos de portabilidad numérica.

La Base de Datos de Referencia de Números Portados es el centro del sistema. Funcionará como la base de datos de enrutamiento maestra para toda Costa Rica. Los operadores mantendrán sus bases de datos locales de enrutamiento sincronizadas con la Base de Datos de Referencia. La Base de Datos de Referencia será actualizada con los cambios de enrutamiento para un número como resultado de una portación completada o un retorno de número. Las actualizaciones de enrutamiento serán comunicadas a todos los operadores a través de una transferencia de archivos (o mensaje de difusión, si fuese requerido); y el operador las usará para actualizar su propia copia local de la Base de Datos de Referencia.

Además de la Base de Datos de Referencia, la Base de Datos Administrativa Central contendrá los siguientes conjuntos de Datos de Aplicaciones. (Cabe destacar que ésta es una vista lógica de los datos y no una representación física de la base de datos).

- Los datos para las Reglas de Negocio modelan cómo el sistema debe responder ante un mensaje recibido, incluyendo cómo validar el mensaje, a quién se debe reenviar el mensaje, cómo actualizar el estado de la portación; y definiciones y valores de parámetros de los temporizadores.
- Los Datos de Transacciones son los mensajes y el estado asociado a cada solicitud de portabilidad o solicitud de retorno; y la documentación respaldatoria. Existe una diferencia entre las Transacciones Abiertas, para las cuales todavía se esperan mensajes, y el Histórico de Transacciones, que contiene datos de las transacciones que han sido completadas. Las transacciones del Histórico de Transacciones pueden ser archivadas en un almacenamiento fuera de línea después de que haya transcurrido un intervalo de tiempo especificado.
- Los Datos de Confirmación de NIP mantienen una asociación entre un número de teléfono y el NIP asignado a ese número, como resultado de una Solicitud de Generación de NIP recibida por el Sistema de Intercambio de Información (SMSG).
- Los Datos Administrativos y de Parámetros contienen valores para propiedades como horas para programar actividades, perfiles de usuario y datos de configuración necesarios para administrar el sistema.

- Los Datos de Identificación del Operador contienen datos utilizados para identificar a cada operador, incluyendo su SOAP o URL REST e información de contacto; y los IDs de Inicio de Sesión y contraseñas del usuario.
- El Plan de Numeración mantiene una copia de los bloques de números asignados a cada operador.
- Los Códigos de Enrutamiento contienen los códigos usados para enrutar llamadas a cada operador.

Base de Datos de Reportes: La Base de Datos de Reportes contiene una copia de los datos de transacciones que se actualizan a intervalos programados regularmente. (La Generación de Reportes usa la Base de Datos de Reportes en lugar de la copia de producción de los datos de transacciones para no impactar en el rendimiento del sistema de producción). Los datos de transacciones se usan como fuente de datos para los reportes.

2. Sistema de Intercambio de Información

El Sistema de Intercambio de Información está compuesto por Componentes del Servidor de Aplicaciones Java EE y los Procesos de Java.

Los siguientes Componentes del Servidor de Aplicaciones Java EE se ejecutan en el Servidor de Aplicaciones JBoss.

- La GUI de Portabilidad, la primera de las dos interfaces a través de la cual los operadores pueden intercambiar información mediante NPCDB, es una GUI HTML a la que accede el usuario en su estación de trabajo, usando el Navegador Web estándar.

La GUI de Consulta Pública es utilizada por el público en general para consultar el sistema y obtener el estado del número (es decir, conocer el estado de portación actual del número). El acceso a la GUI pública es a través de internet usando HTTP y se utiliza reCAPTCHA para evitar acceso automático a la Interfaz Pública.

La GUI de Consulta Pública ofrecerá una interface basada en Angular, intuitiva y moderna, donde los usuarios pueden ingresar su número de teléfono y NIP asociado; y visualizar el estado de la transacción, que incluye operador actual, operador donante y ventana de cambio programada, lo cual asegura total transparencia del proceso de portabilidad.

- La Interfaz de Web Services, la segunda de las dos interfaces, es una interfaz máquina a máquina por la cual se intercambian los datos, usando el protocolo SOAP (XML transportado sobre HTTPS) o el protocolo REST (JSON transportado sobre HTTPS). La Interfaz de Web Services tiene dos componentes, el Servidor de Web Services y el Cliente de Web Services (el Cliente de Web Services se describe a continuación). El Servidor de Web Services es el componente por el cual el TNPC recibe mensajes de un operador y los coloca en la cola de entrada.
- La GUI de Reportería es utilizada por los operadores, SUTEL o usuarios autorizados para generar los reportes.

Los siguientes Procesos Java se ejecutan en la capa de aplicaciones fuera del Servidor de Aplicaciones JBoss.

- Proceso Cliente SOAP o REST. Además del Servidor SOAP/REST, el segundo componente de la Interfaz SOAP o REST es el Proceso Cliente SOAP/REST. Este proceso levanta mensajes desde la cola de salida y los envía al destino correspondiente.
 - Para mensajes destinados a un operador, el Cliente SOAP/REST envía el mensaje al servidor SOAP/REST del operador.
 - Los mensajes de la Solicitud de Generación de NIP son enviados por el Cliente SOAP/REST al SMSG Listener.
 - El Cliente SOAP/REST es un proceso Java. Múltiples instancias del proceso Cliente SOAP/REST se ejecutan simultáneamente en los Servidores de Aplicaciones.

- **Procesador de Mensajes.** El Procesador de Mensajes es un proceso Java que aplica las reglas de negocio para controlar el flujo de mensajes entre los operadores, mantiene el estado de todas las portaciones y actualiza el enrutamiento para un número cuando se activa la portación. Las funciones realizadas incluyen, específicamente:
 - Levantar mensajes de la cola de entrada.
 - Validar el contenido de cada mensaje entrante.
 - Verificar que el mensaje entrante se reciba dentro del intervalo definido por el temporizador del mensaje.
 - Determinar el mensaje o mensajes a enviar en respuesta a cada mensaje recibido.
 - Crear cada mensaje a ser enviado y colocarlo en la cola de salida.
 - Configurar los temporizadores necesarios con anterioridad a las respuestas a los mensajes salientes.
 - Actualizar el estado de la portabilidad según el mensaje recibido.
- Para alcanzar la disponibilidad y producción requeridas, múltiples instancias del Procesador de Mensajes se ejecutan simultáneamente en los Servidores de Aplicaciones.
- **Procesador de Temporizadores.** El Procesador de Temporizadores detecta el vencimiento de los temporizadores que hayan sido establecidos con anterioridad a alguna acción requerida por parte de un operador, por ejemplo una respuesta a un mensaje. Además de tomar nota de las violaciones de los temporizadores, este proceso también realizará cualquier acción requerida asociada al vencimiento de un temporizador específico, por ejemplo, enviar una notificación. Múltiples instancias de este proceso se ejecutan simultáneamente en los Servidores de Aplicaciones.
- **Motor de Reportería:** El Motor de Reportería es invocado en respuesta a las solicitudes emitidas a través de la GUI Web. Este proceso generará el reporte solicitado.
- **Generador de Archivos.** El Generador de Archivos es un proceso Java, que se invoca para crear archivos que contienen notificaciones de actualizaciones de enrutamiento como resultado de portaciones ejecutadas o números retornados. Los archivos se generan a diario y se ponen a disposición para descarga del operador. Además de los archivos diarios, se encuentran disponibles a solicitud las descargas completas o incrementales de la Base Datos Números Portados.

3. Aplicación Gateway de SMS/SMPP

La Aplicación del Gateway de SMS/SMPP es un subsistema que envía el NIP generado al suscriptor. Los siguientes componentes se ejecutan dentro del Servidor de Aplicaciones Java EE.

- Listener. Listener recibe las solicitudes SOAP/REST del Sistema de Intercambio de Información, que contienen el número, el NIP generado como resultado de la Solicitud de Generación de NIP enviada por un operador; y la identidad del operador actual (Operador Donante) del suscriptor. Al recibir una solicitud, Listener invocará una instancia en el Motor de SMS para enviar el NIP.
- Motor de SMS. El Motor de SMS es un Conector Socket SMPP que envía el NIP vía SMPP al Centro de Servicio de Mensajes Cortos (SMSC) del Operador Donante.
- Base de Datos de SMSG. La Base de Datos de SMSG contiene datos de configuración y datos de transacciones.
 - Los Datos de Configuración mantienen la información necesaria para enviar mensajes SMS a cada operador, incluyendo la dirección IP del operador y los ID y contraseñas del sistema para las conexiones SMSC.
 - Los Datos de Transacciones incluyen un registro para cada solicitud recibida del Sistema de Intercambio de Información y cada respuesta enviada a este último, el "Ack" (acuse de recibo) del SMSC y el estado de la solicitud.

4. Sistema Automático de Verificación (SAV)

TNPC implementa un Sistema Automático de Verificación (SAV) como funcionalidad que abarca tanto al Sistema de Intercambio de Información como al Subsistema de la Aplicación SMSG. Las funciones del SAV son las siguientes:

Al recibir el *Mensaje Solicitud de Generación de NIP* del Operador Receptor, el Sistema de Intercambio de Información:

- Generará el NIP y creará un registro en la Base de Datos de NIP, asociando el número o grupo de números que será portado con el NIP.
- Enviará una solicitud vía SOAP/REST al SMSG, pidiendo que el NIP sea entregado al número.

El SMSG:

- Al recibir la solicitud del Sistema de Intercambio de Información, enviará el NIP a través del Gateway de SMS a la red del Operador Donante usando el protocolo SMPP.
- Al recibir el accuse de recibo del SMSC del Operador Donante, enviará al operador solicitante (Operador Receptor) la *Confirmación de Entrega de NIP*, informando al operador que el NIP se envió con éxito.
- En caso de que el Sistema Automático de Verificación (SAV) no esté disponible para entregar el NIP con éxito al suscriptor a través del SMSC del operador donante, TNPC asegura la continuidad del proceso de portabilidad a través de un mecanismo de respaldo controlado y en total cumplimiento. Primero, la plataforma detecta la falla en base a la ausencia del accuse de recibo de la entrega de SMSC dentro del marco de tiempo definido en el SLA y automáticamente inicia hasta tres intentos de entrega, que incluyen un intento final del mejor esfuerzo. Si la entrega sigue sin éxito, TNPC posibilita un mecanismo alternativo basado en IVR, que permite al suscriptor recuperar el NIP mediante una llamada a un número designado desde la línea móvil que será portada, donde el sistema identifica quien llama, en forma segura, y ofrece el NIP vigente en forma audible. En paralelo, TNPC notifica a los operadores involucrados del problema con la entrega del SMS para que tomen una medida correctiva. Este enfoque asegura que la disponibilidad del NIP nunca sea un factor de bloqueo, manteniendo así la experiencia del usuario, integridad del proceso y garantizando el total cumplimiento de los requerimientos regulatorios de SUTEL.

Cuando el Sistema de Intercambio de Información recibe una Solicitud de Portabilidad del Operador Receptor, validará que el NIP provisto en la Solicitud de Portabilidad sea, de hecho, el NIP generado para el

número que será portado, verificando el registro para el número en la Base de Datos de NIP. Como resultado de esta validación, el Sistema de Verificación Automática (SAV) informará al Operador Receptor una de las siguientes condiciones que ha determinado:

- La Validación del NIP fue exitosa. El NIP provisto por el Operador Receptor es idéntico al NIP almacenado para ese número en la base de datos de NIP; y el NIP es válido para el marco de tiempo actual.
- NIP inexistente. No existe registro para el número que será portado en la Base de Datos de NIP.
- Validación errónea del NIP. Existe un registro para el número en la Base de Datos de NIP, pero el NIP provisto en la Solicitud de Portabilidad no coincide con el NIP asociado al número en la Base de Datos de NIP.
- NIP vencido. Existe un registro en la Base de Datos de NIP para el número y el NIP provisto en la Solicitud de Portabilidad es el mismo que el NIP asociado al número en la Base de Datos de NIP, sin embargo, ha vencido el plazo de vigencia del NIP.

5. Respuesta Interactiva de Voz (IVR)

Cuando el usuario no recibe el NIP vía SMS, podrá consultarlo a través del sistema de respuesta interactiva de voz (IVR) de TNPC. El usuario deberá llamar desde el número de teléfono utilizado en la solicitud de NIP y desde el cual desea conocer el NIP a través del sistema IVR. El sistema IVR detectará el número que origina la llamada y proporcionará el NIP al suscriptor.

- El IVR de TNPC ofrecerá la funcionalidad de repetir el NIP al suscriptor en la llamada. TNPC definirá un parámetro configurable de cantidad máxima de repetición del NIP para el llamado del IVR.
- El subsistema del IVR de TNPC valida con seguridad el MSISDN del originador contra el registro de NIP activo almacenado en NPCDB y comunica el NIP en forma audible al suscriptor. El IVR soporta la funcionalidad configurable de repetición de IP, recuperación de NIP en tiempo real, autenticación segura del suscriptor y registro completo de auditoría para garantizar la continuidad operativa, trazabilidad y cumplimiento con los requerimientos de SUTEL.
- TNPC diseñará y configurará las opciones del menú del IVR, flujos de llamadas, mensajes y lógica de interacción para soporte de la recuperación segura del NIP para los suscriptores cuando no se entregue el SMS con éxito. La plataforma del IVR interactuará en forma segura con la lógica de negocios de TNPC y NPCDB a través de web services autenticados para recuperar el NIP activo asociado con el MSISDN del originador. Cuando el suscriptor llama al IVR desde el mismo número móvil utilizado para solicitar el NIP, el sistema automáticamente valida el número del originador y transmite un mensaje de voz en forma segura, comunicando el NIP vigente que incluye una funcionalidad configurable para repetir el NIP.

Arquitectura del hardware de TNPC

La solución de TNPC propuesta por TNS, denominada la solución de ERP, aprovechará la infraestructura en la nube para alojar el Servicio de Administración de PN, usando Amazon Web Services (AWS). La solución AWS en la nube ofrece un beneficio rentable respecto de la infraestructura física, sin sacrificar rendimiento, funcionalidad ni seguridad. Los servidores de las bases de datos se implementarán en dos zonas de disponibilidad separadas, lo cual es crítico en caso de desastre.

La solución de ERP de TNS usará la infraestructura en la nube de Amazon Web Services (AWS) para alojar el sistema de portación. La solución de ERP de TNS ha utilizado AWS para otras tres implementaciones exitosas del sistema en la nube. Alojar la solución de ERP de TNS en la nube de AWS ofrecerá:

- Escalabilidad vertical y horizontal para cumplir con las demandas en constante cambio.
- Elasticidad para cumplir con las demandas de portación pico, permitiendo el incremento de la capacidad en minutos.
- Arquitectura resiliente y redundante con alta disponibilidad.

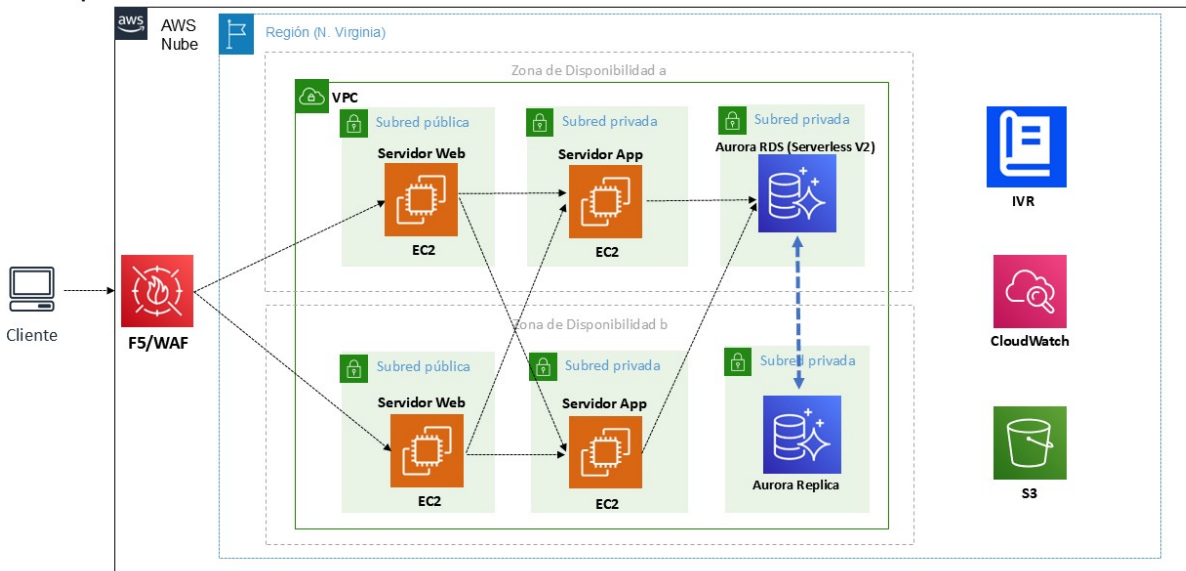
- Una arquitectura flexible para la rápida implementación de las nuevas capacidades del sistema de TNS.
- Servicios de encriptación y seguridad confiables, que incluyen resguardos físicos y de datos sólidos.

La Arquitectura de Hardware para el Sistema de Producción (Principal), Pruebas y Recuperación ante Desastres (DR/Secundario) se ilustra en las siguientes subsecciones.

Sistema de Producción

El sistema de TNPC se implementará en la Región de Web Services Amazon (AWS), en US-EAST. Se utilizará AWS **US-EAST** como región de producción principal, con redundancia a través de múltiples Zonas de Disponibilidad.

Arquitectura AWS de TNPC



El diagrama anterior muestra la arquitectura para múltiples zonas de disponibilidad (Multi-AZ) de AWS con alta disponibilidad y escalabilidad utilizando instancias EC2. La solución propuesta consta de una Nube Privada Virtual (VPC) con subredes distribuidas en dos zonas de disponibilidad diferentes. Se utilizará AWS **US-EAST** como región de producción principal, con redundancia a través de múltiples Zonas de Disponibilidad. Se utilizará AWS **US-WEST** como región de recuperación ante desastre, con separación geográfica. La infraestructura también incluye Internet Gateway para permitir el acceso a Internet desde la VPC y el Balanceador de Carga de Aplicaciones de cara al público. Las capas de base de datos y aplicaciones se ubican en subredes privadas para proteger esas instancias de la exposición directa a Internet. Todas las solicitudes serán enrutadas través de F5/Palo Alto o un firewall similar (un firewall web que también puede facilitar el balanceo de carga). La arquitectura presentada ofrece un alto nivel de escalabilidad y disponibilidad mediante la introducción de redundancia con instancias implementadas en dos zonas de disponibilidad diferentes; y el uso de grupos de escalamiento automático que ofrecen escalamiento y gestión automáticos del estado del sistema.

La capa Web y de Aplicación se implementan en una instancia AWS EC2, donde cada nodo está ubicado en un EC2 por separado. Esto permite tener una arquitectura de red segura al separar los servidores web de cara al exterior, ofreciendo de esta manera una estrategia de defensa por capas que mitigan el riesgo de amenazas externas.

La capa de base de datos incluye Aurora RDS, un servicio gestionado de base de datos que ofrece AWS.

El sistema TNPC se configura de la siguiente manera:

1. Un router/firewall externo conectado a Redes ISP de Protocolo de Internet (IP) para permitir la accesibilidad de la red externa, detectar intrusiones y defensa contra ataques a la red.
2. Cada Operador de Redes accederá al sistema TNPC a través de un Firewall de Aplicaciones Web (WAF) seguro conectado a una Nube Privada Virtual (VPC) de Amazon.
3. Los dos Servidores Web están ubicados detrás del firewall externo para prestar Web Services al mundo exterior. Los Servidores Web también actúan como servidores proxy, reenviando solicitudes al Servidor de Aplicaciones y redireccionando las respuestas del Servidor de Aplicaciones al usuario.
4. Los dos Servidores de Aplicaciones, sobre los cuales se ejecuta la aplicación del TNPC, operan en modo cluster. Múltiples instancias de cada proceso se ejecutan de manera simultánea en ambos servidores
5. El servicio Aurora RDS serverless V2 ofrece capacidad de base de datos e incluye todos los datos de transacciones y recursos para operar el sistema.

Es una configuración de escalamiento automático a demanda y escala la capacidad hacia arriba o hacia abajo en base a las necesidades de su aplicación. Permite ejecutar la base de datos en la nube sin gestionar ninguna capacidad de base de datos.

Amazon Aurora es completamente administrada por el Servicio de Base de Datos Relacional (RDS) de Amazon, que automatiza las tareas administrativas, como aprovisionamiento de hardware, configuración de bases de datos, parches y copias de seguridad.

Amazon Aurora ofrece un sistema de almacenamiento distribuido, con tolerancia a fallas y autorrecuperación que realiza el escalamiento automático de hasta 128 TB por instancia de base de datos. Ofrece alto rendimiento y disponibilidad con hasta 15 réplicas de lectura de baja latencia, recuperación en un momento determinado y copias de seguridad continuas en Amazon S3.

6. El firewall interno está configurado para formar una red privada a fin de evitar el acceso no autorizado al sistema hacia los Servidores de Aplicaciones desde otras redes y permitir el reenvío de mensajes desde los dos Servidores Web.
7. **CloudWatch:** Amazon CloudWatch es un servicio de monitoreo y observación. CloudWatch ofrece datos e información para poder actuar con el fin de monitorear las aplicaciones, responder ante cambios en el rendimiento de todo el sistema y optimizar la utilización de recursos. CloudWatch colecta datos de monitoreo y operativos en la forma de logs, métricas y eventos. CloudWatch ofrece una vista unificada de la salud operativa y visibilidad de los recursos, aplicaciones y servicios AWS que corren en AWS. CloudWatch se puede utilizar para detectar comportamientos anómalos en los entornos, configurar alarmas, visualizar logs y métricas lado a lado, realizar acciones automáticas, detectar y resolver problemas; y descubrir información para mantener el funcionamiento de las aplicaciones sin inconvenientes.
8. **S3:** Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimientos líderes en la industria. S3 almacena y protege los datos de portabilidad para el sistema TNPC. S3 ofrece varias clases de almacenamiento y prestaciones de administración, que se pueden optimizar para organizar datos y se pueden configurar para contar con controles de acceso que cumplan con requerimientos de negocio, organizativos y de cumplimiento específicos. TNPC usará S3 para almacenar archivos Linux (log files), respaldo y scripts de DB (como bulk sync utility, startup scripts etc.).

Se especificó la configuración de hardware para satisfacer los siguientes requerimientos.

- **Escalabilidad:** El sistema puede crecer para alojar futuros incrementos en los requerimientos de capacidad por medio del agregado de nuevos servidores virtuales. Para lograr manejar tanto picos de tráfico como cargas de trabajo irregulares, la arquitectura propuesta aprovecha el escalamiento automático con escalamiento de seguimiento de objetivos a fin de escalar en forma dinámica la

capacidad del grupo de escalamiento automático en base a métricas de EC2. Estas métricas se pueden configurar para monitorear el nivel de utilización o producción promedio de forma tal que si se supera un umbral particular, el Escalamiento Automático EC2 de Amazon puede ampliar el grupo (agregar más instancias) para manejar la carga de tráfico. Nótese que tener, como mínimo, dos AZ activas en simultáneo contribuye a la escalabilidad general de la solución, ya que los picos de tráfico pueden disparar el escalamiento automático en múltiples sitios simultáneamente.

- **Seguridad:** La infraestructura de firewall de TNPC está diseñada para ofrecer seguridad perimetral de la red y protegerla contra accesos no autorizados. El firewall monitorea todos los paquetes entrantes y sólo permite que pasen paquetes legítimos de datos desde fuentes autorizadas. Todo el tráfico desde el exterior es dirigido hacia los Servidores Web, sin permitir el acceso directo a los Servidores de Aplicaciones y de Base de Datos.
- **Confiabilidad y Disponibilidad:** El sistema está diseñado para alta disponibilidad y operación continua. Todos los servicios AWS y las aplicaciones de seguridad, incluyendo firewalls, servidores web y de aplicaciones son redundantes; no hay un único punto de falla en el sistema. En cada capa, los servidores están activos en ambos servidores brindando operación continua durante las actualizaciones del sistema o en caso de falla operativa. Los datos se replican en múltiples zonas de disponibilidad dentro de una sola región y esto permite ofrecer alta disponibilidad en caso de fallas en una AZ.

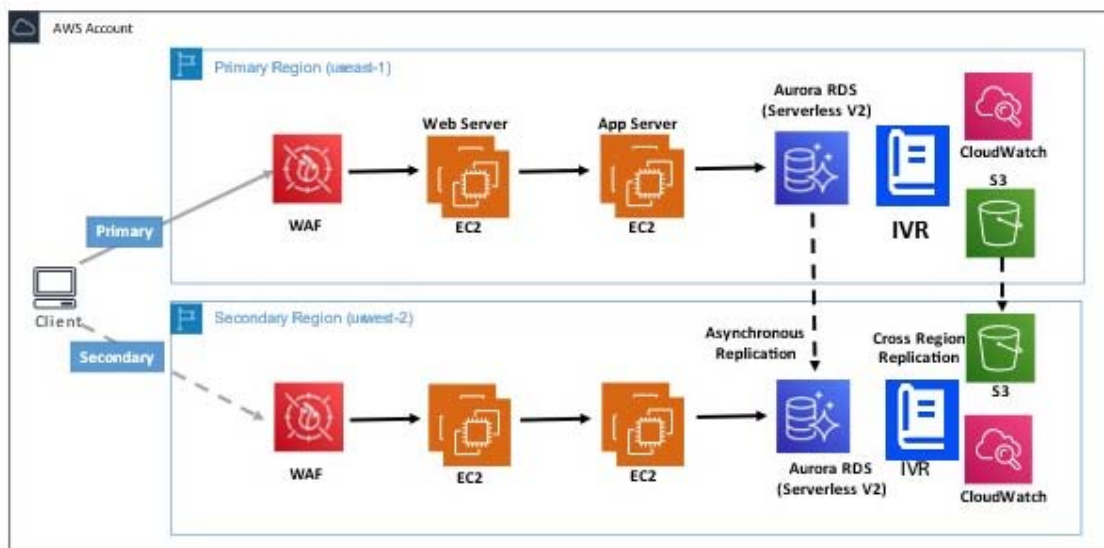
Como la disponibilidad general de la solución está dada por la disponibilidad individual de los componentes del servicio de AWS que se utilizan en la ruta crítica (Acuerdos de Nivel de Servicio publicados por AWS), la arquitectura aporta un impulso significativo a la disponibilidad general ofreciendo rutas paralelas redundantes, por ejemplo, para el SLA a nivel regional para EC2 con todas las instancias de ejecución implementadas en simultáneo en dos o más AZ en la misma región; también ofrece disponibilidad mensual de, al menos, 99,99%.

Sistema de Pruebas

Se utiliza un Sistema de Pruebas implementado en AWS para soportar las Pruebas de Aceptación de Software por parte de los operadores previo a la implantación inicial del Sistema TNPC. Después del lanzamiento del sistema, todo nuevo software se instalará y probará en el Sistema de Pruebas antes de colocarlo en el entorno de producción.

Al igual que el sistema de producción, el entorno de pruebas también se implementará en AWS en la región us-east-1. El Sistema de Pruebas consta de una única instancia EC2 del Servidor Web/de Aplicaciones combinada atendida por Aurora RDS como servicio de base de datos.

Sistema de Recuperación ante Desastres



CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

El Sistema de Recuperación ante Desastres consta de una semiréplica del Sistema de Producción que se implementará en una región de AWS separada para ofrecer redundancia geográfica. Sin embargo, a diferencia del sitio de producción, este sitio standby tendrá una única instancia de EC2 en ejecución para soportar la capa web y de aplicaciones. Durante una falla real, gracias a las capacidades de escalamiento automático y las imágenes de máquina web y de aplicaciones preconfiguradas de Amazon (AMI), el sistema de Recuperación ante Desastres (DR) se puede escalar rápido para convertirse en una réplica exacta de producción que soporta los mismos SLA y producción. El servicio Amazon Serverless Aurora se configurará como una base de datos global que permitirá replicación casi en tiempo real (<1 seg de retraso) a la región secundaria. El procedimiento de recuperación ante fallas consistirá en promover la instancia de la región secundaria al modo escritura y la capacidad nativa escalará automáticamente la escritura después de la recuperación ante fallas. Todos los servicios de soporte de AWS que contengan datos de TNPC (por ejemplo, S3) se configurarán en el modo de replicación continua para evitar pérdida de datos.

2.2 *El SIPN podrá desarrollarse en un centro de datos en infraestructura ubicada dentro o fuera del país (on-premise) o en la nube (on-cloud), siempre que garantice el cumplimiento de los niveles de servicio, seguridad y disponibilidad planteados en su propuesta.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La solución de TNPC aprovecha la **arquitectura de grado operadora, nativa en la nube y segura**, diseñada para cumplir con los requerimientos de SUTEL y CTPN-M destinados a **escalabilidad, resiliencia, seguridad, continuidad operativa y evolución futura** de la plataforma del SIPN. La implementación basada en AWS ofrece **alta disponibilidad a través de una arquitectura de múltiples zonas de disponibilidad, con recuperación ante desastres con resiliencia geográfica a lo largo de las regiones de AWS, con escalamiento automático, monitoreo en tiempo real y mecanismos de protección de datos continua**, lo cual garantiza las operaciones del SIPN y el cumplimiento regulatorio sin interrupciones.

La arquitectura propuesta entrega **mayor agilidad operativa, tiempos de implementación más rápidos, controles de ciberseguridad sólidos, recuperación ante desastres simplificada y escalabilidad sin inconvenientes**, alineado con el mercado futuro y el crecimiento regulatorio. Este enfoque permite que TNS ofrezca una **plataforma del SIPN moderna, altamente resiliente, segura y lista para el futuro**, a la vez que garantiza sustentabilidad operativa a largo plazo, alto rendimiento y confiabilidad de servicio para el ecosistema de portabilidad numérica nacional de Costa Rica.

2.2.1 *En caso de que resulte aplicable, deberá disponer de una infraestructura de contingencia geográficamente separada que, a su vez, garantice diversidad de enlaces de comunicaciones.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La solución de TNPC ofrece **una infraestructura de contingencia totalmente dispersa a nivel geográfico**, lo cual garantiza la resiliencia, redundancia y continuidad de las operaciones del SIPN, a la vez que soporta múltiples vías de comunicación con los operadores y SUTEL.

Con la **implementación de AWS en la nube**, el entorno de producción primario está alojado en la región **AWS US-EAST**, con las capas de aplicación y base de datos distribuidas a lo largo de múltiples zonas de disponibilidad para ofrecer redundancia dentro de la región. Además, se implementa un **entorno de recuperación ante desastres secundario en la región AWS US-WEST**, lo que garantiza separación geográfica a nivel regional. Los datos se replican casi en tiempo real entre las regiones, que permite la continuidad de las operaciones en caso de falla regional. Se soportan múltiples vías de comunicación a través de gateways de internet redundantes, balanceadores de carga y conexiones VPN seguras, lo cual garantiza conectividad ininterrumpida con los operadores y sistemas externos.

TNPC está diseñado con **ningún punto único de falla a nivel de infraestructura, red o aplicación**, y se dispone de múltiples enlaces de comunicación para mantener la conectividad con todos los interesados (como operadores, plataforma de prepago de SUTEL, etc.). Este diseño garantiza alta disponibilidad, cumplimiento regulatorio y servicios de portabilidad ininterrumpidos bajo todas las condiciones operativas.

2.2.2 *Contar con capacidad de recuperación ante fallos sin pérdida de información.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La solución TNPC de TNS está diseñada para ofrecer capacidad de recuperación ante fallas sin inconvenientes, sin pérdida de información, lo cual garantiza la operación continua del SIPN bajo todos los escenarios de falla. Esto se logra a través de una combinación de replicación de datos en tiempo real, infraestructura redundante y sólidos mecanismos de recuperación ante fallas con la arquitectura descrita en la Sección 2.1. TNPC está diseñado para garantizar integridad de datos, alta disponibilidad y cumplimiento total con los requerimientos de SUTEL.

Con la **implementación en la nube de AWS**, TNPC aprovecha la arquitectura multirregional y de múltiples zonas de disponibilidad. El sistema de producción se implementa a lo largo de múltiples zonas de disponibilidad dentro de la región AWS US-EAST, al tiempo que se mantiene el entorno de recuperación ante desastres totalmente configurado en la región AWS US-WEST. NPCDB se implementa usando AWS Aurora, que ofrece un sistema de almacenamiento distribuido, tolerante a fallas, con replicación de seis vías a lo largo de las zonas de disponibilidad. Se replican todos los datos sincrónicamente dentro de la región y se replican continuamente a la región de recuperación ante desastres (DR) con latencia de sub-segundo para garantizar la consistencia casi en tiempo real. La recuperación ante fallas es automática y se ejecuta dentro de minutos, con Objetivo de Punto de Recuperación (RPO) cerca de cero y Objetivo de Tiempo de Recuperación (RTO) muy bajo. Los servicios de soporte como almacenamiento S3, datos de configuración y registros también se replican continuamente, lo cual asegura la recuperación completa del sistema sin inconsistencia de datos. Consultar la sección 2.2.3 para detalles exactos de RPO y RTO.

TNPC asegura que todas las transacciones de portabilidad, actualizaciones de enrutamiento y registros históricos que se almacenan en NPCDB estén continuamente protegidos y sincronizados. La arquitectura garantiza que los eventos de recuperación ante fallas no impacten la integridad de datos ni la continuidad de servicio, cumpliendo totalmente con los requerimientos de SUTEL para confiabilidad, disponibilidad y protección de datos de portabilidad críticos.

2.2.3 *En caso de utilizar infraestructura en la nube, el oferente deberá indicar el proveedor, la región o país donde se alojarán los datos, así como describir los esquemas de Alta Disponibilidad y Recuperación ante Desastres, incluyendo los valores de RTO y RPO comprometidos.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC está alojada en **Amazon Web Services (AWS)**, aprovechando una infraestructura en la nube grado empresarial, altamente resiliente. El entorno de producción se implementará en la **región AWS US-EAST**, con las capas de aplicación y base de datos distribuidas a lo largo de múltiples zonas de disponibilidad para garantizar alta disponibilidad dentro de la región. Se **implementará un entorno de recuperación ante desastres**, totalmente configurado, **en la región AWS US-WEST**, que ofrece redundancia geográfica a nivel regional. Se replicarán todos los datos, incluso NPCDB, datos de transacciones y registros de auditoría, continuamente entre las regiones usando mecanismos de replicación nativa de AWS, que garantiza redundancia de datos e integridad a lo largo de los entornos.

La arquitectura de TNPC en AWS está diseñada para cumplir los objetivos estrictos de disponibilidad y recuperación mediante el uso de implementación en **múltiples zonas de disponibilidad, balanceo de carga, escalamiento automático y almacenamiento distribuido**. Se implementa NPCDB con **AWS**

Aurora, que ofrece replicación de seis vías a través de zonas de disponibilidad y copias de resguardo continuo Amazon S3. En caso de falla a nivel de instancia o zona de disponibilidad, se maneja la recuperación ante fallas en forma automática dentro de la región sin interrupción de servicio. En caso de falla regional, se puede pasar el sistema al entorno de recuperación ante desastres en la región secundaria con mínimo tiempo de inactividad. En base a esta arquitectura, TNPC se compromete a un **Objetivo de Tiempo de Recuperación (RTO) de menos de 15 minutos para fallas dentro de la región y menos de 30 minutos para recuperación ante desastres entre regiones**; y un **Objetivo de Punto de Recuperación (RPO) de casi cero (en general, pérdida de datos de menos de un segundo)** debido la replicación continua.

Además los servicios AWS como CloudWatch, S3 y los componentes de redes se configuran con redundancia y replicación a lo largo de las regiones para garantizar que todos los componentes del sistema, incluidos registros, copias de resguardo y datos de configuración, estén protegidos. Esta implementación en la nube garantiza alta disponibilidad superior a 99,99 por ciento, rápida recuperación ante desastres y total cumplimiento de los requerimientos de SUTEL para protección de datos, continuidad de servicio y resiliencia operativa.

2.3 *Garantizar la compatibilidad con las plataformas de portabilidad numérica actualmente en operación por parte de los operadores/proveedores de servicios de telefonía móvil en Costa Rica y la Sutel. Así las cosas, el SIPN que se implemente deberá realizar los procesos que se detallan en el “Manual de Interfaces y Procesos” (Anexo 2) y cumplir con toda la interacción requerida con todas las partes de conformidad con dicho documento.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC cumple totalmente con el **Manual de Interfaces y Procesos definido en el Anexo 2** e incorpora todas las **mejoras requeridas bajo el Anexo 3**, lo cual garantiza interoperabilidad sin inconvenientes con los operadores móviles, los sistemas de SUTEL y demás plataformas regulatorias de Costa Rica. La solución implementa una **arquitectura accionada por mensajes**, donde todas las transacciones de portabilidad se ejecutan través de intercambios de mensajes estandarizados que usan interfaces **SOAP (XML sobre HTTPS) y REST (JSON sobre HTTPS)**. Se realiza un seguimiento singular de cada transacción usando el identificador de transacción e ID del mensaje asociado. Todos los mensajes, estados, marcas de tiempo e interacciones del operador **se almacenan persistentemente en NPCDB**. El Procesador de Mensajes **orquesta el flujo de trabajo**, mientras que el Procesador de Temporizadores garantiza el cumplimiento de todos los **temporizadores y SLA definidos**. Antes de aceptar un mensaje a procesar, TNPC valida la carga de trabajo entrante contra el XSD aplicable, aplica las reglas de negocio, verifica el estado del proceso y luego enruta la transacción a través del flujo de trabajo adecuado. Los objetos REST JSON están diseñados para hacer espejo de la estructura y semántica de los esquemas XML existentes, lo cual asegura que los operadores que usan REST reciban la equivalencia funcional con el proceso actual basado en XML, sin introducir ambigüedad ni lógica de negocio paralela.

A lo largo de todos los procesos, TNPC asegura el estricto cumplimiento de los flujos de mensajes, definiciones de procesos y requerimientos de interacciones de los Anexos 2 y 3. Todos los mensajes son procesados a través de los componentes del Procesador de Mensajes y Procesador de Temporizadores de TNPC, lo cual garantiza la secuenciación, validación y aplicación de SLA en forma correcta.

La plataforma de TNPC garantiza la completa integridad de las transacciones, aplicación consistente de reglas de rechazo, integración sin inconvenientes con los sistemas de los operadores y plataformas de SUTEL; y la trazabilidad total de todos los procesos a través de NPCDB. Al combinar la estricta adhesión a los requerimientos del Anexo 2 y el Anexo 3 con capacidades mejoradas como **APIs en tiempo real, tableros operativos, reportería avanzada y orquestación de flujos de trabajo automáticos**, TNPC entrega una implementación del SIPN robusta, escalable, resiliente y lista para el futuro a Costa Rica.

Todas las estructuras de mensajes, parámetros y elementos de datos **se adhieren estrictamente a la definición de WSDL y esquemas XML (XSD)** provistos en el Manual de Interfaces, lo cual garantiza que

todos los mensajes entrantes y salientes sean validados contra los esquemas definidos antes del procesamiento.

Se realiza un seguimiento singular de cada transacción a través del identificador de transacción e identificadores de mensajes asociados. TNPC almacena todas las solicitudes, respuestas, respuestas de rechazo, cambios de estado, marcas de tiempo, identificadores del operador, cambios de enrutamiento, eventos de NIP, eventos de temporizadores y registros de auditoría en NPCDB. Esto garantiza la trazabilidad completa desde la primera transacción hasta el cierre final. El **Procesador de Mensajes de TNPC** orquesta el flujo de procesos, el **Procesador de Temporizadores de TNPC** aplica los temporizadores regulatorios y umbrales de SLA, el **SAV de TNPC** y el **Gateway de SMS/SMPP** gestionan la generación y entrega de NIP, el subsistema del **IVR de TNPC** ofrece respaldo de recuperación de NIP, el **Generador de Archivos de TNPC** crea los archivos de difusión/actualización de enrutamiento y sincronización; y el **Motor de Reportería de TNPC** ofrece reportes en tiempo real e históricos. Los estados de transacciones se almacenan persistentemente en NPCDB, incluidos los estados como NIP generado, NIP entregado, prevalidación solicitada, prevalidación completada, solicitud de portabilidad recibida, respuesta del donante pendiente, aprobada, rechazada, programada, activada, cancelada, retornada, sincronizada y cerrada. Solo se marca un número como portado en NPCDB después de la ejecución exitosa del proceso de activación durante la ventana de cambio aprobada. En este momento, TNPC actualiza los datos de enrutamiento, guarda la marca de tiempo de activación, registra la relación entre donante y receptor e incluye el número en la próxima difusión/actualización de enrutamiento y sincronización.

TNPC **soporta todos los reportes operativos, de rendimiento, SLA, auditoría y regulatorios requeridos** en relación con estos procesos, que incluyen actividad de portaciones entrantes y salientes, análisis de rechazos por motivo y operador, estadísticas de generación y entrega de NIP, tasas de portaciones exitosas y no exitosas, estadísticas de cancelaciones, reportes de números retornados, estado de entrega de difusión/actualización de enrutamiento, estado de sincronización, cumplimiento de SLA y reportes de auditoría. Los reportes están disponibles a través de tableros basados en roles y formatos exportables como XLSX, CSV y PDF conforme a los derechos de acceso de SUTEL, los operadores y usuarios autorizados.

TNPC soporta todos los procesos a continuación definidos en el Anexo 2:

Proceso 00 – Generación, Reenvío y Entrega de NIP

El proceso de NIP se inicia a través del **Mensaje 0001, Solicitud de Generación de NIP**, enviado por el operador receptor. TNPC valida el mensaje contra las definiciones de WSDL y XSD aplicables, confirma formato de MSISDN, identificadores de operador, validez de plan de numeración y si el proceso es elegible; y luego invoca el Sistema Automático de Verificación (SAV). El SAV genera un NIP seguro y lo guarda en NPCDB con el MSISDN, ID de transacción, donante, receptor, generación de marcas de tiempo, período de vigencia, estado de NIP, estado de entrega y asociación de NIP grupal cuando corresponda. Para transacciones con múltiples números, TNPC soporta NIP individual y NIP grupal, a la vez que conserva la validación y auditoría por número.

TNPC también soporta **Solicitud de Reenvío de NIP del receptor** como parte del proceso de entrega de NIP. Cuando el receptor solicita el reenvío de NIP, TNPC valida que el MSISDN tenga un NIP activo vigente, verifica el receptor, donante, contexto de la transacción y datos de referencia del NIP; y enruta la solicitud a través del Procesador de Mensajes de TNPC al Gateway de SMS/SMPP de TNPC. El Gateway de SMS/SMPP de TNPC reenvía la solicitud de entrega de NIP al SMSC del donante, utilizando el **protocolo SMPP seguro** para que se pueda entregar o volver a entregar el mismo NIP vigente al suscriptor. TNPC registra la solicitud de reenvío, el envío a SMSC, resultado del acuse de recibo, conteo de reintentos, estado de entrega y resultado final en NPCDB.

Si el SMSC del donante no acusa recibo dentro del temporizador definido, TNPC automáticamente reintenta entregar el NIP hasta 3 veces, incluyendo un reintento final de mejor esfuerzo. Si la entrega de SMS sigue sin tener éxito, TNPC devuelve la respuesta de falla de entrega de NIP correspondiente, usando los códigos de rechazo o respuesta existentes definidos en el Manual de Interfaces y activa el **mecanismo de respaldo de IVR**. A través del IVR, el suscriptor llama desde el número que será portado, TNPC detecta el MSISDN del originador, consulta NPCDB, verifica la existencia de un NIP vigente y brinda el NIP en forma audible con la repetición configurable. Si no existe un NIP vigente, se informa a quien llama y se termina la llamada. Los escenarios de rechazo para el Proceso 00 incluyen formato de MSISDN inválido, número fuera del plan de

numeración, número no asociado a un operador válido, falla en validación de esquema, contexto de receptor inválido, NIP vencido, NIP no disponible o falla en entregar por SMS después de reintentos. Todas las respuestas usan los códigos de rechazo y respuesta predefinidos del Manual de Interfaces; TNPC no introduce códigos de rechazo propietarios.

Proceso 02 – Prevalidación

El receptor inicia el proceso de prevalidación a través del **Mensaje 2001, Consulta de Prevalidación**. TNPC valida el mensaje entrante contra el WSDL y XSD, autentica el emisor y determina si se puede completar la validación internamente o si se debe reenviar al donante. Se realizan las validaciones internas contra el NPCDB e incluyen verificaciones de la validez del plan de numeración, operador actual, si el número pertenece al receptor, si el número ya tiene un proceso de portación activo, si el suscriptor superó el límite de portaciones permitidas y si el **MSISDN tiene un NIP activo** cuando sea requerido.

Cuando se requiere validación asistida por el donante, TNPC reenvía la consulta al donante y aplica el temporizador de respuesta aplicable. TNPC almacena la consulta saliente, respuesta del donante, estado de temporizador, resultado de validación y respuesta final en NPCDB. TNPC también **se integra con la Plataforma de Registro de Prepago de SUTEL**, a través de web services seguros para validar la identidad del suscriptor prepago y la titularidad, cuando corresponda. Esto permite al SIPN admitir validación de prepago sin interrumpir el flujo de trabajo del operador. Las respuestas de rechazo incluyen numeración inválida, número no asociado a ningún suscriptor, número ya se encuentra en proceso de portación, número inactivo o suspendido, no coincide la titularidad, superó límite de portaciones anuales, contexto de NIP inválido o vencido, timeout del donante, error en validación de esquema o servicio de validación externa no disponible. Cuando el web service del operador o SUTEL no está disponible, TNPC aplica la lógica de reintentos definida y permite que los usuarios autorizados envíen o gestionen la prevalidación a través de la capacidad de respaldo de GUI, a la vez que mantiene todos los temporizadores, estados y registros de auditoría.

Proceso 01 – Proceso de Portación y Activación

El proceso de portación comienza cuando el receptor envía la **Solicitud de Portabilidad** después de obtener y validar el NIP requerido. TNPC valida la estructura del mensaje contra el WSDL y XSD, verifica el NIP contra NPCDB, **confirma que el NIP sea válido** y esté dentro del período de vigencia, valida la información del suscriptor y operador, verifica que la transacción sea elegible y garantiza que no exista ningún proceso de portación activo para ese mismo número. Luego TNPC reenvía la solicitud al donante y registra el estado de la transacción como respuesta del donante pendiente.

El donante responde con aprobación o rechazo dentro del temporizador definido. TNPC valida cualquier rechazo contra los códigos de rechazo existentes y motivos de rechazo permitidos definidos en el Manual de Interfaces. Los escenarios de rechazo incluyen numeración inválida, no coincide titularidad, número inactivo o suspendido, solicitud de portabilidad duplicada, restricción de contrato de subsidio, supera límite de portaciones, NIP inválido, NIP vencido, número pertenece al receptor u otros motivos de rechazo regulatorios definidos en los esquemas actuales o catálogo de códigos de rechazo. Si el donante no responde dentro del período definido, TNPC aplica la regla regulatoria que trata la solicitud como aceptada y evita cualquier demora inadecuada del derecho del suscriptor a la portabilidad. **Una vez aprobado, TNPC programa la portación para la ventana de cambio aplicable** y guarda el estado programado en NPCDB.

Durante la ventana de activación, TNPC procesa el evento de activación, actualiza el registro de enrutamiento de NPCDB, cambia el estado del número a portado, registra al receptor como operador actual, conserva la relación del donante y asignatario original, guarda marca de tiempo de activación y dispara procesamiento de difusión/actualización de enrutamiento y sincronización. Solo se considera portado el número después de que el estado de activación sea exitosamente colocado en NPCDB. En caso de problemas en la interfaz del operador o SUTEL, se pone a disposición el procesamiento en base a la GUI para mantener la continuidad en condiciones controladas. TNPC informa todos los resultados de la portación, incluyendo las tasas de éxito, motivos de rechazo, tiempos de respuesta del donante, activación completada, cumplimiento de SLA y rendimiento de ventana de cambio.

Proceso 03 – Cancelación de Portación

El proceso de cancelación de portación se inicia a través de la **Solicitud de Cancelación de Portación**, que puede enviar SUTEL o el receptor conforme a las condiciones regulatorias permitidas. TNPC valida la solicitud contra el WSDL y XSD y verifica que la parte solicitante esté autorizada, que la transacción esté todavía pendiente de activación y que se permita la cancelación para el estado de portación actual. TNPC reenvía la solicitud de cancelación al donante cuando sea requerido y realiza el seguimiento de la respuesta con el temporizador aplicable.

Las respuestas de rechazo incluyen intento de cancelación no autorizado, cancelación solicitada fuera de la ventana permitida, transacción ya activada, ID de transacción inválido, estado de proceso inválido, falla en la validación del esquema o rol inconsistente del operador. Todos los resultados de la cancelación, incluidas las respuestas de rechazo, se guardan en NPCDB con marcas de tiempo e identificadores del usuario/operador. Si web services no está disponible, los usuarios autorizados pueden realizar la cancelación a través de la capacidad de respaldo de la GUI, sujeto a los mismos controles de autorización y registros de auditoría. TNPC informa los volúmenes de cancelaciones, motivos de cancelación, tiempos de respuesta, acciones del usuario y cumplimiento de SLA.

Proceso 04 – Retorno y Repatriación de Número

El proceso de retorno de número se inicia a través de la **Solicitud de Retorno de Número** cuando un número portado cumple con las condiciones de inactividad o retorno definidas por la regulación. TNPC valida la solicitud contra el esquema, verifica que el operador solicitante sea el operador actual, confirma el estado del número portado en NPCDB, valida la inactividad o condiciones de ser elegible para retorno e identifica al operador asignatario original. Si es válido, TNPC actualiza NPCDB para reflejar que el número ya no está portado y registra el evento de retorno, marca de tiempo del retorno, transición del operador actual, asignatario original e histórico de transacciones.

Los escenarios de rechazo incluyen período de inactividad inválido, número no está actualmente portado, operador solicitante incorrecto, datos inválidos del asignatario original, estado de transacción inválido o falla en validación del esquema. Una vez que se retorna el número, TNPC incluye el número retornado en el proceso diario de difusión/actualización de enrutamiento y en el archivo de actualización de números retornados para que todos los operadores actualicen sus bases de datos de enrutamiento locales. Los números retornados también están disponibles a través de los mecanismos de sincronización completa o incremental. TNPC ofrece reportes sobre números retornados por operador, motivo de retorno, tiempo de retorno, motivo de rechazo y estado de finalización de difusión/actualización de enrutamiento.

Proceso 05 – Sincronización

TNPC soporta archivos de sincronización completa e incremental a demanda, que permite a los operadores y SUTEL conciliar sus copias locales de enrutamiento con NPCDB cuando sea requerido. Además de la entrega por SFTP, TNPC ofrece REST API para consultas de enrutamiento y acceso a sincronización en tiempo real. Se registran las fallas de entrega, falta de coincidencia en verificación de suma de archivos, rutas SFTP no disponibles, descargas no exitosas o inconsistencias de sincronización; se reintenta cuando corresponda e informa. Se dispone de descarga de archivos en base a GUI para los operadores autorizados y SUTEL si el acceso SFTP o por API no está temporalmente disponible. TNPC informa el estado de descarga al operador, disponibilidad de archivo, finalización de sincronización y cualquier excepción de entrega.

Generación de Archivos Diarios

TNPC genera los archivos de difusión diarios con las actualizaciones de enrutamiento para todos los números portados activados y todos los números retornados. El Generador de Archivos genera estos archivos en cada ventana de cambio definida y los pone a disposición de cada operador a través de las rutas SFTP seguras. Para los números activados, la difusión incluye información de enrutamiento actualizada, que incluye MSISDN y número de enrutamiento para que los operadores puedan actualizar sus bases de datos locales de enrutamiento. Para los números retornados, la difusión incluye el estado de no portado o retornado actualizado y la información del asignatario original para poder corregir las tablas de enrutamiento y para que no quede ningún enrutamiento de portación obsoleto en los sistemas del operador.

Administración centralizada de datos y modelo de enrutamiento

Además del cumplimiento a nivel de proceso antes descrito, TNPC garantiza plena adhesión a la **administración centralizada de datos y modelo de enrutamiento del Anexo 2** a través de la implementación de la NPCDB como repositorio único autorizado de todos los datos de portación. NPCDB no solo mantiene el estado de enrutamiento actual de cada número, sino también el ciclo de vida histórico completo de cada transacción, incluyendo eventos de generación de NIP, validación, portación, rechazo, cancelación y retorno. Todos los registros se guardan con marcas de tiempo, identificadores de operador y referencias de mensajes; y se mantienen en **formato inmutable, solo lectura**, para soporte de las auditorías regulatorias y trazabilidad legal. TNPC garantiza que los operadores mantengan copias locales de enrutamiento sincronizadas a través de archivos de difusión diarios y sincronización completa o incremental a demanda, al tiempo que todas las decisiones de enrutamiento surgen de la NPCDB centralizada en cumplimiento con el modelo ACQ. Los números de enrutamiento (NE) se gestionan conforme al plan de numeración, que garantiza el enrutamiento correcto y transparente de las llamadas sin impacto en el usuario final.

TNPC también asegura la estricta aplicación de **validación de datos, manejo de rechazos y controles regulatorios**. Todas las respuestas de rechazos a lo largo de los procesos se adhieren estrictamente a los códigos de rechazo y reglas de validación predefinidas establecidas en el Manual de Interfaces. Se incluyen validación de titularidad de numeración, prevención de duplicación o simultaneidad de solicitudes de portabilidad, aplicación de límites de portación y validación de las condiciones para que el suscriptor sea elegible. TNPC valida centralmente todas las condiciones de rechazo para evitar el uso indebido o la aplicación inconsistente a lo largo de los operadores. Además, la plataforma aplica todos los temporizadores regulatorios a través del Procesador de Temporizadores, lo cual asegura el cumplimiento con la entrega de NIP, respuesta de prevalidación, aprobación del donante y tiempos de ejecución de ventanas de cambio. Todos los eventos de temporizadores se registran en NPCDB y son auditables.

Continuidad operativa, reportes y respaldo de GUI

Para garantizar la continuidad operativa conforme a todas las condiciones, TNPC ofrece soporte para una **funcionalidad del operador fuera de línea** que permite a los operadores continuar procesando las transacciones de portaciones a través de la interfaz GUI en caso de falla del sistema o comunicación. Esto asegura que no se bloquee ninguna transacción debido a problemas de integración con los sistemas del operador o SUTEL, a la vez que se aplican todas las reglas de validación, temporizadores y requerimientos de auditoría. TNPC también garantiza el cumplimiento de los **requerimientos de seguridad y confidencialidad de datos**, que incluyen encriptación de datos en tránsito y en reposo, estricto control de acceso basado en roles y acceso controlado a NPCDB solo por entidades autorizadas. El acceso por parte de SUTEL, organismos autorizados y los operadores está regido por permisos definidos y es totalmente registrado. A través de estas capacidades, TNPC no solo cumple todos los requerimientos funcionales del Anexo 2 y el Anexo 3, sino que también garantiza el cumplimiento con un marco regulatorio más amplio en relación con la protección de datos, transparencia e integridad operativa.

Reportes: TNPC ofrece todos los reportes operativos, de rendimiento, SLA, incidencias y auditoría requeridos. Incluyen estadísticas de portaciones entrantes y salientes, motivos de rechazo por operador y por SIPN, generación de NIP y métricas de entrega, estadísticas de llamadas atendidas por IVR, tiempos de prevalidación, tiempos de respuesta del donante, finalización de activación, estadísticas de números retornados, estado de sincronización y difusión, estadísticas de uso del portal público, estadísticas de generación de tickets y cumplimiento de SLA. Los reportes están disponibles a través de acceso basado en roles. Los operadores tienen el acceso restringido a su actividad como donante o receptor y SUTEL tiene visibilidad privilegiada a lo largo de todos los operadores y procesos.

La plataforma de TNPC ofrece **dos interfaces gráficas de usuario (GUI) distintivas y en total cumplimiento**, tal como lo requiere el Anexo 3. Están diseñadas para soporte de interacciones operativas con los operadores y para ofrecer transparencia al usuario final, a la vez que garantizan la seguridad, usabilidad y cumplimiento regulatorio. Estas GUI están totalmente integradas a la plataforma central de TNPC y NPCDB, lo cual garantiza que toda la información presentada sea exacta, en tiempo real y consistente con las transacciones del sistema y datos de enrutamiento.

GUI operativa del operador y SUTEL

La primera GUI es una **interfaz operativa segura, basada en roles**, que utilizan los operadores, SUTEL y los interesados autorizados para gestionar e interactuar con todos los procesos de portabilidad numérica. Esta GUI permite a los usuarios realizar acciones como solicitudes de generación de NIP, reenvío de NIP, consultas de prevalidación, presentación de solicitud de portabilidad, procesamiento de cancelaciones, solicitudes de retorno de número (repatriación) y gestión de archivos de sincronización. La interfaz brinda visibilidad total sobre los estados de las transacciones, incluyendo intercambios de mensajes, resultados de validaciones, motivos de rechazo, estado de temporizadores y avance del flujo de trabajo. Todas las interacciones que se realizan a través de la GUI siguen la misma lógica de validación, estructura de mensaje y secuenciación de procesos que las interfaces automáticas SOAP y REST, lo cual garantiza consistencia a través de todos los canales de integración.

La GUI operativa también sirve como **mecanismo de respaldo en caso de caídas del web service del operador o SUTEL** y permite a los usuarios autorizados iniciar o procesar las transacciones manualmente sin interrupción de las operaciones del SIPN. Todas las acciones realizadas a través de la GUI se registran en NPCDB y tienen pistas de auditoría completas, que incluyen identidad de usuario, marcas de tiempo y detalles de las transacciones. La interfaz incluye capacidades avanzadas de reportería y tableros que permiten a los usuarios generar reportes históricos y en tiempo real sobre la actividad de portación, escenarios de rechazos, métricas de NIP, uso de IVR, estado de sincronización y cumplimiento de SLA. El acceso es estrictamente controlado a través de mecanismos de autenticación, autorización basada en roles y autenticación multifactorial, que garantiza el uso seguro y controlado de la plataforma.

GUI pública del usuario final (Portal del suscriptor)

La segunda GUI es un **portal web público seguro diseñado para los usuarios finales (suscriptores)**, que ofrece transparencia y accesibilidad a los servicios de portabilidad numérica en Costa Rica. Esta interfaz permite a los usuarios consultar el estado de sus transacciones de portación al ingresar el número de teléfono y NIP asociado para la **Autenticación de Factor Doble**. El sistema recupera la información de NPCDB en tiempo real y presenta los detalles clave como estado actual de la transacción, donante, receptor y ventana de cambio programada, lo cual asegura que los usuarios estén totalmente informados durante el proceso de portación.

La GUI pública Angular está diseñada con una **moderna interfaz de respuesta compatible con los dispositivos móviles, tabletas y computadoras de escritorio y cumple con los estándares de accesibilidad como WCAG 2.2**, que garantiza la usabilidad para todos los usuarios, incluyendo aquellos con necesidades especiales. Soporta múltiples idiomas que incluyen español de Costa Rica e inglés, con capacidad para extenderse a idiomas adicionales si fuese requerido. Se implementan mecanismos de seguridad como CAPTCHA y los controles de acceso para evitar el uso indebido y garantizar la protección de los datos. El portal también incluye capacidades de gestión de contenido que permite a SUTEL gestionar el contenido informativo relativo a las reglamentaciones de portabilidad numérica, procesos y derechos del usuario sin requerir cambios del sistema.

Además, TNPC ofrece una **interfaz web con acceso restringido a las entidades autorizadas**, tal como sea requerido, que permite a los organismos aprobados por SUTEL consultar el histórico de portaciones e información del operador actual. Esta interfaz incluye controles de autenticación sólidos, registro de auditorías y restricciones de acceso a datos para garantizar el cumplimiento con los requerimientos de privacidad de datos y regulatorios.

- 2.3.1** *Para la Sutel, la ERPN deberá ofrecer los servicios que sean requeridos para el funcionamiento de las plataformas regulatorias como: Plataforma de Registro Prepago, Plataforma para Comunicaciones no Solicitadas, Sistema de Gestión de Terminales Móviles y demás que la Sutel comunique de manera oportuna. Cuando corresponda, la Sutel brindará el detalle de sus servicios con los cuales deberá interactuar la ERPN.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC está diseñada para la integración sin inconvenientes con el ecosistema regulatorio de SUTEL y prestará los servicios que sean requeridos para el funcionamiento integrado con las plataformas regulatorias, que incluyen **Plataforma de Registro Prepago, Plataforma para Comunicaciones no Solicitadas, Sistema de Gestión de Terminales Móviles** y cualquier sistema adicional definido por SUTEL durante la contratación. TNPC logra esto a través de una **capa de integración orientada a servicios, basada en estándares y segura**, que expone interfaces seguras usando los protocolos **SOAP (XML sobre HTTPS) y REST (JSON sobre HTTPS)**. Todas las interacciones de servicio se adhieren estrictamente a las **definiciones de WSDL y los esquemas XML provistos por SUTEL**, que aseguran compatibilidad, interoperabilidad y cumplimiento con las interfaces regulatorias existentes. Cuando se utilizan servicios REST, TNPC asegura que las cargas de trabajo JSON estén en espejo con la estructura de esquema XML para garantizar el intercambio de datos consistentes a lo largo de todas las plataformas.

Para la **Plataforma de Registro Prepago**, TNPC ofrece integración en tiempo real para validar la identidad del suscriptor, titularidad y estado del servicio durante los procesos de prevalidación y portación. Esta integración asegura que las solicitudes de portabilidad que involucren usuarios prepago cumplan con los requerimientos regulatorios, operativos y de validación; y sean validadas contra fuentes de datos autorizadas. Para la **Plataforma para Comunicaciones no Solicitadas**, TNPC soporta mecanismos de intercambio de datos que permiten la verificación y aplicación de las preferencias del usuario, que garantiza que las transacciones de portación no violen los controles regulatorios relativos a comunicaciones no solicitadas. Del mismo modo, para el **Sistema de Gestión de Terminales Móviles**, TNPC soporta la integración para validar el estado del dispositivo cuando sea requerido, que permite a SUTEL aplicar políticas relativas a la elegibilidad del dispositivo, prevención del fraude y cumplimiento regulatorio.

Todas las integraciones se implementan a través de una **arquitectura segura y resiliente** que soporta interacciones sincrónicas y asincrónicas con mecanismos de reintento, manejo de errores y controles integrales de trazabilidad y registros de auditoría. TNPC asegura que todas las solicitudes, respuestas y resultados de validaciones intercambios con las plataformas de SUTEL se almacenen en NPCDB con trazabilidad completa, que incluye marcas de tiempo, identificadores de mensajes y respuestas de sistemas. En caso de indisponibilidad temporaria de las plataformas externas, TNPC soporta mecanismos de lógica de reintento y respaldo controlado para garantizar la continuidad de las operaciones del SIPN, sin comprometer la integridad de los datos ni el cumplimiento regulatorio.

Además, TNPC ofrece **extensibilidad flexible** para acomodar sistemas o mejoras futuras de SUTEL. El marco de integración modular de la plataforma permite que se incorporen nuevos servicios sin impacto en las funcionalidades existentes, lo cual garantiza que TNPC siga estando alienado con los requerimientos regulatorios, operativos y de integración en constante evolución. Mediante este enfoque, TNPC no solo cumple con los necesidades de integración actuales, sino que además ofrece una **plataforma lista para el futuro con capacidad para soportar servicios regulatorios adicionales tal como sean definidos por SUTEL**.

2.4 Garantizar la operación continua del SIPN en un esquema 24x7 (24 horas, 7 días a la semana), 365 días al año fungiendo como ERPN.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC está diseñada y opera para asegurar la **disponibilidad del servicio continuo del SIPN 24x7x365**, ofreciendo operaciones de portabilidad numérica ininterrumpidas para todos los operadores, SUTEL y los usuarios finales. Esto se logra mediante una combinación de **arquitectura altamente resiliente, monitoreo en tiempo real, mecanismos de recuperación ante fallas automáticos y soporte operativo proactivo**, lo cual asegura que los servicios del SIPN estén disponibles bajo todas las condiciones operativas, que incluyen períodos de demanda pico, ventanas de mantenimiento y eventos imprevistos del sistema.

Desde la perspectiva de la infraestructura, TNPC aprovecha la arquitectura desplegada en AWS, altamente disponible, tal como se define en la Sección 2.1. El sistema está alojado a lo largo de múltiples zonas de disponibilidad dentro de la región primaria, con un entorno de recuperación ante desastres totalmente replicado en la región secundaria. Esta arquitectura asegura que las capas de aplicación, base de datos e integración operen en **configuraciones activa-activa o en cluster**, con capacidades de recuperación ante desastres automáticas y sin ningún punto de falla. NPCDB es continuamente replicada y protegida para garantizar que todas las transacciones y datos de enrutamiento sean consistentes y estén disponibles en todo momento.

A nivel de aplicación, TNPC emplea un **marco de procesamiento accionado por mensajes** soportado por los componentes del Procesador de Mensajes y el Procesador de Temporizadores, lo cual garantiza que todas las transacciones sigan siendo procesadas aún durante interrupciones transitorias del sistema. El procesamiento encolado asegura que no se pierda ninguna transacción y que todos los mensajes sean procesados una vez restablecida la estabilidad del sistema. Además, la plataforma incluye mecanismos incorporados para **lógica de reintento, recuperación de transacciones y conciliación de estados**, lo cual garantiza que las operaciones del SIPN sean consistentes y completas bajo todos los escenarios.

A nivel operativo, TNPC tiene soporte del **Centro de Operaciones de Red (NOC) 24x7** y un modelo de soporte por capas que involucra a TNS. Se realiza el monitoreo continuo con herramientas como el sistema de monitoreo AWS CloudWatch que ofrece visibilidad de la salud, rendimiento y disponibilidad del sistema en tiempo real. Se generan alertas automáticas ante cualquier anomalía que permite la respuesta y resolución inmediatas. Se ejecutan el mantenimiento preventivo, parches y actualizaciones con estrategias de implementación continuas para garantizar que no se impacte la disponibilidad del sistema durante las actividades de mantenimiento.

Más aún, TNPC asegura que todos los componentes críticos, que incluyen interfaces del operador, Gateway de SMS, sistemas IVR, servicios de sincronización y módulos de reportería estén continuamente operativos. En caso de fallas externas del sistema, como problemas con la interfaz del operador o SUTEL, TNPC ofrece **mecanismos de respaldo que incluyen procesamiento de respaldo en base a GUI**, para garantizar la continuidad de servicios del SIPN sin interrupciones.

A través de esta combinación de arquitectura resiliente, monitoreo en tiempo real, recuperación automática y soporte operativo continuo, TNPC garantiza la entrega del servicio del SIPN en forma ininterrumpida, cumple totalmente con los requerimientos de SUTEL en las operaciones 24x7x365, a la vez que mantiene altos niveles de rendimiento, confiabilidad y cumplimiento regulatorio.

2.5 *Brindar el servicio de mantenimiento preventivo y correctivo del SIPN en un esquema 24x7 (24 horas, 7 días a la semana) en todos los niveles de atención, 365 días al año en idioma español.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El servicio de TNPC ofrecerá mantenimiento preventivo y correctivo integral 24x7x365 a lo largo de todos los niveles de atención de servicio, lo cual garantiza la operación continua y confiable del SIPN. Se ejecuta el mantenimiento a través de un modelo global de ingeniería y operaciones de TNS que combina un profundo conocimiento técnico en plataformas con soporte operativo responsivo. Todas las interacciones de mantenimiento con los operadores y SUTEL se realiza en idioma español, a través de ingenieros y personal de soporte de habla hispana, lo cual garantiza una clara comunicación, triage rápido y resolución efectiva en línea con las prácticas operativas de Costa Rica.

El mantenimiento preventivo es proactivo para minimizar riesgos y evitar interrupciones del servicio. Esto incluye el monitoreo continuo de la salud de las capas de aplicación, base de datos e integración; planificación de capacidad y ajustes de rendimiento; parches de seguridad y remediación de vulnerabilidades, verificación de copias de resguardo y pruebas de restauración; y revisiones periódicas de registros, alertas y tendencias. Se implementan actualizaciones y parches en forma continua o usando tiempo inactivo cero, o con tiempo inactivo mínimo acordado, durante los procedimientos de las ventanas de mantenimiento a lo largo de los nodos redundantes, lo cual garantiza que no se impactarán las transacciones en curso ni los SLA. Se programan las actividades preventivas en coordinación con SUTEL y los operadores, cuando corresponda, y se documentan y auditan en forma completa.

Se gestiona el mantenimiento correctivo a través del proceso de gestión de incidencias alineado con ITIL con niveles de severidad, tiempos de respuesta y rutas de escalado definidas. Se detectan las incidencias a través de herramientas de monitoreo en tiempo real como Amazon CloudWatch y los eventos informados por los usuarios; y se generan alertas automáticas hacia el Centro de Operaciones de Red 24x7. TNS ofrece soporte de Nivel 1 y Nivel 2 en español para manejo de diagnóstico inicial, coordinación y comunicación con el operador; mientras que TNS ofrece ingeniería de Nivel 3 para resoluciones técnicas profundas. Se realiza el análisis de causa principal para todas las incidencias significativas y se hace seguimiento de las acciones correctivas y medidas preventivas hasta el cierre.

La solución incluye una plataforma centralizada de generación de tickets accesible para los operadores, SUTEL y ERPN, que soporta registro de incidencias, seguimiento durante el ciclo de vida, monitoreo de SLA y reportería. Se emiten notificaciones por correo electrónico y otros canales convenidos para los hitos de creación, escalado y resolución de incidencias. Todas las acciones de mantenimiento, preventivo y correctivo, se registran y son trazables en NPCDB y los sistemas de soporte, lo cual garantiza transparencia total y cumplimiento con los requerimientos de auditoría.

A través de este modelo integrado de soporte operativo y de ingeniería, TNPC garantiza una respuesta rápida, resolución efectiva y mejora continua, a la vez que ofrece soporte operativo y servicio en idioma español, en pleno cumplimiento con los requerimientos de SUTEL para mantenimiento 24x7x365 a lo largo de todos los niveles de servicio.

- 2.6** *Dar soporte técnico a operadores y proveedores de servicios y a la Sutel en un esquema 24x7 (24 horas, 7 días a la semana), 365 días al año a través de diversos medios de contacto en todos los niveles de atención y en idioma español. Deberá contar al menos con las siguientes opciones: plataforma de tickets, correo electrónico y llamadas telefónicas a un número costarricense.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El servicio de TNPC **ofrecerá soporte técnico integral 24x7x365** a todos los operadores, proveedores de servicio y SUTEL, cubriendo todos los niveles de atención y garantizando asistencia ininterrumpida para las operaciones del SIPN. Se ofrece este soporte a través del marco de soporte y operaciones globales de TNS, que garantiza conocimiento técnico profundo y soporte operativo responsivo. Todas las interacciones de soporte son en idioma español con personal de soporte de TNS que habla español y actúa como punto de contacto principal, lo cual garantiza una comunicación efectiva, un rápido manejo del problema y alineación con las expectativas operativas de Costa Rica.

TNPC ofrece múltiples canales de soporte, tal como se requiere, que incluyen **plataforma centralizada de tickets, soporte por correo electrónico y acceso telefónico a través de un número de Costa Rica**. La plataforma de tickets permite a los usuarios registrar, hacer seguimiento y gestionar incidencias, solicitudes de servicio y consultas con visibilidad total del ciclo de vida, seguimiento de SLA y registros de auditoría. El soporte por correo electrónico permite una comunicación directa para la coordinación y escalado operativo, al tiempo que la línea telefónica dedicada de Costa Rica asegura soporte de voz inmediato para problemas críticos. Se categorizan todas las solicitudes de soporte en base a la severidad y se manejan conforme a los objetivos de tiempo de respuesta y resolución definidos, lo cual asegura una prestación de servicio a tiempo y consistente.

El modelo de soporte sigue la **estructura de niveles alineada con ITIL**, donde TNS ofrece soporte de Nivel 1 y Nivel 2 en español, que incluye triada inicial, diagnóstico del problema, coordinación con el operador y gestión de escalado. TNS ofrece soporte de Nivel 3, que aborda problemas complejos del sistema, defectos de software y mejoras a nivel de plataforma. Las herramientas de monitoreo continuo detectan proactivamente las anomalías del sistema y alertan al equipo de soporte, que permite una respuesta rápida aún antes de que los problemas sean informados. Todas las interacciones, resoluciones y escaladas se registran en el sistema de soporte y vinculan a los registros de transacciones de NPCDB, cuando corresponda, lo cual garantiza trazabilidad y reportaría total.

A través de este marco de soporte por nivel, multilingüe y en múltiples canales, TNPC garantiza que los operadores, proveedores de servicio y SUTEL reciban **soporte técnico de alta calidad, responsivo y confiable en todo momento**, con pleno cumplimiento del requerimiento de disponibilidad de servicio 24x7x365, en idioma español.

- 2.7** *Mantener el SIPN actualizado y de acuerdo con la más reciente versión disponible al público. Las fechas de actualización deberá ser consensuada con el CTPN-M y la Sutel.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC se mantiene en forma alineada con la última versión publicada, lo cual garantiza que el SIPN esté actualizado, sea seguro y en pleno cumplimiento con los requerimientos regulatorios, operativos y tecnológicos en constante evolución. TNS sigue un **marco de gestión de ediciones y versiones** conforme al cual se desarrollan, prueban e implementan todas las actualizaciones, mejoras y parches en forma controlada. Esto incluye las actualizaciones regulatorias exigidas por SUTEL, las mejoras solicitadas por CTPN-M, las actualizaciones de seguridad, optimizaciones de rendimiento y mejoras funcionales. Todas ellas se incorporan a la plataforma sin impacto en las operaciones en curso.

Todas las actividades de actualización se **planifican y ejecutan en estricta coordinación con CTPN-M y SUTEL**. Los programas de actualización, alcance y ventanas de implementación se acuerdan formalmente con anticipación. TNPC soporta versiones menores y mayores. En general, las actualizaciones mayores responden a cambios regulatorios o mejoras estructurales; y las actualizaciones menores incluyen mejoras incrementales, cambios de configuración y parches de seguridad. Las actualizaciones son primero implementadas y validadas en el entorno de pruebas con la participación de los operadores y SUTEL, lo cual garantiza la compatibilidad y estar listas antes de la entrada en producción.

Para garantizar la continuidad de servicio, TNPC usa **estrategias de implementación en forma continua o con tiempo inactivo cero durante la ventana de mantenimiento**, aprovechando su arquitectura AWS altamente disponible, con múltiples zonas de disponibilidad y redundante; por ello las actualizaciones se pueden aplicar sin interrumpir las operaciones del SIPN. Se documentan todas las actualizaciones que incluyen histórico de versión, registros de cambios y evaluaciones de impactos; y se ponen a disposición a través del repositorio de documentos accesible a los miembros de CTPN-M. A través de este enfoque controlado y colaborativo, TNPC asegura que el SIPN esté continuamente actualizado, en cumplimiento y alineado con los requerimientos de SUTEL, a la vez que se mantiene la estabilidad y transparencia operativa.

2.8 *El SIPN ofertado deberá ser modular, parametrizable y escalable para facilitar ajustes libres de costo.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC está diseñada como una **solución totalmente escalable, configurable modular**, que permite una rápida adaptación a los cambios regulatorios, operativos y del mercado sin necesidad de costos por rediseño del sistema ni desarrollos adicionales. La arquitectura consta de módulos funcionales independientes como el Procesador de Mensajes, Procesador de Temporizadores, Sistema Automático de Verificación (SAV), Gateway de SMS/SMPP, subsistema de IVR, Motor de Reportería y Generador de Archivos. Todos ellos interactúan a través de interfaces bien definidas. Este diseño modular permite introducir mejoras, cambios de configuración o nuevas funcionalidades de manera controlada, sin impacto en otros componentes ni en las operaciones en curso del SIPN.

Dentro de TNPC la parametrización se logra fundamentalmente a través de un enfoque por configuración, donde se mantienen las reglas de negocio, parámetros de procesos, temporizadores, lógica de validaciones, condiciones de rechazo, formatos de reportería y comportamiento de interfaces en estructuras de datos configurables dentro de NPCDB. Esto permite realizar actualizaciones frente a requerimientos regulatorios como cambios en motivos de rechazo, límites de portaciones o tiempos de procesos que se implementarán a través de cambios de configuración en lugar de con modificaciones de código. Del mismo modo, se pueden ajustar los parámetros de interfaces, reglas de manejo de mensajes y resultados de reportería; y procesos de actualización de enrutamiento para cumplir con los requerimientos de SUTEL y CTPN-M en constante evolución. Todos los ajustes se presentan como parte del servicio sin incurrir en costos adicionales de desarrollo, lo cual garantiza el cumplimiento con el requerimiento de fácil configuración para adaptabilidad sin costo alguno.

Se garantiza la escalabilidad a través del diseño arquitectónico y la flexibilidad de la implementación AWS. Conforme al modelo de implementación de AWS, TNPC soporta escalamiento dinámico horizontal y vertical a través de una infraestructura con escalado automático, que permite al sistema manejar mayores volúmenes de transacciones y cargas pico, sin degradación del rendimiento. El sistema tiene capacidad para soportar el crecimiento por etapas alineado con la evolución del mercado y el ingreso de nuevos operadores, sin requerir interrupción ni rediseño del sistema.

A través de la estructura modular, la parametrización por configuración y la arquitectura escalable, TNPC garantiza que el SIPN pueda evolucionar en forma eficiente, rentable y en pleno cumplimiento con el requerimiento de SUTEL para una plataforma flexible y lista para el futuro, con capacidad para adaptar los cambios en curso, sin costo adicional ni interrupción operativa.

- 2.9** *Tener capacidad para realizar, al menos, dos actualizaciones mayores y tres menores por año, todos libres de costo para que el SIPN desarrollado se mantenga vigente, seguro y moderno, de acuerdo con las mejores prácticas y según los requisitos evolutivos del CTPN-M. La ERP seleccionada deberá liderar y guiar estos procesos en común acuerdo con los operadores/proveedores miembros del CTPN-M.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

En coordinación con CTPN-M y SUTEL, TNS realizará los cambios requeridos. Esto garantiza que la plataforma del SIPN se mantenga **actual, segura, resiliente y alineada con los requerimientos regulatorios, operativos y tecnológicos en constante evolución.**

TNPC sigue un **marco estructurado de gestión de versiones y ciclo de vida en base a las mejores prácticas de la industria.** Todas las mejoras, actualizaciones de seguridad, mejoras operativas, optimizaciones de rendimiento y cambios funcionales se desarrollan, validan, prueban e implementan en forma controlada y totalmente auditable. En general, las versiones mayores abordan cambios regulatorios, nuevas capacidades funcionales, mejoras arquitectónicas o ingreso de nuevos operadores/proveedores, al tiempo que las versiones menores incluyen actualizaciones de configuración, mejoras de reportería, parches de seguridad, mejoras de usabilidad y optimizaciones operativas.

Todas las versiones se planifican y ejecutan mediando mutuo acuerdo con los operadores/proveedores, miembros de CTPN-M y SUTEL, a través de un **proceso de gobierno colaborativo y gestión de cambio liderado por TNS.** Esto incluye evaluación de impacto, planificación de implementación, talleres técnicos, coordinación de pruebas, programación de versiones y actividades para estar listos operativamente a fin de garantizar una evolución transparente y sin inconvenientes de la plataforma.

Las actualizaciones son primero implementadas y validadas en el entorno dedicado de pruebas basado en AWS, con la participación de los operadores y SUTEL antes de implementación. TNPC utiliza **estrategias de mantenimiento con implementación continua y mínimo tiempo inactivo, aprovechando la arquitectura altamente disponible de AWS** a fin de garantizar la implementación de actualizaciones sin interrupción de las operaciones en curso del SIPN.

Todas las actualizaciones se documentan en forma completa a través de las **notas de versión con control de versión, histórico de cambios, documentación técnica y evaluaciones del impacto operativo.** Se ponen a disposición de los interesados autorizados a través del repositorio de documentos de TNPC. A través de este enfoque estructurado y colaborativo, TNPC garantiza la **innovación continua, estabilidad operativa, cumplimiento operativo y sustentabilidad a largo plazo** de la plataforma SIPN de Costa Rica.

- 2.9.1** *Actualización mayor: cambios regulatorios debidamente aprobados por el Consejo de la Sutel. El ingreso o salida de nuevos operadores/proveedores será considerado una actualización mayor. No incluye modificaciones de parámetros operativos del SIPN.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC soporta plenamente la implementación de **actualizaciones mayores conforme a los cambios regulatorios aprobados por el Consejo de SUTEL,** así como también el ingreso o salida de operadores y proveedores de servicios dentro del ecosistema del SIPN. Estas actualizaciones mayores se manejan a través de un **marco de gobierno y gestión de versiones,** que asegura que todos los cambios sean implementados en forma consistente, auditable y sin interrupciones. TNPC está específicamente diseñado para adaptar los cambios a través de una arquitectura modular y diseño por configuración, que permite a la plataforma incorporar nuevos requerimientos regulatorios sin necesidad de rediseño del sistema.

Para actualizaciones regulatorias, TNPC permite nuevas reglas, lógica de validación, condiciones de rechazo, flujos de procesos y requerimientos de cumplimiento que serán implementados a través de marcos de reglas de negocio configurables mantenidos dentro de NPCDB. Esto garantiza que las actualizaciones requeridas por SUTEL se puedan implementar en forma eficiente a la vez que están totalmente alineadas con el Manual de Interfaces y Procesos. Cada actualización regulatoria es desarrollada, validada en el entorno de pruebas con la participación de los operadores y SUTEL e implementada en producción siguiendo la aprobación formal y los tiempos convenidos.

Para el ingreso y salida de operadores, TNPC ofrece un **proceso estructurado de integración y configuración**, que incluye registro de identificadores del operador, números de enrutamiento, puntos finales de interfaz, credenciales de seguridad y configuración de conectividad. La plataforma soporta la incorporación y baja de operadores sin inconvenientes, sin impacto en los participantes existentes y con garantía continua de las operaciones y manteniendo la exactitud del enrutamiento a lo largo del sistema. Todos los cambios se reflejan en NPCDB y se propagan automáticamente a través de los mecanismos de sincronización y difusión a todos los operadores.

Tal como se requiere, los **cambios a los parámetros operativos del SIPN se tratan por separado y no se consideran como actualizaciones mayores**. Se gestionan a través de las configuraciones del sistema sin impacto en el ciclo de las versiones mayores. El ingreso y salida de nuevos operadores se hace a través de un proceso configurable y sin costo adicional.

2.9.2 *Actualización menor: mejoras al SIPN, parámetros operativos, parches de seguridad, cambios en reportes, optimizaciones de rendimiento y mejoras visuales en la interfaz en la plataforma sean propuestos por la ERPN o el CTPN-M.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC soporta una línea continua de actualizaciones menores que incluyen mejoras a las funcionalidades del SIPN, parámetros operativos configurables, parches de seguridad, mejoras de reportería, optimizaciones de rendimiento y mejoras visuales a las interfaces de la plataforma. Estas actualizaciones se entregan como parte del servicio estándar de TNS y se gestionan a través de un marco estructurado de mejoras continuas y gestión de versiones, lo cual asegura que el sistema sea moderno, seguro y esté alineado con las necesidades operativas en constante evolución definidas por SUTEL y CTPN-M.

Las actualizaciones menores se implementan fundamentalmente a través de la arquitectura por configuración de TNPC, que permite ajustes a los parámetros de procesos como temporizadores, reglas de validación, comportamientos de enrutamiento, formatos de reportería y elementos de la interfaz de usuario, sin requerir cambios de código ni rediseño del sistema. Esto permite una rápida implementación de las mejoras a la vez que minimiza riesgos; y garantiza que se apliquen las actualizaciones con eficiencia y en forma consistente en todos los entornos. Las actualizaciones de seguridad, que incluyen remediación de vulnerabilidades y parches, se aplican en forma proactiva conforme a las mejores prácticas de la industria a fin de mantener la integridad y protección de los datos y operaciones del SIPN.

Todas las actualizaciones menores siguen un ciclo de vida controlado que incluye desarrollo, validación en el entorno de prueba con la participación del operador y SUTEL; y la implementación coordinada en producción. TNPC utiliza **estrategias de implementación en forma continua o con tiempo inactivo cero durante la ventana de mantenimiento**, que asegura que las actualizaciones no interrumpan las operaciones continuas del SIPN, ni tengan impacto en la disponibilidad del servicio más allá de los umbrales convenidos. Se introducen las mejoras a las capacidades de reportería e interfaces del usuario como respuesta al feedback operativo de CTPN-M, que mejora las capacidades de usabilidad, visibilidad y toma de decisiones para todos los interesados.

A través de este enfoque, TNPC asegura la evolución continua del SIPN para cumplir con los requerimientos operativos, regulatorios y tecnológicos, entregando mejoras incrementales con eficiencia y sin costo adicional, a la vez que mantiene estabilidad, rendimiento y cumplimiento total con las expectativas de SUTEL.

2.9.2.1 Integración, adaptación e interacción con otras plataformas regulatorias.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC está diseñada como un **hub de integración abierto, en base a estándares**, que permite la interacción sin inconvenientes con las plataformas regulatorias actuales y futuras de SUTEL, que incluyen, sin carácter limitativo, la Plataforma de Registro Prepago, Plataforma de Comunicaciones No Solicitadas y el Sistema de Gestión de Equipos Terminales; y cualquier otro sistema adicional. TNPC logra esto a través de una **arquitectura orientada a servicios** que soporta tanto interfaces **SOAP XML sobre HTTPS como REST JSON sobre HTTPS**, que garantiza compatibilidad total con las integraciones existentes, a la vez que permite modernización cuando sea requerido. Todos los intercambios de mensajes se adhieren estrictamente a las definiciones de WSDL y esquemas XML provistos por SUTEL; y todas las cargas REST se estructuran para hacer espejo con estos esquemas para garantizar consistencia, integridad de datos e interoperabilidad a lo largo de los sistemas.

TNPC ofrece capacidades de integración en tiempo real que soportan flujos de trabajo de validaciones sincrónicas y procesamiento asincrónicos. A modo de ejemplo, durante los procesos de prevalidación y portación, TNPC interactúa con la Plataforma de Registro Prepago para validar la identidad y titularidad del suscriptor para garantizar el cumplimiento regulatorio para servicios prepago. Todos los puntos de integración se implementan con manejo de errores, mecanismos de reintento y controles de timeout robustos, que garantiza que la indisponibilidad temporaria de los sistemas externos no interrumpan las operaciones del SIPN. Cuando sea necesario, TNPC soporta mecanismos de respaldo controlado, que incluyen interacción en base a GUI, para mantener la continuidad operativa.

El diseño modular de TNPC garantiza que la integración con las plataformas regulatorias adicionales se implemente con eficiencia, sin impacto en los servicios existentes. Se pueden agregar nuevas plataformas con interfaces SOAP XML sobre HTTPS y REST JSON sobre HTTPS, a través de puntos finales de servicios estandarizados y configuración, lo cual permite a SUTEL extender el ecosistema regulatorio sin requerir el rediseño del sistema.

Todas las interacciones con las plataformas externas se registran en NPCDB con trazabilidad total, que incluyen datos de la solicitud y respuesta, marcas de tiempo y resultados para cumplir con los requerimientos de auditoría y reportería. Además, TNPC ofrece capacidades de monitoreo y reportería que ofrecen a SUTEL visibilidad del rendimiento de la integración, tasas de éxito de las transacciones y condiciones de error a lo largo de todos los sistemas conectados.

La implementación y las actualizaciones a nuevas plataformas de integración siguen un ciclo de vida controlado, que incluyen pruebas en el entorno de prueba dedicado con la participación de SUTEL, nueva plataforma y los operadores. Las actualizaciones de producción se implementan usando estrategias de cero tiempo inactivo o implementación continua, o durante las ventanas de mantenimiento convenidas para tener un impacto mínimo o controlado en el servicio. A través de este enfoque, TNPC ofrece un marco de integración flexible, seguro y listo para el futuro que no solo cumple con los requerimientos regulatorios actuales, sino que además permite la adaptación sin inconvenientes hacia nuevas plataformas y las necesidades regulatorias en constante evolución definidas por SUTEL.

2.9.2.2 *La conectividad y operatividad de la plataforma debe evolucionar de acuerdo con las mejores prácticas de la industria de modo que se garantice el funcionamiento óptico y la ciberseguridad del SIPN.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC está diseñada para la evolución continua, en alineación con las **mejores prácticas de la industria para conectividad, excelencia operativa y ciberseguridad**, lo cual asegura el funcionamiento óptimo del SIPN durante todo el período de la contratación. La solución aprovecha la **arquitectura modular, segura y en base a estándares** que permite a la plataforma adoptar nuevas tecnologías, protocolos y controles de seguridad sin interrumpir los servicios en curso. La conectividad con los operadores, SUTEL y las plataformas regulatorias externas se implementa con protocolos seguros como HTTPS, VPN y enlaces dedicados, con soporte tanto para interfaces SOAP XML como REST JSON, lo cual garantiza la interoperabilidad, a la vez que permite la modernización progresiva en línea con los estándares globales de telecomunicaciones e IT.

Desde la perspectiva de ciberseguridad, TNPC sigue una **estrategia de defensa en profundidad** que incorpora seguridad de redes, seguridad de aplicaciones, protección de datos y monitoreo continuo. Esto incluye el uso de Web Application Firewalls, detección de intrusos y sistemas de prevención, encriptación de datos en tránsito y en reposo, control de acceso basado en roles y autenticación multifactorial para todas las interfaces críticas. Se monitorea continuamente a la plataforma usando herramientas de observación de avanzada que permiten la detección temprana de anomalías, la respuesta proactiva ante amenazas potenciales y la rápida remediación de vulnerabilidades. Se aplican actualizaciones de seguridad, parches y mejoras conforme a las mejores prácticas de la industria y la inteligencia ante la evolución de las amenazas para garantizar que el SIPN esté protegido contra los riesgos que surgen.

TNPC adopta las mejores prácticas en **optimización de rendimiento, alta disponibilidad y escalabilidad** que incluyen una arquitectura redundante, balanceo de carga y escalado dinámico de recursos. El monitoreo y análisis continuos ofrecen visibilidad en tiempo real del rendimiento del sistema y salud de la conectividad, que permiten realizar ajustes proactivos para mantener una óptima operación. La plataforma soporta la evolución continua a través de actualizaciones y mejoras estructuradas que se implementan con estrategias de cero tiempo inactivo o implementación continua, o durante las ventanas de mantenimiento convenidas con impacto mínimo o controlado en el servicio.

A través de este enfoque, TNPC garantiza que la conectividad y operaciones del SIPN sigan alineadas con las mejores prácticas internacionales, entregando una plataforma segura, resiliente y lista para el futuro, que soporta mejora continua, cumplimiento regulatorio y sustentabilidad a largo plazo para el ecosistema de portabilidad numérica de Costa Rica.

2.10 *Según resulten aplicables, deberá brindar sin costo alguno, capacitaciones en línea a los operadores/proveedores y la Sutel para cada cambio o actualización funcional u operativa del SIPN según el punto 2.9.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS brindará capacitación de Usuario Final para el sistema TNPC a los operadores y Sutel. En caso de que algún nuevo operador ingrese al mercado de telecomunicaciones de Costa Rica, TNS podrá adaptar la capacitación de Usuario Final del sistema TNPC. Las sesiones de capacitación y todos los materiales serán proporcionados en inglés/español.

La capacitación se organizará en módulos y se elaborarán materiales para cada uno de ellos con una reseña, ejercicios de muestra y resumen.

Los módulos de capacitación incluirán:

- **Capacitación de Usuario Final:** Este curso describe las funciones de TNPC y ofrece instrucciones a los usuarios del operador que usan la GUI:
 - Reseña de TNPC - Introducción a la portabilidad numérica, funciones realizadas por TNPC, interfaces y conceptos de portabilidad
 - Procesos de Portación de TNPC - Reseña de cada proceso de portación, diagramas de secuencias, intercambio de mensajes
 - GUI Web de TNPC - Cuándo usar la GUI de TNPC, cómo acceder, ejemplos de mensajes de portación, reseña de flujos de portaciones
 - Servicio Web de TNPC - Descripción, flujo de procesos, creación de mensajes SOAP, comparación con GUI, registros
 - Acceso al SFTP de TNPC - Descripción, acceso
 - Reportes de TNPC - Reportes generados por el usuario, reportes programados, acceso, lista completa de reportes con descripciones, reportes de muestra.

2.11 *El SIPN desarrollado deberá ser escalable de acuerdo con lo siguiente:*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado. Por favor consultar nuestras respuestas a continuación.

2.11.1 *Capacidad de crecimiento progresivo acorde con la evolución del mercado.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC está diseñada para ofrecer **escalabilidad por etapas, predecible y rentable**, en línea con la evolución del mercado de telecomunicaciones de Costa Rica. La arquitectura soporta el crecimiento incremental del volumen de transacciones, número de operadores y complejidad regulatoria sin requerir el rediseño o interrupción del servicio. Esto se logra a través de un **diseño modular, horizontalmente escalable**, en el cual se pueden expandir los recursos de computación, aplicación y base de datos en forma independiente a medida que aumenta la demanda. La plataforma soporta ambos modelos de implementación definidos en la Sección 2.1, lo cual garantiza que se mantiene la escalabilidad.

Con el **modelo de implementación de AWS**, TNPC aprovecha las capacidades de escalamiento automático que permiten a la plataforma agregar y retirar dinámicamente los recursos de computación en base a las métricas de carga de trabajo en tiempo real, tal como producción de transacciones, profundidad de cola y utilización de CPU. La capa de aplicación incluye el Procesador de Mensajes, Procesador de Temporizadores y servicios de integración, hace escalado horizontal a través de múltiples instancias concurrentes, mientras que la capa de base de datos usa las capacidades de Aurora, tal como réplicas de lectura y escalado automático de almacenamiento para acomodar los crecientes volúmenes de datos. Esto permite realizar un manejo sin inconvenientes del crecimiento gradual del mercado, así como también los incrementos de la actividad de transacciones sin impacto en el rendimiento ni en los SLA.

Desde la perspectiva operativa, TNPC soporta una configuración por escalabilidad y flexibilidad de procesos, que permite el ingreso de nuevos operadores, la introducción de nuevos requerimientos regulatorios y la expansión de los servicios sin rediseño del sistema. Todos los cambios de escalabilidad se implementan con estrategias de cero tiempo inactivo o implementación continua, o durante las ventanas de mantenimiento convenidas con impacto mínimo o controlado en el servicio. A través de este enfoque, TNPC entrega una plataforma lista para el futuro que puede evolucionar con el crecimiento del mercado de Costa Rica; y mantener el rendimiento, la confiabilidad y el cumplimiento en cada etapa de la expansión.

2.11.2 Soporte para incrementos sostenidos o abruptos en el volumen de transacciones.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC está diseñada para manejar tanto el **crecimiento significativo en los volúmenes de transacciones** como **picos repentinos en la demanda**, sin degradación del rendimiento, ni afectar la disponibilidad de servicio ni el cumplimiento de SLA. Se logra esta capacidad a través de una combinación de infraestructura elástica, procesamiento distribuido y arquitectura encolada, lo cual garantiza que todos los procesos del SIPN, incluidos la generación de NIP, prevalidación, portación y sincronización continúen funcionando en forma confiable bajo condiciones de carga diferentes.

Con el **modelo de implementación de AWS**, TNPC aprovecha la infraestructura de escalamiento automático que ajusta dinámicamente los recursos de computación en base a los indicadores de carga de trabajo en tiempo real, tal como producción de transacciones, profundidad de cola y utilización de CPU. La capa de aplicación que incluye los componentes del Procesador de Mensajes y el Procesador de Temporizadores funciona en un cluster escalable horizontalmente que permite múltiples instancias para procesar transacciones en forma concurrente. En períodos de demanda repentina, como campañas promocionales o eventos de portación masiva por regulación, se aprovisionan las instancias en forma automática para absorber la carga. La capa de base de datos, que se implementa con AWS Aurora, soporta el procesamiento de transacciones de alta producción con almacenamiento distribuidos y réplicas de lectura, que aseguran que las mayores demandas de acceso a datos no impacten la capacidad de respuesta del sistema.

A nivel de aplicación, TNPC usa un **modelo de encolado de mensajes y procesamiento asíncrono**, que asegura que se encolen las transacciones entrantes y procesen en forma confiable, incluso durante las cargas pico, lo cual evita la pérdida de datos y la sobrecarga del sistema. Las transacciones se priorizan y procesan en secuencia. Todos los estados y eventos se registran en NPCDB para garantizar la consistencia y recuperabilidad. Además, TNPC monitorea constantemente el rendimiento del sistema y dispara alertas automáticas y acciones de escalado para mantener el funcionamiento óptimo.

Se implementan todas las acciones de escalado con estrategias de implementación en forma continua o con tiempo inactivo cero durante la ventana de mantenimiento, que asegura que los ajustes de capacidad y mejoras de infraestructura no tengan impacto en las operaciones en curso del SIPN. A través de este enfoque integral, TNPC garantiza que la plataforma pueda soportar tanto el crecimiento a largo plazo, como los incrementos repentinos en el volumen de transacciones; y mantiene la estabilidad, el rendimiento y el cumplimiento regulatorio bajo todas las condiciones operativas.

2.11.3 Cumplimiento de los temporizadores definidos en el Manual de Interfaces y Procesos, pero a su vez configurables para los procesos de portación.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC **cumple completamente con todos los temporizadores definidos en el Manual de Interfaces y Procesos**, lo cual asegura que cada etapa del ciclo de vida de la portabilidad numérica se ejecute dentro de los marcos de tiempos regulatorios prescritos. Esto incluye, sin carácter limitativo, los temporizadores para generación y entrega de NIP, respuestas de prevalidación, aprobación del donante, programación de cancelaciones, ejecución de ventana de cambio, manejo de cancelaciones y procesos de sincronización. TNPC aplica estos temporizadores a través del **componente del Procesador de Temporizadores**, que monitorea continuamente todas las transacciones activas, valida la llegada de mensajes dentro de los intervalos esperados; y dispara automáticamente acciones predefinidas en caso de eventos de timeout. Todos los eventos de temporizadores, que incluyen inicio, vencimiento y acciones resultantes del sistema se registran en NPCDB con trazabilidad total, que asegura la auditoría y cumplimiento de los requerimientos de SLA.

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

TNPC permite que SUTEL y CTPN-M ajusten los tiempos de los procesos conforme a la evolución de los requerimientos regulatorios y operativos. Los valores de temporizadores, umbrales y reglas de escalado se mantienen como parámetros configurables dentro de NPCDB y se pueden modificar sin requerir cambios en el código de la aplicación. Esto ofrece flexibilidad para adaptarse a las actualizaciones regulatorias futuras, tal como reducciones en los tiempos de portación o ajustes en los tiempos de respuesta de validación, a la vez que garantiza que todos los operadores participantes funcionen bajo un marco de tiempos aplicados centralmente y con consistencia.

2.11.4 *Monitoreo continuo del desempeño y capacidad de ajuste dinámico de recursos.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC incorpora un **marco de gestión de recursos dinámico y monitoreo de desempeño continuo** para garantizar el funcionamiento óptimo del SIPN en todo momento. La solución ofrece visibilidad en tiempo real de toda la salud del sistema, procesamiento de transacciones, rendimiento de interfaces y uso de infraestructura a lo largo de todos los componentes que incluyen el Procesador de Mensajes, Procesador de Temporizadores, Gateway de SMS, subsistema del IVR, servicios de bases de datos e interfaces de integración con las plataformas de los operadores y SUTEL. Se implementa el monitoreo usando herramientas de observación de grado empresarial como el sistema de monitoreo AWS CloudWatch, que recolecta y analiza métricas, registros y eventos a lo largo de toda la plataforma. Estas herramientas permiten la detección proactiva de anomalías, degradación del rendimiento o fallas potenciales, lo cual asegura que se identifiquen y aborden los problemas antes de que impacten en la disponibilidad del servicio o cumplimiento del SLA.

Se logra el ajuste dinámico de recursos a través de **mecanismos de escalado automático y optimización de recursos** que responden a las condiciones de carga de trabajo en tiempo real. Con el modelo de implementación de AWS, TNPC aprovecha las capacidades de escalado automático para ajustar la capacidad de computación en forma dinámica, en base a métricas como producción de transacciones, profundidad de cola, uso de CPU y tiempos de respuesta. Se pueden aprovisionar instancias de aplicaciones adicionales en forma automática para manejar una mayor carga; mientras que se pueden reducir los recursos inutilizados durante los períodos de menor demanda, lo cual asegura tanto la eficiencia en el rendimiento como la optimización de los costos.

A nivel de aplicación, TNPC usa un **modelo de encolado de mensajes y procesamiento asíncrono** que asegura que se amortigüen y procesen las transacciones entrantes y en forma confiable durante las condiciones de carga pico. Este enfoque evita la sobrecarga del sistema, mantiene la integridad de las transacciones y permite que la plataforma absorba los picos repentinos en la demanda sin impacto en los tiempos de respuesta. El sistema evalúa constantemente los indicadores de desempeño y dispara alertas automáticas y acciones de escalado cuando se superan los umbrales predefinidos, lo cual asegura que se ajusten los recursos en forma dinámica para mandar un óptimo desempeño.

Todas las métricas de desempeño y los datos de monitoreo se almacenan y correlacionan con los registros de transacciones en NPCDB, que permiten la reportería y análisis detallado del comportamiento del sistema, cumplimiento de SLA y tendencias operativas. TNPC ofrece tableros en tiempo real y reportes configurables que permiten a SUTEL y los operadores monitorear el desempeño del sistema, realizar el seguimiento de los indicadores clave e identificar potenciales mejoras. Se implementan ajustes a la asignación de recursos y ajustes de desempeño con estrategias de implementación en forma continua o con tiempo inactivo cero durante la ventana de mantenimiento, que asegura que las actividades de optimización de desempeño no interrumpen las operaciones del SIPN.

A través de este enfoque integrado del monitoreo y gestión dinámica de recursos, TNPC garantiza que el SIPN mantenga altos niveles de desempeño, confiabilidad y escalabilidad, en pleno cumplimiento con los requerimientos de SUTEL para funcionamiento continuo y gestión adaptativa de la capacidad.

- 2.12** Asegurar que todo el personal que se relacione con los miembros del CTPN- M para la implementación y la prestación de los servicios del SIPN deberá hablar y escribir en idioma español con fluidez, incluyendo, pero no limitado al soporte, reuniones periódicas, implementaciones y al desarrollo de las actualizaciones. Este requisito no se verá cumplido a través de la intervención de traductores.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS garantizará que todo el personal que interactúa con los miembros del CTPN-M durante todo el ciclo de vida de los servicios del SIPN hable y escriba en español con fluidez; y que esta capacidad se entregue directamente con los miembros asignados del equipo y no con la intervención de traductores. TNS ofrece un equipo dedicado de ingenieros, especialistas de soporte, gerentes de proyecto y personal operativo de habla española, que será la interfaz primaria para las interacciones diarias con los operadores y SUTEL. Esto incluye las actividades de implementación, soporte de integración, reuniones periódicas técnicas y de gobierno, coordinación de control de cambios, manejo de incidencias y comunicación operativa en curso. TNS ofrece recursos técnicos que hablan español y garantiza que todo el soporte global de ingeniería será coordinado a través del modelo de contratación consistente y primero en español.

El soporte técnico incluye Nivel 1 y Nivel 2, gestión de incidencias e interacciones con la mesa de ayuda que TNS ofrece en español para garantizar un rápido entendimiento y resolución de los problemas sin demoras de traducción. Toda la documentación que incluye Manuales de Interfaces y Procesos, notas de versiones, procedimientos operativos, reportes y materiales de capacitación se brindarán en español con soporte bilingüe, cuando corresponda. Las sesiones de capacitación, talleres y actividades de ingreso se realizarán en español, usando una metodología estructurada que garantice la transferencia efectiva del conocimiento a todos los miembros de CTPN-M.

Además, se estructuran los procesos de gobierno y comunicaciones para garantizar la contratación continua en español. Las reuniones regulares, revisiones de estado, talleres de implementación y conversaciones de actualización serán en español, con una comunicación clara y consistente con todos los interesados. Todos los canales de comunicación, que incluyen los sistemas de tickets, correspondencia por correo electrónico y soporte telefónico a través de un número de Costa Rica, se manejarán en español. Este enfoque garantiza claridad, eficiencia y alineación con las prácticas operativas locales, a la vez que elimina la dependencia de niveles de traducción.

A través de este marco global de soporte operativo coordinado, TNPC garantiza que todas las interacciones con los miembros de CTPN-M se realicen con fluidez y profesionalismo en idioma español, en pleno cumplimiento con el requerimiento de SUTEL y garantizando la colaboración efectiva a través de la implementación y funcionamiento de los servicios del SIPN.

- 2.12.1** Los cambios de personal por parte de la ERPN deberán ser comunicados con antelación al CTPN-M para su análisis y autorización.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS garantizará que cualquier cambio del personal involucrado en la implementación, operación, soporte o gestión de los servicios del SIPN sea **formalmente comunicado con antelación a CTPN-M para su revisión y autorización**, en total alineación con los requerimientos de gobierno. Se establece un **proceso estructurado de transición y gestión de recursos** para garantizar transparencia, continuidad de servicio y mantenimiento de las competencias requeridas en todo momento.

Para cualquier cambio de personal propuesto, TNPC entregará una notificación previa que incluya el rol, responsabilidades, calificaciones, experiencia del individuo y detalles del reemplazo, cuando corresponda. Esto permite a CTPN-M revisar y confirmar que el recurso propuesto cumple con los estándares técnicos y operativos requeridos. No se implementará ningún cambio de personal que afecte roles críticos sin antes obtener la aprobación necesaria para garantizar el pleno cumplimiento de los requerimientos de supervisión.

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

Para garantizar la continuidad y minimizar cualquier impacto operativo, TNPC sigue un **marco de transferencia de conocimiento y transición** controlado, donde se superpone el personal saliente y entrante durante un período definido de tiempo para la transferencia de conocimiento, responsabilidades y contexto operativo. Se mantiene toda la documentación, procedimientos y conocimiento del sistema en repositorios centralizados para soporte de las transiciones sin inconvenientes. TNS asegura la continuidad de las interacciones en idioma español, a la vez que conserva el conocimiento técnico, conocimiento operativo y continuidad del servicio durante las transiciones de personal.

Todos los cambios de personal, aprobaciones y actividades de transición se documentan y son auditables para garantizar trazabilidad y alineación totales con las expectativas de gobierno. A través de este enfoque disciplinado, TNPC asegura que los cambios de personal se gestionen con transparencia, sin interrupción de las operaciones del SIPN, niveles de servicios ni sin la participación de los interesados.

2.13 *El SIPN desarrollado deberá permitir su evolución tecnológica sin afectar la continuidad del servicio ni su funcionamiento para los operadores/proveedores y los usuarios finales.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC está diseñada para permitir la evolución tecnológica continua, a la vez que protege las operaciones ininterrumpidas del SIPN para los operadores, proveedores de servicio y usuarios finales. Esto se logra a través de una **arquitectura modular orientada a servicios** que desacopla los componentes de procesamiento central, tales como Procesador de Mensajes, Procesador de Temporizadores, NPCDB, VAS, Gateway de SMS, IVR y servicios de integración. Esta separación permite la mejora, actualización o reemplazo de los componentes individuales sin impacto en el sistema total ni en las transacciones en curso. Por consiguiente, se pueden introducir nuevas capacidades, cambios regulatorios o requerimientos de integración en forma incremental para asegurar que la plataforma evolucione en línea con los estándares de la industria y los requerimientos de SUTEL sin afectar la continuidad del servicio.

Desde la perspectiva de implementación y operaciones, TNPC aplica un **marco de control de cambios y versiones**, donde todas las mejoras se validan primero en los entornos de desarrollo y prueba dedicados con la participación de los operadores y SUTEL. Se mantiene la retrocompatibilidad de interfaces en todo momento para garantizar que las integraciones existentes de los operadores sigan funcionando sin requerir cambios inmediatos, a la vez que se introducen nuevas interfaces o mejoras en forma controlada y transparente.

Además TNPC asegura la continuidad a través de la **gestión de los estados de las transacciones y persistencia de datos** en NPCDB, donde se registran todas las transacciones en curso y completadas y se las pueden retomar o conciliar en caso de cambios en el sistema o interrupciones temporales. Las capas de integración se diseñan con mecanismos de reintento, control de versión y compatibilidad de esquemas para permitir que las nuevas versiones coexistan con las existentes durante los períodos de transición. Además, las capacidades de monitoreo continuo y gestión de rendimiento garantizan que se detecte y aborde proactivamente cualquier impacto en la evolución del sistema.

A través de esta combinación de diseño modular, prácticas de implementación controlada, interfaces con retrocompatibilidad y gestión de transacciones robusta, TNPC permite el avance tecnológico continuo, a la vez que conserva la estabilidad operativa y asegura que los servicios del SIPN sean confiables, consistentes y en cumplimiento durante todo el ciclo de vida de la plataforma.

2.14 *Garantizar la integridad, consistencia, unicidad y trazabilidad para la auditoría de los procesos.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC está diseñada para garantizar los mayores niveles de **integridad, consistencia, unicidad y trazabilidad total de datos** a lo largo de todos los procesos del SIPN para garantizar que se pueda auditar cada transacción en forma confiable conforme a los requerimientos regulatorios de SUTEL. La NPCDB centralizada es la parte central de esta capacidad que actúa como **única fuente autorizada de la verdad** para todos los datos de portabilidad numérica. Todas las transacciones, incluida la generación de NIP, prevalidación, solicitudes de portabilidad, aprobaciones, rechazos, cancelaciones, retornos y eventos de sincronización se registran en NPCDB con identificadores únicos de transacción, referencias de mensajes, marcas de tiempo, identificadores de operador y estados de procesos para garantizar que cada transacción sea singularmente identificable y no pueda ser duplicada ni alterada.

TNPC aplica **integridad y consistencia de datos** a través de estrictos mecanismos de validación en cada etapa del procesamiento de mensajes. Se validan todos los mensajes entrantes y salientes contra los esquemas WSDL y XSD definidos para asegurar que sean estructural y semánticamente correctos antes del procesamiento. Las reglas de negocio y las limitaciones regulatorias se aplican centralmente a través del Procesador de Mensajes, que asegura que todos los operadores se adhieran a la misma lógica de validación y condiciones de rechazo. El sistema garantiza la **unicidad de las transacciones** al evitar solicitudes duplicadas, operaciones concurrentes en conflicto y transiciones de estado inconsistentes a través del control centralizado y la validación en tiempo real contra la NPCDB.

Para asegurar la **trazabilidad** total, TNPC mantiene registros de auditoría inmutables de todas las actividades del sistema, que incluyen intercambios de mensajes, acciones del usuario, eventos generados por el sistema, disparadores de temporizadores e interacciones de integración con plataformas externas. Cada evento tiene una marca de tiempo y se relaciona a la transacción correspondiente para permitir la reconstrucción total del ciclo de vida de la transacción desde el inicio hasta la finalización. Se guardan los registros de auditoría en formato solo lectura y se protegen contra modificaciones para garantizar el cumplimiento con los requerimientos regulatorios y de auditorías legales. TNPC también ofrece capacidades integrales de reportería y consulta para permitir que SUTEL y los interesados autorizados tengan acceso a la información detallada de las auditorías, hagan el seguimiento de la ejecución del procesos y verifiquen el cumplimiento con los SLA y normas regulatorias.

A través de esta combinación de gestión centralizada de datos, estrictos controles de validación, registros de auditoría inmutables y reportería integral, TNPC asegura que todos los procesos del SIPN sean ejecutados con total integridad, consistencia, unicidad y trazabilidad para cumplir plenamente con los requerimientos de auditoría y gobierno de SUTEL.

2.14.1 *Disponer de un registro de ocurrencias (logs) el cual contendrá cualquier evento en la base de datos, los archivos, el sistema de intercambio de información y todos los sistemas implementados.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece **registro** centralizado e integral de **eventos a lo largo de todas las capas del sistema** para garantizar que cada actividad relativa a las operaciones del SIPN sea capturada, almacenada y puesta a disposición para fines de monitoreo, auditoría y reportería. Se generan registros de eventos para todos los componentes que incluyen NPCDB, procesos de sincronización y generación de archivos, sistemas de intercambio de información, interfaces de integración y subsistemas de soporte tales como el Procesador de Mensajes, Procesador de Temporizadores, Gateway de SMS, IVR y servicios de

reportería. Estos registros ofrecen conjuntamente una vista completa y detallada de toda la actividad del sistema.

A nivel de base de datos, TNPC registra todos los eventos de transacciones, que incluyen envíos de mensajes, respuestas, resultados de validaciones, transiciones de estado, actualizaciones de enrutamiento y acciones de auditoría. Cada evento se asocia a un identificador único de transacción e incluye metadata tal como marcas de tiempo, identificadores del operador, referencias de mensajes y estados de procesos. Los eventos relativos a archivos, que incluyen generación de difusión diaria, creación de archivos de sincronización, carga y descarga SFTP y acceso a archivos por parte de los operadores o SUTEL, también se registran para su total trazabilidad. Para los sistemas de intercambio de información, TNPC registra todo el tráfico de mensajes entrantes y salientes, que incluyen transacciones exitosas, reintentos, timeouts y respuestas de rechazos, para garantizar la visibilidad total de los flujos de comunicaciones.

Todos los registros se mantienen en un **marco de registro centralizado y seguro** con segregación e indizado adecuados para soporte eficiente de consultas y análisis. Los registros se almacenan en formato solo lectura, resistentes a adulteración, para garantizar la integridad y cumplimiento con los requerimientos de auditoría. TNPC soporta monitoreo y generación de alertas en tiempo real sobre eventos de registro para permitir una detección proactiva de anomalías, fallas o incidencias de seguridad. Además, la plataforma ofrece capacidades de reportería y tableros integrales que permiten a SUTEL y a los usuarios autorizados analizar datos de eventos, hacer seguimiento del comportamiento del sistema y verificar el cumplimiento con los requerimientos regulatorios y SLA.

A través de esta capacidad de registro integrada, TNPC asegura que todos los eventos a lo largo del ecosistema del SIPN sean totalmente capturados, seguidos y auditables para ofrecer transparencia total y soporte efectivo a la gestión operativa y supervisión regulatoria.

2.14.2 *La información será almacenada por la totalidad del periodo de contratación.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC asegura que toda la **información relativa al SIPN se almacenará en forma segura y será conservada por todo el período de contratación**, en línea total con los requerimientos regulatorios y de auditoría de SUTEL. La NPCDB centralizada mantiene registros integrales de todas las transacciones de portabilidad y actividades del sistema, que incluyen generación y validación de NIP, consultas de prevalidación, solicitudes de portabilidad, aprobaciones y rechazos, cancelaciones, retornos de números, eventos de sincronización y todos los intercambios de mensajes asociados. Cada registro se guarda con toda la metadata completa, tal como identificadores de transacción, marcas de tiempo, identificadores del operador, estados de procesos y referencias de auditoría para garantizar el ciclo completo de vida de cada transacción conservada.

Además de los datos transaccionales, TNPC retiene toda la información de soporte, que incluye registros de eventos, registros de sincronización y generación de archivos, interacciones de integración con los sistemas externos, datos de reportería y registros de actividades del usuario. Los datos se almacenan en formato estructurado e indizado para permitir la recuperación, reportería y análisis de auditoría eficientes en cualquier punto durante el período de contratación. La plataforma soporta acceso en línea para estrategias de datos recientes y archivos gestionados para datos históricos con el fin de garantizar el rendimiento óptimo a la vez que se mantiene total accesibilidad a los registros.

Se protege toda la información almacenada a través de controles de seguridad sólidos, incluyendo encriptación en reposo y en tránsito, control de acceso basado en roles y estricto cumplimiento de la aplicación de titularidad de datos. Se asegura la integridad de datos a través de mecanismos de validación y almacenamiento inmutable para registros de auditoría críticos y para evitar modificaciones o eliminaciones no autorizadas. A través de este enfoque, TNPC garantiza que toda la información del SIPN sea completa, segura, accesible y esté en cumplimiento durante todo el período de contratación, en pleno cumplimiento con los requerimientos de SUTEL para transparencia, trazabilidad y supervisión regulatoria.

2.14.3 *El registro tendrá características de sólo lectura y no podrá ser modificado.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC aplica una estricta política de registros solo lectura e inmutables para todos los datos transaccionales y de auditoría del SIPN a fin de garantizar que, una vez registrada la información, la misma no puede ser modificada, alterada ni borrada. Todas las transacciones, que incluyen generación de NIP, prevalidación, solicitudes de portabilidad, aprobaciones y rechazos, cancelaciones, retornos de números, eventos de sincronización e interacciones del sistema, se almacenan en NPCDB con atributos de auditoría completos, tales como marcas de tiempo, identificadores de mensajes, identificadores de operadores y estados de procesos. Estos registros representan el histórico autorizado de las operaciones del SIPN y se conservan en su forma original para garantizar el cumplimiento regulatorio y la integridad de las auditorías.

Se aplica la inmutabilidad a través de una combinación de controles a nivel de aplicación y salvaguardas a nivel de base de datos. No se permiten las actualizaciones de los registros existentes; por el contrario, cualquier cambio posterior en el ciclo de vida de la transacción se registra como entrada de nuevos estados relacionados con la transacción original. Este enfoque garantiza que se mantenga el histórico cronológico completo de cada proceso sin sobrescribir información anterior. El acceso a los registros está estrictamente controlado mediante autorización en base a roles para garantizar que los operadores, SUTEL y las entidades autorizadas solo visualicen datos dentro del alcance permitido, a la vez que se registran todos los eventos de acceso para fines de auditoría.

Para mayor protección y cumplimiento de los datos, TNPC aplica **mecanismos integrales de encriptación para datos en reposo y en tránsito**. Todos los datos almacenados en NPCDB, que incluyen registros de transacciones, registros de auditoría e información sensible del suscriptor, se protegen usando la encriptación estándar de la industria, tal como **AES-256 encriptación en reposo**. El intercambio de datos entre TNPC y los sistemas externos, que incluyen las plataformas de los operadores y SUTEL, está asegurado con los **protocolos de encriptación TLS 1.2 o superior** para garantizar la confidencialidad e integridad durante la transmisión. Las claves de encriptación se manejan en forma segura con procesos de gestión controlada de llaves para garantizar que solo los componentes y servicios autorizados pueden acceder a datos protegidos.

Además, TNPC mantiene registros de auditoría a prueba de adulteración y aplica mecanismos de validación de integridad para detectar cualquier intento de acceso no autorizado o anomalías de datos. A través de este enfoque combinado de inmutabilidad, encriptación, acceso controlado y capacidad de auditoría, TNPC asegura que todos los registros del SIPN sean seguros, confiables y totalmente en cumplimiento con los requerimientos regulatorios durante todo el período de contratación, brindando a SUTEL un sistema de registro confiable y auditable.

2.14.4 *Cada operador únicamente podrá consultar los registros generados por acciones propias y la ERPN.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC aplica estrictos **controles de segregación de acceso a datos y consulta por operador específico** para garantizar que cada operador solo puede acceder y consultar registros asociados a sus propias transacciones e interacciones con la ERPN. Esto se logra a través de un **marco de control de acceso basado en roles** integral donde se asigna a cada operador credenciales y permisos únicos que definen el alcance de la visibilidad de datos e interacción con el sistema. Todas las consultas presentadas por los operadores, ya sea a través de las interfaces SOAP, REST, API o acceso GUI, se validan contra estos permisos antes de que pueda recuperar los datos de NPCDB.

A nivel de datos, TNPC asegura que todos los registros en NPCDB estén etiquetados con los identificadores del operador, que incluyen roles como donante y receptor, para permitir el filtrado preciso de los resultados de la consulta. Cuando un operador realiza una consulta, el sistema automáticamente restringe el conjunto de datos devuelto a solo las transacciones en las cuales el operador está directamente involucrado, ya sea como donante, receptor o como parte de un proceso gestionado por la ERPN. Esto garantiza que la información sensible relativa a otros operadores siga totalmente protegida y sea inaccesible para mantener la confidencialidad y el cumplimiento con los requerimientos regulatorios.

Además, TNPC aplica mecanismos de estricta validación y auditoría a todas las solicitudes de acceso a datos. Cada consulta se registra con detalles como identidad del operador, marca de tiempo, parámetros de consulta y resultados accedidos para garantizar la trazabilidad y responsabilidad total. Se protegen los datos usando encriptación en tránsito y en reposo. Los intentos de acceso no autorizados se detectan y bloquean a través de controles de seguridad y sistemas de monitoreo. A través de este enfoque, TNPC asegura que los operadores solo acceden a sus propios datos relevantes, a la vez que mantiene la integridad, confidencialidad y seguridad de todo el entorno del SIPN.

2.15 *La Sutel podrá verificar los registros pertenecientes a todos los operadores/proveedores, sus funcionarios y la ERPN.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece a SUTEL **acceso privilegiado, integral y seguro a todos los registros del SIPN a lo largo de todos los operadores, proveedores, sus funcionarios y las actividades de la ERPN**, para garantizar una total supervisión y transparencia regulatoria. Este acceso se entrega mediante una **GUI administrativa de SUTEL** basada en roles y dedicada, así como también a través de interfaces SOAP y REST seguras, cuando corresponda, para permitir que el personal autorizado de SUTEL consulte, monitoree y analice todas las transacciones en tiempo real y en forma histórica. La GUI ofrece capacidades avanzadas de búsqueda, filtrado y buceo para permitir que SUTEL visualice el ciclo de vida completo de las transacciones, que incluyen generación de NIP, validación, solicitudes de portabilidad, aprobaciones, rechazos, cancelaciones, retornos y eventos de sincronización, junto con las marcas de tiempo asociadas, identificadores del operador, detalles del mensaje y registros de auditoría almacenados en NPCDB.

El acceso de SUTEL está regido por un marco de **control de acceso basado en roles y con altos privilegios** para garantizar la visibilidad irrestricta a lo largo de todos los operadores, a la vez que se mantiene estricta seguridad y responsabilidad. La plataforma permite a SUTEL acceder no solo a los datos de las transacciones, sino también a los registros del sistema, registros de eventos, actividad del usuario y pistas de auditoría para ofrecer una vista holística de las operaciones del SIPN. Todos los accesos por los usuarios de SUTEL están autenticados en forma segura. Se soporta autenticación multifactorial, cuando sea requerido, y se registra totalmente para garantizar la trazabilidad y el cumplimiento con los estándares de auditoría y gobierno.

Además, TNPC ofrece capacidades integrales de reportería y tableros a través de la GUI para permitir que SUTEL genere reportes en tiempo real e históricos sobre el desempeño operativo, escenarios de rechazos, cumplimiento de SLA, uso de NIP e IVR, estado de sincronización y salud del sistema. Estas capacidades permiten que SUTEL realice monitoreo regulatorio, verificación de cumplimiento y análisis forense sin depender de la intervención del operador ni la ERPN. A través de este robusto modelo de acceso, TNPC asegura que SUTEL tenga visibilidad total, segura y transparente de todas las actividades del SIPN, cumpla plenamente con los requerimientos regulatorios y soporte el gobierno efectivo del ecosistema de portabilidad numérica.

2.16 *Brindar accesos privilegiados de monitoreo y auditoría a la Superintendencia de Telecomunicaciones.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece a la Superintendencia de Telecomunicaciones **acceso privilegiado, integral y en tiempo real** a todas las operaciones del SIPN para soporte del monitoreo continuo, auditoría y supervisión regulatoria. Se entrega esta capacidad a través de una **interfaz administrativa (GUI) de SUTEL** que se complementa con el acceso seguro a través de las interfaces estandarizadas SOAP y REST, cuando corresponda. La interfaz permite que el personal autorizado de SUTEL monitoree la actividad del sistema, consulte los datos de las transacciones, revise los flujos de procesos y analice el desempeño operativo a lo largo de todos los operadores, proveedores y actividades de la ERPN sin restricciones.

A través de este acceso privilegiado, SUTEL puede visualizar el **ciclo de vida completo de cualquier transacción de portación**, que incluye generación y entrega de NIP, resultados de prevalidaciones, solicitudes de portabilidad, aprobaciones, rechazos, cancelaciones, retornos de números, eventos de sincronización y actualizaciones de enrutamiento. Todos los estados de las transacciones, intercambios de mensajes, marcas de tiempo, roles de los operadores y acciones del sistema se almacenan en NPCDB y son accesibles para fines de auditoría. La plataforma también ofrece **acceso a registros de eventos, registros del sistema y registros de actividades del usuario** para permitir que SUTEL realice análisis forenses detallados y verifique el cumplimiento con los requerimientos regulatorios y los SLA.

El acceso se asegura a través de un **marco de control de acceso robusto basado en roles**, con soporte para mecanismos de autenticación sólidos y registro completo de auditorías de todas las actividades del usuario. Cada consulta y acción realizada por los usuarios de SUTEL se registra con marcas de tiempo e identificadores de usuarios para garantizar la trazabilidad y responsabilidad total. Se protegen los datos con encriptación en tránsito y en reposo para garantizar la confidencialidad e integridad, a la vez que se mantiene la total accesibilidad a todos los usuarios regulatorios autorizados.

Además, TNPC ofrece **tableros de monitoreo y capacidades de reportería** avanzada que permiten a SUTEL hacer seguimiento de los indicadores clave de rendimiento, cumplimiento de SLA, tendencias de rechazos, disponibilidad del sistema y salud total del SIPN en tiempo real. Se pueden generar reportes a demanda o en forma programada para soportar el monitoreo proactivo y la toma de decisiones regulatorias. A través de este marco de acceso integral y seguro, TNPC asegura que la SUTEL tenga visibilidad, control y capacidad de auditoría total sobre las operaciones del SIPN, en pleno cumplimiento con el requerimiento de monitoreo privilegiado y supervisión regulatoria.

2.17 *Incorporar funcionalidades para gestiones, ejecución, validación de procesos y consulta en línea sobre los trámites de portación por parte de los operadores/proveedores.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece un conjunto integral de **capacidades en línea para gestión de procesos, ejecución de consultas y validación de transacciones de portación** para permitir que los operadores, proveedores y SUTEL interactúen con el SIPN en forma eficiente y en tiempo real. Estas capacidades se entregan a través de una **interfaz GUI web** segura basada en roles que se complementa con las interfaces SOAP XML y REST JSON para garantizar que todos los participantes puedan gestionar y ejecutar los procesos de portación a través de canales automáticos e interactivos.

A través de la GUI operativa de TNPC, los usuarios autorizados pueden iniciar y gestionar todos los procesos relativos a la portación, que incluyen generación y reenvío de NIP, consultas de prevalidación, presentación de solicitudes de portabilidad, manejo de cancelaciones, procesamiento de retorno de números y actividades de sincronización. La interfaz ofrece visibilidad en tiempo real de los estados de las

transacciones para permitir que los usuarios monitoreen el avance, visualicen los resultados de las validaciones, hagan seguimiento de los tiempos e identifiquen cualquier paso pendiente o no exitoso en el flujo de trabajo. Todas las acciones realizadas a través de la GUI siguen la misma lógica de validación y reglas del procesos aplicadas por el Procesador de Mensajes para garantizar la consistencia con las interacciones automáticas basadas en mensajes.

La plataforma también soporta **capacidades de gestión de consultas** de avanzada que permiten a los usuarios buscar y recuperar datos de las transacciones en base a múltiples criterios como MSISDN, ID de transacción, rol del operador, estado del proceso, rango de fechas y tipo de mensaje. Las consultas devuelven datos en tiempo real directamente de NPCDB para garantizar que los usuarios siempre tengan acceso a la información más reciente y precisa. La validación de todas las consultas y transacciones se realiza a nivel central para garantizar que solo se accede a los datos autorizados y que todas las entradas cumplen con los esquemas WSDL y XSD definidos.

La ejecución y validación de las transacciones de portaciones están totalmente integradas dentro de la plataforma. El Procesador de Mensajes aplica todas las reglas de negocio, condiciones de rechazo y secuenciación de procesos. El Procesador de Temporizadores asegura el cumplimiento con los tiempos regulatorios, mientras que las verificaciones de validación evitan que haya solicitudes inválidas o duplicadas. En caso de problemas con la interfaz con los sistemas del operador o SUTEL, la GUI ofrece un **mecanismo de respaldo controlado** para permitir que los usuarios ejecuten y gestionen las transacciones en forma manual, sin interrupción de las operaciones del SIPN.

La ejecución de todos los procesos, actividad de consulta y resultados de validaciones se registran en NPCDB y tienen pistas de auditoría completas, que incluyen identidad de usuario, marcas de tiempo y respuestas del sistema. Además, TNPC ofrece capacidades de reportería y tableros para permitir que los operadores y SUTEL analicen el rendimiento de las transacciones, tendencias de validaciones y métricas operativas. A través de este marco integrado de gestión en línea, TNPC garantiza la ejecución eficiente, transparente y en cumplimiento de todos los procesos de portación, en pleno cumplimiento del requerimiento de gestión de procesos y consultas en tiempo real dentro del SIPN.

La plataforma de TNPC ofrece una **Interfaz Gráfica de Usuario (GUI) basada en la web** que permite a los operadores, administradores, reguladores y usuarios autorizados interactuar con el sistema de TNPC para la gestión de los procesos de portación en Costa Rica.

La GUI de TNPC ofrece soporte total para las capacidades operativas y administrativas y está diseñada para soportar todas las funciones definidas en las especificaciones funcionales existentes para la Portabilidad Numérica Móvil en Costa Rica.

La solución de la GUI de TNPC consta de tres componentes principales:

- Interfaz Gráfica de Usuario web de TNPC (Operador/Portal de SUTEL)
- Sitio web público de TNPC
- Tablero de Reportería de TNPC

Todos los componentes de la GUI se incluyen como parte de la solución de TNPC y se proporcionan dentro de la oferta de servicio gestionado de TNPC.

Interfaz Gráfica de Usuario web de TNPC (Operador/Portal de SUTEL)

El sistema de TNPC ofrece una Interfaz Gráfica de Usuario (GUI) basada en la web, que permite a los participantes acceder e interactuar con el sistema de TNPC usando un navegador web estándar.

La GUI de TNPC se implementa en una **interfaz moderna basada en Angular**, accesible vía HTTPS usando URL del sistema de TNPC. La autenticación del usuario se realiza a través de inicio de sesión seguro con **ID de usuario y contraseña junto con MFA** para garantizar el control de acceso basado en roles.

Una vez autenticados, los usuarios pueden acceder a todas las funcionalidades relevantes de su rol operativo dentro del ecosistema de la portabilidad numérica.

La GUI de TNPC permite a los operadores:

- iniciar solicitudes de portabilidad numérica
- procesar las solicitudes de portabilidad entrantes
- monitorear las transacciones de portación
- visualizar el histórico de mensajes y detalles de las transacciones
- responder mensajes operativos
- acceder a reportería y estadísticas
- monitorear la actividad del sistema y estado de sincronización

La GUI permite a los participantes realizar todas las actividades de portabilidad numérica cuando no están disponibles las interfaces automáticas para garantizar la continuidad de las operaciones.

Gestión de portaciones y manejo de transacciones

La GUI ofrece a los operadores la capacidad de visualizar y gestionar las transacciones de portaciones a través **visualizar Lista de Portaciones**, que despliega todos los casos de portaciones en base a criterios de búsqueda seleccionados por el usuario.

Visualizar Lista de Portaciones ofrece:

- identificador de transacción (ID de Transacción)
- estado de portación
- marcas de tiempo de portación
- operadores receptor y donante
- información del caso de portación
- indicadores para mensajes que requieren respuesta del operador

Las transacciones de portación que requieren acción del operador se indican claramente en la interfaz con una flecha verde.

The screenshot displays the 'Port Request List' interface. At the top, there's a navigation bar with tabs: 'Port', 'Equip & Num Query', 'Ownership & Acct. Query', 'CAP Generation', 'Blocked Equipment', and 'Reports'. The user is logged in as 'Participant ID: 219' and 'User ID: 219u2'. Below the navigation bar, the 'Port Request List' section has a 'Search Filter Criteria' area with the following fields:

- ☐ Operator Request ID: [text input]
- ☐ Port ID: [text input]
- ☐ TN: [text input]
- ☒ Last Message sent between:
 - Start Date: 2026-04-21 00:00:00 (Format: YYYY-MM-DD HH:mm:ss)
 - End Date: 2026-05-21 23:59:59 (Format: YYYY-MM-DD HH:mm:ss)
 - Request Status: [dropdown menu]
 - Donor ID: [dropdown menu]
 - Recipient ID: [dropdown menu]

Below the filters are 'Retrieve' and 'Clear' buttons. The 'Search Results' section shows 'Showing 1 to 3 of 3 entries' and a table with the following data:

| Operator Request ID | Port ID | Request Status | Update Timestamp | Donor ID | Recipient ID |
|---------------------------|-------------------------|----------------|---------------------|----------|--------------|
| ▶ SOLPO213202605211111111 | PORTA213202605211111111 | Ported | 2026-05-21 03:38:57 | 219 | 213 |
| ▶ SOLPO213202605203540487 | PORTA213202605203540487 | Ported | 2026-05-21 03:27:21 | 219 | 213 |
| ▶ SOLPO213202605203633839 | PORTA213202605203633839 | Ported | 2026-05-21 03:26:17 | 219 | 213 |

At the bottom, it says 'Showing 1 to 3 of 3 entries' and 'Page: 1'.

Para cada transacción, la GUI permite que el usuario expanda los detalles de la transacción para desplegar una **sección de Datos de Portación**, que incluye:




- detalles de solicitudes de portabilidad
- enlaces de información del número del suscriptor
- información de enrutamiento
- identificadores del operador
- marcas de tiempo de la transacción
- enlaces de histórico de mensajes
- enlaces de la lista de NT

A continuación se presenta una muestra de la sección de Datos de Portación, que despliega los datos, hipervínculo del próximo mensaje posible (por ej., Solicitud de Cancelación de Portación), hipervínculo de información del Suscriptor, hipervínculo de la Lista de NT e hipervínculo del histórico de mensajes asociados a un ID de Transacción específico.

Search Results

Showing 1 to 20 of 21 entries

Page: 1

| Operator Request ID | Port ID | Request Status | Update Timestamp | Donor ID | Recipient ID |
|---|-------------------------|----------------|---------------------|----------|--------------|
|  SOLPO213202605204029845 | PORTA213202605204029845 | Port Canceled | 2026-05-20 06:40:46 | 219 | 213 |
|  SOLPO213202605203754943 | PORTA213202605203754943 | Port Canceled | 2026-05-20 06:38:08 | 219 | 213 |
|  SOLPO213202605203633839 | PORTA213202605203633839 | Port Scheduled | 2026-05-20 06:36:51 | 219 | 213 |

Port Request Data

[\[Create Document Delivery Request \]](#) | [\[Create Port Cancel Request \]](#)

Operator Request ID:
SOLPO213202605203633839

Create Timestamp:
2026-05-20 06:36:44

Donor ID:
219

TN List

Port ID:
PORTA213202605203633839

Service Type (Donor):
Mobile

Recipient ID:
213

Message History

SGP Request ID:
PFACT219202605200000006

Modality (Donor):
Postpaid

Verification Type:
Physical

Request Status:
Port Scheduled

Service Type (Recipient):
Mobile

[Subscriber Information](#)

Los operadores pueden bucear el **histórico de mensajes** asociados a una transacción para visualizar la secuencia completa de mensajes intercambiados durante el proceso de portación.

Incluye:

- mensajes de la solicitud
- respuesta de aceptación o rechazo
- mensajes de ejecución
- notificaciones de difusión
- mensajes completados

Se puede expandir la entrada de cada mensaje para desplegar los **datos detallados del mensaje**, que incluyen todos los elementos contenidos en el mensaje XML o JSON del web service.

Si un mensaje requiere una respuesta del operador, la GUI ofrece la capacidad de responder directamente a través de la sección Datos de Portación, al seleccionar la acción de respuesta adecuada.

A continuación se presenta una muestra de la ventana que indica los detalles de un mensaje de Solicitud de Portabilidad.

213202605202132026052021320260520213202605202132026042421320260424213202604242132026032621320260422213202604222132026042221320260421213202604212132026042121320260420052038213202604205906809

Message History - PORTA213202605203633839

Donor ID

21921

La GUI de TNPC también asegura que los operadores solo puedan visualizar las transacciones relevantes para ellos. Específicamente, los operadores pueden visualizar:

- portaciones donde son el **Operador receptor**
- portaciones donde son el **Operador donante**
- mensajes de difusión enviados a todos los operadores cuando se completa la portación

Soporte para Operaciones Automáticas y Manuales

Los participantes pueden elegir interactuar con el sistema de TNPC mediante el uso de:

- la **GUI web**, o
- la **Interfaz de Web Services (SOAP/XML o REST)**.

Los operadores que usan integraciones totalmente automáticas a través de las interfaces SOAP/XML o REST aún pueden visualizar todas las transacciones de mensajes y la actividad de portación a través de la GUI.

Por consiguiente, la GUI sirve como **herramienta de gestión de monitoreo y operativa**, aún para operadores totalmente automáticos.

Soporte multilingüe: inglés, español y francés

La GUI de TNPC está diseñada para soportar múltiples idiomas y conjuntos de caracteres.

El producto TNPC ha sido previamente implementado en interfaces multilingües que soportan idiomas como:

- Inglés
- Francés

- Español
- Griego
- Tailandés
- Árabe

Esta capacidad permite localizar el sistema a los usuarios de Costa Rica, si fuese necesario.

La GUI de TNPC ofrece una interfaz moderna, intuitiva y segura que soporta todos los requerimientos operativos del ecosistema de portabilidad numérica de Costa Rica.

Los beneficios clave incluyen:

- acceso basado en la web sin instalación de software en el cliente
- control de acceso basado en roles
- visibilidad completa de las transacciones de portaciones
- reportería y análisis integrados
- soporte para operadores en forma manual y automática
- soporte en múltiples idiomas
- interfaz segura de consulta de número público

La GUI de TNPC asegura que los operadores, administradores y reguladores puedan gestionar y monitorear con eficiencia el sistema de portabilidad numérica, al tiempo que se mantiene pleno cumplimiento de los requerimientos de portación en Costa Rica.

TNPC ofrecerá un marco integral de control de acceso interactivo, alineado con los estándares, para todos los usuarios de la GUI. Está diseñado para cumplir con los exigentes requerimientos empresariales y regulatorios.

1. **Sólida autenticación e integración de identidad**

TNPC ofrece **Autenticación multifactorial (MFA)** que usa todo el acceso interactivo GUI para asegurar una mayor protección contra acceso no autorizado.

2. **Aplicación de políticas de credenciales y contraseñas**

TNPC aplica **políticas de gestión centralizada de contraseñas** que cumplen con las pautas de seguridad:

- Requerimientos de complejidad y longitud mínimos
- Vencimiento y rotación de contraseñas
- Histórico de contraseñas y prevención de reuso
- Umbrales de cierre de cuenta configurables

Las credenciales se almacenarán usando sólidos algoritmos para garantizar el manejo de datos de autenticación sensibles.

3. **Ciclo de vida del usuario y gobierno de acceso**

La plataforma soporta gestión del ciclo de vida del usuario, controlado por el administrador, que incluye:

- Ingreso y aprovisionamiento seguros
- Activación y desactivación de cuentas
- Revocación inmediata del acceso en base a cambios o terminación de roles

Integración opcional con sistemas de gestión de identidad de acceso y recursos humanos (IAM/HR) empresariales que permite el **aprovisionamiento y desaprovisionamiento automáticos** para garantizar el cumplimiento con las políticas de gobierno interno.

4. Control de acceso basado en roles (RBAC)

TNPC implementa **control de acceso basado en roles (RBAC) granular** para garantizar que se otorga a los usuarios acceso estrictamente en base a sus roles operativos:

- Roles predefinidos y parametrizables
- Permisos refinados alineados con los principios de menor privilegio

5. Gestión de sesión de seguridad

La solución aplica controles de seguridad de sesión robustos:

- Timeout de sesión y cierre de sesión automática después de inactividad configurables

Si fuese necesario, se pueden activar mecanismos de autenticación adaptativos (por ej., en base a IP/ubicación).

6. Auditoría, registros y cumplimiento

Todas las interacciones del usuario y los eventos de autenticación **se registran y rastrean completamente**, incluyen:

- Intentos de inicio de sesión exitosos y fallidos
- Cambios en el ciclo de vida de las cuentas y modificaciones de roles por Administrador
- Operaciones GUI

La solución soporta el cumplimiento de:

- **GDPR** (protección y auditorías de datos)
- **Directiva NIS2** (gestión y reportería de riesgos cibernéticos)
- **ISO/IEC 27001** (gestión de seguridad de la información)

Sitio web público de TNPC:

El sitio web público de TNPC permite a los usuarios consultar el estado de cualquier número de teléfono. El sitio web público de TNPC se incluye en el precio indicado por TNS.

El sitio web público de TNPC está disponible para el público general y ofrece un sitio web accesible a través de un navegador web, que permitirá a todos consultar el sistema y obtener el estado de un número. Se requiere iniciar sesión con el número y NIP; y el acceso es por internet usando HTTP.

Se brindará un captcha para fines de seguridad en la GUI pública de TNPC.

Tablero de reportería de TNPC brindará estadísticas agregadas de portaciones sobre los Indicadores clave de rendimiento (KPIs).

El tablero de reportería gráfica está a disposición de la autoridad regulatoria de Costa Rica y demás usuarios autorizados en base a sus roles. El tablero de reportería ofrece estadísticas agregadas de portaciones. El tablero de reportería ofrece una vista resumida de diversas estadísticas. Consultar la sección 2.18 para detalles sobre los reportes.

- 2.18** Disponer de interfaces y gráficos de reportes en tiempo real (donde resulte aplicable) configurables (capacidad de filtrado de variables) por el usuario y envío mensual de estadísticas a la Sutel y a todos los operadores/proveedores. El plazo de envío de las estadísticas podrá ser compartidas en plazos configurables definidos por el CTPN-M.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece un **marco de reportería y análisis en tiempo real** integral que entrega gráficos dinámicos de reportes, tableros configurables e interfaces de estadísticas flexibles a SUTEL y todos los operadores/proveedores. Estas capacidades se entregan a través de una **GUI de Reportería** segura, basada en roles, que está estrechamente integrada con NPCDB para garantizar que todos los datos presentados reflejen los últimos estados de las transacciones, métricas operativas e indicadores de rendimiento del sistema en tiempo real. La plataforma soporta la visualización interactiva de métricas clave como volúmenes de portaciones entrantes y salientes, tendencias de rechazos, rendimiento en la generación y entrega de NIP, uso de IVR, estado de sincronización, cumplimiento de SLA y disponibilidad del sistema para permitir que los interesados monitoreen las operaciones del SIPN en forma continua.

La interfaz de reportería es **totalmente configurable y accionada por el usuario** para permitir que los usuarios autorizados apliquen filtros variables como operador, tipo de transacción, MSISDN, rangos de fechas y horas, estado del proceso, motivos de rechazo y categorías de SLA. Los usuarios pueden bucear a partir de los tableros resumidos hacia vistas detalladas a nivel de transacción. Todos los datos subyacentes se obtienen directamente de NPCDB para garantizar la precisión y trazabilidad. Estas capacidades facultan a SUTEL y los operadores a realizar análisis operativos, verificación de cumplimiento y toma de decisiones, sin depender de ninguna preparación manual de los datos.

Además de los tableros en tiempo real, TNPC soporta la **entrega manual y programada de reportes estadísticos** a SUTEL y todos los operadores/proveedores. Se pueden generar reportes a demanda o distribuirlos automáticamente a intervalos configurables tal como sea definido en coordinación con CTPN-M, que incluyen ciclos diarios, semanales o mensuales. El cronograma de entrega, los formatos de reportes y alcance del contenido son totalmente configurables para asegurar que estén alineados con los requerimientos regulatorios y operativos. Los reportes se ponen a disposición en formatos estándar como XLSX, CSV y PDF y son accesibles vía la GUI, se pueden descargar en forma segura o distribuir a través de canales automáticos.

Todas las actividades de reportería se rigen por estrictas políticas de control de acceso para garantizar que los operadores solo pueden visualizar los datos relevantes; mientras que SUTEL conserva visibilidad total de todos los participantes. Cada reporte y consulta se registra y es auditable para mantener transparencia y cumplimiento total. A través de este marco de reportería integral, TNPC garantiza que todos los interesados tengan **visibilidad en tiempo real, capacidades analíticas flexibles y reportería estadística confiable** para cumplir plenamente con los requerimientos de SUTEL de monitoreo, gobierno y supervisión operativa.

2.18.1 Estadísticas operativas:

- a) *Portaciones entrantes desagregadas por todas las variables disponibles, fechas/horas y operadores/proveedores.*
- b) *Portaciones salientes desagregadas por todas las variables disponibles, fechas/horas y operadores/proveedores.*
- c) *Rechazos realizados por operador/proveedor según las diferentes causales.*
- d) *Rechazos realizados por el SIPN según las diferentes causales.*
- e) *Tiempo promedio de validación según la modalidad de pago y tipo de aprobación (operador/proveedor o SIPN). Para las validaciones del operador, tiempos menor, promedio y mayor y cantidad. Para las validaciones que realiza el SIPN, deberá entregar la cantidad que lleva a cabo.*
- f) *Repatriaciones por operador/proveedor que la gestiona y el que la recibe.*
- g) *Cantidad de NIP generados a la interfaz SMSC de cada operador/proveedor por fecha/hora.*
- h) *Cantidad de NIP entregados a la interfaz SMSC de cada operador/proveedor por fecha/hora.*
- i) *Tiempo mínimo, máximo, promedio y desviación estándar para la entrega de los NIP para cada operador/proveedor por fecha/hora.*
- j) *Llamadas atendidas por el IVR por operador fecha/hora.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece un **marco de reportes estadísticos operativos** que permite a SUTEL y a todos los operadores/proveedores tener acceso preciso, en tiempo real y conocimiento histórico de las operaciones del SIPN. Todas las estadísticas operativas se generan directamente a partir de NPCDB que mantiene datos completos a nivel de transacciones e incluye estados de procesos, marcas de tiempo, roles del operador, resultados de validaciones e interacciones de mensajes. Esto asegura que todas las métricas reportadas sean consistentes, auditables y estén alineadas con el comportamiento real del sistema.

TNPC entrega reportes detallados para la **actividad de portación** que incluyen portaciones entrantes y salientes, desglosadas por todas las variables relevantes como operador, roles de donante y receptor, tipo de servicio, estado de transacción y rangos de fechas y horas configurables. La plataforma también ofrece visibilidad granular de las **estadísticas de rechazo**. Distingue entre rechazos iniciados por los operadores/proveedores y aquellos generados por el SIPN, con categorización total por motivos de rechazo predefinidos. Esto permite a SUTEL monitorear el cumplimiento, detectar anomalías y garantizar que los códigos de rechazo se apliquen consistentemente a lo largo de todos los participantes.

La plataforma además ofrece análisis avanzado sobre rendimiento de las validaciones que incluye tiempos promedio de validación en base a la modalidad de pago o tipo de aprobación, así como métricas detalladas para validaciones por operador como tiempos de respuesta mínimo, promedio y máximo; y cantidades totales. Para las validaciones en base al SIPN, TNPC reporta las cantidades totales de validaciones y el rendimiento del procesamiento. Además, TNPC realiza el seguimiento y reporta las **estadísticas de retorno (repatriación) de números** e identifica tanto al operador iniciador como al operador receptor, junto con las marcas de tiempo asociadas y los resultados de las transacciones.

Para el proceso de NIP, TNPC ofrece visibilidad completa de las **métricas de generación y entrega de NIP**, que incluyen cantidad de NIP generados y entregados a cada interfaz SMSC del operador, desglosado por fecha y hora. La plataforma calcula y reporta los **tiempos de entrega mínimo, máximo y promedio**; y la desviación estándar para posibilitar un análisis detallado del rendimiento y cumplimiento de SLA. Del

mismo modo, TNPC reporta el **uso de IVR**, que incluye cantidad de llamadas respondidas por operador y período de tiempo, para ofrecer información sobre el uso de respaldo (fallback) y del comportamiento del usuario.

Todas las estadísticas operativas están disponibles a través de la GUI de Reportería con capacidades avanzadas de filtrado para permitir que los usuarios parametricen las vistas por operador, período de tiempo, tipo de transacción y otras variables. Se pueden generar reportes en tiempo real, exportados en formatos estándar como XLSX, CSV y PDF, entregados en forma manual o a intervalos programados, tal como sea definido por CTPN-M. A través de esta robusta capacidad de reportería, TNPC garantiza total transparencia, visibilidad operativa y cumplimiento regulatorio para todos los interesados del SIPN.

2.18.2 Estadísticas de desempeño.

- a) *Tasa de éxito/falla por procesos.*
- b) *Disponibilidad del sistema, uptime monitoring semanal (concordante con el SLA).*
- c) *Estadísticas del sitio WEB público.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece capacidad integral de reportes de estadísticas de desempeño que permite a SUTEL y a todos los operadores/proveedores monitorear la eficiencia del sistema, confiabilidad y calidad de servicio en tiempo real y forma histórica. Todas las métricas de desempeño surgen de los datos a nivel de transacción almacenados en NPCDB y en las herramientas de monitoreo del sistema, lo cual asegura la precisión, consistencia y trazabilidad total para supervisión regulatoria y auditorías.

Los reportes de TNPC detallan las tasas de éxito y fracaso para todos los procesos del SIPN, que incluyen generación y entrega de NIP, prevalidación, portación, cancelación, retorno de números y sincronización. Las tasas de éxito y fracaso se calculan en base a los resultados de las transacciones. Los fracasos se categorizan por causa principal como errores de validación, condiciones de rechazo, fallas de comunicación o excepciones del sistema. Esto permite a SUTEL y a los operadores identificar las tendencias, monitorear el desempeño operativo y garantizar el cumplimiento de las expectativas regulatorias y umbrales de SLA.

La plataforma también ofrece monitoreo continuo y reportería de la disponibilidad y tiempo activo del sistema, alineado con los requerimientos definidos en los SLA. TNPC mide la disponibilidad en base al tiempo operativo total versus el tiempo inactivo, que excluye las ventanas de mantenimiento convenidas y eventos de fuerza mayor; y ofrece reportes mensuales del tiempo activo con desgloses detallados de cualquier interrupción de servicio, duración y causas principales. Estas métricas tienen el soporte de herramientas de monitoreo en tiempo real que hacen seguimiento de la salud de todos los componentes del sistema, que incluyen interfaces web, procesamiento de mensajes, servicios de integración y operaciones de las bases de datos para garantizar la detección proactiva y la resolución de problemas.

Para el sitio web público, TNPC se integra con herramientas analíticas como Google Analytics, Matomo o plataformas equivalentes a través de una **capa de instrumentación segura embebida dentro de la GUI pública**. Esta integración se implementa al incorporar scripts de seguimiento de análisis o SDK en la interfaz web para permitir la captura de los eventos de interacción del cliente como visitas a la página, duración de la sesión, flujos de navegación, tipo de dispositivo, información del navegador y patrones de acceso geográficos. Estos eventos se transmiten en forma segura a la plataforma analítica en la cual son agregados y procesados para generar información accionable. TNPC asegura que esta integración sea configurable para permitir que SUTEL seleccione la herramienta analítica preferida y defina las políticas de recolección de datos. Cuando sea requerido, se aplica anonimización de datos y controles de privacidad para cumplir con los requerimientos regulatorios y de protección de datos. Los datos analíticos son luego puestos a disposición a través de tableros y reportes accesibles a SUTEL para ofrecer visibilidad sobre el comportamiento del usuario, uso del sistema y desempeño del portal.

Todas las estadísticas de desempeño, que incluyen datos analíticos, son accesibles a través de tableros y reportes configurables dentro de la interfaz de reportería de TNPC, con controles de acceso basado en roles para garantizar la visibilidad adecuada a los operadores y el acceso total a SUTEL. Se pueden generar reportes en tiempo real, exportados en formatos estándar y entregados conforme a cronogramas configurables según sea definido por CTPN-M. A través de este marco integrado de reportes de desempeño, TNPC garantiza la visibilidad total del desempeño del sistema, soporte de monitoreo de cumplimiento de SLA; y permite la mejora continua de las operaciones del SIPN.

2.18.3 Estadísticas de incidencias

a) *Estadísticas atinentes a la plataforma de tiquetes, fechas/horas y operadores/proveedores, ERP, Sutel*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC ofrece reportes operativos y estadísticas de incidencias integrales a través de la plataforma centralizada de gestión de servicios de IT y tiquetes que permite tener una visibilidad total de las incidencias, solicitudes de servicio, eventos operativos y desempeño de SLA a lo largo de todos los interesados, incluidos los operadores/proveedores, ERP y SUTEL:

La plataforma captura y mantiene estadísticas detalladas para todas las incidencias y actividades de soporte, que incluyen fecha y hora de creación del ticket, tiempo de acuse de recibo, tiempo de respuesta, tiempo de resolución, estado de cierre, clasificación de severidad, operador/proveedor afectado, servicios impactados, histórico de escalaciones, equipos de soporte asignados y detalles de la resolución final. Todos los registros de incidencias son totalmente trazables, se pueden buscar y auditar para garantizar transparencia operativa y responsabilidad.

TNPC ofrece tableros y capacidades de reportería en tiempo real configurables que permiten a los usuarios autorizados analizar las tendencias de incidencias, cumplimiento de SLA, problemas recurrentes, desempeño operativo y capacidad de respuesta de soporte por parte del operador/proveedor, categoría de la incidencia, nivel de severidad, período de tiempo o grupo de soporte asignado. Se pueden generar reportes a demanda o programar en forma automática y están disponibles en formatos que incluyen PDF, XLSX y CSV.

El marco de reportería también soporta gobierno operativo y mejora continua mediante métricas como volúmenes de incidencias, Tiempo Medio para Acuse de Recibo (MTTA), Tiempo Medio de Resolución (MTTR), estadísticas de escalado, análisis de corte de servicio, identificación de incidencias recurrentes, antigüedad del ticket, análisis de violaciones de SLA e indicadores de disponibilidad de servicio. Las notificaciones, los flujos de trabajo de escalaciones y el seguimiento de SLA se manejan directamente a través de la plataforma centralizada de tiquetes para garantizar la gestión de respuesta y resolución a tiempo.

A través de esta capacidad integrada de gestión de incidencias y reportería, TNPC asegura que SUTEL, los operadores/proveedores y los interesados autorizados mantengan la visibilidad continua del desempeño operativo, calidad de servicio, efectividad del soporte y cumplimiento de SLA a lo largo del ecosistema del SIPN.

2.18.4 Exportación de estadísticas en formatos XLSX, CSV (delimitado por comas).

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece capacidades integrales para **exportar todos los datos de estadísticas y reportes a formatos estándar, que incluyen XLSX y CSV (delimitado por coma)** para garantizar la compatibilidad con las herramientas analíticas comunes y facilitar el uso por parte de SUTEL y todos los

operadores/proveedores. Todos los reportes generados dentro del marco de reportería de TNPC, que incluyen estadísticas operativas, métricas de desempeño, indicadores de SLA y datos de auditorías se pueden exportar directamente desde la GUI de reportería en base a filtros definidos por usuario como operador, tipo de transacción, rango de fecha y hora; y estado del proceso.

La funcionalidad de exportación está totalmente integrada a la interfaz de reportería que permite a los usuarios generar y descargar reportes a demanda o programar la exportación automática a intervalos configurables según sea definido en coordinación con CTPN-M. Los archivos exportados mantienen un formato estructurado y estandarizado que incluyen encabezados claramente definidos, campos de datos y marcas de tiempo, a fin de garantizar que se puedan consumir los datos fácilmente para su posterior análisis, reportería regulatoria o integración con sistemas externos. Los archivos CSV se presentan en formato delimitado por comas para compatibilidad con las herramientas de procesamiento de datos, mientras que los archivos XLSX soportan capacidades avanzadas de formateo y análisis.

Todas las operaciones de exportación están regidas por el control de acceso basado en roles para garantizar que los operadores puedan exportar solo datos relevantes a sus propias transacciones, mientras que SUTEL tiene acceso total a lo largo de todos los operadores y procesos. Cada acción de exportación se registra con la identidad del usuario, marca de tiempo y parámetros del reporte para garantizar trazabilidad y cumplimiento de auditoría totales. A través de esta capacidad, TNPC asegura que todos los interesados puedan acceder y utilizar los datos estadísticos del SIPN en forma eficiente y en formatos estandarizados, en pleno cumplimiento de los requerimientos de reportería e intercambio de datos de SUTEL.

2.18.5 *El acceso a las estadísticas será diferenciado según los perfiles.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC implementa un robusto **marco de control de acceso en base a perfiles** para garantizar que el acceso a todas las estadísticas y reportes sea estrictamente diferenciado en base a los roles y responsabilidades del usuario. Esto se logra a través de un **modelo de control de acceso basado en roles** centralizado, donde a cada usuario se le asigna un perfil que define el alcance de la visibilidad de los datos, capacidades de reportería y funciones del sistema a los que está autorizado a acceder. Se configuran los perfiles para diferentes grupos de interesados que incluyen los operadores, SUTEL, miembros de CTPN-M y terceros autorizados, para asegurar que cada usuario solo puede acceder a la información relevante a su rol.

Para los operadores y proveedores de servicio, el acceso queda restringido a estadísticas y reportes relativos a las transacciones en las cuales estuvieron directamente involucrados como donante o receptor. Esto incluye estadísticas operativas, métricas de desempeño, análisis de rechazos y datos de SLA específicos de sus actividades. Por el contrario, SUTEL tiene **acceso privilegiado a lo largo de todos los operadores y todos los procesos del SIPN** para permitir un monitoreo, auditoría y supervisión regulatoria integrales. Se pueden configurar perfiles para que las entidades autorizadas accedan a subconjuntos específicos de datos, tal como sea requerido por SUTEL, para asegurar la flexibilidad y el cumplimiento de los requerimientos de gobierno.

Todo el acceso a las estadísticas está controlado por mecanismos de autenticación segura y se registran completamente para fines de auditoría, que incluyen identidad de usuario, tiempo de acceso y acciones realizadas. La interfaz de reportería aplica dinámicamente estos controles de acceso para garantizar que todas las consultas, tableros y exportaciones reflejen solo los datos permitidos para el perfil del usuario. A través de este enfoque estructurado y seguro, TNPC asegura que los datos estadísticos sean accesibles, controlados y que cumplan con los requerimientos regulatorios, a la vez que se mantiene la confidencialidad e integridad de los datos a lo largo del ecosistema del SIPN.

2.18.6 *El SIPN debe permitir y habilitar a la Sutel y miembros del CTPN- M, sin costo alguno, la generación de reportes estadísticos personalizados a partir de la información que consta en las bases de datos.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece una **capacidad de reportes estadísticos personalizados** para permitir que SUTEL y los miembros de CTPN-M puedan crear, configurar y generar reportes personalizados directamente a partir de los datos almacenados en NPCDB, sin costo adicional. Esta capacidad se entrega a través de una GUI de reportería intuitiva, basada en roles, que permite a los usuarios autorizados definir los parámetros del reporte, seleccionar los campos de datos, aplicar filtros y configurar la lógica de agregación en base a necesidades analíticas y regulatorias específicas.

Los usuarios pueden crear reportes personalizados al seleccionar variables como operador, tipo de transacción, etapa del proceso, motivo del rechazo, rango de MSISDN e intervalos configurables de fecha y hora. La plataforma soporta filtrado avanzado, agrupaciones y opciones de orden para permitir que los usuarios generen tanto tableros a nivel resumido como reportes detallados a nivel de transacción. Estos reportes pueden incluir estadísticas operativas, métricas de desempeño, indicadores de SLA, datos de uso de IVR y NIP, estado de sincronización e información de auditorías. Todos ellos surgen directamente de NPCDB para garantizar la precisión y consistencia.

El motor de reportería está diseñado para soportar la generación de reportes especiales y plantillas reutilizables de reportes para permitir a los usuarios guardar las configuraciones de reportes de uso frecuente en caso de volver a utilizarlos. Se pueden generar reportes en tiempo real, visualizados a través de gráficos y tableros; y exportados en formatos estándar como XLSX, CSV y PDF. El acceso a los reportes personalizados está regido por los permisos en base al perfil para garantizar que los operadores pueden generar reportes solo de sus propios datos; mientras SUTEL y los miembros autorizados de CTPN-M tienen acceso mayor, según sea requerido para supervisión y análisis.

Todas las actividades de generación de reportes se registran para fines de auditoría; y la plataforma asegura que los reportes personalizados no tengan impacto en el desempeño de los sistemas operativos, al aprovechar la base de datos dedicada de reportes o los mecanismos optimizados de acceso a datos. A través de este marco integral de reportería, accionado por el usuario, TNPC faculta a SUTEL y a los miembros de CTPN-M a analizar los datos del SIPN en forma independiente, obtener información y soporte para la toma de decisiones, en pleno cumplimiento con el requerimiento para reportes de estadísticas personalizadas, sin costo adicional y flexibles.

2.19 *Asegurar que cada operador/proveedor únicamente acceda y consulte a las gestiones de portabilidad y estadísticas en las cuales está involucrado (como donante o receptor). La Sutel podrá participar y consultar gestiones en cualquier proceso y etapa de cualquier operador/proveedor.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC aplica estrictos **controles de acceso basado en roles y segregación de datos** para garantizar que cada operador o proveedor de servicio pueda acceder y consultar solo las transacciones de portación y los datos estadísticos en los cuales estuvieron directamente involucrados como donante o receptor. Esto se implementa a través de un **marco de control de acceso basado en roles** centralizado, donde cada usuario es autenticado y se le asigna un perfil específico que rige sus derechos de acceso. Todos los datos almacenados en NPCDB están rotulados con los identificadores del operador y los roles en las transacciones para permitir que TNPC filtre dinámicamente y solo devuelva el subconjunto de datos relevante para cada operador durante la ejecución de la consulta, **ya sea que haya accedido por la GUI, interfaces SOAP o REST API.**

Al mismo tiempo, TNPC ofrece a SUTEL **acceso privilegiado e irrestricto** a todos los datos del SIPN para permitir la participación y supervisión totales a lo largo de todos los operadores, procesos y etapas de la transacción. A través de la interfaz administrativa de SUTEL, el personal autorizado puede consultar cualquier transacción de portación, revisar los ciclos de vida completos de los procesos, analizar las estadísticas a lo largo de todos los operadores y monitorear el desempeño del sistema en tiempo real y en forma histórica. Esto garantiza que SUTEL pueda realizar la supervisión regulatoria, la verificación de cumplimiento y las actividades de auditoría sin limitaciones.

Todas las operaciones de acceso y consulta se controlan en forma segura y registran en forma total, incluyen identidad del usuario, marca de tiempo, parámetros de consulta y datos accedidos para garantizar una completa trazabilidad y responsabilidad. Se protegen los datos usando encriptación en tránsito y en reposo y se previenen los intentos de acceso no autorizado a través de robustos controles de seguridad. A través de este enfoque, TNPC garantiza la separación estricta de los datos del operador, al tiempo que permite visibilidad regulatoria total a SUTEL para garantizar el cumplimiento de los requerimientos de confidencialidad, gobierno y auditoría dentro del ecosistema del SIPN.

2.20 *Contar con una plataforma de monitoreo de tiempo en línea (uptime monitoring) provista por un tercero independiente que será informado oportunamente por la ERPN seleccionada.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC ofrecerá una plataforma de monitoreo de tiempo en línea (*uptime monitoring*) aprovechando los servicios de monitoreo y observación nativos de la nube de AWS para garantizar la visibilidad continua de la disponibilidad de servicios del SIPN, el estado operativo y el cumplimiento de SLA. La solución de monitoreo supervisará continuamente los componentes críticos del SIPN, que incluyen APIs, conectividad del operador, servicios de procesamiento de transacciones, servicios de actualización de enrutamiento, servicios de IVR, portales web e interfaces de integración con los sistemas de los operadores y de SUTEL.

La plataforma utilizará las capacidades de monitoreo de AWS, que incluyen Amazon CloudWatch, verificación de salud, alertas automáticas, monitoreo sintético de transacciones y tableros operativos en tiempo real para la detección proactiva de caídas del sistema, degradación de servicio, latencia anormal o violaciones de umbrales de SLA. El monitoreo se realiza en forma independiente desde los flujos de trabajo de la aplicación en producción para asegurar una visibilidad transparente y objetiva de la disponibilidad de la plataforma y la salud operativa.

Los interesados autorizados que incluyen SUTEL, CTPN-M y los operadores/proveedores tendrán acceso seguro vía web a los tableros en tiempo real, estadísticas de tiempo en línea histórico, histórico de caídas del sistema, métricas de desempeño, indicadores de SLA y notificaciones de incidencias. Se generarán alertas automáticas y notificaciones de escalado a través de correo electrónico y los canales operativos configurados para garantizar una rápida concientización y respuesta ante eventos operativos.

El marco de monitoreo mantiene disponibilidad histórica y datos de desempeño para fines de auditoría, reportería, análisis de las tendencias y verificación de SLA. Todas las actividades de monitoreo se integran al marco de soporte operativo de TNPC y los procesos de gestión de incidencias para garantizar servicio continuo, rápida resolución de problemas y transparencia operativa.

A través de esta capacidad de monitoreo de tiempo en línea basado en AWS, TNPC asegura la visibilidad operativa continua, detección proactiva de incidencias, monitoreo transparente de SLA y aseguramiento de alta disponibilidad para la plataforma del SIPN en Costa Rica.

- 2.21** *Ofrecer una página WEB pública, segura de información general sobre el proceso de portación en Costa Rica, que permita a los usuarios finales obtener información de la regulación aplicable, cómo se realizan las gestiones de cambio de operador y consultar el estado de su trámite de portación. Esta página deberá cumplir con lo siguiente:*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC ofrece un portal web público altamente disponible, seguro y moderno, diseñado para soportar transparencia, accesibilidad y concientización del usuario para el ecosistema del SIPN en Costa Rica. El portal servirá como el sitio de información pública oficial para los servicios de portabilidad numérica, a fin de permitir que los usuarios finales accedan fácilmente a la información regulatoria, procedimientos de portabilidad, orientación en el cambio de operador e información del estado de la transacción de portación en tiempo real.

El portal público ofrecerá información integral acerca de las reglamentaciones aplicables de SUTEL, derechos del suscriptor, elegibilidad para la portación, tiempos de portabilidad, preguntas frecuentes y orientación paso a paso sobre cómo cambiar de operador y retener el mismo número de teléfono. El sitio también ofrecerá una funcionalidad segura para que los usuarios finales consulten el estado de su transacción de portación, mediante el ingreso del número de teléfono y credenciales de validación asociadas, para ofrecer visibilidad del avance de la transacción, operador donante, operador receptor e información de la ventana de cambio programada.

El portal se implementará en una interfaz web basada en Angular, amigable para el usuario, responsiva y moderna, compatible con los navegadores de escritorio, tabletas y dispositivos móviles. La solución soportará las interfaces de idioma español de Costa Rica e inglés y cumplirá con los estándares de accesibilidad reconocidos, que incluyen las pautas de WCAG, a fin de asegurar la usabilidad para todos los usuarios, incluyendo personas con capacidades especiales.

La plataforma aprovechará los servicios nativos de la nube de AWS y las tecnologías web seguras para garantizar alta disponibilidad, resiliencia, escalabilidad y protección para ciberseguridad. Los controles de seguridad incluyen encriptación HTTPS/TLS, protección CAPTCHA, acceso administrativo basado en roles, registro de auditoría, protección de firewall para la aplicación web y monitoreo continuo mediante los servicios de seguridad y observación nativos de AWS.

El portal público soportará capacidades de gestión de contenido que permitirán al personal autorizado de SUTEL y CTPN-M actualizar el contenido informativo, anuncios, procedimientos, preguntas frecuentes y orientación regulatoria, sin requerir cambios de software ni interrupción del servicio.

Además, el portal se integrará con los sistemas operativos de TNPC y NPCDB en tiempo real para garantizar que la información de estado de todas las transacciones, información de actualización de enrutamiento y datos operativos que sean presentados a los suscriptores sean precisos, actuales y estén sincronizados con la plataforma del SIPN.

A través de este portal público basado en Angular seguro y moderno, TNPC asegura la transparencia operativa, accesibilidad del suscriptor, cumplimiento regulatorio y mejor experiencia del cliente para todos los usuarios de la portabilidad numérica en Costa Rica.

- 2.21.1** *El sitio deberá contar con una URL pública, segura, previamente aprobada por la Sutel.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El portal público de TNPC es accesible a través una URL/dominio público seguro, previamente aprobado por SUTEL antes de la entrada en producción. El portal usará comunicación HTTPS/TLS y protecciones de

seguridad web estándar para garantizar el acceso público seguro y confiable a los suscriptores e interesados.

La estructura de la URL, la configuración de DNS y los mecanismos de acceso público serán coordinados con SUTEL y CTPN-M a fin de asegurar la alineación con los requerimientos operativos y regulatorios. Cualquier cambio futuro a la URL pública o configuración de acceso externo será manejado a través de los procedimientos de control de cambios en coordinación con SUTEL y CTPN-M.

2.21.2 *El sitio web debe tener un diseño gráfico moderno, realizado por profesionales demostrados, con un diseño de imagen basado en la experiencia del usuario y que muestre la información de forma ordenada y fácilmente accesible. Este deberá contar con la aprobación de la Sutel.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El portal web público de TNPC tendrá un diseño gráfico centrado en el usuario, profesional y moderno, desarrollado conforme a las mejores prácticas de la industria para un diseño web responsivo y centrado en la experiencia del cliente. Se diseñará la interfaz web para presentar información en forma clara, intuitiva y ordenada, con fácil acceso, para permitir que los suscriptores e interesados accedan rápido a la información de la portabilidad, estado de la transacción, pautas regulatorias y recursos de soporte.

El sitio web utilizará una interfaz moderna basada en Angular optimizada para dispositivos de escritorio, tabletas y móviles a fin de garantizar usabilidad y accesibilidad consistentes en todas las plataformas. Las estructuras de navegación, menús, elementos visuales, flujos de trabajo y organización del contenido serán cuidadosamente diseñados para maximizar la capacidad de uso, lectura y acceso para todos los usuarios, que incluyen personas con capacidades especiales, en línea con los estándares de accesibilidad reconocidos y las mejores prácticas.

El diseño del portal, elementos de marca, representaciones visuales, flujos de navegación y el enfoque de experiencia del usuario serán presentados a SUTEL para su revisión y aprobación previo a la entrada en producción. Cualquier actualización de diseño o cambio visual significativo también será coordinado con SUTEL a fin de garantizar la alineación con las expectativas regulatorias, estándares de comunicación pública y objetivos de experiencia del usuario.

A través de este enfoque en el usuario con diseño profesional, TNPC asegura un portal web moderno, accesible, visualmente atractivo y fácil de usar que mejora la transparencia, experiencia del suscriptor y participación pública en la plataforma del SIPN en Costa Rica.

2.21.3 *La página WEB debe permitir ser utilizada por grupos de personas con necesidades especiales, por lo que, al menos, debe cumplir con las recomendaciones WAI Nivel A de la W3C, norma INTE ISO IEC 40500 2020:*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El portal web público de TNPC estará diseñado y será implementado para garantizar accesibilidad, inclusión y usabilidad para todos los usuarios, incluidas las personas con capacidades y necesidades especiales. La plataforma cumplirá, como mínimo, con los requerimientos de accesibilidad de WAI Nivel A de la W3C, norma INTE ISO IEC 40500 2020: Pautas de Accesibilidad para el Contenido Web (WCAG) 2.2 o equivalente.

El portal incorporará las mejores prácticas de accesibilidad reconocidas, que incluyen soporte de navegación con teclado, compatibilidad de lectura en pantalla, texto alternativo para imágenes y elementos gráficos, formas y controles de accesibilidad, representaciones de páginas responsivas, texto escalable, contraste adecuado de color y estructuras de navegación claras a fin de garantizar una experiencia inclusiva y amigable para el usuario a lo largo de dispositivos de escritorio y móviles.

La interfaz del portal basada en Angular estará diseñada con un enfoque de experiencia del usuario moderna e intuitiva para garantizar que la información relativa a los procesos de portación, regulaciones, derechos del suscriptor y estado de la transacción se presenta en forma clara, ordenada y de acceso fácil para todos los usuarios. Se validará el cumplimiento con la accesibilidad durante el diseño, desarrollo, pruebas y ciclo de vida de la implementación para garantizar la alineación con los estándares aplicables y requerimientos de SUTEL.

A través de este enfoque en la accesibilidad, TNPC asegura un portal web seguro, moderno e inclusivo que promueve el acceso equitativo a los servicios e información del SIPN a todos los suscriptores e interesados de Costa Rica.

2.21.4 *La interfaz deberá ser responsiva de modo que se adapte a dispositivos móviles, tabletas y computadoras en sus diferentes sistemas operativos y resoluciones.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El portal web público de TNPC ofrece una interfaz de usuario totalmente responsiva y adaptativa, diseñada para operar sin inconvenientes en dispositivos móviles, tabletas, laptops y computadoras de escritorio con diferentes sistemas operativos, tamaños de pantalla, navegadores y resoluciones de pantalla.

La interfaz del portal basada en Angular ajustará automáticamente las representaciones, elementos de navegación, presentación de contenido, formatos y componentes gráficos para ofrecer una experiencia de usuario optimizada y consistente, independientemente del tipo de dispositivo o resolución de pantalla. Se aplicarán principios de diseño responsivos y estándares web modernos para garantizar la capacidad de uso, lectura, acceso y desempeño a lo largo de Android, iOS, Windows, macOS y las principales plataformas de navegadores web.

Se diseñará el portal para que soporte dispositivos táctiles, rendición de contenido escalable, menús adaptativos, tablas responsivas y carga optimizada de páginas para garantizar acceso eficiente y amigable para el usuario a los suscriptores, operadores e interesados autorizados que accedan los servicios del SIPN desde diferentes dispositivos y entornos de red.

A través de este enfoque de diseño responsivo e independiente del dispositivo, TNPC asegura una experiencia de usuario moderna, accesible y consistente que permite el acceso seguro y confiable a la información de portabilidad y los servicios de la transacción en cualquier momento y desde cualquier plataforma de dispositivo que sea soportada.

2.21.5 *Deberá permitir al usuario seleccionar el idioma que desea visualizar en las interfaces WEB. Los idiomas que debe desplegar el sistema para seleccionar por parte del usuario deberán ser, al menos, español de Costa Rica e inglés de Estados Unidos y deseable, francés de Francia.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El portal web público de TNPC y las interfaces web asociadas soportarán funcionalidad multilingüe que permite a los usuarios seleccionar fácilmente el idioma preferido, a través de una selección intuitiva del idioma que está disponible en todas las interfaces soportadas.

Como mínimo, la plataforma ofrecerá soporte total para español de Costa Rica e inglés americano. Además, TNPC puede soportar capacidades de idioma francés (Francia) como preferido, aprovechando el marco multilingüe configurable de la plataforma. Todos los elementos de la interfaz, menús, componentes de navegación, notificaciones, contenido de ayuda, páginas de información pública y materiales de pautas del usuario se presentarán consistentemente en el idioma seleccionado para garantizar una experiencia del usuario amigable y sin inconvenientes.

La arquitectura del portal basado en Angular está diseñada para soportar capacidad de internacionalización y localización escalables para permitir la introducción de idiomas adicionales en el futuro, sin requerir cambios arquitectónicos importantes. Las preferencias de idioma se aplicarán dinámicamente a lo largo de las interfaces de escritorio, tableta y móvil para garantizar uso y acceso consistente a lo largo de todos los dispositivos y sistemas operativos.

A través de este enfoque multilingüe, centrado en el usuario, TNPC asegura una interacción accesible, inclusiva y amigable para el usuario a los suscriptores, operadores, SUTEL y todos los interesados autorizados dentro del ecosistema del SIPN en Costa Rica.

2.21.6 *La página WEB deberá ser rápida y fácilmente editable sin cargos adicionales como parte del servicio. El CTPN-M proporcionará al adjudicatario la información que debe colocarse. El sitio WEB debe permitir el despliegue de imágenes, vídeos, archivos, estadísticas, entre otros.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El portal web público de TNPC está diseñado como una plataforma de alto rendimiento, moderna y de fácil mantenimiento que permite realizar actualizaciones de contenido con rapidez y gestión eficiente, sin costos de desarrollo adicionales, como parte del servicio en curso. El portal usará un enfoque de gestión de contenido flexible y amigable para el usuario, que permitirá al personal autorizado de CTPN-M actualizar y gestionar la información pública rápida y eficientemente, sin requerir conocimiento técnico ni interrupción del servicio.

CTPN-M podrá ofrecer contenido, documentos, imágenes, videos, anuncios, estadísticas, preguntas frecuentes, notificaciones públicas, información regulatoria y otros materiales informativos para publicación en el portal. La plataforma soportará capacidades de gestión dinámica de contenido que permite actualizaciones rápidas, presentación ordenada del contenido y flujos de trabajo con publicación controlada, a fin de que la información esté actualizada, sea precisa y fácilmente accesible para los suscriptores e interesados.

La interfaz del portal basada en Angular soportará la representación y gestión de contenido multimedia y descargable, que incluye imágenes, videos, documentos PDF, hojas de cálculo, estadísticas, gráficos, reportes y otros recursos de información pública. La arquitectura responsiva basada en Angular asegura rendimiento optimizado, carga rápida de páginas y experiencia del usuario consistente a lo largo de dispositivos de escritorio, tabletas y móviles.

La plataforma aprovechará los servicios nativos de la nube de AWS y las tecnologías web escalables para asegurar alta disponibilidad, entrega rápida de contenido, resiliencia operativa y desempeño eficiente incluso durante períodos de alta actividad del usuario. A través de esta arquitectura web moderna y flexible, TNPC asegura que el portal público sea rápido, fácil de mantener y atractivo visualmente y que esté continuamente alineado con las necesidades de comunicación e información de CTPN-M y SUTEL en constante evolución.

2.21.6.1 *La Sutel tendrá acceso a un portal WEB para edición de contenido.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

SUTEL tendrá acceso seguro y controlado a las capacidades de gestión de contenido del portal web público de TNPC para permitir que el personal autorizado cree, edite, actualice, publique y gestione el contenido del portal en forma directa y eficiente.

El portal incluirá una interfaz de gestión de contenido intuitiva y amigable para el usuario que permitirá a SUTEL mantener información pública como anuncios, actualizaciones regulatorias, procedimientos de portabilidad, pautas del suscriptor, preguntas frecuentes, imágenes, videos, documentos descargables,

estadísticas y contenido informativo, sin requerir actividades de desarrollo de software ni intervención técnica de parte de TNS.

El acceso a las funciones de gestión de contenido será a través de autenticación segura y permisos basados en roles a fin de garantizar la administración, auditoría y protección controlada del contenido publicado. La plataforma soportará vista previa del contenido, flujos de trabajo de publicación controlada, gestión de versiones y administración de contenido multilingüe a fin de facilitar comunicaciones públicas eficientes y precisas.

A través de esta capacidad de administración de contenido flexible y autogestionable, TNPC permite que SUTEL mantenga información a tiempo, precisa y actualizada en el portal público del SIPN, a la vez que su independencia operativa, usabilidad y control administrativo.

2.21.7 *Una sección para consulta del estado del trámite deberá realizarse de manera sencilla mediante el ingreso del número telefónico y el correspondiente NIP asociado y vigente*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El portal público de TNPC ofrecerá una **interfaz de consulta del estado de la transacción simple, intuitiva y amigable para el usuario**, que permita a los suscriptores verificar con seguridad el estado de su solicitud de portabilidad al ingresar el número de teléfono y NIP activo y vigente que corresponda, asociado a la transacción.

El proceso de consulta de transacciones incorpora mecanismos de **Autenticación de Doble Factor segura (2FA)**, donde el suscriptor debe brindar el MSISDN y NIP vigente generado durante el proceso de portación. TNPC valida el NIP en tiempo real contra NPCDB, verifica la autenticidad del NIP, período de vigencia, asociación de la transacción y estado activo antes de mostrar ningún detalle de la transacción. Este enfoque asegura que la **información de la transacción es solo accesible** a los usuarios autorizados, a la vez que protege la privacidad del suscriptor y evita accesos no autorizados.

Una vez validado con éxito, el portal representará la información relevante en tiempo real que incluye estado de la transacción, operador donante, operador receptor, ventana de cambio programada y estado de procesamiento actual, para permitir que los suscriptores hagan fácilmente seguimiento del avance de su solicitud de portabilidad. Si el NIP es inválido, venció o no corresponde al número de teléfono presentado, el sistema denegará el acceso y presentará un mensaje de validación adecuada sin exponer información sensible de la transacción.

La interfaz responsiva basada en Angular será optimizada para navegadores de dispositivos móviles, tabletas y de escritorio, para garantizar un acceso rápido y conveniente a lo largo de diferentes sistemas operativos y resoluciones de pantalla. El portal también incluirá instrucciones claras, navegación con fácil accesibilidad, **encriptación HTTPS/TLS, protección CAPTCHA y gestión de sesión segura**, para ofrecer una experiencia segura y sin inconvenientes a todos los usuarios, que incluyen personas con necesidades especiales.

A través de esta **capacidad de consulta de transacciones fácil de usar**, TNPC mejora la transparencia, concientización del usuario, seguridad operativa y experiencia del cliente en forma total, dentro del ecosistema del SIPN en Costa Rica.

- 2.21.8** La información deberá mostrar claramente el estado de su trámite de portabilidad, el operador receptor y operador donante y, cuando corresponda, la fecha de ventana de cambio.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El portal público de TNPC presentará la información del trámite de portabilidad en **formato claro, intuitivo y fácil de comprender**, que permite a los suscriptores identificar rápidamente el estado actual de su solicitud de portabilidad. Una vez que el suscriptor es autenticado con éxito, usando **MSISDN y NIP vigente**, el portal representará los detalles relevantes de la transacción en tiempo real, que incluye **estado actual del trámite de portabilidad, operador receptor, operador donante y, cuando corresponda, fecha y hora de ventana de cambio programada**.

La información del estado del trámite se presentará usando una **interfaz amigable para el usuario con etiquetas claras, indicadores de estado y avance estructurado del flujo de trabajo**, a fin de mejorar el entendimiento del suscriptor y la transparencia durante todo el proceso de portación. El portal ofrecerá visibilidad de las etapas de procesamiento como **generación de NIP, prevalidación, aprobación de solicitud, programación, activación, cancelación y estado completado**, que permitirá a los suscriptores hacer fácil seguimiento del avance de su solicitud.

La **interfaz responsiva basada en Angular** asegurará que la información de la transacción se despliega en forma clara y consistente a lo largo de los navegadores de dispositivos móviles, tabletas y de escritorio, ofreciendo una **experiencia amigable para el usuario, accesible y sin inconvenientes** a todos los suscriptores e interesados.

A través de esta **capacidad de visibilidad de transacciones transparente y centrada en el cliente**, TNPC mejora la concientización del usuario, transparencia operativa y experiencia del cliente en forma total, dentro del ecosistema del SIPN en Costa Rica.

- 2.21.9** Una sección para información general sobre la portabilidad numérica en Costa Rica y la regulación aplicable cuyo contenido será definido de común acuerdo con la Sutel.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El portal público de TNPC incluirá una sección dedicada y fácilmente accesible que contendrá **información general acerca de la portabilidad numérica en Costa Rica**, diseñada para promover la concientización del suscriptor, transparencia y entendimiento de los servicios de portabilidad y derechos regulatorios.

Esta sección ofrecerá información clara y amigable para el usuario acerca del **proceso de portabilidad numérica, elegibilidad del suscriptor, tiempos de la portabilidad, regulaciones aplicables, derechos y obligaciones del usuario, preguntas frecuentes, procedimientos operativos y pautas sobre cambio de operador conservando el mismo número de teléfono**. La información se presentará en formato estructurado e intuitivo, usando principios de diseño web modernos para garantizar la fácil navegación y accesibilidad a todos los usuarios.

Todo el contenido del portal, materiales informativos, notificaciones públicas, cuadros, videos, documentos descargables y pautas regulatorias serán **mutuamente convenidos, revisados y definidos en coordinación con SUTEL y CTPN-M** antes de su publicación. La plataforma también permitirá que el personal autorizado de SUTEL actualice y gestione el contenido directamente a través de una interfaz de gestión de contenido segura, sin requerir ninguna modificación del software ni interrupción del servicio.

El **portal responsivo basado en Angular** asegurará que todo el contenido informativo mostrado sea consistente y claro a lo largo de computadoras de escritorio, tabletas y dispositivos móviles, a la vez que soportará estándares de presentación y accesibilidad multilingües.

A través de esta sección informativa pública centrada en el usuario, TNPC mejora la transparencia, concientización regulatoria, educación del suscriptor y participación pública general dentro del ecosistema del SIPN en Costa Rica.

- 2.21.10** *El sitio WEB debe contar con mecanismos de seguridad para la página de tipo igual o superior a reCAPTCHA para realizar las consultas del trámite. El costo de este sistema de seguridad corre por parte de la ERPN.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El portal web público de TNPC incorporará **mecanismos de seguridad robustos** para proteger las funciones de consulta de transacciones y para evitar acceso no autorizado, abuso automático, actividades fraudulentas y excesivos intentos de consulta. La plataforma implementará **reCAPTCHA o mecanismos de verificación humana inteligentes equivalentes** para las consultas de estado de transacción y formas de interacción pública a fin de garantizar acceso seguro y confiable a los usuarios legítimos, a la vez que minimiza las solicitudes automáticas o maliciosas.

Además de las protecciones basadas en CAPTCHA, el portal utilizará **comunicaciones HTTPS/TLS seguras, controles de gestión de sesión**, validación de solicitud y mecanismos de monitoreo para mayor seguridad y protección de la información del suscriptor y datos de las transacciones. Estas protecciones se integrarán sin inconveniente a la experiencia del usuario para mantener la usabilidad, al tiempo que garantiza la seguridad operativa y el cumplimiento regulatorio.

Los mecanismos de seguridad serán totalmente gestionados, mantenidos y financieramente asumidos por la ERPN, como parte del servicio total del SIPN, sin generar ningún costo adicionales ni carga operativa a SUTEL, CTPN-M, los operadores ni usuarios finales.

A través de este marco de protección seguro y proactivo, TNPC garantiza un entorno del portal público seguro, confiable y resiliente, a la vez que mantiene la accesibilidad, transparencia y confianza del usuario en todo el ecosistema del SIPN en Costa Rica.

- 2.21.11** *Deberá tener un módulo que permite acceso a alguna herramienta con funciones avanzadas de análisis de visitantes a la página, como cantidad de usuarios, dispositivo, análisis de comportamiento, entre otras. Por ejemplo, herramientas tipo Google Analytics, Adobe Analytics, Matomo, Piwik Pro, entre otros.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El portal web público de TNPC incluirá un **módulo analítico y de análisis de visitantes de avanzada que ofrecerá visibilidad integral del uso del portal, comportamiento del usuario y conocimiento operativo**. La capacidad analítica será entregada a través de una combinación de servicios analíticos internos integrados y soporte óptimo para las plataformas analíticas reconocidas de la industria como **Google Analytics, Adobe Analytics, Matomo, Piwik PRO o tecnologías equivalentes**.

El marco analítico interno de TNPC aprovechará los servicios de monitoreo, registro y análisis nativos de AWS para recolectar, procesar y visualizar la actividad del portal y las métricas operativas en tiempo real. La plataforma capturará y analizará información, que incluye **cantidad de visitantes, usuarios únicos, duración de sesión, rutas de navegación, visualizaciones de página, tipos de dispositivos, patrones de acceso geográficos, tendencias del comportamiento del usuario, rendimiento de la página, actividad de búsqueda y estadísticas de uso del portal**.

Los servicios analíticos serán directamente integrados a la arquitectura del portal basado en Angular y el entorno en la nube de AWS para permitir procesamiento escalable y de alto rendimiento sin impactar en la capacidad de respuesta del portal ni la experiencia del usuario. Este enfoque ofrece flexibilidad para que

SUTEL y CTPN-M utilicen la capacidad analítica incorporada o bien se integren con las plataformas analíticas externas, en base a las preferencias operativas y requerimientos de gobierno.

A través de este marco analítico integrado, TNPC ofrece a SUTEL y CTPN-M inteligencia operativa poderosa y conocimiento accionable para la mejora continua de la transparencia, accesibilidad, usabilidad y participación del suscriptor a lo largo del portal público del SIPN en Costa Rica.

2.21.12 *La página no deberá permitir el acceso a direcciones IP fuera del territorio costarricense y mostrará el mensaje correspondiente para información a quien la intente acceder.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El portal público de TNPC incorporará **mecanismos de control de acceso por geolocalización** para restringir el acceso exclusivamente a usuarios originarios de rangos de direcciones IP costarricenses de acuerdo con los requerimientos de SUTEL. La plataforma utilizará filtrado de IP seguro, validación de geolocalización y controles de listas blancas dentro de la red de AWS y la arquitectura de seguridad para garantizar la aplicación de las políticas de acceso en forma consistente y confiable.

Los usuarios que intenten acceder al portal desde direcciones IP fuera del territorio costarricense quedarán automáticamente restringidos y se les presentará un mensaje informativo claro y amigable para el usuario que indicará que el acceso al portal queda limitado a Costa Rica conforme a las políticas regulatorias y operativas.

La solución soportará **capacidades de listas blancas de IP** configurables para las entidades autorizadas, usuarios administrativos, entornos de pruebas, acceso regulatorio o excepciones operativas aprobadas tal como sea definido por SUTEL y CTPN-M. Ese enfoque ofrece flexibilidad para un acceso externo controlado, a la vez que cumple con los requerimientos de seguridad y cumplimiento total.

Estos controles serán integrados a los servicios de seguridad nativos de AWS, capacidades de monitoreo y registro a fin de garantizar la aplicación segura, escalable y auditable de las restricciones de acceso geográfico, sin impacto en el rendimiento del portal ni experiencia del usuario dentro de Costa Rica.

A través de este marco de acceso seguro y controlado, TNPC garantiza el cumplimiento de los requerimientos de acceso territorial, a la vez que mantiene la seguridad operativa, transparencia y gestión eficiente de las excepciones de acceso autorizado.

2.21.12.1 *El oferente deberá proponer un esquema de seguridad para la plataforma y que a su vez permita agregar direcciones IP permitidas fuera del territorio costarricense a decisión del CTPN-M.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC propone un **marco de control de acceso y seguridad centralmente gestionado y flexible** que restringe el acceso al portal al territorio costarricense, en forma predeterminada, a la vez que permite excepciones autorizadas a través de mecanismos para posibilitar IP controlados, aprobados por CTPN-M.

La plataforma utilizará **filtrado de geolocalización, listas de control de acceso en base a IP, políticas de listas blancas, reglas de red segura y servicios de seguridad nativos de AWS** para aplicar las restricciones de acceso territorial y gestionar las solicitudes de acceso externo autorizadas. En forma predeterminada, el acceso al portal quedará limitado a direcciones IP que se originan en Costa Rica; sin embargo, la solución soportará el agregado controlado de direcciones de IP externas o rangos de IP aprobados, tal como sea autorizado por CTPN-M para entidades regulatorias, operadores, actividades de pruebas, administración remota o requerimientos operativos excepcionales.

El marco de seguridad incluirá capacidades de gestión de listas blancas configurables que permitan a los administradores autorizados posibilitar, modificar, revisar o revocar, en forma segura, acceso IP externo aprobado a través de los procedimientos controlados de gobierno y control de cambios. Todas las solicitudes de acceso de listas blancas, modificaciones y actividades de conexiones se registrarán y serán auditables para garantizar la transparencia, trazabilidad y cumplimiento con los requerimientos de seguridad operativa.

La arquitectura propuesta aprovecha los controles de seguridad nativos en la nube de AWS que incluyen políticas de acceso a la red, protecciones con firewalls, monitoreo, registros y mecanismos de alerta para garantizar la aplicación segura, escalable y resiliente de restricciones de acceso, sin impacto en el rendimiento del sistema ni experiencia del usuario.

A través de este enfoque adaptable con foco en la seguridad, TNPC ofrece a CTPN-M y SUTEL un marco de control de acceso territorial robusto que balancea la seguridad operativa, cumplimiento regulatorio, flexibilidad y gobierno centralizado para la gestión de acceso externo autorizado.

2.22 *Ofrecer una página WEB pública segura (independiente a la del usuario final), de acceso a través de credenciales y autenticación en doble factor, responsiva, que permita consultar los registros históricos de portación y operador actual con su modalidad de pago por parte de los organismos autorizados por el CTPN-M.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece un portal web seguro y dedicado que es independiente del sitio público del usuario final; y está específicamente diseñado para soporte del acceso de organismos autorizados por CTPN-M. Este portal está construido con sólidos controles de seguridad, que incluyen autenticación basada en credenciales y autenticación multifactorial, para garantizar que solo los usuarios autorizados puedan acceder a datos sensibles del SIPN. El acceso es a través de un marco de control de acceso basado en roles estrictos, donde se asigna a cada usuario permisos en línea con el alcance aprobado por el organismo para garantizar que solo se permitan las consultas y operaciones autorizadas.

A través de este portal, los organismos autorizados pueden consultar los registros históricos de portaciones, información sobre el operador actual y atributos asociados como modalidad de pago. Los datos se recuperan en tiempo real desde NPCDB para garantizar que toda la información presentada sea precisa y consistente con los registros actuales del sistema. La interfaz ofrece capacidades de búsqueda y filtrado de avanzada en base a parámetros como MSISDN, rangos de fechas, operador y tipo de transacción, para permitir un análisis eficiente y detallado. El portal está diseñado como una aplicación web responsiva que soporta el acceso con sistemas de dispositivos móviles, tabletas o de escritorio y garantiza la usabilidad y accesibilidad en todos los entornos operativos.

Desde la perspectiva de la seguridad, el portal está protegido con un modelo de seguridad en capas que cubren identidad, acceso, red, aplicación y protección de datos. Todas las comunicaciones entre los usuarios y el portal están encriptadas con HTTPS con TLS 1.2 o superior para garantizar la confidencialidad e integridad de los datos transmitidos. Los datos sensibles almacenados en NPCDB, que incluyen registros históricos de portaciones, información del operador y registros de auditoría, están encriptados en reposo con la encriptación estándar de la industria como AES 256. El acceso a los datos está controlado por autorización basada en roles, controles a nivel de base de datos y validación a nivel de aplicación para evitar accesos no autorizados.

La plataforma incluye protección contra las amenazas de seguridad web comunes como ataques de fuerza bruta, intentos de acceso no autorizado, inyección SQL, *cross site scripting*, falsificación de solicitud entre sitios y *scraping* automatizado. Controles adicionales tales como limitación de tasa, bloqueo de cuenta después de intentos de inicio de sesión fallidos, repetidos y listados con IP permitidos opcionales para los organismos autorizados mejoran aún más la seguridad del sistema. La gestión de sesiones se implementa con token de sesión segura, timeout automático y protección contra secuestro de sesión.

Todas las actividades de acceso y consulta se registran en forma total para garantizar la trazabilidad y auditoría. Cada interacción se registra con la identidad del usuario, marca de tiempo, parámetros de consulta, datos accedidos y resultados, junto con la información IP de la fuente. Estos registros se mantienen en formato a prueba de adulteración y están disponibles a SUTEL para auditoría y verificación de cumplimiento. Los eventos de seguridad y las anomalías se monitorean en tiempo real. Se generan alertas para investigación y respuesta.

Además, el portal soporta capacidades de exportación segura de datos y reportería en formatos estándar, cuando sea permitido, para posibilitar que los organismos autorizados realicen análisis posteriores, según sea requerido. El sistema se mantiene a través de actualizaciones de seguridad y procesos de gestión de vulnerabilidades. Las actualizaciones se aplican con estrategias de cero tiempo inactivo o implementación continua, o durante las ventanas de mantenimiento convenidas con impacto mínimo o controlado en el servicio.

A través de este portal seguro, responsivo y auditable, TNPC garantiza que los organismos autorizados cuenten con acceso confiable y controlado a los datos del SIPN, al tiempo que se mantienen los más elevados estándares de seguridad, confidencialidad y cumplimiento regulatorio.

2.23 *Permitir el acceso y descarga segura, por parte de terceros autorizados por el CTPN-M, a la base de datos de números portados total y diferencial.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece un marco seguro y controlado que permite a los terceros autorizados por CTPN-M acceder y descargar los datos de números portados, que incluyen conjuntos de datos totales y actualizaciones diferenciales, en pleno cumplimiento con los requerimientos regulatorios y de gobierno de datos. El acceso a estos datos queda estrictamente restringido a través de un modelo de control de acceso basado en roles, donde se aprovisiona a cada entidad autorizada con las credenciales y permisos alineados al alcance aprobado. Todos los accesos se autentican con sólidos mecanismos de seguridad, que incluyen autenticación multifactorial, cuando corresponda, para garantizar que solo los usuarios autorizados puedan recuperar datos del SIPN.

La plataforma soporta múltiples mecanismos de entrega seguros para el acceso y la descarga de datos. Los usuarios autorizados pueden recuperar datos desde una interfaz web dedicada, accesos SFTP seguro o API basadas en REST, dependiendo de sus requerimientos operativos. TNPC ofrece acceso a conjuntos de datos completos, que representan el conjunto completo de números portados, y a conjuntos de datos diferenciales, que representan cambios incrementales como números recientemente portados o retornados. Estos conjuntos de datos se generan directamente en NPCDB y reflejan la información de enrutamiento más actual y precisa que está disponible en el sistema. Los archivos diferenciales se alinean con las ventanas de cambio y los procesos de difusión diaria para garantizar que las partes autorizadas reciban actualizaciones a tiempo, sin necesidad de procesar innecesariamente todos los conjuntos de datos.

Todas las transferencias de datos se protegen con protocolos seguros, que incluyen HTTPS y SFTP, con encriptación en tránsito usando TLS y encriptación en reposo con los mecanismos estándar de la industria. El acceso a datos se controla aún más con filtrado y validación para garantizar que solo se exponen los datos permitidos a cada parte autorizada. La plataforma además soporta cronogramas de descarga configurables y recuperación a demanda, que permite a CTPN-M definir cómo y cuándo los datos están disponibles.

Cada actividad de acceso y descarga se registra y se puede rastrear completamente, incluye identidad de usuario, hora de acceso, conjunto de datos recuperado y ubicación de la fuente, para garantizar la auditoría completa y cumplimiento total con los requerimientos regulatorios. TNPC también ofrece capacidades de reportería que permiten a SUTEL y CTPN-M monitorear los patrones de acceso, verificar el uso autorizado y detectar cualquier anomalía.

A través de este marco de acceso a datos seguro, flexible y auditable, TNPC garantiza que los terceros autorizados puedan obtener confiablemente los datos de números portados requeridos, a la vez que se mantiene un estricto control sobre la confidencialidad e integridad de los datos; y el cumplimiento regulatorio.

2.23.1 *El acceso será realizado de manera segura a través de credenciales.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC aplica puntos de acceso en todo el sistema en base a credenciales y seguros para garantizar que solo los usuarios, sistemas y entidades externas autenticados y autorizados pueden interactuar con los servicios del SIPN. Cada canal de acceso, de cara al cliente o sistema a sistema, está protegido con sólida autenticación, autorización basada en roles y comunicación encriptada para garantizar pleno cumplimiento con los requerimientos de seguridad y regulatorios.

Todas las **interfaces de cara al usuario**, que incluyen GUI del operador, portal administrativo de SUTEL, tableros de reportería, interfaz de consulta al portal público y portal seguro para organismos autorizados requieren credenciales únicas de usuario. Se aplica la autenticación a través de mecanismos de inicio de sesión segura con soporte de autenticación multifactorial, políticas de contraseñas, controles de gestión de sesión y mecanismos de bloqueo de cuenta. Se asigna a cada usuario un perfil basado en el rol que determina el acceso a privilegios para garantizar que los usuarios solo pueden realizar las acciones y visualizar los datos dentro de su alcance autorizado. Todas las actividades del usuario, que incluyen intentos de inicio de sesión, consultas y acceso a datos, se registran con marcas de tiempo e identificadores del usuario para fines de auditoría.

Para las **integraciones sistema a sistema**, que incluyen interfaces SOAP XML y REST API, TNPC aplica acceso seguro usando credenciales como claves de API, certificados de clientes o mecanismos de autenticación en base a token. Todas las interacciones API se protegen usando HTTPS con encriptación TLS para garantizar que las credenciales y los datos se transmiten en forma segura. Se restringe el acceso a los puntos finales del operador previamente registrado y los sistemas autorizados con validación de la identidad de la fuente, estructura del mensaje y contexto de la transacción, antes del procesamiento. Los puntos finales de integración se configuran con estrictos controles de acceso para evitar accesos no autorizados o uso indebido.

Para el **acceso en base a archivos**, que incluye descargas de archivos de difusión y sincronización en base a SFTP, TNPC ofrece autenticación segura en base a credenciales usando el nombre de usuario y contraseña, o con mecanismos de autenticación en base a llaves. Se asigna a cada operador o tercero autorizado un perfil de acceso dedicado y una estructura de directorio para garantizar el aislamiento de los datos y el acceso controlado. Las transferencias de archivos son encriptadas y monitoreadas con registro total de las actividades de carga y descarga.

También se aseguran los puntos de acceso adicionales como integración de IVR, interacciones con Gateway de SMS y conexiones con plataformas regulatorias externas usando conexiones autenticadas y validadas para garantizar que solo los sistemas confiables pueden intercambiar datos con TNPC. Las medidas de seguridad a nivel de la red, que incluyen firewalls y listas de control de acceso, restringen aún más la conectividad a los puntos finales aprobados.

A través de este marco de acceso integral en base a credenciales a lo largo de todas las interfaces, que incluyen GUI, API, SFTP e integraciones de sistemas, TNPC garantiza que todo el acceso al SIPN sea seguro, controlado, auditable y en cumplimiento con los requerimientos de SUTEL para protección de datos e integridad operativa.

2.23.2 *Los accesos que se otorguen no generarán costos adicionales para los operadores/proveedores.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC garantiza que todos los accesos a los operadores, proveedores de servicio, SUTEL y terceros autorizados, tal como se define en el alcance del SIPN, se entreguen **sin ningún costo adicional**. Esto incluye acceso a través de todos los canales soportados como GUI del operador, portal administrativo de SUTEL, interfaces de reportería y analíticas, portal de organismo seguro, interfaces SOAP XML, REST API y acceso a archivos en base a SFTP para sincronización y datos de difusión.

Todas las capacidades necesarias para acceder a los servicios del SIPN, que incluyen procesamiento de transacciones, gestión de consultas, reportería, descargas de datos y acceso de auditoría, se incluyen como parte de la oferta de servicio estándar de TNPC. Esto también contempla mecanismos de acceso seguro como gestión de credenciales, servicios de autenticación y autorización basada en roles para garantizar que los operadores y proveedores puedan interactuar con el sistema, sin incurrir en ningún costo de licencias, integración ni tarifas de uso.

Además, TNPC garantiza que las funcionalidades avanzadas como tableros de reportería en tiempo real, reportes estadísticos configurables, acceso a datos históricos y capacidades de sincronización a través de SFTP o API estén disponibles a los operadores y proveedores dentro del alcance del servicio acordado, sin costos adicionales. Las interfaces, herramientas o puntos de acceso requeridos que son necesarios para cumplir con las operaciones del SIPN se ofrecen como parte de la solución básica para garantizar transparencia y predictibilidad en la estructura de costos.

A través de este enfoque, TNPC garantiza que todos los interesados tengan acceso completo y equitativo a los servicios y datos del SIPN, con soporte eficiente de las operaciones y cumplimiento regulatorio, sin imponer ninguna carga financiera adicional a los operadores ni proveedores de servicios; en pleno cumplimiento con el requerimiento definido por SUTEL.

2.23.3 *La ERPN seleccionada realizará un seguimiento del acceso por parte de cada uno de los autorizados. Este reporte estará disponible bajo solicitud por parte de los operadores/proveedores y/o la Sutel.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece capacidades integrales para **hacer seguimiento, registrar y reportar todo los accesos por parte de usuarios autorizados** a lo largo del entorno del SIPN a fin de garantizar transparencia total, auditorías y cumplimiento regulatorio. Cada interacción del usuario con el sistema, ya sea a través de la GUI del operador, portal administrativo de SUTEL, portal del organismo autorizado, interfaces de reportería, API o acceso SFTP se registra en detalle dentro del marco de registro centralizado y seguro que está integrado con NPCDB.

Para cada evento de acceso, TNPC registra la información clave, que incluye identidad del usuario, rol y organización, marca de tiempo del acceso, dirección IP segura, tipo de interfaz de acceso utilizada, acciones realizadas, parámetros de consulta y datos accedidos o descargados. Esto incluye actividades como intentos de inicio de sesión, autenticaciones exitosas, consultas de transacciones, generación de reportes, descargas de archivos y acciones administrativas. Todos los registros se mantienen en formato resistente a adulteración para garantizar la integridad y evitar modificaciones no autorizadas; cumpliendo así con los requerimientos de auditoría y análisis forense.

TNPC ofrece capacidades para generar **acceso a reportes de auditoría a demanda**, que se pueden poner a disposición de los operadores, proveedores de servicio y SUTEL, según sea requerido. Estos reportes se pueden filtrar en base a usuario, organización, período de tiempo, tipo de acceso o categoría de actividad

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

para permitir una revisión detallada del uso del sistema y cumplimiento con las políticas de acceso. Se pueden entregar los reportes a través de la GUI de Reportería o exportados a formatos estándar como XLSX o CSV para análisis posterior.

Además, TNPC soporta monitoreo y generación de alertas en tiempo real frente a intentos de acceso sospechosos o no autorizados que permite una gestión proactiva de la seguridad. A través del marco de seguimiento de acceso y reportería integral, TNPC asegura visibilidad total de las actividades del usuario, soporta la supervisión regulatoria y cumple con los requerimientos de SUTEL para acceso controlado y auditable de los datos del SIPN.

2.24 *Realizar una migración exitosa de todos los procesos, información y bases de datos de portación históricos desde el 2013 hasta el 20 de noviembre de 2027.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS realizó la primera migración de portabilidad numérica a nivel mundial en Perú en el 2014, en donde se migró exitosamente toda la base de datos del proveedor anterior sin interrupciones e inconvenientes dentro de los tiempos acordados con la industria. Para más detalles pueden revisar el caso de estudio adjunto en el anexo 1 – *Caso de Estudio : Implementación de la Portabilidad Numérica Móvil y Fija en Perú*. TNS realizará la **migración integral, segura y totalmente controlada** de todos los datos históricos del SIPN y los procesará en la plataforma de TNPC para garantizar la conservación completa de la integridad de los datos, continuidad del servicio y cumplimiento regulatorio. Este enfoque de migración se basa en **metodologías probadas que se implementaron con éxito en implementaciones nacionales como Perú y Estados Unidos**, donde se hizo la transición de sistemas de portabilidad de gran escala sin interrupción de servicio y con la conservación total de los datos históricos. Estas implementaciones anteriores ofrecen una sólida base de las mejores prácticas, herramientas y modelos de gobierno que se aplicarán a la migración del SIPN de Costa Rica.

La migración se realizará a través de un plan estructurado por etapas diseñado para minimizar el riesgo, asegurar la transparencia y mantener las operaciones del SIPN ininterrumpidas:

1. Etapa de Planificación y Evaluación

TNS trabajará estrechamente con SUTEL, CTPN-M y todos los operadores para realizar la evaluación detallada del entorno existente del SIPN. Esto incluye análisis de las estructuras de datos, esquemas, interfaces y procesos operativos. Se desarrollará un plan de migración integral, que incluye reglas de mapeo de datos, criterios de validación, métricas de aceptación, líneas de tiempo y estrategias de mitigación de riesgos. Participarán todos los interesados a través de talleres y sesiones técnicas para garantizar la alineación y alistamiento.

2. Etapa de Extracción y Transformación de Datos

Los datos históricos del sistema legacy del SIPN se extraerán en forma segura y transformarán al formato compatible con TNPC. Esto incluye transacciones de portación, datos de enrutamiento, registros de NIP, registros de auditoría e histórico de procesos. La transformación de datos garantiza la alineación con los esquemas de NPCDB, a la vez que conserva las relaciones, marcas de tiempo y estados de las transacciones. Se realizarán actividades de limpieza y normalización de datos para garantizar la consistencia y precisión a lo largo de todos los conjuntos de datos.

3. Etapa de Carga y Migración Inicial de Datos

Se cargarán los datos transformados en NPCDB de TNPC mediante procesos de carga masiva controlada y validada. Esta etapa establece el conjunto de datos históricos completos dentro de TNPC para garantizar que todos los registros a partir de 2013 estén disponibles para consulta y reportería inmediata. Se realizarán verificaciones de conciliación de datos para confirmar que los datos migrados estén completos e íntegros.

4. Etapa de Ejecución y Sincronización en Paralelo

TNPC operará en paralelo el sistema existente del SIPN para garantizar la sincronización en tiempo real de todas las nuevas transacciones y actualizaciones. Los datos incrementales del sistema legacy se aplicarán

continuamente al TNPC para mantener alineación total entre ambos entornos. Esta etapa permite que los operadores y SUTEL validen el comportamiento del sistema, procesamiento de transacciones y consistencia de datos bajo condiciones operativas reales, que reduce significativamente el riesgo de migración.

5. Etapa de Pruebas y Validación

Se realizarán actividades de validación extensivas, que incluyen pruebas funcionales de todos los procesos como generación de NIP, prevalidación, cancelación de portación y retorno de número. La conciliación de datos entre los sistemas legacy y de TNPC confirmará 100 por ciento de exactitud. Las pruebas de aceptación del operador y la validación de SUTEL garantizarán que se cumplan todos los requerimientos regulatorios, operativos y de rendimiento previo a la entrada en producción.

6. Etapa de Corte y Entrada en Producción

Se ejecutará un corte controlado durante la ventana de mantenimiento acordada. Se realizará la sincronización final de los datos y todas las conexiones de los operadores harán la transición hacia TNPC. Se ejecutará el corte con estrategias de cero tiempo inactivo o implementación continua con mínimo tiempo inactivo acordado durante la ventana de mantenimiento para garantizar que cualquier impacto sobre el servicio estará controlado y dentro de los umbrales de los SLA. Inmediatamente después del corte, TNPC será la plataforma primaria del SIPN.

7. Etapa de Estabilización después de la Migración

Después de la entrada en producción, TNPC ingresará en la etapa de estabilización con monitoreo, validación y soportes mejorados. El monitoreo continuo del rendimiento, la verificación de datos y la rápida resolución de problemas garantizarán operaciones estables. Todas las transacciones históricas y en curso serán totalmente accesibles en NPCDB que cumplirá con los requerimientos de consultas, reportería y auditorías en tiempo real.

Toda la migración se realiza dentro de un marco de gobierno y gestión de proyecto estructurado conducido por TNS. Una Oficina de Gestión de Proyecto dedicada supervisará la planificación, ejecución, gestión de riesgos y comunicación con los interesados. El proyecto incluirá generación de informes de avance en forma regular, seguimiento de hitos y mecanismos de escalada para garantizar la entrega a tiempo y la transparencia. Este modelo de gobierno garantiza la alineación con SUTEL y CTNP-M durante todo el ciclo de vida de la migración.

Los elementos clave del enfoque de migración incluyen:

- Metodología probada validada a través de migraciones exitosas en Perú y Estados Unidos
- Preservación completa de datos históricos, que incluyen todas las transacciones, registros de enrutamiento y registros de auditoría
- Operación de sistema en paralelo y sincronización continua para eliminar el riesgo de la migración
- Pruebas de validación y aceptación integrales con los operadores y SUTEL
- Corte controlado para asegurar las operaciones ininterrumpidas del SIPN
- Sólido gobierno del proyecto con gestión de riesgos y participación de los interesados

A través de este plan de migración estructurado, probado y cuidadosamente dirigido, TNPC garantiza una **transmisión sin inconvenientes hacia la nueva plataforma del SIPN**, mantiene la continuidad total del servicio, preserva todos los datos históricos y entrega un sistema listo para el futuro, alineado con los requerimientos regulatorios y operativos de SUTEL.

2.24.1 *La totalidad de la información asociada a los procesos de portabilidad deberá estar disponible para consulta inmediata desde la misma plataforma WEB.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC garantiza que, **después de la migración y entrada en producción, toda la información relativa a los procesos de portabilidad estará disponible para consulta inmediata desde la misma plataforma web**, ofreciendo visibilidad y acceso en tiempo real a los operadores, SUTEL y los usuarios autorizados. Esta capacidad se posibilita a través de la integración de las interfaces web con la NPCDB centralizada, que actúa como fuente autorizada de todos los datos de transacciones, que incluyen tanto registros históricos migrados del sistema legacy como todos los procesos en curso del SIPN. Tan pronto ocurre cualquier evento dentro del ciclo de vida del SIPN, como generación de NIP, prevalidación, presentación de solicitud de portabilidad, aprobación, rechazo, activación, cancelación o retorno de número, los datos correspondientes quedan comprometidos en NPCDB y se ponen a disposición al instante para consulta, sin demora alguna.

La plataforma web ofrece acceso seguro basado en roles a esta información a través de GUI intuitivas y responsivas, que permite a los usuarios recuperar datos de transacciones usando múltiples criterios de búsqueda tales como MSISDN, ID de transacción, rol del operador, estado del proceso o rango de tiempo. Las consultas devuelven resultados en tiempo real que reflejan el estado actual de cada transacción, junto con el contexto histórico completo que incluye marcas de tiempo, intercambio de mensajes, resultados de validaciones y registros de auditoría. Esto garantiza que los usuarios puedan rastrear el ciclo de vida completo de cualquier proceso de portabilidad en cualquier etapa y da soporte al monitoreo operativo, detección y resolución de problemas, y supervisión regulatoria.

TNPC logra que esto esté inmediatamente disponible a través de una arquitectura de alto rendimiento, optimizada para acceso a datos en tiempo real. La plataforma web interactúa directamente con NPCDB o las capas de reportería optimizadas diseñadas para una rápida respuesta a la consulta, sin impacto en el rendimiento del procesamiento de transacciones. Los mecanismos de acceso a datos e indizado de avanzada aseguran que se puedan consultar incluso grandes conjuntos de datos en forma eficiente. Además, el sistema soporta tanto modelos de procesamiento síncrono como asíncrono para garantizar que las actualizaciones de las transacciones se vean reflejadas en la base de datos, tan pronto ocurren.

Todas las actividades de consulta son seguras, se registran y son auditable para garantizar un acceso controlado y trazable. La plataforma también soporta capacidades de reportería y exportación de datos que permite a los usuarios extraer la información relevante en los formatos estándar para análisis posterior. A través de este diseño, TNPC garantiza que toda la información de portabilidad sea accesible de inmediato, precisa y consistente después de la migración y entrada en producción, en pleno cumplimiento con el requerimiento de SUTEL de visibilidad de los procesos del SIPN en tiempo real.

2.25 *Contar con tres ambientes independientes: un ambiente de desarrollo, uno para pruebas de los operadores/proveedores/Sutel y el entorno de producción.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC se implementa en **tres ambientes lógicamente segregados, totalmente independientes**, a saber, Desarrollo, Pruebas y Producción, para garantizar la evolución controlada del sistema, validación confiable y operaciones ininterrumpidas del SIPN. Cada ambiente es aprovisionado con infraestructura dedicada, configuraciones de redes aisladas y almacenamiento de datos independientes para garantizar que las actividades en un ambiente no tengan impacto en los otros. Esta separación garantiza que las actividades de desarrollo y pruebas se puedan realizar en forma segura, a la vez que se mantiene la integridad y disponibilidad del sistema de producción.

El **ambiente de Desarrollo** se usa exclusivamente para diseño, configuración y actividades de mejoras, que incluye implementación de cambios regulatorios, nuevas prestaciones, actualizaciones de interfaces y mejoras de rendimiento. Este ambiente soporta la innovación continua y la evolución del sistema que permite a TNPC adaptarse a los requerimientos de SUTEL y a las mejores prácticas de la industria, sin afectar las operaciones en vivo.

El **ambiente de Pruebas** se pone a disposición de los operadores, proveedores y SUTEL para las actividades de validación y certificación. Replica la configuración de producción en la medida que sea necesario para realizar pruebas realistas, lo cual permite que los interesados puedan realizar la validación de las interfaces, pruebas de procesos punta a punta, pruebas de aceptación del usuario y pruebas de regresión para las actualizaciones del sistema. Este ambiente tiene un rol crítico para garantizar que todos los cambios sean cuidadosamente verificados y aprobados antes de entrar en producción.

El **ambiente de Producción** es un sistema operativo en vivo que soporta todos los procesos del SIPN, que incluyen generación de NIP, prevalidación, portación, cancelación, retorno de número, sincronización, reportería y monitoreo regulatorio. Está diseñado para alta disponibilidad, rendimiento y seguridad para garantizar la entrega continua del servicio a todos los interesados.

Todas las implementaciones y actualizaciones en los ambientes siguen un ciclo de vida estructurado. Primero se desarrollan los cambios en el ambiente de Desarrollo, se validan en el ambiente de Pruebas con la participación de los operadores y SUTEL; y luego se pasan a Producción. Las actualizaciones de producción se implementan con **estrategias de cero tiempo inactivo o implementación continua con mínimo tiempo inactivo acordado durante la ventana de mantenimiento** para garantizar que los servicios del SIPN están continuamente disponibles y que cualquier impacto sobre el servicio estará controlado y dentro de los umbrales acordados de los SLA.

A través de este enfoque estructurado de múltiples ambientes, TNPC garantiza la evolución controlada del sistema, validación robusta y entrega de servicio ininterrumpido, en pleno cumplimiento de los requerimientos de SUTEL para segregación de ambientes y confiabilidad operativa.

2.25.1 *Garantizar que el funcionamiento de los entornos de desarrollo y entornos para pruebas no generen afectación alguna y que sean transparentes para los usuarios finales, operadores/proveedores interconectados y la Sutel.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC está diseñada para garantizar el **funcionamiento de entornos de desarrollo, laboratorio y pruebas totalmente aislados del ambiente de producción**, para garantizar que ninguna actividad en estos ambientes pueda tener impacto en las operaciones en vivo del SIPN. Cada entorno se implementa en una **infraestructura separada, con segmentación de red independiente, controles de acceso distintivos y bases de datos dedicadas** para garantizar una total separación lógica y operativa. Esto evita cualquier interferencia con los procesos de producción, que incluyen generación de NIP, prevalidación, portación, sincronización y actividades de reportería; y así se mantiene el servicio ininterrumpido para los usuarios finales, operadores y SUTEL.

Desde la perspectiva operativa, TNPC aplica estrictos controles para asegurar que las **actividades de desarrollo y pruebas son transparentes para todos los interesados de producción**. Los datos de pruebas se segregan desde los datos de producción y cualquier uso de los conjuntos de datos como producción se anonimizan cuidadosamente o replican bajo condiciones controladas. Las interfaces utilizadas en los entornos de desarrollo y pruebas se configuran para solo comunicarse dentro de sus respectivos entornos para garantizar que ningún mensaje o transacción de prueba sea enrutado a los sistemas en vivo del operador. Del mismo modo, ninguna transacción de producción se procesa en los entornos de no producción para preservar la integridad y precisión de las operaciones en vivo del SIPN.

Además la plataforma asegura la transparencia a través de **puntos finales de acceso independientes, credenciales distintivas y URL específicas del entorno**, que permiten a los operadores, proveedores y

SUTEL diferenciar claramente entre entornos de desarrollo, pruebas y producción. Todas las actividades de pruebas, que incluyen pruebas de integración, pruebas de aceptación del usuario y validación de regresión, se realizan exclusivamente en el entorno de pruebas y los resultados son verificados antes de promover cualquier cambio a producción. La implementación de actualizaciones sigue un ciclo de vida controlado. Los cambios validados se introducen en producción usando estrategias de cero tiempo inactivo o implementación continua con mínimo tiempo inactivo acordado durante la ventana de mantenimiento, para garantizar que cualquier impacto sea controlado y dentro de los umbrales acordados de los SLA.

A través de este estricto aislamiento de entornos, manejo controlado de datos y enfoque de implementación disciplinada, TNPC garantiza que las actividades de desarrollo y pruebas sean completamente transparentes a los usuarios finales y todos los interesados, en pleno cumplimiento con el requerimiento de SUTEL para que las operaciones del SIPN no sean interrumpidas ni afectadas.

2.25.2 *En caso de que el SIPN sea aprovisionado en un centro de datos on-premise, deberá existir un entorno de contingencia totalmente funcional ubicado en un país distinto al principal. Este deberá asegurar la misma disponibilidad que el de producción.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Tal como se describe en la Sección 2.1, TNPC ofrece una arquitectura de contingencia totalmente resiliente, que garantiza que las operaciones del SIPN están continuamente disponibles incluso en caso de falla en un sitio o falla regional.

TNPC aprovecha la **arquitectura multirregional** para ofrecer redundancia geográfica incorporada. El entorno primario de producción se implementa en la región US-East de AWS, distribuida a lo largo de múltiples zonas de disponibilidad para garantizar resiliencia dentro de la región. Un entorno de recuperación ante desastres totalmente configurado se implementa en una región separada de AWS, como US-West, para garantizar separación geográfica a nivel regional. NPCDB, que está implementada con AWS Aurora, soporta replicación continua a lo largo de las regiones con sincronización casi en tiempo real para garantizar que todos los datos se encuentran consistentemente disponibles en ambas regiones. En caso de falla regional, TNPC puede hacer la transición de sus operaciones a la región secundaria con el Objetivo de Tiempo de Recuperación alineado con los compromisos de servicio y el Objetivo de Recuperación cerca de cero para asegurar que no se pierden datos críticos de transacciones.

En ambos modelos de implementación, el entorno de contingencia está diseñado para ofrecer **disponibilidad, rendimiento y seguridad equivalente al sistema de producción** a fin de garantizar que los servicios del SIPN permanecen ininterrumpidos bajo todos los escenarios de fallas. Los procedimientos de recuperación ante fallas se definen, prueban regularmente y soportan mediante sistemas de monitoreo y alertas a fin de permitir una transición rápida y controlada de los servicios. La activación del entorno de contingencia se realizará con estrategias de cero tiempo inactivo o implementación continua con mínimo tiempo inactivo acordado durante la ventana de mantenimiento para garantizar que cualquier impacto sobre el servicio estará controlado y dentro de los umbrales acordados de los SLA.

A través de esta arquitectura de contingencia geográficamente resiliente, TNPC asegura una **plataforma del SIPN robusta y geográficamente resiliente**, totalmente alineada con los requerimientos de SUTEL y consistente con la arquitectura de alta disponibilidad descrita en la Sección 2.1.

2.26 *Usar interfaces y protocolos de comunicación modernos, seguros, estandarizados y reconocidos por la industria de telecomunicaciones que se mantengan actualizados durante el periodo de prestación del servicio.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC está desarrollada sobre un **marco de comunicaciones interoperable, basado en estándares**, que usa interfaces y protocolos modernos, seguros y reconocidos por la industria durante todo el período de prestación del servicio. Todas las integraciones con los operadores, SUTEL y las plataformas regulatorias externas se implementan usando **SOAP (XML sobre HTTPS)**, en estricta alineación con el Manual de Interfaces y Procesos, complementadas con interfaces **REST (JSON sobre HTTPS)** para hacer espejo con los esquemas XML para compatibilidad futura. Este enfoque de doble interfaz garantiza la interoperabilidad sin inconvenientes con los sistemas existentes, a la vez que permite la modernización sin interrupciones.

Todas las comunicaciones son seguras con **HTTPS con TLS 1.2 o superior** y tienen el soporte de sólidos conjuntos de cifrado y autenticación en base a certificados. TNPC soporta **TLS mutuo, cuando sea requerido**, autenticación con llave API o basada en token para servicios REST y opciones de conectividad de VPN segura o dedicada para la integración con el operador. Para mensajería y entrega de NIP, TNPC usa **SMPP sobre canales seguros** para hacer interfaz con los SMSC de los operadores, a fin de garantizar una entrega confiable y segura. Los intercambios en base a archivos, que incluyen los archivos de difusión y sincronización, se realizan vía **SFTP seguro**, con opciones de autenticación en base a llave y listas permitidas de IP. Todas las interfaces son validadas contra los **esquemas WSDL y XSD** para garantizar cumplimiento estructural y semántico, y evitar el procesamiento de mensajes mal formados o no autorizados.

TNPC sigue un **enfoque de gestión de ciclo de vida y versiones** disciplinado para mantener los protocolos actualizados con las mejores prácticas de la industria. Esto incluye revisión y actualización periódicas de las versiones de TLS, conjuntos de cifrado, gestión de certificados, estándares de API y librerías de dependencias en respuesta a las pautas de seguridad y directivas regulatorias en constante evolución. La retrocompatibilidad se mantiene para proteger las integraciones existentes del operador, con políticas de versiones controladas y deprecación, a fin de garantizar una suave transición a las interfaces actualizadas. Las actualizaciones de interfaces y protocolos se prueban en los entornos de desarrollo y pruebas con la participación del operador y SUTEL y se implementan con estrategias de cero tiempo inactivo o implementación continua con mínimo tiempo inactivo acordado durante la ventana de mantenimiento para garantizar la continuidad de los servicios del SIPN.

Además, TNPC incorpora **controles de monitoreo y seguridad continuos** a lo largo de todos los canales de comunicación, incluyendo validación, limitación de velocidad, detección de anomalías y registro de auditoría de todas las interacciones entrantes y salientes. Esto garantiza la detección temprana de problemas, protección contra uso indebido y trazabilidad total para fines de auditoría.

A través de este enfoque integral, TNPC garantiza que todas las comunicaciones son **seguras, cumplen con los estándares y están listas para el futuro**, en pleno cumplimiento de los requerimientos de SUTEL; a la vez que ofrece un marco de integración robusto y adaptable durante todo el ciclo de vida del servicio.

2.27 *El adjudicatario deberá garantizar y proveer todos los certificados y demás elementos de seguridad para los sitios y servicios WEB (internos como externos) los cuales no implicarán costos adicionales. Asimismo, deberá contar con sistemas de monitoreo de su uso.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece y gestiona **todos los certificados y elementos de seguridad requeridos para los sitios web y servicios, tanto a nivel interno como externo**, como parte de la oferta de servicio

estándar y **sin ningún costo adicional** para SUTEL ni los operadores/proveedores. Esto incluye la gestión del ciclo de vida completo de los certificados digitales usados para comunicación HTTPS/TLS, autenticación TLS mutua, cuando sea requerido, seguridad de API, servicios SFTP e integraciones con sistemas seguros. Los certificados son emitidos por autoridades de certificación confiables, renovados con regularidad y son centralmente gestionados para garantizar la validez y cumplimiento continuo con los estándares de seguridad de la industria. TNPC también gestiona la generación, almacenamiento, rotación y revocación de claves mediante prácticas de gestión segura de claves para garantizar la protección contra los accesos no autorizados y que nada sea comprometido.

Todas las aplicaciones web, API e interfaces de sistemas se aseguran usando **TLS 1.2 o encriptación superior**, con sólidas configuraciones de cifrado y mecanismos de autenticación seguros. Los servicios internos son del mismo modo protegidos a través de canales de comunicación encriptados y segmentación controlada de la red. Los elementos de seguridad adicionales incluyen protección con Web Application Firewall, mecanismos de detección de intrusos, aplicación de controles de acceso y gestión de sesión segura. Estos controles garantizan que todos los componentes del SIPN, que incluyen las interfaces del operador, portales de SUTEL, sistemas de reportería y servicios web públicos, funcionan dentro de un entorno seguro y en cumplimiento.

Además de los controles de seguridad, TNPC incorpora **sistemas de monitoreo de uso** integrales, que rastrean y analizan continuamente el acceso al sistema, patrones de uso y comportamiento operativo. Las herramientas de monitoreo recolectan las métricas, registros y eventos en todos los componentes para permitir visibilidad en tiempo real del rendimiento del sistema, actividad del usuario y eventos de seguridad. Esto incluye seguimiento de acceso del usuario, uso de API, transferencia de archivos, intentos de autenticación e interacciones del sistema. Se generan alertas frente a comportamientos anormales, intentos de acceso no autorizado o anomalías de rendimiento para permitir una rápida respuesta y mitigación.

Todos los datos de monitoreo se correlacionan con los registros de transacciones y auditoría almacenados en NPCDB para ofrecer una vista completa de la actividad del sistema y permitir reportería y análisis detallados. Los tableros y reportes de monitoreo están a disposición de SUTEL y los interesados autorizados para dar soporte a la supervisión, verificación de cumplimiento y mejora continua. A través de este enfoque integrado, TNPC garantiza que todos los elementos y certificados de seguridad requeridos son totalmente gestionados, continuamente actualizados y tienen el soporte de sólidas capacidades de monitoreo; y entregan un entorno seguro, en cumplimiento y rentable del SIPN.

2.28 *Garantizar la confidencialidad, seguridad e integridad de la información en tránsito, procesada y almacenada.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC garantiza los más elevados estándares de **confidencialidad, seguridad e integridad de todos los datos en tránsito, durante el procesamiento y en reposo**, en plena alineación con los requerimientos regulatorios y las mejores prácticas de la industria. Los datos en tránsito entre los operadores, SUTEL, las plataformas externas y los servicios de TNPC están protegidos usando **HTTPS con TLS 1.2 o superior**, con sólidos conjuntos de cifrado y autenticación en base a certificados. Cuando sea requerido, se pueden implementar mecanismos de autenticación mutua para garantizar que ambas partes en la comunicación están verificadas. Todos los canales de comunicación, incluyendo interfaces SOAP XML, REST API, transferencia de archivos SFTP e integraciones con el gateway de SMS, son seguros para evitar interceptaciones, adulteración y acceso no autorizados.

Durante el procesamiento, TNPC aplica estrictos **controles de seguridad y mecanismos de validación a nivel de la aplicación** para garantizar que todos los datos sean manejados en forma segura y consistente. Se validan todos los mensajes entrantes y salientes contra los esquemas WSDL y XSD definidos para asegurar que sean estructural y semánticamente íntegros antes del procesamiento. El Procesador de Mensajes aplica reglas de negocio y condiciones de rechazo para evitar que datos inválidos o maliciosos ingresen al sistema. El acceso a datos durante el procesamiento queda restringido a través de autorización basada en roles para garantizar que solo los componentes y usuarios autorizados pueden interactuar con

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

información sensible. Todas las actividades de procesamiento se registran y son trazables conforme a los requerimientos de auditoría y cumplimiento.

Para los datos en reposo, toda la información almacenada dentro de NPCDB, que incluye datos de transacciones, registros de enrutamiento, datos de NIP, registros de auditoría y datos de reportería, está protegida usando **encriptación estándar de la industria como AES 256**. Se implementan prácticas de gestión de llaves seguras para control de las llaves de encriptación a fin de garantizar que solo los servicios autorizados puedan acceder a los datos encriptados. La integridad de los datos se asegura todavía más a través de mecanismos como sumas de verificación, reglas de validación y estructuras de registros inmutables para evitar modificaciones no autorizadas o corrupción de la información almacenada.

Además, TNPC incorpora un **marco de monitoreo de seguridad y detección de amenazas** integral que analiza continuamente la actividad del sistema a fin de detectar anomalías, intentos de acceso no autorizado o potenciales amenazas de seguridad. Se generan alertas para eventos sospechosos que permiten una investigación y respuesta inmediata. Todos los controles de seguridad son regularmente revisados y actualizados para estar alineados con los estándares de ciberseguridad y los escenarios de amenazas en constante evolución.

A través de este enfoque de seguridad de múltiples capas, TNPC asegura que todos los datos del SIPN se mantienen **confidenciales, seguros y precisos durante todo el ciclo de vida**, en pleno cumplimiento con los requerimientos de SUTEL y ofreciendo una plataforma confiable y resiliente para las operaciones de portabilidad numérica.

2.29 *Incorporar una funcionalidad de autenticación y autorización basadas en roles y perfiles para uso del SIPN.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece un **marco de autenticación y autorización basado en roles y perfiles** integral y seguro para garantizar que el acceso a las funcionalidades y datos del SIPN sea estrictamente controlado y esté alineado con las responsabilidades del usuario. Cada usuario, sistema o entidad externa que interactúa con TNPC es singularmente autenticada mediante credenciales seguras, con soporte para mecanismos robustos de autenticación y autenticación multifactorial para interfaces sensibles como SUTEL, operadores y organismos autorizados. Todos los accesos son a través de un modelo centralizado de identidad y gestión de acceso que aplica políticas de seguridad consistentes a lo largo de todos los componentes de la plataforma.

La autorización dentro de TNPC se implementa a través de una **estructura de control de acceso basada en roles granular**, donde se definen los roles y perfiles según las responsabilidades funcionales de cada grupo de interesados. Cada rol se asocia a permisos específicos que determinan las acciones permitidas y la visibilidad de los datos. Estos controles son consistentemente aplicados a lo largo de todos los canales de acceso, que incluyen interfaces GUI, integraciones SOAP XML, REST API, sistemas de reportería y mecanismos de acceso a archivos para garantizar que los usuarios solo pueden acceder a la información relevante para su rol.

La plataforma incorpora **autenticación multifactorial para todos los accesos de usuarios privilegiados y autenticados** a fin de mejorar la seguridad más allá de la verificación básica de credencial. TNPC soporta las aplicaciones de autenticador estándar de la industria como **Google Authenticator y Microsoft Authenticator**, con contraseñas de un solo uso basadas en el tiempo para verificación de inicio de sesión seguro. Esto garantiza que el acceso a las funciones y datos sensibles del SIPN esté protegido contra acceso no autorizado o credenciales comprometidas. Se puede aplicar la autenticación multifactorial en base al rol del usuario, sensibilidad del sistema o contexto del acceso, lo cual brinda flexibilidad a la vez que mantiene sólidos controles de seguridad.

Para la **GUI pública utilizada por los usuarios finales**, TNPC implementa un mecanismo de autenticación seguro en base a la **combinación de MSISDN y NIP**, donde el NIP sirve como factor de verificación de una

sola vez, vinculado a una solicitud de portabilidad específica. Este enfoque garantiza que solo el suscriptor asociado al número pueda acceder a la información del estado de la transacción. Se implementan protecciones adicionales como CAPTCHA, limitación de velocidad y controles de sesión para evitar el uso indebido o intentos de accesos automáticos a fin de garantizar acceso público seguro y controlado, sin requerir procesos de autenticación complejos.

Todas las actividades de autenticación y autorización se validan en tiempo real y se registran por completo, incluyendo identidad de usuario, rol, método de autenticación, marca de tiempo y acciones realizadas. Se bloquean y registran los intentos de acceso no autorizados conforme a los requerimientos de auditoría y monitoreo de seguridad. Las configuraciones de roles y perfiles se gestionan centralmente y son configurables para permitir que SUTEL defina o actualice las políticas de acceso cuando sea requerido, sin rediseño del sistema.

A través de un marco robusto que combina control basado en roles, autenticación multifactorial con uso de los autenticadores estándar de la industria y acceso seguro en base a NIP, TNPC garantiza que todos los accesos al SIPN sean seguros, controlados y estén totalmente alineados con los requerimientos regulatorios y de ciberseguridad.

2.30 *La ERPN seleccionada deberá proponer e implementar los mejores mecanismos de ciberseguridad para proteger la plataforma y garantizar la operación continua frente a ataques informáticos. Dicha propuesta será validada por el CTPN-M.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC implementará un **marco de ciberseguridad** integral y de múltiples capas, **diseñado para proteger las operaciones del SIPN y asegurar la disponibilidad continua del servicio incluso bajo escenarios de ataques adversos de IT**. Este marco está alineado con los estándares reconocidos a nivel internacional como ISO 27001, Marco de Seguridad de NIST y las mejores prácticas de la industria; y se presentará formalmente ante CPTN-M para su revisión y validación previo a la implementación. El enfoque propuesto combina controles de seguridad preventivos, detectivos y correctivos a lo largo de las capas de red, aplicación, datos y operativa a fin de garantizar un entorno resiliente y seguro del SIPN.

A nivel de la red, TNPC emplea una arquitectura de defensa en profundidad, que incorpora firewalls, segmentación de red, acceso VPN seguro y protección Web Application Firewall para proteger todos los puntos de entrada. Se implementan mecanismos de protección contra amenazas de avanzada, que incluye capacidades de detección y prevención de intrusión, a fin de identificar y mitigar tráfico malicioso e intentos de acceso no autorizado. También se implementan mecanismos de protección de Denegación de Servicio distribuidos para garantizar la continuidad del servicio durante escenarios de ataques de alto volumen.

A nivel de las capas de aplicación y datos, TNPC aplica sólidos controles de seguridad, que incluyen prácticas de codificación segura, validación de entrada contra esquemas WSDL y XSD, protección contra vulnerabilidades comunes como ataques de inyección y *cross site scripting*; y estricto control de acceso basado en roles. Se protegen los datos a través de encriptación en tránsito con TLS y encriptación en reposo con los algoritmos estándar de la industria. Los mecanismos de autenticación incluyen autenticación multifactorial para usuarios privilegiados y gestión de sesión segura para evitar acceso no autorizado.

Para garantizar operaciones continuas, TNPC integra las **capacidades de monitoreo en tiempo real, detección de amenazas y respuesta automática**. Las herramientas de monitoreo de seguridad analizan continuamente los registros del sistema, actividad del usuario y tráfico de red a fin de detectar anomalías y amenazas potenciales. Los procedimientos de alertas y respuesta automáticos permiten realizar una rápida contención y mitigación de las incidencias; y minimizan el impacto en las operaciones del SIPN. La plataforma también incorpora capacidades de redundancia y recuperación ante fallas para garantizar que los servicios son operativos incluso en caso de ataques específicos.

Los procesos de repuesta y recuperación ante incidencias se definen y alinean con las mejores prácticas, que incluyen rutas claras de escalado, procedimientos de comunicación y pasos de remediación. Las

evaluaciones regulares de vulnerabilidades, pruebas de penetración y auditorías de seguridad se realizan para identificar y abordar debilidades potenciales. Todos los hallazgos y acciones de mejora se documentan y comparten con CTPN-M, como parte del proceso de gobierno.

Toda la propuesta de ciberseguridad, que incluye arquitectura, controles, mecanismos de monitoreo y marco de respuesta ante incidencias, será formalmente documentada y presentada a CTPN-M para su validación. Esto garantiza transparencia, alineación con las expectativas regulatorias y mejora continua en base al retroalimentación de los interesados.

A través de esta estrategia de ciberseguridad integral y proactiva, TNPC garantiza que la plataforma del SIPN sea **segura, resiliente y continuamente operativa**, totalmente protegida contra ciberataques, a la vez que se mantiene la integridad y disponibilidad de los servicios de portabilidad numérica.

2.31 *Garantizar capacidad de integración simultánea con los operadores y proveedores actuales y escalabilidad sencilla, para nuevos participantes o la salida operativa de alguno(s), libre de costos por concepto de desarrollo e incorporación.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC está diseñada para soportar la **integración simultánea de todos los operadores y proveedores**, a la vez que posibilita el ingreso sin inconvenientes de nuevos participantes y la salida controlada de los existentes, sin requerir cambios de desarrollo ni incurrir en costos adicionales. Se logra esta capacidad a través de un **marco de integración en base a estándares y configurable**, que usa las interfaces SOAP XML sobre HTTPS y REST JSON sobre HTTPS para garantizar la compatibilidad con los sistemas de los operadores existentes y para simplificar la integración de nuevos participantes.

Para los operadores existentes, TNPC mantiene interfaces estables y retrocompatibles para garantizar la conectividad ininterrumpida y las operaciones continuas del SIPN. Los puntos finales de integración, credenciales, identificadores de enrutamiento y reglas de negocio para cada operador son gestionadas a través de estructuras de datos configurables dentro de NPCDB, que permite la implementación de cambios a través de la interfaz en lugar de con desarrollo de código. Esto asegura que todos los operadores pueden continuar interactuando con el sistema en forma simultánea, incluso cuando se introducen actualizaciones o mejoras.

Para los nuevos operadores o proveedores que ingresan al mercado, TNPC ofrece un proceso de ingreso mejorado que incluye configuración de perfiles del operador, asignación de números de enrutamiento, configuración de puntos finales de la interfaz, credenciales de seguridad y validación de conectividad a través del entorno de pruebas. Este proceso permite a los nuevos participantes integrarse en forma rápida y eficiente, sin impacto en los operadores existentes. Del mismo modo, cuando un operador sale del mercado, TNPC soporta la desactivación controlada de su configuración para garantizar que los datos de enrutamiento, registros históricos e integridad de las transacciones se conservan, a la vez que se retira la participación activa de los procesos en curso.

La arquitectura modular y la infraestructura escalable de la plataforma garantizan que el agregado o la eliminación de participantes no afecte el rendimiento ni estabilidad del sistema. Todos los cambios de integraciones se implementan con estrategias de cero tiempo inactivo o implementación continua con mínimo tiempo inactivo acordado durante la ventana de mantenimiento.

Cabe destacar que todas las capacidades de integración, actividades de ingreso, actualizaciones de configuración y prestaciones de escalabilidad se brindan como parte de la oferta de servicio de TNPC, **sin ningún desarrollo adicional ni costo para los operadores o proveedores**. Esto garantiza un modelo operativo transparente y predictivo, a la vez que soporta la evolución dinámica del mercado de telecomunicaciones en Costa Rica.

A través de este marco de integración flexible y listo para el futuro, TNPC garantiza que el SIPN pueda acomodar los participantes actuales y futuros sin inconvenientes, manteniendo la eficiencia operativa, cumplimiento regulatorio y rentabilidad en todo momento.

2.32 *Poner a disposición de los miembros del CTPN-M un repositorio de documentación actualizado con, al menos, la siguiente información: manual operativo, la arquitectura actual, diagramas de comunicaciones, entre otros, con perfiles de acceso acordes para cada miembro.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece un repositorio de documentación centralizado, seguro y continuamente actualizado, que se entrega como un portal basado en la web accesible para todos los miembros de CTPN-M, que asegura transparencia total, trazabilidad y alineación a lo largo de todos los interesados. Este repositorio actúa como la única fuente autorizada de toda la documentación del SIPN e incluye un conjunto integral de materiales específicos de TNPC como Manual Operativo, Manual de Interfaces y Procesos, Documentación de la Arquitectura del Sistema, Diagramas de Comunicación e Integración, Diagramas de Flujos de Procesos, Especificaciones de Flujos de Mensajes, Guías de las Interfaces API y SOAP, Documentación del Modelo de Datos y Esquemas de NPCDB, Documentación del Marco de Seguridad y Ciberseguridad, Guía de Reportería y Analítica, Guía del Administrador, Guía del Usuario para las Interfaces GUI, Procedimientos SFTP y de Sincronización, Guía de Integración de IVR y Gateway de SMS, Plan de Recuperación ante Desastres y Continuidad del Negocio y Procedimiento de Migración y Corte. Conjuntamente, estos documentos ofrecen una vista completa y detallada de las operaciones del SIPN, comportamiento del sistema y requerimientos de integración.

El marco de documentación sigue un **modelo estructurado de gobierno y control de versiones**, consistente con las mejores prácticas usadas en entornos regulados como Bélgica. A cada documento se le asigna un identificador de versión único y se mantiene con un histórico de revisiones completo, que incluyen número de versión, fecha de publicación, autor, estado de aprobación y descripción detallada del cambio. Se mantiene un registro de cambios formal para cada actualización a fin de garantizar que todas las modificaciones a procesos, interfaces, configuraciones o comportamiento del sistema son claramente documentadas y trazables. Todos los documentos se mantienen en inglés y español, se publican en formato PDF, con las revisiones claramente marcadas y se ponen a disposición antes de entrar en vigencia.

El acceso al repositorio se controla a través de **perfiles de acceso basado en roles** para garantizar que cada interesado visualiza solo la documentación relevante para su rol. Los operadores tienen acceso a las guías de integración, flujos de procesos, documentación de API y procedimientos operativos requeridos para la interacción del sistema; mientras que SUTEL tiene acceso completo a toda la documentación, incluso la arquitectura, marcos de seguridad, materiales relativos a auditorías y aplicaciones de gobierno. Se otorga acceso controlado adicional a los organismos o terceros autorizados, según sea requerido. Todos los accesos son seguros a través de mecanismos de inicio de sesión autenticada; y la actividad del usuario dentro del repositorio es totalmente registrada para fines de auditoría y cumplimiento.

El repositorio está diseñado para **uso fácil y eficiencia operativa**, con capacidades de navegación y búsqueda de avanzada que permite a los usuarios localizar rápidamente los documentos, diagramas y especificaciones relevantes. La documentación se presenta en forma estructurada y los formatos visuales garantizan claridad y usabilidad. Las actualizaciones se comunican proactivamente a todos los interesados a través de notificaciones para garantizar la alineación con los cambios y versiones del sistema. Las actualizaciones de documentación se sincronizan con las actualizaciones del sistema con estrategias de cero tiempo inactivo o implementación continua con mínimo tiempo inactivo acordado durante la ventana de mantenimiento, a fin de garantizar acceso ininterrumpido y consistencia en el comportamiento del sistema en vivo.

Además de la documentación básica, el repositorio incluye materiales operativos y de soporte como:

- **Procedimientos para Solicitudes de Proceso**, que describen los procesos de portación, flujos de mensajes, definiciones de temporizadores, interfaces del sistema y manejo de datos.
- **Especificaciones de Interfaces Externas**, que contemplan interfaces SOAP XML y REST para la integración del sistema.

- **Guía del Usuario Participante**, que ofrece instrucciones operativas para el uso del sistema, reportería y administración.
- **Manual de la Mesa de Ayuda**, que detalla los procesos de soporte, procedimientos de tiquetes y flujos de trabajo de escalada.
- **Guía de Planificación de la Red**, que resume la arquitectura del sistema, hardware y configuración de red.
- **Plan de Operaciones**, que define los procedimientos operativos diarios y las pautas de gestión del sistema.

El repositorio también incluye materiales de comunicaciones de actualización continua como:

- **Flashs de noticias**, que ofrecen actualizaciones de los cambios del sistema y anuncios importantes.
- **Cartas de Contenido de Versión**, que detallan las prestaciones entregadas, impactos y acciones requeridas.
- **Boletín de Atención al Cliente**, que ofrece actualizaciones sobre mantenimiento, problemas y asesoramientos sobre el sistema.

Este portal centralizado de documentación será accesible solo para los miembros autorizados de CTPN-M para garantizar la distribución controlada y el acceso seguro a todos los materiales.

A través de este marco de documentación integral, basado en roles y con control de versiones, TNPC garantiza que todos los interesados pueden acceder a **información precisa, actual y totalmente trazable**, con soporte eficiente de las operaciones, integración sin inconvenientes y un fuerte gobierno de la plataforma del SIPN en pleno cumplimiento con los requerimientos de SUTEL.

- 2.33** *La ERP seleccionada deberá diseñar de manera detallada el sistema de comunicación con los operadores/proveedores y Sutel para el sistema principal, los de respaldo (cuando corresponda) y de pruebas con el fin de garantizar una adecuada infraestructura de telecomunicaciones que asegure un óptimo desempeño, seguridad, confidencialidad y una alta disponibilidad.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS diseñará e implementará un **marco de comunicación integral, seguro y de alto rendimiento** que permita la interacción sin inconvenientes entre la plataforma de TNPC, los operadores, proveedores y SUTEL a lo largo del **sistema principal de producción, sistemas de soporte y entornos de pruebas**. Esta arquitectura de comunicación está diseñada para garantizar un óptimo rendimiento, sólida seguridad, confidencialidad de datos y alta disponibilidad, totalmente alineado con los requerimientos de SUTEL y las mejores prácticas de la industria.

El sistema de comunicación se basa en una arquitectura de múltiples capas que soporta interfaces estandarizadas como **SOAP XML sobre HTTPS y REST JSON sobre HTTPS** para intercambios transaccionales, junto con **SFTP** para sincronización en base a archivos y operaciones de difusión. Las opciones de conectividad incluyen túneles de VPN segura, enlaces de comunicaciones dedicadas y accesos a internet basado en HTTPS para ofrecer flexibilidad y, a la vez, mantener estrictos controles de seguridad. La interfaz de cada operador y SUTEL se configura con puntos finales dedicados, credenciales de autenticación y reglas de enrutamiento para garantizar una comunicación segura y confiable con la plataforma de TNPC.

Para el **sistema principal de producción**, la infraestructura de comunicación está diseñada con redundancia y balanceo de carga a lo largo de múltiples rutas de red y puntos finales para asegurar la disponibilidad continua y la resiliencia contra fallas. Todos los canales de comunicación son seguros y usan

encriptación TLS, con soporte de autenticación mutua, cuando sea requerido, para garantizar la confidencialidad e integridad de los datos intercambiados. La segmentación de red y los controles de firewall se implementan para aislar los componentes críticos y evitar accesos no autorizados.

El **sistema de soporte**, que incluye mesa de ayuda, monitoreo e interfaces de mantenimiento, está integrado al marco de comunicación con controles de acceso seguro y conectividad en tiempo real. Esto permite la gestión eficiente de incidencias, detección y resolución de problemas y coordinación entre los equipos de soporte de los operadores, SUTEL y ERPN. Los canales de comunicación para soporte incluyen sistemas de tiquetes, API seguras, correo electrónico y comunicación de voz; todos alineados con los requerimientos operativos.

El **sistema de comunicación del entorno de pruebas** está diseñado para replicar la conectividad de producción, al tiempo que se mantiene totalmente aislado para evitar interferencias con las operaciones en vivo. Los operadores y SUTEL se pueden conectar al entorno de pruebas usando los mismos protocolos e interfaces que producción para posibilitar actividades realistas de validación, ingreso y certificación. Los puntos finales, credenciales y configuraciones de red separadas aseguran una clara diferenciación entre los entornos y evitan filtración de datos entre entornos.

Toda la infraestructura de documentación es continuamente monitoreada para garantizar el rendimiento, disponibilidad y seguridad. Métricas como latencia, producción, tasas de errores y salud de la conexión se rastrean en tiempo real con alertas automáticas en caso de anomalías. La arquitectura soporta escalabilidad para acomodar volúmenes crecientes de transacciones y el ingreso de nuevos operadores, sin impacto en el rendimiento.

Todos los diseños, configuraciones y diagramas de comunicación serán documentados en detalle y puestos a disposición de CPN-M y SUTEL a través del repositorio de documentación. Se implementan actualizaciones a la infraestructura de comunicación con estrategias de implementación en forma continua o con tiempo inactivo cero durante la ventana de mantenimiento, que asegura que las mejoras o cambios no interrumpen las operaciones del SIPN.

A través de este diseño de sistema de comunicación robusto y flexible, TNPC garantiza una infraestructura de telecomunicaciones segura, de alto rendimiento y altamente disponible, que admite todas las actividades operativas, de soporte y pruebas, en pleno cumplimiento con los requerimientos de SUTEL para la conectividad e integración del SIPN.

2.34 *El oferente debe proveer todos los equipos de red y datos necesarios en el extremo del SIPN, para la implementación de la interconexión con los operadores de acuerdo con los medios físicos soportados.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS ofrecerá toda la **infraestructura de red, componentes de conectividad y datos de configuración en el extremo del SIPN**, requeridos para permitir la interconexión segura y confiable con los operadores y SUTEL conforme a todas las opciones de conectividad física aprobadas. La solución de TNPC está diseñada para operar dentro de la arquitectura segura y altamente disponible, en la nube de AWS. Todos los elementos de red necesarios en el extremo de la ERPN están totalmente aprovisionados, configurados y gestionados como parte del servicio, sin requerir ninguna inversión adicional por parte de los operadores.

TNPC está alojado en un entorno seguro de AWS con una Nube Privada Virtual dedicada, subredes segmentadas, balanceadores de carga y gateways de red. TNS brinda todos los componentes de red basados en la nube requeridos que incluyen puntos finales de ingreso seguros, protecciones de firewall, configuraciones de enrutamiento y marcos de conectividad para soporte de la integración con los operadores a través de túneles VPN, conexiones de internet seguras o enlaces dedicados, cuando corresponda. A cada operador se aprovisiona con puntos finales de conexiones dedicadas, credenciales y configuraciones de enrutamiento para garantizar canales de comunicación seguros y aislados. La infraestructura en la red

soporta alta disponibilidad y redundancia a través de múltiples zonas de disponibilidad y rutas de red para garantizar conectividad ininterrumpida.

TNPC asegura que todas las configuraciones de red, esquemas de direcciones, reglas de enrutamiento y políticas de seguridad sean definidas y mantenidas a nivel central. El sistema soporta protocolos e interfaces estandarizados para garantizar la compatibilidad con los sistemas del operador y permitir una integración sin inconvenientes. Todas las interacciones de la red se monitorean en tiempo real, con métricas de rendimiento y alertas para garantizar una conectividad óptima y resolución rápida de cualquier problema.

A través de este enfoque integral, TNPC asegura que todas las capacidades de infraestructura de red y conectividad requeridas sean totalmente aprovisionadas en el extremo del SIPN para posibilitar una interconexión segura, confiable y de alto rendimiento con todos los operadores y SUTEL, en pleno cumplimiento de los requerimientos del pliego de condiciones.

2.35 *Monitorear y garantizar la operación del SIPN de manera continua y según los acuerdos de nivel de servicio suscritos (SLAs).*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece un marco integral para **monitorear, medir y garantizar el funcionamiento continuo del SIPN en estricta alineación con los Acuerdos de nivel de servicio convenidos**. El monitoreo continuo se implementa a lo largo de todas las capas del sistema, que incluyen procesamiento de aplicaciones, rendimiento de bases de datos, conectividad de red, interfaces de integración y canales de acceso del usuario para garantizar una visibilidad completa de la salud del sistema y estado operativo en todo momento.

TNPC aprovecha las herramientas de monitoreo avanzado como AWS CloudWatch para recolectar métricas, registros y eventos de todos los componentes de la plataforma en tiempo real. Estos incluyen tasas de procesamiento de transacciones, producción de mensajes, profundidad de cola, tiempos de respuesta, tasas de errores, disponibilidad de interfaces y utilización de infraestructura. El sistema de monitoreo está configurado con umbrales alineados con los SLA para permitir la detección automática de las desviaciones de los niveles de rendimiento esperados. Cuando se viola un umbral, se generan alertas de inmediato y se enrutan al Centro de Operaciones de Red para una rápida respuesta y resolución.

La plataforma incluye capacidades de monitoreo y reportería de SLA, donde todos los indicadores de SLA, que incluyen disponibilidad del sistema, temporizadores de procesos, rendimiento en la entrega de NIP, disponibilidad del IVR y tiempo de respuesta de soporte, se miden y registran en forma continua. Estas métricas se almacenan en NPCDB y se correlacionan con los datos de la transacción para ofrecer cálculos de SLA exactos y auditables. TNPC brinda tableros y reportes detallados en tiempo real a SUTEL y los operadores para brindar una visibilidad continua del cumplimiento de los SLA y del rendimiento del sistema.

Para asegurar un funcionamiento continuo, TNPC combina controles de monitoreo con controles operativos proactivos, que incluyen escalada automática, mecanismos de recuperación ante fallas, lógica de reintento y procesos de recuperación de transacciones. En caso de anomalías o incidencias, se ejecutan los procedimientos de respuestas predefinidas para restablecer las operaciones normales dentro de los límites de los SLA. Se toman medidas preventivas, como planificación de capacidad, ajuste de rendimiento y verificaciones de la salud del sistema, en forma regular, para evitar potenciales violaciones de SLA.

Todas las actividades de monitoreo y gestión de SLA se realizan bajo un modelo operativo 24x7, con la supervisión continua de los equipos de soporte de TNS. Los reportes sobre el rendimiento de los SLA se generan y comparten periódicamente, tal como sea requerido, y se analiza cualquier desviación e implementan las acciones correctivas o preventivas.

A través de este marco de monitoreo integrado y aseguramiento de SLA, TNPC garantiza que el SIPN funciona en forma continua, confiable y en pleno cumplimiento con los niveles de servicio convenidos, brindando confianza a SUTEL y todos los interesados en el rendimiento y disponibilidad de la plataforma.

2.35.1 *La ERP seleccionada deberá tener herramientas de monitoreo en tiempo real de manera que garantice el funcionamiento continuo y lógico del SIPN y acorde con los acuerdos de nivel de servicio que se suscriban.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC incorpora **herramientas de monitoreo y capacidades de observación en tiempo real** para garantizar el funcionamiento continuo, confiable y lógicamente consistente del SIPN, en total alineación con los acuerdos de nivel de servicio que serán establecidos. El monitoreo se implementa en todas las capas de la plataforma, que incluyen procesamiento de aplicaciones, rendimiento de bases de datos, conectividad de red, brindando una completa visibilidad punta a punta del comportamiento y salud operativa del sistema.

TNPC utiliza soluciones de monitoreo de grado empresarial como AWS CloudWatch para recolectar y analizar las métricas, registros y eventos en forma continua. Esto incluye producción de transacciones, latencia en el procesamiento de mensajes, profundidad de cola, tiempos de respuesta de la interfaz, tasas de errores, utilización de los recursos del sistema y disponibilidad de componentes críticos tales como Procesamiento de Mensajes, Procesador de Temporizadores, Gateway de SMS, IVR y puntos finales de integración con los sistemas de los operadores y SUTEL. Todos los parámetros monitoreados se mapean directamente en los indicadores de SLA para permitir la verificación continua del cumplimiento con los compromisos de rendimiento y disponibilidad.

Además del monitoreo técnico, TPNC ofrece **monitoreo de proceso lógico** para garantizar que los flujos de trabajo del SIPN se ejecutan correcta y consistentemente. La plataforma rastrea los estados de la transacción en tiempo real dentro de NPCDB para verificar la secuenciación correcta de los eventos como generación de NIP, prevalidación, procesamiento de solicitud de portabilidad, manejo de respuesta del donante, activación y sincronización. Cualquier desviación de los flujos de procesos esperados, mensajes faltantes o violaciones de temporizadores se detecta y marca de inmediato. El Procesador de Temporizadores aplica los tiempos de los SLA y genera alertas o acciones automáticas cuando se exceden los umbrales para garantizar que todos los procesos cumplan con los requerimientos regulatorios.

Se proporcionan interfaces de tableros y monitoreo en tiempo real a SUTEL y los usuarios autorizados para ofrecerles visibilidad en el rendimiento del sistema, estado de los procesos, cumplimiento de SLA y métricas operativas. Se generan alertas automáticas ante cualquier anomalía, degradación de rendimiento o violaciones potenciales de SLA para permitir una respuesta y resolución rápida de los equipos operativos. Todos los datos de monitoreo se correlacionan con los registros de transacciones almacenados en NPCDB para garantizar trazabilidad total y en respaldo de la reportería detallada y análisis de auditoría.

Para garantizar el funcionamiento continuo, TNPC integra el monitoreo con los mecanismos de respuesta automática tal como acciones de escalada, procesos de recuperación ante fallas, lógica de reintento y procedimientos de escala de incidencias. Estas capacidades aseguran que cualquier interrupción sea rápidamente contenida y resuelta dentro de los límites de los SLA. El monitoreo y las actualizaciones de las configuraciones de monitoreo se implementan con estrategias de implementación en forma continua o con tiempo inactivo cero durante la ventana de mantenimiento, que asegura la visibilidad y funcionamiento del sistema en forma ininterrumpida.

A través de este marco de monitoreo integrado en tiempo real, TNPC garantiza que el SIPN funciona en forma continua, confiable y en pleno cumplimiento con los requerimientos de los SLA, brindando confianza a SUTEL y todos los interesados en la integridad y el rendimiento operativo de la plataforma.

2.35.2 Proporcionar mensualmente indicadores de desempeño y disponibilidad.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece **indicadores de desempeño y disponibilidad mensuales** para permitir que SUTEL y todos los interesados monitoreen las operaciones del SIPN contra los acuerdos de nivel de servicio convenidos. Estos indicadores surgen de los datos de monitoreo y registros de transacciones en tiempo real almacenados en NPCDB para garantizar la exactitud, consistencia y trazabilidad total para fines de auditoría y regulatorios.

Los indicadores de desempeño mensuales incluyen métricas detalladas sobre el procesamiento de transacciones como generación y entrega de NIP, tiempos de respuesta de prevalidación, tasas de éxito y fracaso de portaciones, procesamiento de cancelaciones y retornos, actividades de sincronización y producción del sistema. Cada métrica se mide contra los umbrales definidos de los SLA para brindar clara visibilidad de la eficiencia del sistema y el desempeño operativo. La plataforma también incluye análisis detallado de los escenarios de rechazo, demoras de procesamiento y tiempos de respuesta para permitir que SUTEL identifique las tendencias y para asegurar el cumplimiento a lo largo de todos los operadores.

Los indicadores de disponibilidad se calculan en base al tiempo en línea del sistema, al medir el tiempo operativo total contra el tiempo inactivo registrado durante un período de reporte. TNPC ofrece un desglose completo de las métricas de disponibilidad, que incluyen duración, frecuencia y causa principal de cualquier interrupción de servicio y excluyen las ventanas de mantenimiento acordadas y los eventos de fuerza mayor. Estos indicadores cubren los componentes críticos del sistema, que incluyen interfaces web, servicios de integración, operaciones de bases de datos y canales de comunicación, para asegurar una visión holística de la disponibilidad del SIPN.

Todos los indicadores se presentan a través de **reportes mensuales y tableros en tiempo real estructurados** accesibles a través de la GUI de Reportería de TNPC. Los reportes se pueden exportar a los formatos estándar tales como XLSX y CSV y se entregan a SUTEL y los operadores/proveedores conforme a los cronogramas convenidos. Además, se mantienen tendencias históricas para permitir la comparación entre períodos de reporte y dar soporte al análisis de desempeño a largo plazo.

A través de este marco de reportería estructurado, TNPC asegura que SUTEL recibe conocimiento claro, exacto y accionable sobre el desempeño y la disponibilidad del SIPN, brindado soporte total al monitoreo de SLA, supervisión regulatoria y mejora continua de la plataforma.

2.35.3 Generar y comunicar a los operadores/proveedores y la Sutel, de manera inmediata, por múltiples medios (correo electrónico, teléfono, aplicaciones de mensajería instantánea) de alertas ante eventos críticos. Simultáneamente, en caso de que se trate de un inconveniente atribuible a la ERPN, deberá iniciar los procesos de corrección que resulten pertinentes. Para el caso de errores atribuibles a los operadores, deberá dar seguimiento a la situación hasta que sea solventada.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece un **marco de generación de alertas y gestión de incidencias en tiempo real** para garantizar que todos los eventos críticos son detectados, comunicados y resueltos de inmediato en forma controlada y a tiempo. El sistema continuamente monitorea todos los componentes, que incluyen procesamiento de transacciones, interfaces de integración, operaciones de bases de datos, conectividad de red, Gateway de SMS, servicios de IVR y procesos de sincronización. Cuando se detecta un evento crítico o anomalía, la plataforma automáticamente genera alertas y las comunica a los operadores, proveedores y SUTEL a través de múltiples canales, que incluyen **correo electrónico, notificaciones telefónica a través**

de un número de soporte en Costa Rica y aplicaciones de mensajería instantánea, tal como sea convenido con los interesados.

La generación de alertas es totalmente configurable en base a los niveles de severidad para garantizar que las incidencias de alta prioridad como interrupciones de servicio, violaciones de SLA, fallas de integración o comportamiento anormal de la transacción se escalan de inmediato. Cada alerta incluye información detallada como naturaleza del problema, componentes afectados, transacciones impactadas, marcas de tiempo y datos iniciales del diagnóstico para permitir que los interesados entiendan y respondan rápido ante la situación.

En paralelo con la comunicación de las alertas, TNPC inicia los **procesos de respuesta y resolución de incidencias** adecuados. Para incidencias atribuibles a la plataforma de ERP, el equipo de soporte de TNS inicia las actividades de investigación y remediación de inmediato, siguiendo los procedimientos de gestión de incidencias definidos. Estos incluyen análisis de causa principal, implementación de acciones correctivas y monitoreo continuo hasta que el problema sea totalmente resuelto para garantizar el restablecimiento del servicio dentro de los marcos de tiempo convenidos de los SLA.

Para las incidencias atribuibles a los operadores o sistemas externos, TNPC rastrea el problema hasta su resolución, en comunicación con las partes afectadas. La plataforma registra todos los eventos, comunicaciones y acciones relativas en el sistema de gestión de incidencias para garantizar la trazabilidad y responsabilidad totales. Se brinda soporte a los operadores mediante la coordinación, diagnóstico y orientación para resolver el problema, al tiempo que se asegura que los procesos del SIPN continúen funcionando tal como se espera.

Todos los eventos, alertas y actividades de resolución críticas se registran y ponen a disposición para fines de reportería y auditoría. A través de este marco integrado de generación de alertas y gestión de incidencias, TNPC asegura la detección rápida, comunicación efectiva y resolución a tiempo de todos los eventos críticos, mantiene el funcionamiento continuo del SIPN y cumple totalmente con los requerimientos de SUTEL.

- 2.36** *Los datos contenidos dentro del SIPN serán propiedad de Sutel y de los operadores y proveedores miembros del CTPN-M involucrados en cada proceso de portabilidad (donante-receptor), por lo que la ERP seleccionada deberá respetar todos los derechos de propiedad correspondientes.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS reconoce y respeta totalmente que todos los datos contenidos en el SIPN, que incluyen toda la información relativa a los procesos de portabilidad numérica, son **propiedad exclusiva de SUTEL y de los operadores y proveedores que son miembros de CTPN-M involucrados en cada transacción**, ya sea como donante o receptor. La plataforma de TNPC está diseñada y funciona bajo un estricto modelo de gobierno de datos que garantiza que todos los derechos de propiedad sean totalmente protegidos, aplicados y preservados durante todo el ciclo de vida del servicio.

TNPC actúa solamente como **procesador y custodio confiable de los datos**, que mantiene y gestiona los datos en nombre de SUTEL y los operadores participantes, sin afirmar ningún derecho de propiedad. Todos los datos almacenados en NPCDB, que incluyen registros de transacciones, información de enrutamiento, datos del NIP, registros de auditoría y datos de reportería, se manejan conforme a las obligaciones contractual y regulatoriamente definidas. TNS no usará, divulgará, compartirá ni procesará estos datos para fines que no sean el funcionamiento de los servicios del SIPN, tal como sea autorizado por SUTEL y CPTN-M.

El acceso a los datos queda estrictamente controlado a través de autorización basada en roles para garantizar que los operadores solo pueden acceder a la información relativa a sus propias transacciones, al tiempo que SUTEL tiene visibilidad total para supervisión regulatoria. La confidencialidad e integridad de los datos se protegen mediante encriptación, controles de acceso seguro y mecanismos de registros de

auditoría para garantizar que el uso de todos los datos sea transparente y trazable. Todas las interacciones con datos quedan registradas para permitir la verificación del cumplimiento con los derechos de propiedad y los requerimientos regulatorios.

Además, TNPC asegura que todos los datos sean mantenidos de manera de brindar soporte a la **portabilidad, accesibilidad y transferencia totales** para permitir que SUTEL conserve el control total sobre los datos en todo momento. Al finalizar el período de contratación, todos los datos serán entregados a SUTEL de manera segura, en los formatos convenidos, usando mecanismos abiertos y no propietarios, a fin de garantizar que no exista ninguna dependencia con los sistemas o tecnologías de TNS para tener acceso continuo.

A través de la estricta adhesión a los principios de titularidad de los datos, acceso controlado y prácticas de gestión segura de datos, TNPC asegura pleno cumplimiento con los requerimientos de SUTEL y garantiza que todos los derechos de propiedad asociados a los datos del SIPN serán respetados y protegidos en todo momento.

2.36.1 *Los datos asociados a los procesos de portabilidad numérica deberán estar cifrados y garantizar la integridad de la información para evitar accesos no autorizados.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC asegura que todos los datos asociados a los procesos de portabilidad numérica sean **encriptados y protegidos, en forma segura, para mantener la confidencialidad, integridad y resistencia al acceso no autorizado** durante todo el ciclo de vida. Esto incluye datos en tránsito entre operadores, SUTEL y TNPC, datos que están siendo procesados dentro de la plataforma; y datos almacenados en NPCDB y sistemas asociados.

Todas las comunicaciones entre los componentes del sistema y partes externas son seguros, con **HTTPS con TLS 1.2 o superior**, para garantizar que los datos transmitidos por las redes no se pueden interceptar ni alterar. Para las transferencias de archivos como datos de difusión y sincronización, TNPC usa protocolos seguros como SFTP con encriptación activada. Las interfaces de integración, que incluyen SOAP XML y REST API, están protegidas a través de canales encriptados y acceso autenticado para garantizar que solo los sistemas autorizados pueden intercambiar datos.

Los datos almacenados en TNPC, que incluyen registros de transacciones, información de enrutamiento, datos de NIP, registros de auditoría y datos de reportería, están protegidos con encriptación estándar de la industria tal como **encriptación AES 256 en reposo o las últimas técnicas de encriptación modernas**. Las llaves de encriptación se gestionan en forma segura a través de procesos de gestión controlada de llaves para garantizar que el acceso a datos encriptados queda estrictamente limitado a los componentes y servicios de sistemas autorizados. Además de la encriptación, TNPC aplica sólidos mecanismos de control de acceso para asegurar que solo los usuarios o sistemas autenticados y autorizados puedan acceder a los datos.

Para garantizar la integridad de la información, TNPC aplica múltiples mecanismos de validación y protección que incluyen validación de mensajes contra esquemas WSDL y XSD, verificación de sumas y procesamiento controlado de transacciones. Todos los cambios de datos se registran como nuevas entradas inmutables en NPCDB para evitar modificación o borrado no autorizado de registros. Los registros de auditoría se mantienen en formato resistente a adulteración, siguiendo la trazabilidad total de todas las interacciones de datos; y asegurando que cualquier anomalía se puede detectar e investigar.

A través de este enfoque de múltiples capas que combina encriptación, comunicaciones seguras, control de acceso y validación de integridad, TNPC asegura que todos los datos de portabilidad estén protegidos contra acceso no autorizado, adulteración o pérdida, en pleno cumplimiento de los requerimientos de SUTEL para operaciones seguras y confiable del SIPN.

2.36.2 *Los datos contenidos en la solución no deberán ser utilizados, vendidos, prestados, alquilados, transferidos ni accedidos por partes no autorizadas por la Sutel y el CTPN-M.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS garantiza estrictamente que **todos los datos contenidos en la solución del SIPN se usan exclusivamente para el funcionamiento y gestión de los servicios de portabilidad numérica, tal como autoriza SUTEL y CTPN-M** y que nunca serán utilizados, vendidos, prestados, alquilados, transferidos ni accedidos por partes no autorizadas. La plataforma de TNPC funciona bajo un **marco de gobierno y cumplimiento de datos** claramente definido, donde los datos se tratan como confidenciales y se manejan solamente conforme a los requerimientos regulatorios y las obligaciones contractuales.

TNPC actúa estrictamente como **procesador y custodio de los datos**, que mantiene y gestiona los datos del SIPN en nombre de SUTEL y los operadores participantes, sin afirmar ningún derecho de propiedad ni uso independiente. El acceso a los datos está estrechamente controlado a través de mecanismos de autorización basados en roles que garantizan que solo las entidades autorizadas puedan acceder a conjuntos de datos específicos dentro de su alcance permitido. Los operadores quedan limitados a acceder a los datos de sus propias transacciones, mientras que SUTEL tiene visibilidad total para fines de supervisión regulatoria. No se permite el acceso de ningún tercero, salvo sea explícitamente autorizado por SUTEL y CTPN-M; y todos dichos accesos estarán regidos por estrictos controles de seguridad y requerimientos de auditoría.

Para aplicar estas restricciones, TNPC implementa **mecanismos de seguridad y control de acceso** integrales, que incluyen autenticación fuerte, encriptación de datos en tránsito y en reposo; y el monitoreo continuo de todas las interacciones del sistema. Todos los accesos a datos se registran para trazabilidad total, que incluyen identidad del usuario, marcas de tiempo y actividad realizada para garantizar la responsabilidad y auditoría totales. Cualquier intento de acceso no autorizado se detecta, bloquea y reporta a través de los sistemas de monitoreo y generación de alertas de la plataforma.

Además, se establecen protecciones contractuales y operativas para garantizar el cumplimiento con las restricciones de uso de datos. Estas incluyen estrictas obligaciones de no divulgación, procedimientos de manejo controlado de datos y procesos de gobierno definidos para aprobación y monitoreo del acceso a datos. Los datos del SIPN nunca serán utilizados para fines comerciales, analíticos o externos, más allá de aquellos explícitamente autorizados por SUTEL.

A través de este marco integral, TNPC garantiza que todos los datos del SIPN están **totalmente protegidos, son confidenciales y se utilizan solo para el fin regulatorio de destino**, lo cual mantiene la confianza, cumplimiento e integridad de los mismos en todo el ecosistema de la portabilidad numérica.

2.36.3 *La ERPN seleccionada deberá notificar, al menos por todos los medios de notificación disponibles, de manera inmediata a la Sutel y al CTPN-M cualquier incidente de seguridad que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de los datos personales, indicando las medidas correctivas y preventivas adoptadas.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC incorpora un **marco de gestión y notificación de incidencias de seguridad** robusto para garantizar que cualquier evento que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de los datos personales sea detectado, accedido y comunicado, de inmediato, a SUTEL y CTPN-M. Las herramientas de monitoreo continuo analizan la actividad del sistema, patrones de acceso y eventos de seguridad en tiempo real para permitir la rápida identificación de anomalías, intentos de acceso no autorizado o violaciones potenciales que afecten las operaciones del SIPN.

Al detectar una incidencia de seguridad, TNPC inicia un **proceso de respuesta ante incidencia** estructurado, que incluye la clasificación de la severidad, evaluación del impacto y acciones de contención

inmediata. En simultáneo, se notifica a SUTEL y CTPN-M a través de los canales de comunicación convenidos tales como correo electrónico, teléfono y plataformas de mensajería seguras para garantizar la toma de conciencia inmediata de la situación. Las notificaciones incluyen información detallada sobre la naturaleza de la incidencia, sistemas o datos afectados, impacto potencial y las acciones tomadas para contener y mitigar el problema.

TNPC asegura que las **medidas correctivas y preventivas sean claramente definidas y comunicadas** como parte del proceso de manejo de incidencias. Las acciones correctivas pueden incluir aislamiento del sistema, restricción de acceso, parches o cambios de configuración, al tiempo que las medidas preventivas pueden implicar el fortalecimiento de los controles de seguridad, actualización de políticas o implementación de capacidades de monitoreo adicional. Todos los detalles de las incidencias, acciones tomadas y resultados se documentan y almacenan en el sistema para fines de auditoría y cumplimiento.

Después de la resolución, TNPC realiza un **análisis de causa principal y una revisión posterior a la incidencia** para brindar a SUTEL y CTPN-M un reporte integral que incluye hallazgos, lecciones aprendidas y recomendaciones para evitar la repetición. Este enfoque de mejora continua asegura que la plataforma evoluciona para abordar las amenazas que surgen y que mantiene los más elevados niveles de seguridad.

A través de este marco de gestión de incidencias proactivo y transparente, TNPC asegura una comunicación inmediata, respuesta efectiva y protección continua de los datos personales, en pleno cumplimiento de los requerimientos de SUTEL para la gestión y notificación de incidencias de seguridad.

2.37 *Garantizar que, al finalizar el período de contratación, toda la información, bases de datos y documentación asociadas a los procesos de portación sean entregadas de forma segura y confidencial, utilizando mecanismos de cifrado abiertos y de uso libre, de manera que no se requiera el pago de licencias, claves propietarias ni costos adicionales para su acceso, descifrado o utilización.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Al final del período de contratación, TNS garantizará la transferencia completa, segura y confidencial de toda la información, bases de datos y documentación del SIPN a SUTEL, preservando la integridad de los datos, accesibilidad y derechos de propiedad en forma completa. La plataforma de TNPC está diseñada para soporte de **todos los datos de la portabilidad** a fin de que SUTEL reciba todos los datos asociados a los procesos de portabilidad numérica, que incluyen registros de transacciones, datos de enrutamiento, histórico de NIP, registros de auditoría, datos de reportería, documentación del sistema y aplicaciones de configuración en formato estructurado y utilizable.

Todos los datos serán entregados usando formatos de la industria y mecanismos de cifrado abiertos para asegurar que SUTEL pueda acceder y usar los datos sin depender de herramientas, licencias ni llaves propietarias. Los datos se exportarán en formatos comúnmente usados como CSV, XML y volcados de bases de datos, acompañados por diccionarios completos de datos, definiciones de esquemas y documentación para asegurar la total interpretación. La encriptación para la transferencia de datos utilizará estándares ampliamente reconocidos y de libre disponibilidad tales como encriptación basada en AES y mecanismos de intercambio de llaves estándar para asegurar la confidencialidad durante la transferencia, a la vez que se permite a SUTEL descifrar y acceder a los datos usando herramientas abiertas y no propietarias.

El proceso de transferencia seguirá un procedimiento controlado y auditable, que incluye validación de datos, verificaciones de integridad y conciliación para asegurar que la información entregada está completa y es exacta. Se usarán mecanismos de transferencia segura como SFTP encriptado o canales seguros equivalentes, con credenciales de acceso y llaves que serán provistas a SUTEL de manera controlada. Todas las actividades de entrega de datos serán registradas y verificadas para garantizar la trazabilidad total y el cumplimiento con los requerimientos regulatorios.

Además de la entrega de datos, TNPC ofrecerá la **transferencia de toda la documentación y conocimiento** asociado, que incluye arquitectura del sistema, manuales de procesos, especificaciones de interfaces y procedimientos operativos para garantizar que SUTEL tenga un entendimiento y control total sobre los datos y su estructura. No se utilizarán métodos de encriptación propietaria, mecanismos de acceso restringido ni tecnología dependiente de licencias para asegurar que SUTEL tenga acceso libre, descifre y utilice los datos sin incurrir en costos adicionales.

A través de este enfoque, TNS asegura que todos los datos del SIPN **se transfieren en forma segura, son totalmente accesibles y completamente independientes de limitaciones propietarias** y mantiene la confidencialidad durante la transferencia, a la vez que garantiza la usabilidad a largo plazo y el cumplimiento con los requerimientos de SUTEL.

- 2.38** *La ERPN seleccionada no podrá ceder ni traspasar sus obligaciones en todo o en parte, de forma directa o indirecta. Cualquier cambio podrá permitir la rescisión del contrato sin responsabilidad para los operadores/proveedores. Los servicios se mantendrán por el plazo que determine el CTPN-M para garantizar la continuidad del servicio.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS confirma que todas las obligaciones conforme al contrato del SIPN serán **totalmente ejecutadas por las entidades de la ERPN contratada y no las cederá ni transferirá, en todo o en parte, directa o indirectamente, sin la autorización previa de CTPN-M y SUTEL**. El servicio de TNPC se entrega mediante un marco operativo y contractual claramente definido en el cual las responsabilidades, roles y obligaciones se mantienen bajo el control directo de TNS. Cualquier cambio propuesto que pueda afectar las obligaciones contractuales será formalmente comunicado en forma anticipada para revisión y aprobación, a fin de garantizar transparencia y cumplimiento totales con los requerimientos de gobierno.

El modelo de entrega de servicio de TNPC está diseñado para asegurar la **estabilidad, responsabilidad y continuidad operativa a largo plazo** para evitar cualquier dependencia en cesiones a terceros que podrían comprometer la integridad del servicio. Todas las funciones básicas, que incluyen operación, mantenimiento, soporte y monitoreo del sistema, y gestión de datos son administradas dentro de la estructura de entrega de TNS para garantizar consistencia en la calidad y control durante todo el período de contratación.

En caso de cualquier cambio estructural u operativo autorizado, TNS asegurará que los **servicios del SIPN continúen sin interrupción** y que mantiene pleno cumplimiento de los compromisos de los SLA y requerimientos regulatorios. Se garantiza la continuidad de servicio a través de procesos operativos robustos, arquitectura redundante y procedimientos definidos de transición para garantizar que los operadores, proveedores y usuarios finales no experimenten ninguna interrupción. TNPC continuará prestando todos los servicios durante el plazo definido por CTPN-M, independientemente de cualquier cambio interno, para asegurar que la plataforma del SIPN sigue siendo operativa y estable en todo momento.

A través de este enfoque, TNS garantiza una estricta adhesión a los requerimientos de no cesión, a la vez que garantiza la entrega ininterrumpida del servicio del SIPN y protege los intereses de SUTEL, CTPN-M, los operadores y los usuarios finales.

3 Principales procesos de operación

3.1 Actualización diaria de las bases de datos durante la ventana de cambios definida.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La solución del SIPN de TNS realiza actualizaciones integrales y automáticas diarias de todas las bases de datos relativas a la portabilidad conforme a la ventana de cambio definida por SUTEL. Tal como se especifica en el Anexo 3 (Manual de Interfaces y Procesos), la ventana de cambio funcionará a diario de lunes a sábado (excepto domingo), con la ejecución de las actividades de difusión de activaciones y retornos entre las 03:00 y 04:00. Los archivos diarios de números portados y retornados se generan al final de cada día hábil (24:00, de lunes a sábado) y contienen todos los números que están programados para portación o retorno en la siguiente ventana hábil.

El SIPN de TNS mantendrá los parámetros de las ventanas de cambio tales como hora de inicio, hora de fin y cronogramas de publicación de base de datos como valores totalmente configurables, ajustables por el Administrador del Sistema de la ERPN a través de una GUI de administración dedicada. Esto permite a SUTEL y CTPN-M modificar los horarios de las ventanas de cambio conforme a la evolución de las necesidades regulatorias u operativas, sin requerir ninguna modificación de software.

Durante la ventana de cambio definida, el SIPN ejecuta las siguientes operaciones de actualización de base de datos en una secuencia transaccional controlada:

NPCDB (Base de Datos de Portabilidad Numérica — Base de Datos Maestra de ERPN)

NPCDB es la base de datos centralizada administrativa mantenida por la ERPN, que contiene toda la información necesaria para enrutar llamadas a números portados. Durante la ventana de cambio, se ejecutan las siguientes actualizaciones:

- Los números que completan con éxito el proceso de portación se actualizan al estado Número Portado en NPCDB, con el enrutamiento mapeado al nuevo operador.
- Si el operador receptor es el operador asignatario original, el estado del número se actualiza para reflejar el estado de no portado y reasignado al operador asignatario original.
- Los números programados para repatriación se procesan y su estado se actualiza para reflejar la reasignación al operador asignatario original.

Las actualizaciones se realizan atómicamente, cada activación se completa en forma total o retrocede para garantizar la integridad de los datos.

BDO (Base de Datos Operativa - por Operador)

Cada proveedor de servicios de telecomunicaciones mantiene su propia BDO, que contiene la información de enrutamiento necesaria para enrutar las llamadas y SMS correctamente a los números portados. Después de la generación de los archivos diarios a medianoche, cada operador descarga los archivos relevantes (Archivo de Nuevos Números Portados, Archivos de Números que retornan) vía SFTP/API y actualiza su BDO antes o durante la ventana de cambio. El SIPN también soporta el Proceso de Sincronización completa que permite a los operadores solicitar descargas completas o incrementales de NPCDB para conciliar sus BDO en cualquier momento.

Archivos Diarios generados por ERPN

El SIPN genera los siguientes archivos diarios a las 24:00 (medianoche), de lunes a sábado, y los pone a disposición a las 02:00 para descarga de los operadores a fin de permitirles que actualicen sus BDO. Estos archivos incluirán:

- Archivo de nuevos números portados
- Archivo de números que retornan

Todos los archivos se pueden entregar a los operadores vía SFTP. Además de ello, TNS también permitirá un servicio API autenticado para descarga de archivos con convenciones definidas de nombres de archivos. Todas las actividades de enrutamiento tendrán una marca de tiempo, serán registradas y totalmente auditables dentro de TNPC.

- 3.2** *Crear un archivo diario con los números telefónicos portados junto con su información de enrutamiento al inicio de cada ventana de cambio. Será entregado por el SIPN inmediatamente después del inicio de cada ventana de cambio en las rutas definidas por cada uno de los operadores y se pondrá a disposición para descarga en cualquier momento por parte de la Sutel y los operadores/proveedores.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La solución del SIPN de TNS genera todos los archivos diarios de actualizaciones de enrutamientos a las 24:00 (medianoche), de lunes a sábado, para asegurar que los operadores tengan tiempo suficiente para descargar y prepararse antes de la ventana de cambio. Todos los archivos se entregan a cada operador vía SFTP en las rutas específicas del operador de inmediato después de cada ventana de cambio; y se ponen a disposición para descarga en cualquier momento por parte de SUTEL y todos los operadores/proveedores. El SIPN de TNS también brindará un servicio de API autenticado para descarga de archivos con convenciones definidas de nombres de archivos. Los archivos se pueden conservar en línea durante un período de retención configurable.

1. **Archivo Nuevos Números Portados:** Contiene todos los números de teléfono portados programados para activación en la próxima ventana de cambio, junto con la información de enrutamiento asociada -- específicamente el Número de Enrutamiento (NE) del Receptor, que permite a los operadores enrutar las llamadas y SMS correctamente a los números portados. El formato y contenido del archivo cumple con los requerimientos detallados en la sección 6.1 del Anexo 3.
2. **Archivo de números que retornan:** Contiene todos los números programados para retornar al operador asignatario original durante la próxima ventana de cambio, generada como parte del Proceso de Retorno. Permite a los operadores actualizar sus BDO para reflejar los números revertidos al enrutamiento original.

- 3.3** *Permitir descargar, de manera segura, un archivo completo de números portados según el operador actual a la fecha de la consulta.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La solución del SIPN de TNS ofrece acceso seguro a demanda al Archivo completo de números portados, tal como se solicita en el Anexo 3 (Sección 6.3). Este archivo es una foto instantánea acumulada completa de todos los números actualmente portados en NPCDB al momento de la solicitud, junto con la información de enrutamiento asociada -- específicamente el Número de Enrutamiento (NE) del Receptor para cada número portado. El contenido y formato del archivo cumplen estrictamente con las especificaciones de la Sección 6.3 en el Anexo 3.

Para ofrecer un mecanismo de descarga segura, el Archivo completo de números portados se pone a disposición para descarga por parte de SUTEL y todos los operadores/proveedores vía SFTP en las rutas específicas del operador, o a través de un servicio de API seguro para descarga de archivos con convenciones estándar de nombres de archivos. Todos los accesos son autenticados, basados en roles y encriptados en tránsito (HTTPS/SFTP con certificados digitales) para garantizar una entrega segura y confidencial por operador.

Cada operador solo puede acceder y descargar el archivo completo de números portados relevante a sus operaciones. El archivo refleja el estado actual de NPCDB a la fecha de consulta y ofrece una vista exacta en un punto de tiempo de todos los números portados y sus asignaciones de enrutamiento a lo largo de todos los operadores de la red. Más allá del Archivo completo de números portados diario, el SIPN de TNS también soporta el Proceso de Sincronización para permitir que los operadores soliciten descargas completas o incrementales de NPCDB en cualquier momento.

- 3.4** *Contar con un sistema automático de verificación que demuestre que la persona tiene acceso al servicio. Para tal, entregará un NIP, el cual se constituirá en un requisito indispensable para autenticar el número a ser portado (de modo que el NIP solo lo conozca el usuario final que cuente con acceso al servicio por portar). La solución técnica requiere una infraestructura que funcionalmente se encargue de generar, almacenar y notificar por SMS de manera segura, al servicio a ser portado, el NIP a solicitud del proveedor receptor. Además, deberá incorporar la solución que permita recibirlo (el mismo código NIP) de manera audible (IVR) únicamente desde el número que desea ser portado.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC incorpora un **Sistema Automático de Verificación (SAV)** totalmente integrado y seguro, diseñado para garantizar que solo el suscriptor legítimo con acceso activo al servicio que se está portando puede autorizar una transacción de portabilidad. SAV ofrece gestión centralizada de generación de NIP, almacenamiento seguro de NIP, validación de NIP, entrega de NIP y recuperación de NIP en base a respaldo, totalmente integrada con el flujo de trabajo de la transacción del SIPN.

Cuando un Receptor envía una Solicitud de Generación de NIP, TNPC valida la solicitud contra las definiciones de esquema WSDL/XSD o REST, verifica la titularidad del número y la autorización del operador; y genera un NIP único seguro asociado al MSISDN que se está portando. El NIP generado se almacena en NPCDB junto con:

- MSISDN
- Identificador de transacción
- Identificadores del donante y receptor
- Marca de tiempo de generación de NIP
- Período de vigencia de NIP
- Estado de entrega

Luego se entrega el NIP vía el subsistema del Gateway de SMS/SMPP de TNPC mediante integración SMPP segura con la infraestructura SMSC del donante. TNPC monitorea continuamente el acuse de recibo de la entrega del SMS y valida la entrega exitosa dentro de los intervalos definidos en los SLA. En caso de fallas temporarias en la entrega de SMS, TNPC automáticamente realiza reintentos controlados y registra todos los eventos de entrega y acuses de recibo dentro de NPCDB para una auditoría total.

El NIP sirve como elemento obligatorio de autenticación dentro del proceso de portación. Durante la etapa de validación de Solicitud de Portabilidad, TNPC valida:

- Correctitud del NIP
- Estado de vencimiento del NIP
- Asociación MSISDN a NIP
- Receptor asociado a NIP

antes de permitir continuar con el flujo de trabajo de la portabilidad.

Para asegurar la continuidad y accesibilidad del servicio, TNPC ofrece un mecanismo de respaldo de IVR totalmente integrado para la recuperación segura del NIP cuando la entrega del SMS no es exitosa o no está disponible. La solución de IVR solo permite la recuperación cuando el suscriptor llama desde el mismo número de teléfono asociado a la solicitud de generación de NIP. TNPC detecta y valida automáticamente el MSISDN del originador, recupera en forma segura el NIP vigente desde NPCDB y comunica en forma audible el mismo NIP vigente al suscriptor. Los controles configurables de IVR permiten límites de repetición del NIP y una gestión interactiva.

El marco de SAV e IVR incorpora:

- Algoritmos de generación segura de NIP
- Gestión centralizada del ciclo de vida del NIP
- Integración en la entrega de SMS basada en SMPP
- Monitoreo de entrega en tiempo real
- Manejo automático de reintentos
- Validación de respaldo de IVR
- Aplicación de vencimiento del NIP
- Registro de auditoría a nivel de transacción
- Controles de acceso basados en roles

Todos los eventos relativos al NIP incluyen:

- Generación de NIP
- Solicitud de envío de NIP
- Acuse de recibo por SMS
- Reintentos
- Resultados de validación de NIP
- Actividades de recuperación de IVR

tienen marcas de tiempo, se registran y monitorean centralmente y son totalmente auditables dentro de NPCDB.

A través de este marco de SAV e IVR seguro, resiliente y totalmente automático, TNPC brinda sólida autenticación del suscriptor, prevención de fraude, autorización de portabilidad segura, continuidad operativa y trazabilidad completa a lo largo de todo el proceso de portabilidad.

3.4.1 *Para la funcionalidad del IVR, el usuario deberá llamar desde el servicio con el número telefónico utilizado en la solicitud de NIP, y desde el cual desea conocerlo. En caso de empresas, se deberá hacer la llamada desde el número para el que se solicitó el NIP.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC aplica una estricta validación de quien llama al IVR para garantizar que la recuperación del NIP solo se permite desde el mismo número de teléfono asociado a la solicitud de NIP original. Cuando el suscriptor llama a la plataforma IVR de TNPC, el sistema automáticamente detecta y valida el MSISDN del originador contra el registro de NIP vigentes almacenados dentro de NPCDB antes de permitir la recuperación del NIP.

El IVR solo ofrece el NIP en forma audible cuando:

- El número del originador coincide con el MSISDN asociado a la solicitud de NIP activa
- El NIP se encuentra dentro del período de vigencia configurado

Para empresas, el proceso de validación de IVR funciona idéntico. Se requiere que la llamada se origine exclusivamente desde el número de teléfono desde el cual se solicitó originalmente el NIP.

Todas las interacciones, validaciones, intentos de recupero y resultados del IVR tienen marcas de tiempo, se registran y son totalmente audibles dentro de TNPC para garantizar la autenticación segura del suscriptor, prevención de fraude y total cumplimiento regulatorio.

3.4.2 *El IVR detectará el número de teléfono originador de la llamada y realizará una consulta a ERPN para dicho número mediante el servicio web que estará disponible.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El subsistema IVR de TNPC detecta automáticamente el MSISDN del originador de la llamada entrante y consulta en forma segura la plataforma de ERPN, a través de interfaces web service disponibles, para validar la existencia y estado del NIP activo asociado al número.

El IVR interactúa directamente con la lógica de negocio de TNPC y con NPCDB a través de web services seguros basados en SOAP/XML o REST a fin de permitir validación en tiempo real de:

- MSISDN del originador
- Estado activo del NIP
- Período de vigencia del NIP

Solo se permite recuperar el NIP de solicitudes validadas y autorizadas para garantizar la autenticación segura del suscriptor, prevención de fraude y total trazabilidad de todas las interacciones del IVR dentro de TNPC.

3.4.3 *Si el servicio tiene un NIP vigente, se lo indicará al usuario dándole la oportunidad de repetírselo.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Si el número del originador tiene un NIP activo y vigente asociado a la solicitud de portabilidad, el subsistema IVR de TNPC recupera en forma segura y comunica audiblemente el NIP al suscriptor. El IVR soporta la funcionalidad configurable de repetición de NIP que permite al suscriptor repetir el NIP la cantidad de veces definida dentro de la misma llamada.

Todas las interacciones de recupero de NIP del IVR tienen marcas de tiempo, se registran y son totalmente audibles dentro de TNPC para garantizar la autenticación segura del suscriptor, trazabilidad operativa y cumplimiento regulatorio.

3.4.4 *Si no tiene un NIP vigente, informará al usuario de ello y finalizará la llamada.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Si no existe un NIP activo y vigente asociado al MSISDN del originador, el subsistema IVR de TNPC informa en forma segura al suscriptor que no existe un NIP de portabilidad vigente disponible para el servicio solicitado y terminará amablemente la llamada. El proceso de validación se realiza en tiempo real contra NPCDB para garantizar la verificación precisa del estado del NIP y para evitar intentos de portabilidad no autorizados.

3.5 *Registrar de los NIPs generados, los cuales se mantendrán almacenados por un período de 8 meses y podrán ser consultados por la Sutel.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Todos los NIP generadores se registran en la Base de datos de NIP que tienen un registro como MSISDN, valor de NIP, marca de tiempo de generación, vencimiento, operador solicitante y operador donante. Tal como se solicita en el pliego de condiciones, los registros del NIP se conservan por un mínimo de 8 meses a partir de la fecha de generación y pueden ser consultados por SUTEL en cualquier momento, vía acceso solo lectura basado en la GUI de TNPC. Se puede configurar la duración de la conservación del NIP si fuese requerido por SUTEL. SUTEL puede hacer búsquedas por MSISDN, rango de fecha, operador o estado de NIP. Más allá de la ventana de solicitud activa de 8 meses, los registros de NIP se conservan como registros de auditoría solo lectura durante todo el período de la contratación.

3.6 *Generar un archivo diario con la totalidad de los números que deben ser retornados al proveedor asignatario de la numeración. El archivo será entregado por el SIPN en las rutas definidas por cada uno de los operadores/proveedores y podrá ser descargado en cualquier momento.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El SIPN de TNS genera el Archivo diario de números que retornan a las 24:00 (medianoche), de lunes a sábado, y contiene todos los números programados para regresar al operador asignatario original en la próxima ventana de cambio hábil (03:00–04:00). Este archivo se genera como parte del Proceso de Retorno y rige la repatriación de los números portados que regresan al proveedor asignatario original.

Para cada número que será retornado, el archivo incluirá MSISDN, operador actual, operador asignatario original al cual se retorna el número y la fecha de retorno programada. Se puede entregar el archivo a cada operador/proveedor vía SFTP en las rutas específicas del operador o usando un servicio autenticado de API con convenciones estandarizadas de nombres de archivos. El archivo se pone a disposición para descarga en cualquier momento por parte de SUTEL y todos los operadores/proveedores; y se conserva en línea durante el período de retención configurable.

3.7 *Gestión automatizada, trazable y auditable del proceso completo de portación.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma TNPC de TNS ofrece gestión totalmente **automática, trazable y auditable** de todos los seis procesos administrativos de portabilidad definidos en el Anexo 3 que incluyen:

- Proceso 00 – Generación y Entrega de NIP
- Proceso 01 – Proceso de Portación
- Proceso 02 – Consulta de Prevalidación
- Proceso 03 – Cancelación de Portación
- Proceso 04 – Proceso de Retorno de Número
- Proceso 05 – Sincronización con ERPN
- Proceso 06 – Subproceso de Detección de Errores

Todos los procesos de portación se ejecutan automáticamente a través del Procesador de Mensajes de TNPC, que aplica reglas de negocio configurables para control del flujo de mensajes entre operadores. Esto incluye retirar mensajes de la cola entrante, validarlos contra las reglas definidas, verificar el cumplimiento del tiempo, determinar y generar los mensajes de respuesta, establecer los tiempos en anticipación a las respuestas del operador y actualizar el estado de portación/número; todo ello sin intervención manual. Múltiples instancias del Procesador de Mensajes y el Procesador de Temporizadores se ejecutan simultáneamente para garantizar la producción y disponibilidad.

A cada transacción de portación se le asignará un identificador único de proceso (formato: OOOOYYYYMMDDHHCCNNNNN - ID de operador, fecha, tipo de proceso, número de secuencia), que vinculará todos los mensajes asociados durante el ciclo de vida de la transacción. TNPC mantendrá un Mantenedor de Registros de Transacción (Transaction Record Keeper - TRK), que registra todos los mensajes con las marcas de tiempo de envío/recepción y el estado. Cada mensaje se almacena en la Base de Datos de Transacciones con el estado de proceso asociado; y cada proceso hace la transición a través de los estados definidos (por ej., 01R01 → 01R02 → 01D01 → 01A04 para una portación exitosa), lo cual ofrece una cadena de custodia completa para cada transacción.

TNPC también mantiene registros de eventos integrales, que cubren todas las acciones a lo largo de las bases de datos, archivos, sistemas de intercambio de información y todos los subsistemas. Los controles clave de auditoría incluyen los siguientes registros:

- Mantiene todos los registros de transacciones y auditorías como **solo lectura** de forma tal que no se puedan realizar modificaciones ni eliminaciones.
- Registro con marca de tiempo de cada evento tal como recepción de mensaje, validación, cambio de estado, activación/vencimiento de temporizador, error, etc.
- Los registros de Acceso del Usuario se almacenan en el sistema. Los operadores pueden consultar los registros que se generan solo para sus propias acciones e interacciones con ERPN. Solo SUTEL tiene acceso privilegiado para auditar los registros a lo largo de todos los operadores, funcionarios y acciones de ERPN.

3.8 *Intercambio transaccional de procesos entre operadores donantes, operadores receptores y la ERPN.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma TNPC de TNS actúa como entidad centralizada de mediación para todos los intercambios transaccionales entre operadores donantes, operadores receptores y la ERPN. No existe mensajería directa operador a operador. Todos los mensajes son recibidos, validados, procesados y enrutados por TNPC para mantener un histórico completo de las transacciones y actualizar NPCDB cuando sea necesario.

TNPC ofrece a los operadores dos interfaces simultáneas para intercambio transaccional. Los operadores pueden usar cualquier de ellas en forma intercambiable para cualquier proceso:

- **Web Services (SOAP/REST):** Intercambio automático máquina a máquina que soporta tanto el protocolo existente basado en SOAP/XML (retrocompatible con las implementaciones de los operadores de Costa Rica) y una moderna interfaz REST/JSON para los operadores que buscan modernizar su integración. TNS ha implementado con éxito este modelo de doble interfaz en las últimas implementaciones para posibilitar un camino de migración por etapas, sin interrumpir los sistemas existentes de los operadores.
- **GUI de Portabilidad:** Una aplicación web basada en Angular accesible a través de un navegador estándar que ofrece a los operadores una interfaz manual para iniciar, responder y monitorear todas las transacciones de portación. La GUI incluye tableros en tiempo real, búsqueda de transacciones y seguimiento de estado; se trata de una capacidad que TNS ha refinado a lo largo de las implementaciones en 17 países.

El Procesador de Mensajes de TNPC aplica reglas de negocio configurables en cada paso de la transacción, validación del contenido del mensaje, aplicación de cumplimiento de temporizadores, mensajes de respuesta de generación automática al vencimiento del temporizador y actualización de estado de portación/número en NPCDB. Múltiples instancias del Procesador de Mensajes y el Procesador de Temporizadores se ejecutan simultáneamente para garantizar una alta producción incluso durante períodos con picos de volumen de portaciones. Este motor basado en reglas es el diferenciador central de TNS. Cuando cualquier regla de negocio cambia (por ej., nuevas causas de rechazos, ajustes de temporizadores), las mismas se implementan a través de configuración, sin cambios de código; lo cual reduce el riesgo de implantación y tiempo de resolución.

3.9 *Validar técnica y lógicamente las solicitudes de portación de modo que se limiten y prevengan errores operativos, inconsistencias y solicitudes duplicadas.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC de TNS implementa un marco de validación de múltiples capas que aplica verificaciones técnicas y lógicas en cada etapa del proceso de portación para garantizar cambios mínimos de errores operativos, inconsistencias de datos y solicitudes duplicadas.

La validación de portación de TNPC comienza desde la validación para reducir errores operativos hasta el proceso de Consultas de Prevalidación, que permite al operador verificar que la portabilidad del número sea elegible antes de enviar la solicitud de portabilidad formal. De esta manera se filtran proactivamente las solicitudes inválidas antes de ingresarlas al flujo de trabajo formal de la portabilidad.

Cada mensaje entrante es primero validado contra el protocolo de la interfaz aplicable --los mensajes SOAP/XML son validados contra los esquemas XML, mientras que los mensajes REST/JSON son validados contra las definiciones de esquemas JSON equivalentes. Los mensajes mal formados o incompletos se

rechazan de inmediato con los códigos de mensajes de la serie ERRSOAP para evitar que los datos corruptos ingresen a la línea de procesamiento.

El Procesador de Mensajes de TNPC luego aplica un conjunto integral de reglas de negocio configurables sobre cada mensaje validado. Todas las reglas de validación, causas de rechazo, umbrales de temporizadores y parámetros coincidentes se gestionan vía el modelo de datos configurable de las Reglas de Negocio, en vez de con lógica de código duro. Esto significa que cuando CTPN-M introduce nuevos códigos de rechazo o modifica parámetros de validación, los cambios se implementan vía configuración, sin modificación de código. Para los procesos de portación de Costa Rica, el motor aplicará las causas de rechazos distintivas de ERPN, tal como se solicita en la Sección 5.3.3. del Anexo 3.

3.10 *Garantizar una asociación segura entre el número a portar, los operadores receptor y donante, así como con los datos del usuario.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC de TNS aplicará asociaciones seguras, validadas y criptográficamente protegidas entre el número a portar, el operador receptor, operador donante y los datos del usuario suscriptor en cada etapa del ciclo de vida de la portabilidad.

Se asignará a cada transacción de portación un identificador único de proceso al momento inicial, que vinculará el(los) número(s), operador receptor, operador donante y todos los datos asociados del suscriptor en una sola cadena de transacciones inmutables. Todos los mensajes siguientes llevan este identificador para garantizar la trazabilidad punta a punta y evitar contaminación cruzada entre transacciones simultáneas.

La Base de Datos de NIP mantiene una asociación criptográficamente generada entre MSISDN, NIP y operador receptor. Durante la validación de la solicitud de portabilidad, TNPC valida que el NIP coincida con la combinación específica de número-operador receptor para garantizar que, solo el receptor autorizado que actúa con el consentimiento explícito del suscriptor puede iniciar la portación de ese número.

Todos los mensajes se intercambian sobre HTTPS con certificados digitales vía túneles IPsec VPN (encriptación AES-256) para garantizar la autenticación, confidencialidad e integridad de los datos en tránsito. A nivel de aplicación, cada operador se autentica vía ID y credenciales de inicio de sesión únicos. TNPC valida aún más que el donante indicado coincida con los registros de NPCDB para evitar suplantación de identidad o solicitudes mal direccionadas.

Todos los datos del usuario en reposo están encriptados y el acceso a la base de datos es controlado a través de controles de acceso y reglas de firewall para garantizar que cada operador solo pueda acceder a los datos de sus propias transacciones, al tiempo que SUTEL tendrá acceso privilegiado a lo largo de todos los operadores para supervisión regulatoria.

3.11 *Permitir la incorporación de reglas de operación configurables y adaptables a la regulación costarricense.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC de TNS tiene un diseño arquitectónico sobre un modelo de datos de Reglas de Negocio configurables y un componente dedicado dentro de la Base de Datos Administrativa Central que rige cómo responde el sistema a cada mensaje recibido. Las Reglas de Negocio de TNPC modelan las reglas que rigen cómo el sistema debería responder ante un mensaje recibido, incluyendo cómo validar el mensaje, a quién se debe reenviar el mensaje, cómo actualizar el estado de la portación; y definiciones y valores de parámetros de los temporizadores. Esto significa que las reglas operativas son accionadas por los datos. No se pueden

agregar nuevas reglas en código duro. La modificación de reglas existentes y el retiro de reglas obsoletas se hace a través de la configuración, sin modificaciones de la aplicación.

Las siguientes categorías de reglas de operación son totalmente configurables y adaptables a la regulación costarricense:

- **Validación y causas de rechazo:** Agregado de nuevas causas de rechazo de ERPN y el Donante, modificación de lógica de validación y ajustes de umbrales con identidad coincidente.
- **Temporizadores de procesos:** Todos los temporizadores de procesos como TVC, TVCP, TNIP, etc. se almacenan como parámetros configurables y se pueden ajustar para reflejar los cambios regulatorios, sin cambios de código.
- **Reglas de enrutamiento de mensajes:** Las reglas que rigen qué mensaje reenviar, a quién y bajo qué condiciones que incluyen aceptación automática al vencimiento del temporizador y lógica de escalada.
- **Configuración de operador y plan de numeración:** Los datos de identificación del operador (ID de participante, URL de interfaces, credenciales), asignación de bloque de números y códigos de enrutamiento se mantienen como datos administrativos, que permiten el agregado de nuevos operadores o rangos de números sin inconvenientes.
- **Parámetros de programación y operativos:** Los horarios de ventanas de cambio, cronogramas de generación de archivos, períodos de vigencia de NIP, etc. son configurables vía la GUI del Administrador del Sistema de ERPN.

El Procesador de Mensajes de TNPC lee el modelo de datos de las Reglas de Negocio en el tiempo de ejecución. A medida que CTPN-M introduce nuevas reglas operativas, TNS configura las nuevas reglas en el modelo de datos de Reglas de Negocio, las valida en el entorno de pruebas y las implementa en producción. Todo ello se realiza sin o con mínimos cambios de código de la aplicación.

3.12 *Diseño flexible de bases de datos y reglas operativas de manera que la inclusión o modificación de campos no implique un rediseño completo de la solución brindada.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La Base de Datos Administrativa Central de TNPC de TNS está diseñada como un modelo de datos lógicamente modulares, que consta de dominios de datos mantenibles independientes, que incluyen Reglas de Negocio, Datos de Transacciones, Datos de NIP, Datos de Identificación del Operador, Plan de Numeración, Códigos de Enrutamiento y Bases de Datos de Reportería. Esto garantiza que los cambios en un dominio, tal como agregado de un campo al catálogo de datos de transacciones, o la introducción de los parámetros de identificación de un nuevo operador, no impacten componentes no relacionados.

Como se mencionó anteriormente, el modelo de datos de Reglas de Negocio rige cómo responde el sistema a cada mensaje entrante -- lógica de validación, enrutamiento de mensajes, transacciones de estado de portación y gestión de temporizadores-- y se mantiene como conjuntos de reglas configurables y no como lógica de código duro. TNPC puede soportar múltiples conjuntos de procesos y mensajes; y es posible implementar procesos y mensajes adicionales mediante la configuración, sin necesidad de modificar el software de la aplicación.

Para agregados o cambios en los campos de datos en los mensajes de portación o tablas de bases de datos, TNPC soporta la evaluación controlada de los esquemas, donde se pueden agregar nuevos campos a los esquemas de bases de datos y los esquemas de mensajes correspondientes (XSD para SOAP/XML, esquema JSON para REST/JSON) a través de extensiones versionadas y retrocompatibles. Sin embargo, cabe destacar que si bien los agregados de campos y reglas de negocio no requieren un rediseño total de la solución, determinados tipos de cambios pueden requerir versiones de software controladas que incluyen desarrollo, pruebas e implementación por etapas. La arquitectura de TNPC minimiza el alcance y riesgo de estos cambios, pero no elimina la necesidad de gestión de versiones en todos los casos.

3.13 *Soportar procesos síncronos y asíncronos del SIPN y los operadores/proveedores asegurando la integridad, seguridad y confidencialidad de las transacciones entre las partes involucradas.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC soporta procesos/mensajes síncronos y asíncronos. La mayoría de los mensajes del SIPN, que incluyen Generación de NIP (Proceso 00), Portación (Proceso 01), Consulta de Prevalidación al Donante (mensajes 2003–2006), Cancelación de Portación (Proceso 03), Retorno de Número (Proceso 04) y Sincronización (Proceso 05) siguen un patrón asíncrono. Al recibir un mensaje asíncrono, el sistema devuelve un ACK para confirmar la recepción exitosa, o NAK (por ej. ERRWS003) si el mensaje no cumple con los esquemas XML o JSON. Luego se almacena el mensaje como pendiente en TRK (buzón de entrada de la transacción) y se procesa mediante el Procesador de Mensajes, que aplica reglas de negocio configurables para validar el contenido, ruta del mensaje, actualización del estado de portación y conjunto de temporizadores relevantes. Si no se recibe ACK/NAK dentro del timeout definido, el emisor podrá reenviarlo. Para mensajes síncronos tal como solicitud de proceso en curso automático (mensajes 2001/2002), Consulta Pública de Estado del Número y solicitud de NIP por IVR, la respuesta inmediata sirve como acuse de recibo. Los resultados en tiempo real se devuelven dentro del timeout definido (por ej., TR20 = 60 segundos).

La integridad de la transacción con ambos patrones se mantiene a través de identificadores únicos de procesos que correlacionan todos los mensajes dentro del ciclo de vida de la transacción. El Procesamiento de Mensajes aplica estados estrictos de máquina; y el procesamiento atómico con reversión garantiza que, en caso de errores, todas las tareas ejecutadas durante el procesamiento se revierten, el proceso se cierra con estado de error y se genera el estado de error para los operadores afectados. Todo esto funciona dentro de un entorno seguro, donde cada intercambio de mensaje se transmite vía HTTPS con certificados digitales vía túneles IPsec VPN (encriptación AES-256), detrás del firewall y WAF, sin acceso externo directo a la aplicación ni los servidores de datos. Los controles de acceso basados en roles garantizan que cada operador interactúa solo con las transacciones en las cuales es parte; mientras que SUTEL conversa acceso privilegiado a lo largo de todos los operadores. Se encriptan los datos en reposo con AES-256 o superior para garantizar la confidencialidad en todas las capas.

3.14 *Capacidad de manejo de eventos, validaciones y notificaciones en tiempo real.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC de TNS procesa todos los mensajes entrantes en tiempo real a través del Procesador de Mensajes, que es el proceso central Java que corre múltiples instancias simultáneas. Cada una de ellas toma mensajes de la cola de entrada, aplica las reglas de negocio configurables, realiza las validaciones (cumplimiento de esquema, integridad de NIP, detección de duplicados, consistencia del operador, verificaciones de identidad del suscriptor, cumplimiento de temporizadores, etc.), actualiza el estado de portación/número en NPCDB y genera los mensajes de respuesta a las partes correspondientes dentro de los milisegundos de recibido el mensaje.

El Procesador de Temporizadores funciona en paralelo, monitorea continuamente todos los temporizadores de procesos activos (TVC, TVCP, TNIP, TR00–TR14, TR20, etc.) y genera acciones correctivas en tiempo real al vencimiento tales como aceptación del donante con generación automática al timeout de TVC, escalada de prevalidaciones no resultas o cierre de registros con NIP vencidos. Las notificaciones de entrega de NIP se procesan a través del subsistema del SMSG dentro de 1 minuto de la solicitud de receptor, sin superar 5 minutos (SLA2); mientras que las respuestas del IVR y retorno síncrono en tiempo real ocurren dentro de milisegundos en TR20 = 60 segundos.

Esta capacidad en tiempo real se entrega a los operadores a través de la interface de web services (SOAP/XML y REST/JSON sobre HTTPS) para el procesamiento automático y la GUI de Portabilidad para monitoreo de transacciones en vivo y para alertas visuales. Esta capacidad está apuntalada por una arquitectura de múltiples instancias, horizontalmente escalable, que TNS ha validado operativamente a lo largo de las implantaciones que manejan más de 10 millones de transacciones de portación por año.

3.15 *Garantizar el registro de estados, tiempos y resultados de cada transacción dentro de un proceso de portación. Se deberá almacenar la información histórica y actual con marcas de tiempo.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El TNPC de TNS registra cada transición de estado, marca de tiempo y resultado de cada transacción dentro del ciclo de vida de la portación como una función inherente del motor de procesamiento. Cuando el Procesador de Mensajes maneja cualquier mensaje a lo largo de todos los seis procesos administrativos y el subproceso de detección de errores, el mismo actualiza el estado de proceso de la transacción en la Base de Datos de Transacciones. Cada transición de estado se registra con una marca de tiempo precisa de su ocurrencia, el mensaje que disparó la transición y la acción resultante que tomó el sistema. TRK (Mantenedor de Registro de Transacciones) registra cada mensaje enviado y recibido dentro de la transacción, captura la fecha de envío, fecha de recepción, estado del mensaje e identificador único del proceso (OOOOYYYYMMDDHHCCNNNNN) que correlaciona toda la cadena de mensajes. Los eventos de temporizadores, es decir, activación, cuenta regresiva y vencimiento reciben una marca de tiempo y se registran a fin de garantizar la trazabilidad total de acciones urgentes tales como timeouts de aceptación del donante (TVC/TVCP), vencimiento de NIP y plazos de respuesta de prevalidación (TR20).

TNPC además mantiene una distinción entre Transacciones Actuales, que son procesos de portación en curso, y Transacciones Históricas, que ya se completaron, cancelaron o cerraron con error. Tanto los registros actuales como históricos tienen marcas de tiempo completas, se almacenan con todos los mensajes asociados, transiciones de estado, resultados de validaciones y eventos de temporizadores. El Histórico de Transacciones se conserva como solo lectura para garantizar que no se permitan realizar modificaciones o eliminaciones, con un período de almacenamiento configurable después del cual se puede enviar a almacenamientos alternativos. SUTEL tendrá acceso privilegiado a consultar todos los registros de transacciones a lo largo de todos los operadores; mientras que cada operador solo podrá acceder a los registros en los cuales participó en las transacciones como donante o receptor.

3.16. *El SIPN desarrollado por la ERPN seleccionada deberá incorporar la lógica operativa y funcional que permita relacionar la respuesta de prevalidación positiva en todos sus extremos por parte del donante con una solicitud de portabilidad realizada en un plazo máximo de 1 hora (posterior a la prevalidación) de modo que no pueda ser rechazada.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC de TNS implementará una relación directa entre el proceso de Solicitud de Validación (Proceso 02) y el Proceso de Portación (Proceso 01) para aplicar este requerimiento. Cuando el donante responde en forma positiva a una solicitud de prevalidación, TNPC registra esta respuesta positiva, que incluye el identificador de proceso, MSISDN, ID del donante y marca de tiempo de la respuesta en la Base de Datos de Transacciones. Si el receptor posteriormente envía una solicitud de portabilidad formal (mensaje 1001) para el mismo número dentro de 1 hora de la respuesta de validación positiva, TNPC correlaciona las dos transacciones usando el MSISDN y NIP como llaves vinculantes.

Una vez correlacionados, TNPC aplica el compromiso de prevalidación para asegurar que el donante no puede rechazar la solicitud de portabilidad sobre la misma base de que ya la validó positivamente durante la prevalidación. Las reglas de negocio configurables del Procesador de Mensajes hacen referencia cruzada

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

con el resultado de prevalidación, cuando evalúan cualquier rechazo del donante, y bloquean o marcan los rechazos contradictorios conforme a ello. La ventana de correlación de 1 hora se mantiene como un parámetro de temporizador configurable, ajustable por el Administrador de la ERPN en caso de que SUTEL o CTPN-M modifiquen este umbral. Todos los eventos de correlaciones como vínculo, verificaciones de temporizadores, rechazos bloqueados se registran con marcas de tiempo para su auditoría total.

3.17 *Repositorio único, lógico y centralizado con el historial de números portados con soporte para consulta inmediata de todos los procesos de portación desde el 2013.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La Base de Datos Administrativa Central de TNPC de TNS actúa como repositorio centralizado, único, lógico para los datos de todos los números portados e histórico de transacciones. La Base de Datos Administrativa Central incluye la Base de Datos de Referencia de Números Portados, así como también Datos de Aplicaciones utilizados para implementar los procesos de portabilidad numérica. La base de datos mantiene dos dominios de datos distintivos, aunque unificados, Transacciones Abiertas (procesos actualmente en curso) e Histórico de Transacciones (todos los procesos completados, cancelados o cerrados por error). Ambos son accesibles mediante una sola interfaz de consulta. Cada registro histórico conserva la cadena completa de la transacción: cada mensaje intercambiado, cada transición de estado, cada resultado de validación, cada evento de temporizador y cada acción del operador. Todo ello tiene marcas de tiempo precisas y se vinculan a través de un identificador único de proceso.

Para la implantación de Costa Rica, TNS migrará el histórico de portaciones completo desde 2013 a la fecha de entrada en producción de TNPC (noviembre 2027) desde la ERPN actual hasta la Base de Datos Administrativa Central de TNPC. TNS ha realizado con éxito migraciones de datos históricos completos en dos transiciones de entrada en producción anteriores en Perú y Estados Unidos y que se completaron con integridad total de los datos y cero pérdida de datos. Después de la migración, todos los registros históricos desde 2013 en adelante podrán ser consultados de inmediato a través de la GUI de Portabilidad y el Motor de Reportería.

3.18 *El SIPN deberá incluir una funcionalidad de carácter excepcional y temporal que se conocerá como “Operador fuera de línea” para permitir que un operador/proveedor con afectaciones en sus plataformas tecnológicas que le impidan interactuar y responder de manera regular a los procesos establecidos, pueda continuar gestionando trámites de portabilidad numérica sin generar mensajes de error o afectaciones a las demás partes.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC de TNS incluye en forma nativa una Interfaz Gráfica de Usuario basada en la web (GUI de Portabilidad), accesible a través de un navegador web estándar, que permite a cualquier operador/proveedor realizar todas las transacciones de portabilidad numérica cuando sus interfaces automáticas (SOAP/XML o REST/JSON) no están disponibles por alguna plataforma de IT afectada. Los participantes tendrán la opción, en cualquier momento, de usar la GUI Web o la Interfaz de Web Services para participar en cualquier proceso de portación. Para cualquiera de los procesos de portación, toda la información intercambiada será idéntica, independientemente de la interfaz elegida para ejecutar el proceso. Esto significa que la GUI ofrece paridad funcional total con interfaces automáticas, que cubre generación de NIP, prevalidación, portación, cancelación, retorno de número y sincronización.

Dado que el operador afectado continúa respondiendo e iniciando las transacciones a través de la GUI, en vez de no estar disponible, no se generará ningún mensaje de error porque TNPC recibe las respuestas válidas dentro de las ventanas definidas de los temporizadores independientemente de la interfaz utilizada. Es más, los otros operadores/proveedores no experimentan ningún impacto. El Procesador de Mensajes de TNPC enruta todos los mensajes a través del mismo motor de procesamiento y Base de Datos de Transacciones, independientemente de si el operador originador usó la interfaz automática o la GUI. Desde la perspectiva de las demás partes, las transacciones aparecen y se comportan igual.

- 3.18.1** *El SIPN deberá permitir a un operador/proveedor llevar a cabo todas las gestiones de sus procesos de portabilidad numérica desde una interfaz WEB. Esta funcionalidad será únicamente utilizada previa autorización expresa del CTPN-M, en la cual se establecerán las condiciones, alcance y vigencia.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Tal como se describe en la sección 3.18, la GUI de Portabilidad de TNPC permite que cualquier operador realice todas las transacciones de portación desde una interfaz web con paridad funcional total con las interfaces automáticas. Esto se aplicará con la autorización expresa de CTPN-N, con condiciones y alcance (qué procesos y transacciones se contemplan) y plazo de vigencia claramente definidos. La pista de auditoría integral de TNPC capturará cada acción del usuario con marcas de tiempo, identidad del usuario, identidad del operador y tipo de acción, ofreciendo trazabilidad total para verificar que la prestación se utilizó estrictamente dentro del período y alcance autorizados. El enfoque de implementación específica para el mecanismo de autorización será definido durante la etapa de diseño detallado en consulta con SUTEL y CTPN-M.

- 3.18.2** *A las gestiones realizadas por el “Operador fuera de línea” le aplicarán todos los temporizadores para la continuidad del proceso y en ningún caso se permitirán rechazos masivos de procesos de portabilidad numérica.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Todos los temporizadores de procesos definidos continuarán siendo aplicados a las transacciones procesadas en la GUI del Operador fuera de línea. El Procesador de Temporizadores de TNPC, que se ejecuta independientemente de la interfaz del operador elegida, continuará monitoreando todos los temporizadores activos y generando las acciones correctivas al momento del vencimiento, no obstante la transacción haya sido iniciada vía la interfaz automática o la GUI. Como el operador afectado interactúa directamente a través de la GUI en vez que quedar indisponible, las transacciones avanzan normalmente dentro de los temporizadores de los SLA, que evitan cualquier escenario de rechazos masivos por falta de respuesta.

- 3.18.3** *El SIPN registrará todas las acciones realizadas por el operador/proveedor y sus usuarios bajo esta modalidad.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Todas las acciones realizadas a través de la GUI del Operador fuera de línea se registran con la misma integridad y granularidad que las transacciones automáticas. Cada acción del usuario, como inicio de sesión, inicio de mensaje, envío de respuesta, cambio de estado de transacción, descarga de archivo, se registran con marcas de tiempo, identidad de usuario y tipo de acción en la Base de Datos de Transacciones y TRK de TNPC.

4 Implementación, continuidad y mejora innovadora del SIPN

- 4.1** *La ERPN seleccionada deberá plantear un cronograma de implementación general del Sistema Integral de Portabilidad Numérica de acuerdo con el Manual de Interfaces y Procesos con plazos máximos acordes al cronograma aprobado por el CTPN que se encuentra en el Anexo 1 y de migración del SIPN. El cronograma deberá contemplar los plazos de implementación y, al menos, lo siguiente:*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPS ofrecerá un **cronograma de implementación integral, estructura y totalmente regulado** para el Sistema Integral de Portabilidad Numérica, alineado con el Manual de Interfaces y Procesos del Anexo 1 y los requerimientos de migración del SIPN. Al momento de la adjudicación del contrato, TNS trabajará en colaboración con SUTEL y CTPN-M para finalizar y acordar el cronograma detallado, a fin de garantizar la alineación con los marcos de tiempos regulatorios, alistamiento de operadores y dependencias de migración.

El programa de implementación será liderado por un equipo de **Gestión de Programa de TNS** dedicado, que garantizará la coordinación punta a punta de las etapas de desarrollo, implementación, integración, pruebas, migración y entrada en producción. Una de las fortalezas clave de TNS es la capacidad de lograr entregas a tiempo a través de la **definición anticipada y estructurada de las especificaciones con aprobación a tiempo de los operadores**. Este enfoque disciplinado permitió a TNS mantener antecedentes excepcionales, **nunca incumplió una fecha programada de entrega de software en ningún país en que implementó soluciones de portabilidad numérica**.

El cronograma propuesto sigue un **modelo de ejecución por etapas accionado por las dependencias**, que garantiza avance controlado y mitigación de riesgos:

- **Etapas de requerimientos y diseño** que incluye talleres con los operadores, definición de flujos de procesos y entrega de especificaciones de interconectividad con validación y aprobación formal.
- **Etapas de configuración de infraestructura** que cubre entornos de producción y pruebas de AWS, conectividad segura y alistamiento para integración de los operadores.
- **Etapas de implementación de software** que incluye la entrega del software de TNPC, instalación en los entornos de producción y pruebas; y disponibilidad de la documentación del sistema.
- **Etapas de pruebas y validación** que incluye pruebas de aceptación, validación del operador y certificación regulatoria.
- **Etapas de capacitación y alistamiento** que asegura la capacitación de los interesados con la plataforma de TNPC cerca de las pruebas.
- **Etapas de pruebas de la industria** que incluye pruebas de conectividad y pruebas entre operadores.
- **Etapas de entrada en producción** que incluye la preparación final, corte y lanzamiento comercial.

La disponibilidad del software de TNPC **conforme al cronograma ofrece ventajas significativas a los operadores**, ya que les permite preparar los sistemas de gateway en forma anticipada, realizar las actividades de integración con eficiencia y participar en las pruebas de la industria con el sistema real listo para entrar en producción. Además, la capacitación se realiza con el sistema en vivo cerca de la etapa de pruebas para asegurar que se retenga el conocimiento y se aplique efectivamente durante las operaciones.

El cronograma detallado define **hitos, dependencias y tiempos claros** y culmina con el lanzamiento comercial en aproximadamente **A+206 días de la suscripción del contrato**. Incluye todas las actividades requeridas como recolección de requerimientos, configuración de entornos, implementación del software, pruebas, capacitación, ingreso de operadores y alistamiento para migración.

El cronograma está diseñado para ser **dinámico y adaptable** y permite realizar ajustes en base a aportes de los interesados, actualizaciones regulatorias o eventos imprevistos. Permite un seguimiento continuo a

través de hitos definidos, mapeo de dependencias e identificación de caminos críticos. El avance se monitorea con herramientas de gestión de proyectos estándares de la industria, compatibles con MS Project. SUTEL y CTPN-M recibirán reportes regulares, que incluyen porcentajes completados y seguimiento de riesgos.

El plan de implementación también incorpora las **actividades de migración del SIPN**, que garantizan una transición sin inconvenientes de los datos históricos y procesos a través de operaciones en paralelo, sincronización y corte controlado para mantener la continuidad total del servicio.

A través de este enfoque de implementación estructurado, probado y regulado, TNS asegura la **implementación del SIPN con entrega a tiempo, riesgo mínimo, fuerte alistamiento del operador y sin inconvenientes**; y sienta una sólida base para el funcionamiento a largo plazo y evolución futura de la plataforma.

A continuación, se presenta el cronograma de implementación.

| Tarea N° | Tarea programada | A+ Fecha (Días Calendario) | Tarea de la Dependencia |
|------------|--|----------------------------|-------------------------|
| 1 | Anuncio de Adjudicación/Suscripción de Contrato | A | |
| | Nota: Si la fecha A+ cae un sábado, el viernes anterior será la fecha de vencimiento. Si la fecha A+ cae un domingo, el lunes siguiente será la fecha de vencimiento. | | |
| 2 | Recolección de Requerimientos de TNPC | | |
| 2.1 | Comienza la sesión de recolección de requerimientos – TNS realiza reuniones con los operadores para la recolección de requerimientos. | A+10 | Nº1 |
| 2.2 | Finaliza la sesión de recolección de requerimientos. | A+14 | Nº2.1 |
| 2.3 | TNS proporciona la documentación borrador de los Flujos de Procesos (con mejoras incluidas) y las Especificaciones de Interconectividad para comentarios | A+42 | Nº2.2 |
| 2.4 | Se proporcionan comentarios a TNS para la documentación de los Flujos de Procesos y las Especificaciones de Interconectividad. | A+56 | Nº2.3 |
| 2.5 | TNS proporciona la documentación final de los Flujos de Procesos (con mejoras incluidas) y las Especificaciones de Interconectividad de TNPC | A+73 | Nº2.4 |
| 3 | Configuración del Entorno en la Nube AWS de TNPC | | |
| 3.1 | Inicio de configuración del entorno de producción en la nube de AWS | A+56 | Nº1 |
| 3.2 | Se establece el acceso VPN al entorno de producción de TNPC en la nube de AWS, no en vivo | A+83 | Nº3.1 |
| 3.3 | Fin de configuración del entorno de producción en la nube de AWS | A+90 | Nº3.2 |
| 3.4 | Inicio de configuración del entorno de pruebas en la nube de AWS | A+91 | Nº3.3 |
| 3.5 | Se establece el acceso VPN al entorno de pruebas de TNPC en la nube AWS, no en vivo | A+91 | Nº3.2 |
| 3.6 | Fin de configuración del entorno de pruebas en la nube de AWS | A+111 | Nº3.5 |
| 4 | Implementación, instalación y documentación de software con licencia de TNPC | | |
| 4.1 | TNS entrega la documentación de la Guía de Usuario del Sistema TNPC | A+112 | Nº2.5 |
| 4.2 | Software TNPC de TNS listo para instalar | A+112 | Nº2.5 |
| 4.3 | TNS inicia la instalación del Software con Licencia de TNPC en el sistema de producción | A+115 | Nº4.2 |
| 4.4 | TNS completa la instalación del Software con Licencia de TNPC en el sistema de producción | A+119 | Nº4.3 |

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

| Tarea N° | Tarea programada | A+ Fecha (Días Calendario) | Tarea de la Dependencia |
|------------|--|----------------------------|-------------------------|
| 4.5 | TNS inicia la instalación del Software con Licencia de TNPC en el sistema de pruebas del cliente | A+122 | Nº4.4 |
| 4.6 | TNS completa la instalación del Software con Licencia de TNPC en el sistema de pruebas del cliente | A+126 | Nº4.5 |
| 5 | Documentación de Aceptación y Pruebas | | |
| 5.1 | TNS entrega el borrador del Plan de Pruebas de Aceptación (ATP) de TNPC | A+76 | Nº2.5 |
| 5.2 | Comentarios a TNS respecto del borrador del Plan de Pruebas de Aceptación (ATP) de TNPC | A+90 | Nº5.1 |
| 5.3 | TNS entrega el Plan de Pruebas de Aceptación (ATP) de TNPC final | A+105 | Nº5.2 |
| 5.4 | TNS inicia la demostración del Plan de Pruebas de Aceptación (ATP) de TNPC | A+122 | Nº5.3 |
| 5.5 | TNS completa la demostración del Plan de Pruebas de Aceptación (ATP) de TNPC | A+123 | Nº5.4 |
| 5.6 | Se otorga la aceptación de la solución de TNPC | A+124 | Nº5.5 |
| 6 | Capacitación | | |
| 6.1 | TNS inicia la capacitación de Usuario Final de TNPC | A+87 | Nº2.5 |
| 6.2 | TNS completa la capacitación de Usuario Final de TNPC | A+88 | Nº6.1 |
| 7 | Mesa de Ayuda y Datacenter | | |
| 7.1 | Servicios de Mesa de Ayuda disponibles para los operadores | A+101 | #2.5,#3.4 |
| 7.2 | Datacenter de Producción no en vivo listo para la conectividad de los operadores | A+109 | Nº3.4, 7.1 |
| 8 | Planes de Pruebas de la Industria | | |
| 8.1 | TNS entrega el borrador del Plan de Pruebas de Conectividad (CTP) | A+70 | Nº2.5 |
| 8.2 | Comentarios del cliente a TNS respecto del borrador del Plan de Pruebas de Conectividad (CTP) | A+77 | Nº8.1 |
| 8.3 | TNS entrega la documentación del Plan de Pruebas de Conectividad (CTP) final | A+84 | Nº8.2 |
| 8.4 | TNS entrega el borrador del Plan de Pruebas entre Operadores (IOTP) | A+70 | Nº2.5 |
| 8.5 | Comentarios del cliente a TNS respecto del Plan de Pruebas entre Operadores (IOTP) | A+84 | Nº8.4 |
| 8.6 | TNS entrega la documentación del IOTP final | A+91 | Nº8.5 |
| 9 | Pruebas de la Industria | | |
| 9.1 | Comienzan las Pruebas de Conectividad | A+87 | Nº8.3 |
| 9.2 | Se completan las Pruebas de Conectividad | A+97 | Nº9.1 |
| 9.3 | Comienza el IOTP | A+132 | Nº5.6, Nº8.6, Nº9.2 |
| 9.4 | Finaliza el IOTP | A+196 | Nº9.3 |
| 10 | Puesta en Servicio | | |
| 10.1 | Se inicia la limpieza de producción y la preparación para la entrada en producción | A+199 | Nº9.4 |

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

| Tarea N° | Tarea programada | A+ Fecha (Días Calendario) | Tarea de la Dependencia |
|----------|---|----------------------------|-------------------------|
| 10.2 | Finaliza la limpieza de producción y la preparación para la entrada en producción | A+203 | N°10.1 |
| 10.3 | Lanzamiento comercial de TNPC | A+206 | N°10.2 |

4.1.1 *Un periodo de validación y pruebas de todo el SIPN con los operadores/proveedores y Sutel.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Tal como se detalla en la Sección 4.1, TNPC incluye una **etapa de validación y pruebas integral que involucra a todos los operadores, proveedores y SUTEL** a fin de asegurar el alistamiento operativo total antes de la entrada en producción. Esta etapa incluye pruebas de conectividad, pruebas de aceptación y pruebas entre operadores, que se ejecutan en un entorno controlado que replica las condiciones de producción. El enfoque estructurado de pruebas asegura la validación de todos los procesos del SIPN, garantiza la integración sin inconvenientes y minimiza los riesgos operativos durante la transición.

4.1.2 *Duración en días de todas las tareas y subtareas por realizar.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

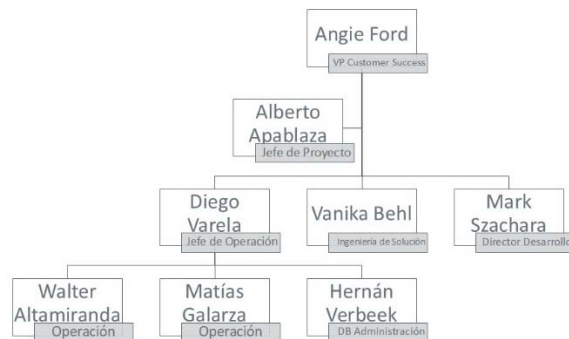
Tal como se detalla en la Sección 4.1, el plan de implementación de TNPC define claramente la **duración de todas las tareas y subtareas**. Usa el modelo en base al calendario A+ desde la suscripción del contrato al lanzamiento comercial. Cada actividad incluye tiempo de inicio y tiempo de fin definidos con dependencias para garantizar la transparencia, predictibilidad y ejecución estructurada a lo largo de todas las etapas.

4.1.3 *Incorporar el recurso humano para cada una de las tareas, es decir, los ingenieros y técnicos dedicados.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Conforme a la Sección 4.1, TNS asignará **recursos dedicados y especializados a cada etapa del proyecto**, que incluye gestión de programa, arquitectura de la solución, desarrollo, integración, pruebas y soporte. La asignación de recursos está alineada con los hitos del cronograma para asegurar la ejecución óptima. TNS ofrecerá el liderazgo técnico global y con profesionales de habla hispana.



4.1.4 *El cronograma debe ser dinámico y tener previsión para modificaciones e imprevistos.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El cronograma de implementación definido en la Sección 4.1 está diseñado como un **marco dinámico y adaptativo**, con capacidad para acomodar cambios, variaciones en el alistamiento de los operadores y eventos imprevistos. El modelo de gobierno estructurado del proyecto asegura el monitoreo continuo, gestión de riesgos y ajustes controlados, sin impacto en los tiempos totales ni en la continuidad de servicio del SIPN.

4.1.5 *Deberá contener un campo que indique el porcentaje de consecución de cada una de las tareas; con el objetivo de que cada semana se pueda evaluar el grado de avance del proyecto.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Como parte del marco de ejecución de la Sección 4.1, TNPC incluye **mecanismos de seguimiento continuo del avance**, donde cada tarea y subtarea es monitoreada con porcentajes de lo completado. Los ciclos de reportes regulares brindan a SUTEL y CTPN-M visibilidad sobre el avance del proyecto, hitos logrados y actividades pendientes para garantizar transparencia total y supervisión efectiva del proyecto.

4.1.6 *Incluir la línea crítica de actividades.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El cronograma de implementación de la Sección 4.1 incorpora el **camino crítico de las actividades** claramente definido; e identifica las dependencias claves tales como finalización de requerimientos, aprobación del operador, alistamiento del entorno y pruebas de la industria. Estas tareas críticas son gestionadas estrechamente para garantizar que se completan a tiempo, adhieren a la línea de tiempo total y se minimizan los riesgos de implementación.

4.1.7 *Presentarse en formato digital compatible con MS Project.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Tal como se indica en la Sección 4.1, el cronograma de implementación de TNPC se entregará en **formato digital totalmente compatible con MS Project** para permitir la visualización detallada de los tiempos, dependencias, asignación de recursos y seguimiento del avance. Esto garantiza colaboración, monitoreo y reportería eficientes durante todo el ciclo de vida del proyecto.

4.1.8 *Incluir una propuesta de mejora de seguridad para los enlaces de comunicación actuales con los operadores para el SIPN de legado desarrollado de acuerdo con el Manual de Interfaces y Procesos.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS incluye y entrega, como parte de esta propuesta, un **marco integral de mejora de la seguridad para los enlaces de comunicación del SIPN**, totalmente alineado con el cronograma de implementación y el enfoque de gobierno definidos en la Sección 4.1.

La arquitectura propuesta adopta un **modelo de seguridad con defensa en profundidad**, que consolida todas las capas de comunicación entre TNPC, los operadores, proveedores, SUTEL y los sistemas regulatorios externos, tal como se describe en la Sección 2.1 y la Sección 2.3. Todas las interfaces, que incluyen SOAP XML, REST APIs, intercambio de archivos SFTP, GUI del operador, portal de SUTEL, sistemas de reportería e integraciones externas están aseguradas con el uso de protocolos modernos como HTTPS con TLS 1.2 o superior, conectividad segura VPN y autenticación basada en certificados, tal como se detalla en la Sección 2.23 y la Sección 2.31. Se aplican mecanismos de autenticación mutua cuando sea requerido para asegurar una comunicación confiable entre todas las entidades.

Una mejora clave en línea con el Anexo 3 y descrita en la Sección 2.3 es la introducción y soporte de **API basadas en REST usando JSON sobre HTTPS como una alternativa segura y moderna respecto de las interfaces SOAP XML existentes**. TNPC soporta interfaces SOAP y REST en paralelo que garantizan retrocompatibilidad a la vez que permiten una modernización gradual. Las REST API están diseñadas con principios de seguridad en primer lugar que incluyen autenticación basada en token, soporte para TLS mutuo, validación estricta de esquemas y puntos finales de acceso controlados, tal como se describe en la Sección 2.23. Las cargas de trabajo JSON hacen espejo con las estructuras XML para garantizar consistencia, a la vez que mejoran el rendimiento, reducen los gastos generales y consolidan la seguridad.

La propuesta incluye la implementación de **mecanismos sólidos de autenticación y control de acceso**, que incluyen **autenticación multifactorial** para todos los usuarios privilegiados, tal como se describe en la Sección 2.29. TNPC soporta MSFA con las aplicaciones de autenticador estándar de la industria como Google Authenticator y Microsoft Authenticator, en base a contraseñas de una sola vez basadas en el tiempo. Esto se aplica a lo largo de las interfaces de los operadores, portales administrativos de SUTEL, tableros de reportería y portales de acceso de organismos autorizados. Para la interfaz pública, la autenticación segura se implementa con el uso de MSISDN y NIP, con protecciones adicionales como CATCHA, limitación de velocidad y controles de gestión de sesión, tal como se describe en la Sección 2.21.

El marco de seguridad incluye además **controles de protección de red y aplicaciones de avanzada** como Web Application Firewall, detección de intrusos y sistemas de prevención, gateway de seguridad de API, filtrado IP y protección contra amenazas que incluyen ataques de inyección y *cross-site scripting*, tal como se describe en la Sección 2.31. Todos los canales de comunicación se monitorean continuamente usando herramientas de observación en tiempo real, tal como se detalla en la Sección 2.8 y la Sección 2.30, que permiten la detección y mitigación inmediatas de anomalías o actividades no autorizadas.

La propuesta también define un **marco integral de monitoreo y respuesta ante incidencias**, donde todas las actividades de comunicación se registran, correlacionan con las transacciones de NPCDB y se analizan para eventos de seguridad, tal como se describe en la Sección 2.18 y la Sección 2.32. Se generan alertas en tiempo real y se comunican a SUTEL y los operadores a través de los canales convenidos; y cualquier incidencia de seguridad se informa con análisis detallado y acciones correctivas.

Esta presentación incluye **arquitectura detallada, descripciones, flujos de comunicación, controles de seguridad y alineación de implementación con el cronograma total del proyecto** para garantizar que las mejoras de seguridad están incluidas desde el inicio. Todas las implementaciones serán validadas en el entorno de pruebas e implementadas con estrategias de implementación en forma continua o con tiempo inactivo cero durante la ventana de mantenimiento, con impacto mínimo o controlado sobre el servicio, tal como se describe en la Sección 2.9 y la Sección 4.1.

A través de este enfoque totalmente integral y de cara al futuro, TNPC asegura que los enlaces de comunicación del SIPN son **modernos, seguros, resilientes y en cumplimiento** para aprovechar las REST API junto con las interfaces existentes a fin de mejorar la seguridad, rendimiento y sustentabilidad de la plataforma a largo plazo.

4.1.8.1 *La propuesta deberá entregarse de manera electrónica por escrito con, al menos, descripción de la propuesta, diagrama de arquitectura y cronograma.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS confirma que entregará la **propuesta completa de manera electrónica como parte de esta presentación**, que incluye todos los elementos requeridos tales como descripciones detalladas, representaciones de arquitectura y cronograma de implementación. Esta presentación brinda una **descripción integral y estructurada de la propuesta**, que contempla el diseño de la solución de TNPC, procesos operativos, marco de seguridad, enfoque de integración y cumplimiento con todos los anexos y requerimientos regulatorios aplicables, tal como se detalla en la Sección 2 y la Sección 4.

La propuesta incluye **descripciones y diagramas detallados de la arquitectura**, que cubren el modelo de implementación de AWS e incluye los entornos de producción, pruebas y recuperación ante desastres. Estas representaciones arquitectónicas ilustran los componentes del sistema, flujos de comunicación, puntos de integración, capas de seguridad y diseño de alta disponibilidad, tal como se describe en la Sección 2.1 y subsecciones asociadas.

Además, la propuesta incluye un **cronograma de implementación completo**, alineado con el Manual de Interfaces y Procesos y los requerimientos de migración del SIPN, tal como se define en la Sección 4.1. El cronograma detalla todas las etapas desde la recolección de requerimientos hasta la implementación, pruebas y lanzamiento comercial, que incluye dependencias, hitos y tiempos.

Toda la documentación se proporciona en formato electrónico estructurado para garantizar una revisión, trazabilidad y accesibilidad sencilla por parte de SUTEL y los miembros de CTPN-M. La presentación está diseñada para ofrecer total transparencia y permitir que los interesados entiendan claramente la solución propuesta, arquitectura, enfoque de implementación y línea de tiempo.

A través de esta presentación electrónica integral, TNS asegura que todos los componentes requeridos de la propuesta se entregan en forma completa, claramente documentados y alineados con los requerimientos de SUTEL para su evaluación y toma de decisiones efectiva.

4.2 *La ERPN seleccionada deberá entregar un Manual de Interfaces y Procesos acorde a la plataforma de legado para la versión que entregue previo a la migración del SIPN actual.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS entregará un **Manual de Interfaces y Procesos integral alineado con la plataforma legacy del SIPN existente** para garantizar la continuidad, compatibilidad y alineación operativa total antes de la migración hacia la plataforma de TNPC. Este manual servirá como referencia autorizada para todos los interesados, que incluyen operadores, SUTEL y CTPN-M que les permita realizar una interacción sin inconvenientes con el sistema durante las etapas previa a la migración y la transición.

El manual se desarrollará en base a un análisis detallado de la implementación actual del SIPN y el Manual de Interfaces y Procesos definido en el Anexo 1, Anexo 2 y Anexo 3, a fin de asegurar que todos los procesos, flujos de mensajes, reglas de validación y procedimientos operativos existentes se documentan con precisión. Incluirá **descripciones completas de todos los procesos de portación**, que incluyen generación de NIP, prevalidación, manejo de solicitudes de portabilidad, respuesta del donante, activación, cancelación, retorno de número y sincronización. Cada proceso tendrá el soporte de diagramas de

secuencias, definiciones de mensajes, configuraciones de temporizadores y reglas de validación para garantizar claridad y consistencia a todos los participantes.

El Manual de Interfaces y Procesos también ofrecerá **especificaciones detalladas de todas las interfaces de comunicación**, que incluyen formatos de mensajes SOAP XML, REST API equivalentes, cuando corresponda, estructura de datos, definiciones de campos, manejo de errores, códigos de rechazo y requerimientos de seguridad. Esto garantiza que los operadores puedan mantener sus integraciones existentes sin interrupción, mientras se preparan para las mejoras futuras. El manual también documentará todos los puntos finales de las interfaces, requerimientos de conectividad y mecanismos de autenticación para asegurar la implementación consistente a lo largo de todos los participantes.

El manual además incluirá **procedimientos operativos, descripciones de flujos de trabajo y definiciones de los comportamientos del sistema** que contemplan gestión del ciclo de vida de las transacciones, registros de auditoría, reportería y manejo de excepciones. Definirá claramente los roles y responsabilidades de cada participante para asegurar la alineación con los requerimientos regulatorios y el gobierno operativo.

El manual se entregará en formato electrónico antes de la migración del SIPN, como parte del cronograma de implementación definido en la Sección 4.1; y se pondrá a disposición a través de un repositorio centralizado de documentación con control de versión y acceso basado en roles. Todas las actualizaciones y revisiones serán rastreadas a través del proceso formal de versiones para garantizar que los interesados siempre tienen acceso a la última versión aprobada, al tiempo que se mantiene una trazabilidad total de los cambios.

A través de este enfoque estructurado y detallado, TNS asegura que el Manual de Interfaces y Procesos ofrece la **continuidad completa de la plataforma legacy del SIPN**, soporta la transición sin inconvenientes durante la migración y establece una base sólida para la evolución futura del sistema de portabilidad numérica.

4.3 *La ERP seleccionada deberá entregar durante el primer semestre de 2028 una propuesta de mejora, rediseño y optimización para los procedimientos actuales de portación con el fin de modernizar de manera completa el SIPN según las mejores prácticas de la industria.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Durante el primer semestre de 2028, TNS entregará una **propuesta integral de mejora, rediseño y optimización de la plataforma** con el fin de modernizar todo el proceso en línea con las mejores prácticas internacionales y los objetivos regulatorios de SUTEL. Esta propuesta se basa en el **conocimiento operativo recolectado durante el uso del sistema en vivo** que incluye rendimiento de transacciones, cumplimiento de SLA, interacciones del operador, experiencia del usuario y análisis del sistema captados dentro de la plataforma de TNPC.

La propuesta de mejora incluirá una **evaluación estructurada de los procesos de portación actual**, que identifiquen las oportunidades de optimización, simplificación y automatización dentro de todo el ciclo de vida e incluyan generación de NIP, prevalidación, ejecución de portación, sincronización y manejo de excepciones. El objetivo es reducir el tiempo de procesamiento, eliminar ineficiencias, mejorar la transparencia y mejorar la experiencia total para los operadores, SUTEL y los usuarios finales.

Un componente clave de esta propuesta será la **evolución del SIPN hacia una plataforma unificada de portabilidad, con soporte tanto de Portabilidad Numérica Móvil como Portabilidad Numérica Fija**. TNPC tiene probada experiencia en la entrega de portabilidad numérica móvil y fija en múltiples países; y la propuesta incluirá una hoja de ruta detallada para extender las capacidades del SIPN a fin de admitir servicios fijos. Esto incluye mejoras al modelo de datos de NPCDB, lógica de enrutamiento, flujos de procesos e interfaces de integración para acomodar operadores de red fija y garantizar una transición escalable y sin inconvenientes hacia un entorno de portabilidad convergente.

Además, la propuesta incluirá la **introducción de validación biométrica con detección de prueba de vida**, en línea con los requerimientos del pliego de condiciones de Costa Rica. TNPC propondrá un módulo biométrico opcional que permite asegurar la autenticación del suscriptor durante el proceso de portación mediante reconocimiento facial o técnicas biométricas equivalentes. La solución incluirá mecanismos de detección de prueba de vida para evitar la suplantación de identidad e intentos fraudulentos; y asegurar que la persona que inicia la solicitud de portabilidad está físicamente presente y está autorizada. El módulo biométrico se integrará al flujo de trabajo de TNPC a través de API seguras para permitir que los operadores invoquen la verificación biométrica como parte de los procesos de prevalidación y solicitud de portabilidad. La propuesta detallará las opciones de implementación, arquitectura de integración, consideraciones de privacidad de datos y cumplimiento con los marcos regulatorios aplicables.

La propuesta de mejora también incluirá la **modernización de interfaces y mecanismos de comunicación** tal como adopción expandida de controles de seguridad mejorada, mejor automatización de las actualizaciones de enrutamiento y sincronización optimizada de procesos. Se brindarán recomendaciones para una mayor consolidación de la ciberseguridad, mejorar la escalabilidad del sistema y mejorar la integración con las plataformas regulatorias de SUTEL.

Como parte del entregable, TNS ofrece un **paquete completo de documentación e implementación** que incluye diagramas de flujos de procesos actualizados, Manual de Interfaces y Procesos con mejoras, diagramas de evolución de la arquitectura y una hoja de ruta detallada de la implementación con línea de tiempo. La propuesta incluirá análisis de impacto, evaluación de riesgos y estrategias de validación para garantizar la adopción sin inconvenientes ni interrupciones en las operaciones en curso del SIPN.

Todas las mejoras propuestas serán validadas en los entornos de desarrollo y producción con la participación de los operadores y SUTEL; y se implementarán con estrategias de implementación en forma continua o con tiempo inactivo cero durante la ventana de mantenimiento, con impacto mínimo o controlado sobre el servicio. La hoja de ruta estará alineada con el marco estructurado de versiones para garantizar la evolución controlada y predecible de la plataforma del SIPN.

A través de este enfoque innovador y de cara al futuro, TNPC asegura que el SIPN evolucione hacia una **plataforma de portabilidad, totalmente moderna, segura y convergente**, que admite servicios móviles y fijos, mecanismos de autenticación de avanzada como los biométricos, y mejora continua alineada con la visión estratégica a largo plazo de SUTEL.

4.3.1 *Deberá entregar una propuesta formal con una descripción completa y un Manual de Interfaces y Procesos acorde a la versión del SIPN que se implementará.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS entregará un **paquete de la propuesta formal e integral** en línea con la versión del SIPN que se implementará para ofrecer una descripción completa y detallada de la solución, procesos, arquitectura y marco operativo. Este entregable será estructurado para servir como **referencia autorizada para la implementación, operación y gobierno del SIPN**, a fin de garantizar claridad, trazabilidad y alineación con los requerimientos de SUTEL y CTPN-M.

La propuesta incluirá una **descripción completa de la solución** que contemple la arquitectura del sistema, modelo de implementación, marco de comunicación, controles de seguridad, gestión de datos, integración con los operadores y plataformas regulatorias, capacidad de reportería y procedimientos operativos. Definirá claramente todas las funcionalidades del SIPN, flujos de trabajo e interacciones para garantizar que todos los interesados tienen un entendimiento consistente del comportamiento y las responsabilidades del sistema.

Un componente central del entregable será el **Manual de Interfaces y Procesos específico para la versión del SIPN que se implementará**, desarrollado conforme a los requerimientos del Anexo y con las mejoras en base a las capacidades de TNPC. Este manual incluirá descripciones detalladas de todos los procesos de portación tales como generación de NIP, prevalidación, ejecución de portación, cancelación,

retorno de número y sincronización. Cada proceso tendrá el soporte de diagramas, flujos de mensajes, definiciones de temporizadores, reglas de validación, códigos de rechazo y transiciones de estado para garantizar una pauta de implementación precisa y sin ambigüedades.

El manual también ofrecerá las **especificaciones de interfaces completas** que incluyen las definiciones SOAP XML y REST API, esquemas de mensajes, modelos de datos, descripciones de campos, requerimientos de seguridad, mecanismos de autenticación y configuraciones de conectividad. Esto asegura la interoperabilidad sin inconvenientes con los sistemas del operador y plataformas regulatorias, a la vez que admite la modernización y mejoras futuras.

Toda la documentación será mantenida bajo un **marco controlado de versiones y gobierno** que asegure que cada versión del SIPN está acompañada por el Manual de Interfaces y Procesos actualizado para reflejar el comportamiento y la configuración exactas del sistema. Se incluirán histórico de versiones, registros de cambios y registros de aprobación para permitir la trazabilidad total de las actualizaciones y la alineación con la evolución regulatoria.

La propuesta formal y la documentación asociada se entregarán electrónicamente y se pondrán a disposición a través del repositorio centralizado de documentación, con acceso basado en roles para SUTEL, los operadores e interesados autorizados. Las actualizaciones serán sincronizadas con las versiones del sistema con estrategias de cero tiempo inactivo o implementación continua, o durante las ventanas de mantenimiento convenidas con impacto mínimo o controlado en el servicio.

A través de este entregable estructurado e integral, TNS asegura que la implementación del SIPN tiene el respaldo de **documentación clara, detallada y autorizada**, que permita la implementación eficiente, integración sin inconvenientes y funcionamiento consistente en pleno cumplimiento de los requerimientos de SUTEL.

4.3.2 *Adicionalmente deberá proponer el cronograma que permita su desarrollo, prueba y puesta en producción.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Como parte de la propuesta de mejora, rediseño y optimización que se entregará en el primer semestre de 2028, TNS ofrece un **cronograma estructurado, por etapas y totalmente regulado para desarrollo, pruebas y entrada en producción**, que está alineado con la versión mejorada del SIPN y la hoja de ruta futura. Este cronograma se basará en el marco de implementación probado descrito en la Sección 4.1 e incorporará las lecciones aprendidas de las operaciones en vivo, aporte de los operadores y análisis de rendimiento recolectados durante la etapa de implementación inicial.

El cronograma propuesto seguirá un **enfoque de ciclo de vida** controlado para asegurar que todas las mejoras sean diseñadas e implementadas, sin impacto en las operaciones en curso del SIPN. La etapa de desarrollo se focalizará en la implementación de las mejoras aprobadas, que incluyen optimización de procesos, mejoras de integración, soporte para portabilidad numérica fija y capacidades avanzadas como validación biométrica. Esta etapa incluirá actualizaciones de las especificaciones detalladas, ajustes de interfaces y actualizaciones del Manual de Interfaces y Procesos para garantizar la alineación total con la versión mejorada del SIPN.

La **etapa de pruebas** será realizada en un entorno dedicado de pruebas e incluirá las actividades de validación integral con los operadores y SUTEL. Esto contemplará pruebas funcionales, pruebas de regresión, validación de rendimiento y pruebas de integración para todos los procesos e interfaces mejorados. Se pondrá énfasis especial en validar la retrocompatibilidad para garantizar que las integraciones de los operadores existentes sigan funcionando sin problema junto con las nuevas mejoras. Se realizará la capacitación con el sistema mejorado durante esta etapa para asegurar el alistamiento de todos los interesados.

Después de la validación exitosa, el cronograma avanzará hacia la **etapa de entrada en producción**, donde se introducirán las mejoras de manera controlada y por etapas. La implementación se ejecutará con

estrategias de cero tiempo inactivo o implementación continua, o durante las ventanas de mantenimiento convenidas con impacto mínimo o controlado en el servicio para garantizar las operaciones ininterrumpidas del SIPN. Cuando corresponda, se podrán introducir mejoras en forma incremental para minimizar el riesgo y permitir la adopción progresiva por parte de los operadores.

El cronograma será entregado en **formato digital detallado compatible con MS Project**, que incluye desglose de tareas, dependencias, hitos, actividades de camino crítico y asignación de recursos. Incluirá indicadores de avance mensurables que permitan a SUTEL y CTPN-M rastrear el estado de implementación y garantizar la alineación con los tiempos acordados. El cronograma también incorporará la gestión de riesgos y la planificación de contingencia para abordar desafíos potenciales durante la ejecución.

A través de este enfoque de cronograma estructurado y de cara al futuro, TNS garantiza que todas las mejoras del SIPN **se implementan con eficiencia, validan integralmente e implantan sin inconvenientes**, para permitir la evolución continua de la plataforma a la vez que se mantiene la estabilidad, seguridad y cumplimiento con los requerimientos de SUTEL.

4.3.3 *Una vez que se implemente el nuevo SIPN, cada actualización que se lleve a cabo considerando lo dispuesto en el punto 2.9 del pliego de condiciones, deberá quedar debidamente incorporada en el Manual de Interfaces y Procesos el cual contendrá un historial de cambios con fecha y descripción de lo que se realizó.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Como parte del **marco de mejora, rediseño y optimización del SIPN** definido en la Sección 4.3, TNS asegurará que todas las actualizaciones realizadas conforme a la Sección 2.9 **se incorporen totalmente en el Manual de Interfaces y Procesos correspondiente a la versión del SIPN mejorado**. Esto asegura la sincronización de la documentación con la evolución del sistema y refleja con precisión todos los cambios funcionales, técnicos y operativos introducidos como parte de la hoja de ruta de mejoras de 2028.

Después de cada actualización aprobada, ya sea menor o mayor, se revisará el Manual de Interfaces y Procesos para incluir las **definiciones de procesos, flujos de mensajes, especificaciones de interfaces, reglas de validación y procedimientos operativos actualizados**, para garantizar que todos los interesados, incluidos SUTEL, CTPN-M y los operadores, tengan una referencia consistente y autorizada en línea con la versión implementada del sistema. Esto es particularmente crítico en el contexto de las mejoras de la Sección 4.3, que pueden incluir optimizaciones de procesos, adopción de REST API, posibilitar la portabilidad numérica fija y las capacidades de validación biométrica.

Cada versión actualizada del Manual de Interfaces y Procesos incluirá una **sección histórica formal y estructurada** que ofrezca trazabilidad total de todas las modificaciones. Este cambio en el historial documentará claramente:

- Número de versión del SIPN asociado a la actualización
- Fecha de implementación
- Descripción detallada del cambio o mejora

Este enfoque asegura que toda la evolución del sistema es transparente, auditable y está alineada con los requerimientos de gobierno definidos por SUTEL y CTPN-M.

Toda la documentación actualizada será publicada en el repositorio centralizado de documentación descrito en la Sección 2, con **control de versión, acceso basado en roles y retención histórica de versión**, que permite a todos los interesados acceder tanto a la versión actual como la anterior, según sea requerido. Las actualizaciones serán comunicadas en forma proactiva a todos los interesados para asegurar la alineación previo o inmediatamente después de la implantación.

Las actualizaciones de documentación estarán estrechamente combinadas con el cronograma de implantación de mejoras definido en la Sección 4.3 y se implementarán con estrategias de cero tiempo

inactivo o implementación continua, o durante las ventanas de mantenimiento convenidas con impacto mínimo o controlado en el servicio para garantizar las operaciones ininterrumpidas del SIPN.

A través de este enfoque estructurado y regulado, TNS asegura que el Manual de Interfaces y Procesos se mantiene **continuamente actualizado, es totalmente trazable y está alineado con las mejoras del SIPN**; y brinda soporte a la implementación, funcionamiento y evolución de la plataforma a largo plazo, con efectividad conforme a la Sección 4.3.

4.4 *Plantear un plan de fortalezas, oportunidades, desafíos y riesgos para cada una de las tareas o hitos que la ERPN seleccionada llevará a cabo para cada cronograma.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS ofrecerá un **marco integral de gestión de Fortalezas, Debilidades, Oportunidades, Amenazas y Riesgos**, alineado con cada tarea y etapa definida en el cronograma de implementación (Sección 4.1) y la hoja de ruta de mejoras (Sección 4.3). Este marco está incorporado dentro de todo el modelo de gobierno total del proyecto y se mantiene en forma continua durante todo el ciclo de vida de la implementación y evolución del SIPN para garantizar la identificación, mitigación y monitoreo activos de riesgos, a la vez que aprovecha las fortalezas y oportunidades.

El plan de **Fortalezas, Debilidades, Oportunidades, Amenazas (FODA)** y riesgos se estructura a lo largo de todas las categorías de tareas importantes dentro del cronograma que incluyen definición de requerimientos, diseño, desarrollo, integración, pruebas, migración, implantación del sistema y operaciones después de la entrada en producción. Para cada etapa, TNS define fortalezas específicas, debilidades potenciales, oportunidades para optimización, amenazas externas y las correspondientes estrategias de mitigación de riesgo para asegurar un **enfoque de gestión de riesgo holístico y accionable**.

Para la **definición de requerimientos y diseño de procesos**, las fortalezas incluyen la experiencia técnica probada y marcos estandarizados de TNS, al tiempo que los riesgos, como demoras en el aporte de los operadores, se mitigan a través de talleres estructurados, participación temprana e hitos de aprobación definidos. Existen oportunidades para mejorar los procesos a través de automatización y las mejores prácticas, a la vez que las amenazas potenciales, como los cambios regulatorios, se gestionan a través de un diseño flexible y configurable del sistema.

Para la **integración y conectividad del operador**, las fortalezas incluyen las interfaces estandarizadas y la interoperabilidad probada, mientras que riesgos, como demoras de integración o en el alistamiento de los operadores, se mitigan a través de pruebas en paralelo, mecanismos de reversión tales como operaciones basadas en GUI y coordinación continua con los operadores. Las oportunidades incluyen ingreso optimizado de nuevos participantes, mientras que las amenazas, como las dependencias de sistemas externos, se abordan a través de mecanismos de reintento y monitoreo.

Para las **etapas de validación, pruebas y migración**, las fortalezas incluyen la capacidad de ejecución en paralelo de TNPC y la experiencia probada en migración, que incluye migraciones en gran escala como Perú y Estados Unidos. Los riesgos relativos a integridad de datos o sincronización se mitigan a través de verificaciones de conciliación, validación continua de datos y procedimientos de corte controlado. Las oportunidades incluyen optimización de procesos en base a aportes sobre pruebas en tiempo real, mientras que las amenazas, como el comportamiento inesperado del sistema, se gestionan a través de pruebas estructuradas y procedimientos de reversión.

Para implantación y operaciones, las fortalezas incluyen arquitectura de alta disponibilidad y monitoreo automático, mientras que los riesgos, como problemas de rendimiento del sistema o amenazas de seguridad, se mitigan a través de monitoreo en tiempo real, escalada automática, mecanismos de recuperación ante fallas y controles de ciberseguridad. Las oportunidades incluyen optimización continua del rendimiento y evolución del sistema, mientras que las amenazas como ciberataques se abordan a través del marco de seguridad con defensa en profundidad.

A lo largo de todas las etapas, el enfoque de gestión de riesgos incluye:

- Identificación y clasificación continua de riesgos en base al impacto y probabilidad
- Planes definidos de mitigación y contingencia para cada riesgo identificado
- Asignación de responsabilidad para monitoreo y resolución del riesgo
- Integración de seguimiento del riesgo en la reportería y gobierno de avance del proyecto
- Revisión y actualización regular de los registros de riesgos en coordinación con SUTEL y CTPN-M

El FODA y el plan de riesgos se documentarán y entregarán como parte de la gestión del proyecto, en línea con el cronograma de implementación en la Sección 4.1 y la hoja de ruta en la Sección 4.3; y se mantendrán en forma dinámica durante todo el ciclo de vida del proyecto. Esto asegura que todos los interesados tengan visibilidad total de los riesgos potenciales, las estrategias de mitigación y las oportunidades de mejora continua.

A través de este enfoque estructurado y proactivo, TNS asegura que todas las tareas dentro del cronograma del SIPN se ejecuten con **riesgo mínimo, máxima eficiencia y total confianza operativa** para una implementación exitosa y para la sustentabilidad de la plataforma a largo plazo.

5 Sistema para interposición de tickets para consultas, incidencias y solicitudes de servicio entre operadores/proveedores, la Sutel y/o la ERPN.

5.1 *Brindar una plataforma para interposición de tickets para consultas, incidencias y/o solicitudes de servicio entre los operadores/proveedores, la Sutel y/o la ERPN.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC ofrece una **plataforma de gestión de interposición de tickets y servicio centralizada, segura y totalmente integrada** para soporte de todas las interacciones operativas, consultas, incidencias, actividades de mantenimiento y solicitudes de servicio entre los operadores/proveedores, SUTEL, CTPN-M y el equipo operativo de la ERPN.

La plataforma soportará la gestión del ciclo de vida completo de las solicitudes operativas, que incluyen **creación de ticket, categorización, priorización, asignación, escalada, monitoreo de SLA, seguimiento de resolución, validación de cierre y capacidad de auditoría histórica**. Los usuarios autorizados tendrán acceso seguro vía web para crear, monitorear, actualizar y rastrear los tickets en tiempo real, a fin de asegurar transparencia operativa total y coordinación eficiente entre todos los interesados.

El entorno de generación de tickets soportará múltiples procesos operativos, que incluyen:

- Gestión de incidencias
- Consultas y coordinación operativa
- Solicitudes de servicio
- Notificaciones de mantenimiento
- Actividades de control de cambios
- Soporte de integración y conectividad
- Problemas de actualización de enrutamiento
- Gestión de escalada
- Comunicaciones operativas regulatorias

La plataforma ofrecerá **flujos de trabajo configurables, control de acceso basado en roles, notificaciones automáticas, reglas de escalada, seguimiento de SLA, reportería de tableros, registros de auditoría y capacidades de análisis histórico** para asegurar una gestión eficiente del servicio y del gobierno operativo. Las notificaciones y actualizaciones se entregarán a través de los canales de comunicación configurables que incluyen alertas por correo electrónico y notificaciones automáticas del flujo de trabajo.

La plataforma de tickets también ofrece capacidades integrales de estadísticas operativas y reportería que incluyen **volumen de tickets, tiempos de respuesta, métricas de resolución, indicadores de cumplimiento de SLA, estadísticas de escalada, tendencias de incidencias, análisis de caídas de sistema, Tiempo Medio para Acusar Recibido (MTTA), Tiempo Medio para Resolución (MTTR) y análisis de rendimiento del servicio**. Los reportes y tableros estarán disponibles en formatos que incluyen PDF, XLSX, y CSV para los usuarios autorizados.

La solución funcionará **24x7x365** y se integrará a los procesos de monitoreo, generación de alertas y soporte operativo de TNPC para asegurar la rápida detección de problemas, gestión de respuesta coordinada y soporte operativo continuo para el ecosistema del SIPN en Costa Rica.

A través de esta capacidad integral de generación de tickets y gestión de servicio, TNPC asegura la **colaboración eficiente, transparencia operativa, rápida resolución de incidencias, gestión proactiva del servicio y servicios de soporte de alta calidad** para SUTEL, los operadores/proveedores y todos los interesados autorizados del SIPN.

5.1.1 Los GAA y GAT tendrán un plazo máximo para responder de 24 horas naturales (plazo configurable por el CTPN-M).

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC garantiza que toda la **Asistencia Administrativa General (GAA) y Tickets Administrativos Generales/Tickets de Asistencia Técnica (GAT)** en consultas, incidencias y solicitudes de servicios se acusan recibo y responden formalmente dentro de las **24 horas naturales o menos**, o dentro del marco de tiempo configurable definido por CTPN-M.

La plataforma centralizada de gestión de tickets y servicios funciona **24x7x365** y soportará una clasificación estructurada de incidencias, gestión de SLA, procedimientos de escalada, seguimiento operativo y flujos de trabajo de resolución a lo largo de todos los interesados autorizados, que incluyen operadores/proveedores, SUTEL y CTPN-M.

El marco de soporte incluirá:

- **Soporte de Nivel 1** para recepción de ticket, categorización, diagnóstico inicial, acuse de recibo, coordinación operativa y comunicación con el usuario
- **Soporte de Nivel 2** para detección y resolución avanzada de problemas, análisis de integración, problemas con actualización de enrutamiento, investigación operativa y actividades de restablecimiento de servicio
- **Soporte de Ingeniería de Nivel 3** para incidencias técnicas complejas, análisis a nivel de plataforma, resolución de defectos de software, investigaciones de base de datos y soporte de ingeniería especializada.

La plataforma soportará modelos de clasificación de severidad y gestión de SLA configurables, que incluyen:

| Niveles de Severidad | Descripción | Objetivo de respuesta inicial | Resolución / Objetivo de restauración |
|------------------------------|---|--|---------------------------------------|
| Severidad 1 (Crítica) | Incidencias que evitan la ejecución total o parcial de las transacciones de portación, caídas del sistema del servicio del SIPN críticas o impacto operativo mayor que afecta los servicios de portabilidad | Escalada inmediata y manejo operativo | 1 hora natural |
| Severidad 2 (Alta) | Incidencias que afectan una transacción de portación específica, degradación parcial de servicio, fallas de interfaz o impacto en la conectividad del operador/proveedor con disponibilidad limitada de solución temporal | Manejo operativo prioritario | 6 horas naturales |
| Severidad 3 (Media) | Consultas operativas generales, solicitudes informativas, actividades de soporte no críticas o aclaraciones operativas de bajo impacto | Manejo operativo estándar | 24 horas naturales |

Todos los tickets incluirán:

- Número de identificación único del ticket
- Marcas de fecha y hora
- Detalles del operador/proveedor solicitante
- Categoría y severidad de incidencia
- Grupo de soporte asignado
- Histórico de escalada
- Estado de seguimiento de SLA
- Detalles de resolución y pista de auditoría

La plataforma ofrecerá **notificaciones automáticas, flujos de trabajo de escalada, tableros en tiempo real, seguimiento de SLA, reportes históricos, auditoría y análisis operativo** para asegurar transparencia, responsabilidad y gobierno operativo eficiente.

A través de un marco estructurado de soporte operativo y gestión de SLA, TNPC asegura una **rápida gestión de respuesta, visibilidad operativa continua, resolución efectiva de incidencias y cumplimiento total con los requerimientos de servicio y operativos de CTPN-M.**

5.1.2 *El sistema provisto por la ERPN seleccionada notificará a las partes involucradas en la atención por correo electrónico, al menos, en las siguientes ocasiones:*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrece un **marco integral de notificaciones por correo electrónico** para asegurar la comunicación a tiempo, transparente y confiable entre los operadores/proveedores, SUTEL, CTPN-M y el equipo operativo de la ERPN. La capacidad de notificaciones será totalmente integrada a los procesos centralizados de tickets, monitoreo operativo y gestión de servicio para una coordinación operativa eficiente y rápida concientización de eventos y actividades importantes.

La plataforma generará notificaciones por correo electrónico configurables para eventos operativos y de gestión de servicio que incluyen, sin carácter limitativo:

- Creación y acuse de recibo de ticket
- Asignación y escalada de incidencias
- Actualizaciones de estado de ticket y notificaciones de resolución
- Actividades de mantenimiento, ventanas de servicio planificadas, alertas operativas críticas, notificaciones de caídas del sistema, eventos de disponibilidad del sistema y notificaciones de recuperación de servicio
- Problemas de conectividad o integración del operador
- Actividades de control de cambios
- Reportes operativos y resúmenes programados

En las notificaciones se podrán configurar grupos de receptores, listas de distribución, políticas de escalada en base a severidad y flujos de trabajo accionados por eventos para asegurar que los interesados correspondientes son informados en tiempo real en base a los roles y responsabilidades operativas.

La plataforma mantendrá capacidad completa de auditoría y trazabilidad de todas las actividades de notificaciones, que incluyen marcas de tiempo, receptores, estado de entrega, histórico de escalada y eventos operativos asociados. Las plantillas de notificaciones, reglas de escalada, grupos de distribución y preferencias de comunicación serán configurables en coordinación con SUTEL y CTPN-M para estar alineados con los requerimientos operativos y de gobierno.

El marco de notificaciones funcionará **24x7x365** y se integrará a los procesos de monitoreo, gestión de SLA y soporte operativo para asegurar una comunicación proactiva, rápida concientización operativa y coordinación eficiente a lo largo de todo el ecosistema del SIPN en Costa Rica.

A través de esta capacidad integrada de notificaciones, TNPC asegura la **visibilidad operativa continua, comunicación proactiva a interesados, coordinación eficiencia de incidencias y transparencia operativa mejorada** para todos los participantes autorizados del SIPN.

5.1.2.1 *Inmediatamente después de la interposición de la incidencia.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC generará **notificaciones inmediatas por correo electrónico** a los operadores/proveedores, SUTEL, CTPN-M y el personal operativo autorizado de la ERPN correspondiente inmediatamente después de que una incidencia, consulta o solicitud de servicio sea formalmente registrada dentro de la plataforma de tickets.

La notificación incluirá detalles operativos relevantes tales como:

- Número de identificación único del ticket
- Fecha y hora de registro de la incidencia
- Categoría y nivel de severidad de la incidencia
- Servicios u operadores/proveedores afectados
- Breve descripción de la incidencia
- Estado actual del ticket
- Grupo de soporte asignado o titular operativo
- Enlaces de referencia o información de seguimiento, cuando corresponda

Esta capacidad de notificación inmediata asegura la **rápida concientización operativa, coordinación oportuna, trazabilidad y gestión eficiente de incidencias** a lo largo de todos los interesados involucrados en las operaciones del SIPN. Todas las actividades de notificación serán registradas y auditables dentro de la plataforma a fin de garantizar transparencia operativa y cumplimiento con los requerimientos de gobierno.

5.1.2.2. *Previo al vencimiento: 2 horas hábiles antes.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC generará **notificaciones proactivas por correo electrónico al menos dos (2) horas hábiles antes del vencimiento de los plazos operativos aplicables, umbrales de SLA, ventanas de mantenimiento o acciones con tickets pendientes.**

Estas notificaciones anticipadas se distribuirán a los operadores/proveedores, SUTEL, CTPN-M y al personal operativo autorizado correspondiente para asegurar la concientización a tiempo, gestión de

escalada y coordinación operativa antes de llegar a las condiciones de vencimiento. Las notificaciones incluirán información relevante tal como:

- Número de identificación del ticket
- Actividad o acción pendiente
- Vencimiento o tiempo de SLA aplicable
- Estado actual del ticket o proceso
- Servicios o interesados afectados
- Titular operativo o grupo de soporte asignado

Esta capacidad de notificación proactiva permite la **gestión operativa eficiente, manejo oportuno de escalada, cumplimiento de SLA y coordinación continua del servicio** en todo el ecosistema del SIPN. Todas las notificaciones previas al vencimiento y las actividades asociadas se registran en forma completa y son auditables dentro de la plataforma para asegurar la transparencia, trazabilidad y responsabilidad operativa.

5.1.2.2 *Al vencimiento del plazo de atención.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC generará **notificaciones inmediatas por correo electrónico al vencimiento de los tiempos de los SLA aplicables para un ticket pendiente de acción.**

Las notificaciones de vencimiento serán automáticamente distribuidas a los operadores/proveedores, SUTEL, CTPN-M, los grupos de soporte asignados y el personal operativo autorizado correspondiente a fin de asegurar la rápida concientización, gestión de escalada y seguimiento operativo a tiempo. Las notificaciones incluirán:

- Número de identificación del ticket
- Fecha y hora de creación del ticket
- Fecha y hora de vencimiento del SLA
- Estado actual del ticket y nivel de severidad
- Servicios o interesados afectados
- Titular operativo o grupo de escalada asignado
- Acciones pendientes o actividades de seguimiento requeridas

El marco de notificaciones soportará reglas de escalada y flujos de trabajo operativos configurables a fin de asegurar que las incidencias no resueltas o vencidas reciban la visibilidad y atención de gestión correspondiente. Todos los eventos de vencimientos, notificaciones, escaladas y las acciones asociadas se registran en forma completa y son auditables dentro de la plataforma para asegurar la transparencia, trazabilidad y responsabilidad operativa.

A través de esta capacidad de notificación proactiva de vencimientos, TNPC asegura la **gestión efectiva de SLA, rápida concientización operativa, manejo eficiente de la escalada y gobierno de servicio continuo** a lo largo de todo el ecosistema del SIPN en Costa Rica.

5.2 *Permitir escalar el ticket, cuando corresponda, a una instancia de resolución final, ya sea el regulador (Sutel) o la entidad centralizada hasta un máximo de 5 días naturales después de la respuesta/solución brindada.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de tickets y gestión de servicios de TNPC soporta un **marco estructurado de escalada, revisión y reapertura** que permite a los tickets permanecer bajo la gestión de escalada y gobierno operativo hasta alcanzar la resolución final y cierre formal.

Después de la emisión de la respuesta inicial o resolución propuesta, la plataforma permitirá que el regulador (SUTEL), CTPN-M, los operadores/proveedores o interesados autorizados **escalen, reabran o soliciten revisión adicional de un ticket por hasta cinco (5) días naturales**, según sea aplicable. Esta capacidad asegura que las incidencias, problemas operativos o solicitudes de servicios no sean prematuramente cerradas; y que todos los interesados tengan suficiente oportunidad para validar la resolución propuesta y el resultado operativo.

El marco de escalada soportará:

- Flujos de trabajo de escalada multinivel
- Reapertura y reasignación de ticket
- Procesos de revisión y validación operativa
- Notificaciones y recordatorios de escalada
- Capacidad de auditoría y seguimiento histórico de todas las acciones de escalada
- Tiempos de escalada y flujos de trabajo de aprobaciones configurables
- Seguimiento de confirmación pendiente de interesados previo al cierre

Todas las actividades de escalada, comentarios, cambios de estado, aprobaciones y validaciones de resolución se registran en forma completa y son auditables dentro de la plataforma para asegurar la transparencia, trazabilidad y responsabilidad operativa. La plataforma también ofrece visibilidad en tiempo real del estado de escalada, acciones pendientes e histórico del ciclo de vida del ticket para los usuarios autorizados.

A través de esta capacidad de gestión controlada de escalada y resolución, TNPC asegura **gobierno operativo efectivo, resolución colaborativa del problema, transparencia para los interesados y gestión de calidad de servicio continua** a lo largo de todo el ecosistema del SIPN en Costa Rica.

5.3 *Permitir la interacción entre los operadores/proveedores de acuerdo con el rol (donante/receptor) según cada proceso.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC soportará la **interacción segura y controlada entre los operadores/proveedores en base al rol operativo como donante o receptor dentro de cada transacción de portación**. La plataforma de tickets y gestión de servicios permitirá a los interesados colaborar, intercambiar información, brindar actualizaciones, solicitar aclaraciones y coordinar las actividades operativas **caso por caso**, al tiempo que mantendrá trazabilidad total y gobierno operativo.

El acceso a tickets, comentarios operativos, adjuntos, acciones del flujo de trabajo y comunicaciones asociadas a las transacciones estará regido por **controles de acceso basados en roles y reglas de**

visibilidad a nivel de transacción para garantizar que cada operador/proveedor pueda acceder solo a la información y actividades operativas relevantes a su rol autorizado dentro del proceso de portación.

La plataforma soportará:

- Interacción entre donante y receptor dentro del mismo ticket
- Hilos de comunicaciones y coordinación operativa del caso específico
- Compartir adjuntos y documentos
- Comentarios operativos y solicitudes de aclaración
- Flujos de trabajo de escalada y colaboración
- Actualizaciones de estado y seguimiento de acciones
- Capacidad de auditoría y seguimiento histórico de todas las interacciones

La plataforma de tickets asegurará que los **operadores/proveedores que no estén asociados a una transacción de portación específica como donante o receptor no tengan visibilidad ni accedan a los detalles de la transacción, contenidos del ticket, comunicaciones operativas, adjuntos o datos asociados a los otros operadores/proveedores**. Este modelo de acceso controlado asegura la confidencialidad, aislamiento operativo, privacidad de datos y cumplimiento con los requerimientos regulatorios y de gobierno operativo.

Todas las interacciones entre los operadores/proveedores, SUTEL, CTPN-M y el equipo operativo de la ERPN se registrarán por completo, tendrán marcas de tiempo y serán auditables para asegurar la transparencia, responsabilidad y cumplimiento de los requerimientos operativos y regulatorios.

A través de este marco de interacción seguro y colaborativo, TNPC asegura una **coordinación operativa eficiente, compartir información en forma controlada, gestión transparente de casos, confidencialidad de datos y una resolución efectiva de las actividades asociadas a la portabilidad** en todo el ecosistema del SIPN en Costa Rica.

5.4 *Tendrá un sistema de autenticación mediante credenciales únicas y autenticación multifactorial.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC incorporará un marco de autenticación y control de acceso seguro en base a credenciales únicas del usuario y mecanismos de autenticación multifactorial (MFA) para garantizar el acceso seguro a todas las funciones de tickets, operativas, administrativas y de soporte.

A cada usuario autorizado se le asignarán **credenciales individuales y únicas** para garantizar total responsabilidad, trazabilidad y acceso controlado a los recursos e información operativa de la plataforma. Las políticas de autenticación soportarán reglas de complejidad de contraseña configurables, políticas de vencimiento de contraseñas, controles de bloqueo de cuenta, gestión de timeout de sesión y administración de credenciales seguras, en línea con las mejores prácticas de la industria y los requerimientos regulatorios y de seguridad.

La plataforma soportará **autenticación multifactorial (MFA)** con métodos de autenticación configurables como códigos de verificación de una sola vez, aplicaciones de autenticador, verificación por correo electrónico o mecanismos de autenticación segura equivalentes, tal como sea aprobado por SUTEL y CTPN-M. Se aplicará MFA a los usuarios privilegiados, administrativos, operativos y autorizados para consolidar la verificación de identidad y reducir el riesgo de acceso no autorizado.

El acceso a las funciones de la plataforma, tickets, información operativa, datos de transacciones y capacidades administrativas será regido por **controles de acceso basado en roles (RBAC)** y políticas de

autorización a nivel de transacción, a fin de asegurar que los usuarios solo acceden a la información y funciones asociadas a su rol operativo autorizado.

Todos los eventos de autenticación, intentos de inicio de sesión, validaciones MFA, actividades de acceso y acciones asociadas a la seguridad serán totalmente registrables y auditables para garantizar transparencia operativa, trazabilidad y cumplimiento con los requerimientos de gobierno y ciberseguridad.

A través de este marco de gestión de autenticación y acceso seguro, TNPC garantiza un **sólido aseguramiento de la identidad del usuario, seguridad operativa, gestión de acceso controlado y protección de información operativa sensible del SIPN** en todo el ecosistema de la portabilidad numérica en Costa Rica.

5.5 *Tendrá un registro obligatorio de marcas de tiempo y personal que interviene en cada proceso.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC incluirá un **marco integral y obligatorio de registro de auditoría** que registra marcas de tiempo, actividades del usuario, acciones operativas y participación de los interesados en todos los procesos de tickets, operativos y de gestión de servicio.

Todas las actividades relevantes realizadas dentro de la plataforma serán automáticamente registradas y mantenidas en registros seguros de auditoría, que incluyen:

- Creación, asignación, actualizaciones, escalada y cierre del ticket
- Eventos de acceso y autenticación de usuario
- Comentarios operativos y cambios de estado
- Aprobaciones de flujos de trabajo e histórico de acciones
- Gestión de incidencias y actividades de resolución
- Eventos de notificación y escalada
- Cambios administrativos y de configuración

Cada entrada del registro incluirá información detallada de trazabilidad tal como:

- Marca de fecha y hora
- Identidad del usuario y rol operativo
- Ticket afectado o referencia del proceso
- Acción realizada
- Valores de estado anterior y actualizado
- Comentarios asociados o notas operativas
- Escalada o actividad de flujos de trabajo asociados

El marco de registro de auditoría soportará **trazabilidad total, transparencia operativa, responsabilidad, análisis histórico y cumplimiento regulatorio** a lo largo de todos los procesos operativos que involucren a los operadores/proveedores, SUTEL, CTPN-M y el equipo operativo de la ERP.

Todos los registros serán almacenados en forma segura, podrán buscarse y auditarse, con acceso controlado a través de permisos basados en roles para garantizar la protección de la información operativa y regulatoria. Los usuarios autorizados podrán revisar las actividades históricas, tiempos de procesos, rutas de escalada e interacciones operativas a través de interfaces de reportería y tableros seguros.

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

A través de esta capacidad integrada de auditoría y registro de marcas de tiempo, TNPC asegura **visibilidad operativa completa, trazabilidad de procesos, cumplimiento de gobierno y responsabilidad** en todo el ecosistema del SIPN en Costa Rica.

5.6 *Incluir un seguimiento del ciclo de vida (abierto, en análisis, interacción, escalado, resuelto, entre otros) del reclamo.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de tickets y gestión de servicio de TNPC ofrece **capacidades integrales de seguimiento durante el ciclo de vida del ticket** que ofrecen visibilidad total, trazabilidad y gestión operativa durante todo el ciclo de vida completo de cada ticket tales como consulta, incidencia o solicitud de servicio.

La plataforma soportará estados de flujos de trabajo configurables que incluyen, sin carácter limitativo:

- Abierto
- Asignado/ En curso
- Bajo revisión
- Escalado
- A la espera de información
- Resuelto
- Cerrado
- Reabierto

Se puede hacer seguimiento de cada etapa del ciclo de vida en tiempo real, con autoría completa, asegurando la visibilidad del avance del ticket, grupos operativos responsables, acciones pendientes, histórico de escalada, marcas de tiempo y actividades de resolución. Los usuarios autorizados podrán monitorear el estado actual y avance histórico de cada ticket a través de tableros e interfaces de seguimiento seguros.

El marco de gestión del ciclo de vida soportará flujos de trabajo configurables, reglas de escalada, procesos de aprobación, disparadores de notificaciones y monitoreo de SLA para garantizar la coordinación operativa eficiente y resolución a tiempo del problema. Todas las transiciones del ciclo de vida, comentarios, acciones operativas e interacciones con los interesados serán totalmente registrables y auditables dentro de la plataforma.

La plataforma también ofrecerá tableros gráficos, reportería histórica y análisis operativo para permitir a SUTEL, CTPN-M, los operadores/proveedores y el personal autorizado de la ERPN monitorear la antigüedad del ticket, tendencias de escalada, rendimiento de la resolución y métricas de eficiencia operativa.

A través de esta capacidad integrada de gestión del ciclo de vida, TNPC asegura **gestión transparente de tickets, responsabilidad operativa, manejo eficiente de escalada y trazabilidad punta a punta** en todos los procesos de soporte del SIPN.

5.7 Realizar notificaciones automáticas para nuevas interacciones.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de tickets y gestión de servicio de TNPC ofrece **notificaciones automáticas en tiempo real para todas las nuevas interacciones de tickets y actualizaciones operativas** para garantizar la comunicación a tiempo, concientización operativa y coordinación eficiente entre los operadores/proveedores, SUTEL, CTPN-M y el equipo operativo de la ERPN.

Las notificaciones serán generadas cuando ocurran nuevas interacciones dentro de un ticket, que incluyen:

- Nuevos comentarios o respuestas
- Cambios de estado
- Actividades de escalada
- Actualizaciones de asignación o reasignación
- Solicitudes de información adicional
- Actualizaciones de resoluciones
- Actividades de reapertura de ticket
- Acciones operativas o de flujos de trabajo

El marco de notificaciones soportará preferencias de comunicaciones configurables, grupos de recepción y políticas de escalada para asegurar que los interesados relevantes son informados de inmediato en base a su rol operativo o participación en el ciclo de vida del ticket. Se podrán enviar las notificaciones por correo electrónico y otros canales de comunicación configurados que sean soportados por la plataforma.

Cada notificación incluirá información contextual relevante tal como:

- Número de identificación del ticket
- Tipo de interacción o actualización
- Estado actual del ticket
- Fecha y hora de la interacción
- Usuario o grupo operativo que realiza la acción
- Resumen de la nueva interacción o actividad operativa

Todas las actividades de notificaciones y el histórico de interacciones se registran en forma completa y son auditables dentro de la plataforma para asegurar la transparencia, trazabilidad y responsabilidad operativa.

A través de esta capacidad integrada de notificaciones, TNPC asegura **visibilidad operativa continua, rápida concientización del interesado, colaboración eficiente y gestión proactiva de tickets** en todo el ecosistema del SIPN en Costa Rica.

5.8 *Soporte para carga y descarga de archivos adjuntos de, al menos, 10 MB para múltiples tipos, incluyendo como mínimo: PDF, DOC, DOCX, XLS, XLSX, CSV, JPEG, JPG, PNG, GIF, TXT, ZIP, RAR.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de tickets y gestión de servicio de TNPC soportará **carga, descarga, almacenamiento y gestión de múltiples tipos de adjuntos en forma segura** para facilitar la coordinación operativa, manejo de incidencias, detección y resolución de problemas, comunicación regulatoria e intercambio de documento eficientes entre los operadores/proveedores, SUTEL, CTPN-M y el equipo operativo de la ERPN.

La plataforma soportará el manejo de adjuntos para archivos con un **tamaño máximo de 10 MB por archivo**, con capacidades configurables de expansión de capacidad cuando sea operativamente requerido. Los formatos de archivos soportados incluirán:

- PDF
- DOC / DOCX
- XLS / XLSX
- CSV
- JPEG / JPG
- PNG
- GIF
- TXT
- ZIP
- RAR

La capacidad de gestión de adjuntos soportará:

- Operaciones de carga y descarga seguras
- Control de acceso basado en roles para la visibilidad de adjuntos
- Asociación de adjuntos con tickets y actividades del flujo de trabajo
- Seguimiento y auditoría de versión
- Verificaciones de validación e integridad del archivo
- Referencias de adjuntos que se pueden buscar dentro del histórico de tickets
- Acceso controlado basado en rol operativo y titularidad del ticket

Todos los archivos cargados y los metadatos asociados serán almacenados en forma segura y protegidos a través de controles de seguridad de la plataforma para asegurar la confidencialidad, integridad, trazabilidad y cumplimiento operativo. Las actividades de los adjuntos incluyen cargas, descargas, modificaciones y eventos de acceso que serán totalmente registrables y auditables dentro de la plataforma.

A través de esta capacidad integrada de gestión de adjuntos, TNPC asegura **colaboración operativa eficiente, intercambio seguro de documentos, soporte mejorado de detección y resolución de problemas y transparencia operativa mejorada** en todo el ecosistema del SIPN en Costa Rica.

5.9 *Garantizar la confidencialidad, integridad y disponibilidad de la información.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC implementará un **marco integral de seguridad y resiliencia**, diseñado para garantizar la confidencialidad, integridad y disponibilidad de toda la información operativa, transaccional, regulatoria y relativa al suscriptor en todo el ecosistema del SIPN.

Se logrará la **confidencialidad** a través de mecanismos de autenticación segura, autenticación multifactorial (MFA), controles basados en roles (RBAC), comunicaciones encriptadas usando protocolos HTTPS/TLS, políticas de acceso controlado y segregación segura de datos operativos entre los operadores/proveedores, SUTEL, CTPN-M y el personal autorizado de la ERPN. La plataforma asegurará que los usuarios solo pueden acceder a la información y funciones operativas asociadas con su rol autorizado y al alcance de la transacción.

Se asegurará la **integridad** a través del procesamiento controlado de transacciones, reglas de validación, registros de auditoría, seguimiento de marcas de tiempo, controles de consistencia de la base de datos, verificación de la integridad del archivo, comunicaciones por API seguras y trazabilidad completa de todas las acciones operativas y eventos del ciclo de vida del ticket. Todas las actividades operativas, actualizaciones, escaladas e interacciones del usuario serán registradas y auditables para asegurar la transparencia y protección contra modificaciones no autorizadas o manipulación de la información.

Se logrará la **disponibilidad** a través de una arquitectura altamente resiliente basada en AWS que aprovecha múltiples Zonas de Disponibilidad, capacidades de recuperación ante desastres, monitoreo continuo, mecanismos de recuperación ante desastres, procesos de copias de resguardo y recuperación, alertas operativas automáticas y soporte operativo 24x7x365. La plataforma está diseñada para eliminar puntos únicos de falla y garantizar la disponibilidad del servicio continuo bajo condiciones normales y de contingencia.

La plataforma también incorporará monitoreo proactivo, generación de alertas operativas, procesos de gestión de incidencias, validación de copias de resguardo, procedimientos de recuperación ante desastres y actividades de mantenimiento preventivo para asegurar la confiabilidad operativa continua y la protección de los activos de información críticos del SIPN.

A través de este marco integrado de seguridad y resiliencia, TNPC garantiza **operaciones seguras, confiables, resilientes y continuamente disponibles**, en pleno cumplimiento con los requerimientos de SUTEL para protección de la información, confidencialidad, integridad y disponibilidad en todo el ecosistema del SIPN en Costa Rica.

5.10 *Imposibilidad de eliminar o alterar registros históricos.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC implementará un **marco de gestión de registros históricos seguro y de auditoría inmutable**, diseñado para evitar la eliminación, alteración o manipulación no autorizada de información histórica, operativa, transaccional, de tickets y de auditoría.

Los registros históricos serán protegidos a través de una combinación de:

- Controles de acceso basado en roles (RBAC)
- Gestión estricta de privilegios
- Mecanismos de registro de auditoría inmutables
- Histórico de transacciones con marcas de tiempo

- Permisos administrativos controlados
- Pistas de auditorías integrales
- Monitoreo y registro continuo

Todos los eventos del ciclo de vida del ticket, acciones operativas, actividades del flujo de trabajo, interacciones del usuario, cambios de estado, escaladas, comentarios, notificaciones y actividades de autenticación serán registrados en forma segura con marcas de tiempo asociadas y la información de identificación del usuario. Una vez registrados, los registros históricos se conservarán y serán rastreables para garantizar la total responsabilidad operativa y el cumplimiento regulatorio.

La plataforma restringirá los privilegios de modificación o eliminación solo a los procesos administrativos autorizados. Todas las actividades administrativas excepcionales serán totalmente registradas, monitoreadas y auditable. Las políticas de retención de datos históricos, mecanismos de copias de resguardo y los procedimientos de recuperación asegurarán aún más la conservación y protección de los registros operativos a largo plazo.

La arquitectura de la plataforma basada en AWS soportará además almacenamiento de copias de resguardo seguras, redundancia, gestión de acceso controlado y capacidades de recuperación de base de datos para garantizar la protección de la información histórica contra la eliminación accidental, modificación no autorizada, corrupción o escenarios de fallas operativas.

A través del marco seguro de protección de registros históricos, TNPC asegura **trazabilidad completa, auditabilidad, integridad operativa, cumplimiento regulatorio y conservación a largo plazo de los registros críticos de transacciones e histórico operativo del SIPN.**

5.11 *Generación y descarga de reportes (en formato PDF y XLSX) por medio de rangos de tiempo (año, mes, día, hora, minutos) y tipo de servicio acordes con el perfil de usuario.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

La plataforma de TNPC ofrecerá un **marco de reportería integral y flexible** que permite a los usuarios autorizados generar, visualizar, programar y descargar registros operativos y analíticos en base a rangos de fechas configurables, categorías de servicio y perfiles de acceso del usuario.

La capacidad de reportería soportará filtrado y generación de reportes por:

- Año
- Mes
- Día
- Hora
- Minuto
- Tipo de servicio
- Operador/proveedor
- Categoría de incidencia
- Estado operativo
- Rol de usuario y permisos de acceso

Los usuarios autorizados podrán generar y descargar reportes en **formatos PDF y XLXS**, con soporte para representaciones configurables, vistas resumidas, datos operativos detallados, gráficos, estadísticas y

análisis históricos. Se podrán generar reportes a demanda o programarse para generación y distribución automática periódica en base a los requerimientos operativos.

El marco de reportería soportará reportería de gestión de servicios, operativa y regulatoria, que incluye:

- Estadísticas de tickets y métricas operativas
- Reportes de incidencias y escalada
- Desempeño de SLA y tiempos de respuesta
- Reportes de actividad de operador/proveedor
- Disponibilidad del sistema y estadísticas operativas
- Reportes de actividad del usuario y de auditoría
- Reportes de análisis y tendencias operativas históricas

El acceso a los reportes y funciones de reportería estará regido por **controles de acceso basado en roles** para garantizar que cada usuario solo accede a la información operativa y los datos de reportería autorizados para su perfil y rol organizativo.

La plataforma ofrecerá **tableros interactivos, capacidades de filtrado de avanzada, visibilidad operativa en tiempo real y análisis histórico** para soporte de una gestión operativa eficiente, supervisión regulatoria, toma de decisiones y gobierno de servicio en todo el ecosistema del SIPN en Costa Rica.

A través de esta capacidad de reportería integrada, TNPC asegura **transparencia operativa eficiente, análisis detallado, acceso seguro a la información y flexibilidad de reportería integral** para SUTEL, CTPN-M, los operadores/proveedores y los interesados autorizados de la ERPN.

5.11.1 *Los reportes deberán incluir datos como cantidad de reclamos, tipificación del reclamo, tiempos de resolución, tipificación, personal que atendió, entre otros.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El marco de reportería de TNPC ofrecerá **reportes analíticos operativos, de incidencias y tickets integrales**, que contendrán la información detallada requerida para la gestión operativa, supervisión regulatoria, análisis de calidad de servicio y actividades de mejora continua.

La plataforma soportará **reportes operativos mensuales** que incluyen, sin carácter limitativo:

- Número de tickets
- Categoría/clasificación de ticket
- Niveles de severidad
- Tiempos de respuesta y resolución
- Representante o grupo operativo asignado
- Estadísticas de escalada y reapertura
- Estadísticas operativas del operador/proveedor
- Indicadores de desempeño de SLA
- Análisis de incidencias recurrentes

El marco de reportería soportará capacidades de agrupaciones y filtrado de avanzada que incluyen:

- Grupo por operador/proveedor
- Grupo por severidad
- Grupo por categoría/clasificación de ticket
- Grupo por representante o grupo operativo
- Grupo por estado de ciclo de vida del ticket
- Grupo por estado de escalada
- Grupo por cumplimiento de SLA
- Grupo por estado de resolución
- Grupo por rangos de fecha y hora configurables

Los usuarios autorizados también podrán generar **reportes parametrizables a demanda** en base a filtros configurables, criterios operativos y períodos de reporte para permitir análisis operativo, revisión de gestión, supervisión regulatoria y actividades de gobierno.

La frecuencia predeterminada de reportes será mensual; sin embargo, el cronograma de reportes se puede configurar como **diario, quincenal y otros intervalos de reportería acordados**, en base a los acuerdos regulatorios, operativos o de gobierno establecidos con SUTEL y CTPN-M.

La plataforma de reportería soportará **tableros en tiempo real, filtrado avanzado, análisis gráficos, análisis de tendencias históricas y vistas configurables de reportes**, en base al perfil de usuario, rol operativo, categoría de servicio, rango de tiempo, operador/proveedor, nivel de severidad y estado operativo.

Los usuarios autorizados podrán generar y descargar reportes en **formatos PDF y XLSX**, con representaciones configurables y capacidades de exportación para permitir la revisión operativa, reportes de gestión, análisis regulatorios y actividades de gobierno.

El acceso a los reportes operativos e información de tickets estará regido por **controles de acceso basado en roles** para garantizar que cada interesado solo accede a los datos operativos e información de reportería autorizados para su rol y responsabilidades organizativas.

A través de esta capacidad de reportería de avanzada, TNPC asegura **una completa visibilidad operativa, medición de rendimiento, monitoreo de calidad de servicio, auditabilidad y gestión operativa en base a datos** en todo el ecosistema del SIPN en Costa Rica.

6 Acuerdos de nivel de servicio mensuales (SLA)

Se establecen los siguientes umbrales de niveles de acuerdo de servicio mensuales a partir de los cuales aplicará una penalidad de acuerdo con lo siguiente:

$$I = \frac{F_I}{F_T} \times 100$$

Donde

I = Inconformidad

F_I = Factor Inconforme

F_T = Factor Total

Cuando corresponda aplicar una penalidad, el cálculo será realizado por la ERPN y presentado ante el CTPN-M quienes se encargarán de analizar la propuesta y brindar su aprobación o rechazo justificado. En caso de que, en un plazo máximo de 30 días naturales desde su presentación no sea posible llegar a un acuerdo entre los operadores y la ERPN, las partes aceptan que el Consejo de la Sutel resuelva el asunto mediante acto motivado.

| Indicador | Descripción | Umbral (U) | Penalidad | Peso del SLA sobre costos fijos |
|---|---|------------|---|---------------------------------|
| SLA 1 Temporizadores de los procesos de portación del usuario final | Cumplimiento de los temporizadores (duración máxima) de cada uno de los procesos involucrados en el cambio de operador en el proceso del usuario final. | 2% | Si $I > U$ $SLA\ 1 = I \times k$ donde: k : grado de rigurosidad = 5 | 10% |
| SLA 2 Temporizador para generación y envío del NIP | Generar y entregar el NIP a la interfaz SMSC de los operadores en un lapso no mayor a un (1) minuto desde que el donante lo solicitó. En ningún caso, este lapso podrá ser mayor a cinco (5) minutos. | 3% | Si $I > U$ para retrasos > 1 min $SLA\ 2 = I \times k$ donde: k : grado de rigurosidad = 5 | 5% |
| SLA 3 Disponibilidad y usabilidad del IVR | Disponibilidad y posibilidad de entrega audible del NIP para el usuario final desde el número que se desea portar en un lapso. Este deberá estar disponible desde que se generó la solicitud de NIP y mantenerse durante todo su periodo de vigencia. | 5% | Si $I > U$ $SLA\ 3 = I \times k$ donde: k : grado de rigurosidad = 5 | 5% |
| SLA 4 Temporizadores de los procesos de portación hacia el operador | Cumplimiento de los temporizadores (duración máxima) de cada uno de los procesos involucrados en el cambio de operador durante las ventanas de cambio. | 2% | Si $I > U$ $SLA\ 4 = I \times k$ donde: k : grado de rigurosidad = 5 | 5% |

| Indicador | Descripción | Umbral (U) | Penalidad | Peso del SLA sobre costos fijos |
|--|---|------------|---|---------------------------------|
| SLA 5 Disponibilidad, usabilidad, integridad y operatividad del SIPN. | Disponibilidad, usabilidad, integridad y correcto funcionamiento de todas las interfaces WEB, sistemas de intercambio de información, interfaces de comunicación y demás aplicaciones del SIPN. Se contabilizará cada vez que cualquiera de los módulos funcionales que lo conforman se encuentren afectados de forma total o parcial (que no permitan su operación y uso normal o realice procesos de manera inadecuada) | 99,7%* | Si $I > 0,3\%$ $SLA\ 5 = I \times k$ donde: k : grado de rigurosidad = 5 | 55% |
| SLA 6 Disponibilidad de la plataforma para interposición de tickets de servicio (mesa de ayuda). | Disponibilidad, usabilidad, integridad y correcto funcionamiento de todas las interfaces WEB, para la imposición de tickets de servicio. Se contabilizará cada vez que cualquiera de los módulos funcionales que lo conforman se encuentren afectados de forma total o parcial. | 99%* | Si $I > 1\%$ $SLA\ 6 = I \times k$ donde: k : grado de rigurosidad = 2 | 10% |
| SLA 7 | Ver descripción en el punto 6.1 | | | 10% |

*Este será reportado mensualmente, pero contabilizado en intervalos semanales, de lunes a domingo.

Los SLA se redondean a dos decimales hacia arriba en dirección contraria a cero.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS está totalmente comprometida a cumplir y superar todos los Acuerdos de nivel de servicio definidos por SUTEL y CTPN-M. La plataforma de TNPC tiene la arquitectura de una **solución del SIPN nativa en la nube y de grado operadora**, específicamente diseñada para entregar disponibilidad, resiliencia, rendimiento, integridad y continuidad operativa excepcionales a través de una infraestructura AWS altamente redundante, con orquestación centralizada de flujos de trabajo, capacidad automática de recuperación ante fallas, monitoreo en tiempo real y gestión operativa proactiva, tal como se describe en las Secciones 2.1, 2.3, 2.28, 2.29 y 2.34.

TNPC está diseñada para lograr una **disponibilidad superior a 99,99% durante el tiempo inactivo no planificado**, ya que aprovecha los componentes de software en cluster resiliente y la infraestructura en la nube, totalmente redundante, implementada a lo largo de múltiples zonas de disponibilidad y regiones de AWS. La arquitectura de la plataforma elimina los puntos únicos de fallas y asegura la operación continua de todos los procesos del SIPN que incluyen generación de NIP, prevalidación, portación, sincronización, reportería, servicios de IVR e integraciones regulatorias.

La infraestructura en la nube de AWS de TNPC incorpora:

- Arquitectura de implementación en múltiples zonas de disponibilidad
- Capacidades de recuperación ante desastres a lo largo de las regiones
- Replicación continua AWS Aurora con sincronización casi en tiempo real

- Balanceo de carga elástico y escala automática
- Capas web, de aplicaciones y bases de datos redundantes
- Mecanismos de copias de resguardo y recuperación continua
- Capacidades de recuperación ante fallas y autosanación automáticas

Todos los componentes de infraestructura importantes que incluyen balanceadores de carga, firewalls, web services, servicios de aplicaciones, clusters de bases de datos y gateways de integración operan en configuraciones activas redundantes para garantizar el funcionamiento ininterrumpido del SIPN durante las actividades de mantenimiento, actualizaciones de software, fallas de hardware o eventos operativos inesperados.

La disponibilidad de la plataforma está continuamente monitoreada a través de **AWS CloudWatch**, que ofrece observación centralizada a lo largo de todas las capas de infraestructura y aplicaciones. CloudWatch monitorea continuamente:

- Salud de aplicaciones e infraestructura
- Producción y latencia de transacciones
- Profundidad de cola y rendimiento de procesamiento
- Disponibilidad de API e interfaces
- Utilización de recursos
- Estado de sincronización y difusión
- Replicación de base de datos y eventos de recuperación ante fallas
- Seguridad y anomalías operativas

Las alertas automáticas y los procedimientos de escalada se disparan en tiempo real cuando se alcanza o supera un umbral y permiten la remediación proactiva antes de que impacte un SLA.

La disponibilidad de TNPC se mide de acuerdo con la siguiente fórmula:

Disponibilidad = (Total Horas/Minutos de Operación de TNPC durante el período informado menos Total de tiempo inactivo de TNPC durante el período informado) dividido por Total Horas/Minutos de Operación durante el período informado x 100%

Las siguientes condiciones quedan excluidas de los cálculos de disponibilidad del servicio mensual:

- Períodos de mantenimiento programado y ventanas de mantenimiento acordadas
- Eventos de fuerza mayor
- Caídas del sistema atribuibles a software de terceros o hardware de terceros

Todas las métricas de SLA, eventos de transacciones, estados de procesos, marcas de tiempo, alertas y estadísticas operativas se almacenan centralmente en NPCDB y son totalmente auditables mediante los marcos de reportería y monitoreo de TNPC.

SLA 1 – Temporizadores de los procesos de portación del usuario final

TNPC asegura el cumplimiento con los temporizadores de los procesos de portación del usuario final a través de los módulos centralizados **Procesador de Mensajes** y **Procesador de Temporizadores** descritos en la Sección 2.3. Estos módulos orquestan los flujos de trabajo del SIPN, aplican los umbrales de los temporizadores definidos en el Manual de Interfaces y Procesos, validan la secuenciación de todos los eventos de portabilidad y automáticamente disparan las alertas y los procedimientos de escalada cuando se acercan los umbrales. Todos los eventos de temporizadores y estados de la transacción se registran en NPCDB para su total auditoría y reportería de SLA.

SLA 2 – Temporizador de generación y entrega de NIP

El cumplimiento con la generación y entrega de NIP se logra a través del **Sistema Automático de Verificación (SAV)**, **Gateway de SMS/SMPP** y **Procesador de Temporizadores** integrados. Las solicitudes de NIP se procesan en tiempo real, validan contra los esquemas WSDL/XSD y se transmiten en forma segura a través de las interfaces SMPP. La entrega de acuses de recibo, reintentos, tiempos de respuesta y métricas de entrega se monitorean continuamente y almacenan en NPCDB.

SLA 3 - Disponibilidad y usabilidad del IVR

TNPC asegura la disponibilidad del servicio de IVR a través de un **subsistema del IVR** integrado con NPCDB y el marco de SAV. El servicio de IVR valida continuamente los números de origen, recupera los NIP activos y entrega el NIP en forma segura y audible. El monitoreo de la arquitectura redundante en la nube y CloudWatch aseguran que la funcionalidad del IVR y el cumplimiento de SLA no se interrumpen.

SLA 4 - Temporizadores de los procesos de portación hacia el operador

Los temporizadores de procesos del operador se aplican centralmente a través del **Procesador de Temporizadores** y el **Procesador de Mensajes** que gestionan las respuesta del donante, ventanas de cambio, eventos de sincronización y reglas de tiempos regulatorios. TNPC valida continuamente el cumplimiento de los temporizadores, registra todos los eventos de procesos dentro de NPCDB y escala proactivamente cualquier anomalía en los tiempos por los sistemas automáticos de monitoreo y notificación.

SLA 5 - Disponibilidad, usabilidad, integridad y operatividad del SIPN

TNPC logra la disponibilidad grado operadora del SIPN a través de la arquitectura nativa en la nube de AWS descrita en la Sección 2.1. La plataforma utiliza una implementación de múltiples zonas de disponibilidad, replicación Aurora continua, recuperación ante fallas automática, procesamiento distribuido, balanceo de carga y monitoreo CloudWatch en tiempo real para garantizar el funcionamiento ininterrumpido de todas las interfaces web, API, servicios de sincronización, bases de datos e integraciones regulatorias.

SLA 6 - Disponibilidad de la plataforma de mesa de ayuda

La mesa de ayuda de TNPC y la plataforma de tiquetes funcionan bajo una infraestructura AWS y un marco de monitoreo resilientes como la plataforma central del SIPN. El monitoreo continuo a través de CloudWatch, combinado con los servicios redundantes en la nube y el soporte operativo 24x7 de TNS garantizan la disponibilidad ininterrumpida de los servicios de tiquetes y soporte.

SLA 7 - Soporte y resolución de incidencias

TNPC asegura el cumplimiento con los SLA a través de un modelo operativo integral que combina:

- Centro de Operaciones de Red 24x7
- Monitoreo CloudWatch en tiempo real
- Plataforma centralizada de tiquetes
- Generación de alertas y escalada automática
- Personal de soporte operativo que habla español
- Ingeniería y soporte de plataforma de Nivel 3 de TNS

La gestión del ciclo de vida de las incidencias, manejo de escalada, métricas de respuesta y seguimiento de resoluciones son totalmente registrables, monitoreados y auditables para garantizar el cumplimiento de las obligaciones de los SLA de Categoría 1, 2 y 3.

TNPC ofrece:

- Tableros de SLA en tiempo real
- Reportes de cumplimiento de SLA mensuales
- Tendencias y análisis de históricos

- Estadísticas de disponibilidad y tiempo en línea
- Reportes de análisis de incidencias y causa principal
- Alertas operativas y de escala automáticas

Todos los cálculos de los SLA surgen directamente de los datos transaccionales de NPCDB y las métricas operativas de CloudWatch para garantizar la completa transparencia, trazabilidad y cumplimiento regulatorio.

A través de esta combinación de:

- Arquitectura resiliente nativa en la nube de AWS
- Recuperación ante desastres multirregional
- Orquestación centralizada de flujos de trabajo
- Observación de CloudWatch en tiempo real
- Aplicación automática de temporizadores
- Soporte operativo 24x7
- Monitoreo y mantenimiento preventivo proactivos

TNPC ofrece una **plataforma del SIPN segura, altamente disponible, resiliente y lista para el futuro**, totalmente alineada con las expectativas de los SLA y los requerimientos operativos establecidos por SUTEL y CTPN-M.

- 6.1** *Para efectos del SLA 7, mantendrá un registro de los tiempos de atención de soporte e información los cuales también aplican para solicitudes realizadas para los entornos de prueba. Cada solicitud deberá contar con una bitácora en la cual se registren todos los días y horas de cada interacción hasta alcanzar su solución efectiva. El tiempo máximo para recibir una solución efectiva (humana) por evento se define a continuación.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Para SLA 7, la plataforma de TNPC mantendrá un **registro integral y totalmente auditable de todas las actividades de atención al cliente, interacciones de gestión de tickets y tiempos de resolución** que incluye solicitudes generadas en ambos entornos de producción y pruebas.

Cada ticket mantendrá un **registro completo del histórico del ciclo de vida** que contiene todas las fechas, marcas de tiempo, interacciones con el usuario, comentarios, escaladas, asignaciones, cambios de estado y actividades de resolución desde la creación inicial del ticket hasta el cierre y la validación final. La plataforma garantiza total trazabilidad de todas las interacciones entre los operadores/proveedores, SUTEL, CTPN-M y el equipo operativo de la ERP.

El marco de gestión de tickets registrará:

- Fecha y hora de creación del ticket
- Hora de acuse de recibo
- Histórico de asignación y reasignación
- Marcas de tiempo de interacciones y respuestas
- Actividades de escalada
- Marcas de tiempo de resoluciones
- Comentarios y actualizaciones del usuario

- Representante o grupo operativo responsable
- Estado actual e histórico del ciclo de vida del ticket
- Resolución final y validación de cierre

La plataforma soportará el seguimiento y monitoreo configurable de SLA para garantizar que todos los tiempos de atención al cliente, objetivos de respuesta de ticket y obligaciones de resolución son continuamente medidos, monitoreados y auditables. Los mismos controles de seguimiento y gobierno se aplicarán a los tickets generados dentro de los entornos de prueba para garantizar calidad de servicio consistente, trazabilidad y responsabilidad operativa a lo largo de todos los entornos.

La plataforma de tickets también ofrecerá **tableros, análisis históricos, visibilidad de escalada y reportería operativa en tiempo real** para permitir a SUTEL, CTPN-M, los operadores/proveedores y personal autorizado de ERPN monitorear el avance del ticket, la capacidad de respuesta y el cumplimiento con los tiempos de atención al cliente acordados.

A través de esta capacidad integrada de seguimiento y monitoreo de SLA, TNPC asegura **transparencia operativa completa, trazabilidad, responsabilidad y gestión eficiente de tickets** en todo el ecosistema del SIPN en Costa Rica.

6.1.1 *Categoría 3 (bajo): 24 horas naturales desde la hora de interposición de la gestión. Con una ponderación (k) de 20. Se utilizará, por ejemplo, para consultas generales.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC soportará solicitudes de **atención al cliente y gestión de tickets de Categoría 3 (Baja)** con un objetivo máximo de resolución de 24 horas naturales desde la hora de manejo/procesamiento de ticket, totalmente alineado con los requerimientos operativos y de SLA establecidos por CTPN-M. El factor de ponderación aplicable (**k = 20**) será soportado dentro del marco de monitoreo, puntaje operativo y reportería de SLA.

Los tickets de Categoría 3 incluyen, en general:

- Consultas operativas generales
- Solicitudes de información
- Actividades de soporte no críticas
- Solicitudes menores de configuración o usabilidad
- Reportería y asistencia administrativa
- Aclaraciones operativas de bajo impacto

La plataforma centralizada de gestión de tickets monitoreará continuamente los tiempos de los tickets de Categoría 3, las interacciones, escaladas, acuses de recibo y actividades de resolución para garantizar el cumplimiento de los objetivos de atención al cliente acordados. Todas las actividades de ciclo de vida del ticket que incluyen marcas de tiempo, representantes asignados, comentarios operativos, transiciones de estado y detalles de la resolución final serán registrados y auditables dentro de la plataforma.

La plataforma soporta parámetros de ponderación de SLA configurables que incluyen el **factor de ponderación k (k = 20)** para solicitudes de Categoría 3 aplicable, que permiten la priorización operativa, medición de SLA, seguimiento de calidad de servicio, gestión de escalada y reportes de cumplimiento conforme a los requerimientos de CTPN-M.

Se logra el cumplimiento con el objetivo de resolución de la Categoría 3 a través de:

- Monitoreo de tickets 24x7x365

- Flujos de trabajos automáticos de seguimiento y escalada de SLA
- Mecanismos de notificación y recordatorios en tiempo real
- Procesos de soporte operativo en capas
- Gestión centralizada del ciclo de vida del ticket
- Supervisión y reportería operativa continua

La plataforma también ofrecerá:

- **Seguimiento de SLA en tiempo real**
- **Tableros y reportería operativa**
- **Análisis histórico de tickets**
- **Monitoreo del tiempo de resolución**
- **Visibilidad del desempeño de atención al cliente**

A través de este marco estructurado de atención al cliente y gestión de SLA, TNPC asegura el **manejo oportuno de las solicitudes de baja prioridad, transparencia operativa, comunicación eficiente con los interesados, cumplimiento mensurable de SLA y total alineación con las obligaciones de gestión de servicio de Categoría 3** en todo el ecosistema del SIPN en Costa Rica.

6.1.2 *Categoría 2 (medio): 6 horas naturales desde la hora de interposición de la gestión. Con una ponderación (k) de 30. Se utilizará, por ejemplo, para afectaciones en un trámite de portación puntual.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC soportará solicitudes de **atención al cliente y gestión de tickets de Categoría 2 (Media)** con un objetivo máximo de resolución de **6 horas naturales desde la hora de manejo/procesamiento de ticket**, totalmente alineado con los requerimientos operativos y de SLA establecidos por CTPN-M. El factor de ponderación aplicable (**k = 30**) será soportado dentro del marco de monitoreo, puntaje operativo y reportería de SLA.

Los tickets de Categoría 2 incluyen, en general:

- Incidencias que afectan una transacción de portación específica
- Degradación parcial del servicio
- Problemas de integración del operador/proveedor
- Anomalías en el procesamiento de transacciones
- Problemas de conectividad o interfaz con impacto operativo limitado
- Problemas de funcionalidad operativa que requieren manejo prioritario.

La plataforma centralizada de gestión de tickets monitoreará continuamente los tiempos de los tickets de Categoría 2, las interacciones, escaladas, acuses de recibo y actividades de resolución para garantizar el cumplimiento de los objetivos de atención al cliente acordados. Todas las actividades de ciclo de vida del ticket que incluyen marcas de tiempo, representantes asignados, comentarios operativos, transiciones de estado y detalles de la resolución final serán registrados y auditables dentro de la plataforma.

La plataforma soporta parámetros de ponderación de SLA configurables que incluyen el **factor de ponderación k (k = 30)** para solicitudes de Categoría 2 aplicable, que permiten la priorización operativa,

medición de SLA, seguimiento de calidad de servicio, gestión de escalada y reportes de cumplimiento conforme a los requerimientos de CTPN-M.

Se logra el cumplimiento con el objetivo de resolución de la Categoría 2 a través de:

- Monitoreo de tickets 24x7x365
- Flujos de trabajo de escalada en base a prioridad
- Mecanismos de notificación y alertas en tiempo real
- Soporte operativo y de ingeniería por capas
- Seguimiento y supervisión operativa continua de SLA
- Gestión centralizada del ciclo de vida del ticket
- Tableros y análisis operativos en tiempo real

La plataforma también ofrecerá:

- Visibilidad de SLA en tiempo real
- Tableros y reportería operativa
- Seguimiento de escalada y análisis histórico
- Monitoreo del tiempo de resolución
- Medición del desempeño de atención al cliente

A través de este marco estructurado de atención al cliente y gestión de SLA, TNPC asegura el **manejo rápido de las solicitudes de prioridad media, coordinación operativa eficiente, cumplimiento mensurable de SLA y gestión efectiva de la resolución** en todo el ecosistema del SIPN en Costa Rica.

6.1.3 *Categoría 1 (crítico): 1 hora natural desde la hora de interposición de la gestión. Con una ponderación (k) de 50. Se utilizará, por ejemplo, cuando existe una afectación tal que impida ejecutar portaciones de forma total o parcial.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC soportará solicitudes de **atención al cliente y gestión de tickets de Categoría 1 (Crítica)** con un objetivo máximo de resolución de **1 hora natural desde la hora de manejo/procesamiento de ticket**, totalmente alineado con los requerimientos operativos y de SLA establecidos por CTPN-M. El factor de ponderación aplicable (**k = 50**) será soportado dentro del marco de monitoreo, puntaje operativo, gestión de escalada y reportería de SLA.

Los tickets de Categoría 1 incluyen, en general:

- Incidencias que evitan la ejecución total o parcial de las transacciones de seguridad
- Caídas críticas de servicio del SIPN
- Fallas mayores de procesamiento de transacciones
- Interrupciones severas en la conectividad del operador/proveedor
- Fallas críticas en interfaces o integraciones
- Condiciones operativas que impactan significativamente la disponibilidad o funcionalidad del SIPN

La plataforma centralizada de gestión de tickets monitoreará continuamente los tiempos de los tickets de Categoría 1, las interacciones, escaladas, acuses de recibo y actividades de resolución para garantizar la respuesta operativa inmediata y el cumplimiento de los objetivos de atención al cliente acordados. Todas las

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

actividades de ciclo de vida del ticket que incluyen marcas de tiempo, representantes asignados, comentarios operativos, acciones de escalada, transiciones de estado y detalles de la resolución final serán registrados y auditables dentro de la plataforma.

La plataforma soporta parámetros de ponderación de SLA configurables que incluyen el **factor de ponderación k (k = 50)** para solicitudes de Categoría 1 aplicable, que permiten la priorización de eventos operativos críticos, manejo de escalada acelerada, seguimiento de calidad de servicio y reportes de cumplimiento conforme a los requerimientos de CTPN-M.

Se logra el cumplimiento con el objetivo de resolución de la Categoría 1 a través de:

- Monitoreo y soporte operativos 24x7x365
- Flujos de trabajo de escalada y notificación inmediata
- Manejo operativo en base a prioridades
- Soporte técnico y de ingeniería por capas
- Gestión de seguimiento y escalada de SLA en tiempo real
- Supervisión operativa y coordinación del incidente en forma continua
- Gestión centralizada del ciclo de vida del ticket
- Tableros y análisis operativos en tiempo real

La plataforma también ofrecerá:

- Alertas operativas y visibilidad de SLA en tiempo real
- Seguimiento y auditoría de escalada
- Análisis y reportes históricos de ticket
- Monitoreo del tiempo de resolución
- Medición del desempeño de atención al cliente

A través de este marco de gestión de eventos críticos, CTPN asegura **respuesta rápida, gestión de resolución acelerada, continuidad operativa, cumplimiento mensurable con SLA y manejo efectivo de eventos de servicio críticos** de SIPN en todo el ecosistema del SIPN en Costa Rica.

6.2 *La ERP seleccionada pondrá a disposición de los miembros del CTPN-M de una interfaz WEB para la consulta de cada uno de los SLA anteriores. Además, de los indicadores para el periodo actual, deberá mantener disponible el histórico de todo el periodo de la contratación.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC ofrecerá una **interfaz de monitoreo y reportería de SLA basada en la web**, accesible para todos los miembros de CTPN-M, que permita la visibilidad en tiempo real de todos los indicadores aplicables de SLA, métricas operativas, actividades de gestión de tickets, tiempos de atención al cliente y mediciones de desempeño de servicio definidos en el marco operativo del SIPN.

La interfaz ofrecerá visibilidad de ambos:

- Indicadores y métricas de desempeño de SLA durante el período operativo actual
- Registros históricos completos de SLA e histórico operativo para todo el período de contratación

Los usuarios autorizados podrán consultar, monitorear y analizar en forma segura:

- Cumplimiento con SLA de Categorías 1, 2 y 3
- Tiempos de respuesta y resolución de ticket
- Actividades de escalada y reapertura
- Métricas de desempeño de atención al cliente
- Estadísticas operativas y de disponibilidad
- Registros de ciclo de vida histórico del ticket
- Tendencias operativas e indicadores de calidad de servicio
- Reportes de SLA mensuales y a demanda
- Registros de auditoría históricos y de marcas de tiempo

La plataforma ofrecerá **tableros interactivos, análisis gráficos, filtros configurables, análisis de tendencias históricas y capacidades de reportes descargables** en formatos PDF y XLSX para permitir las actividades de revisión operativa, gobierno, supervisión regulatoria y gestión de calidad de servicio.

El acceso a los datos de SLA, reportes operativos y registros históricos estará regido por **controles de acceso basado en roles y mecanismos de autenticación segura** para garantizar que cada interesado autorizado solo accede a la información operativa relevante a su rol y permisos.

Todas las métricas de SLA, marcas de tiempo, interacciones, escaladas y actividades operativas serán continuamente registradas, almacenadas en forma segura y mantenidas durante todo el período de contratación a fin de asegurar la **completa trazabilidad, auditoría, transparencia operativa y visibilidad histórica a largo plazo**.

A través de esta capacidad de monitoreo de SLA y reportería histórica, TNPC asegura la **visibilidad operativa continua, gobierno de servicio transparente, cumplimiento mensurable de SLA y análisis histórico integral** a CTPN-M, SUTEL, los operadores/proveedores y los interesados autorizados de la ERPN.

6.3 *El cálculo del SLA se enviará mensualmente a cada uno de los miembros del CTPN-M de la siguiente manera:*

$$SLA_{Monthly} = \left(\sum_{h=1}^{71} weight_h \cdot X \cdot SLA_h \right) \cdot X \cdot CFM$$

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Cada reporte de SLA mensual incluirá:

- Cálculos detallados de SLA por categoría
- Estadísticas de disponibilidad y tiempo en línea
- Cumplimiento con los temporizadores de procesos de portación
- Métricas de generación y entrega del NIP
- Indicadores de disponibilidad y usabilidad del IVR
- Desempeño de gestión de incidencias y soporte
- Excepciones e incidencias de SLA
- Análisis de causa principal para desviaciones de SLA

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

- Acciones correctivas y preventivas implementadas
- Análisis de tendencias históricas e indicadores de desempeño comparativo

Los reportes de SLA mensuales serán puestos a disposición de los miembros de CTPN-M a través de la **GUI del Tablero de SLA de TNPC** basada en roles y segura descrita en la Sección 6.1, que permite a los miembros visualizar el desempeño actual e históricos de los SLA a través de gráficos, tableros operativos y análisis de buceo en tiempo real. Además del acceso por el portal, TNPC distribuirá los reportes formales de SLA mensuales en forma electrónica en formatos configurables que incluyen PDF, XLSX y CSV.

El marco de reportería de SLA mantendrá:

- Registros históricos completos de SLA para todo el período de contratación
- Capacidad de auditoría de todos los cálculos y métricas
- Comparación histórica y análisis de tendencias
- Estadísticas operativas que se pueden buscar y exportar
- Visibilidad transparente del cumplimiento y desempeño operativo de los SLA

El acceso a los reportes y tableros de SLA se asegurará a través de:

- Control de Acceso basado en Roles
- Autenticación multifactorial usando Google Authenticator o Microsoft Authenticator
- HTTPS con TLS 1.2 o superior
- Monitoreo total de registros y actividad de auditoría

El proceso de reportes de SLA mensuales funcionará bajo la misma arquitectura nativa en la nube y altamente disponible de TNPC, usada por la plataforma del SIPN, para garantizar la visibilidad ininterrumpida y la continuidad de la reportería. Todos los cálculos y reportes de SLA serán continuamente accesibles a través de la GUI de TNPC durante todo el período de contratación.

A través de este robusto marco de reportería y gobierno de SLA, TNPC ofrece a los miembros de CTPN-M una **capacidad de gestión de SLA precisa, altamente transparente y operativamente rica** para permitir una supervisión efectiva, verificación de cumplimiento, análisis operativo y mejora continua del servicio durante todo el ciclo de vida de las operaciones del SIPN.

6.4 *En caso de que algún SLA no pueda ser aplicado durante un periodo, este podrá trasladarse a alguno posterior.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC incorpora un marco de gobierno de SLA flexible y totalmente auditable que soporta el diferimiento controlado de las mediciones de SLA a períodos de reporte posteriores, toda vez que no se pueda aplicar un SLA en forma razonable o válida durante un período operativo específico. Este enfoque asegura que la evaluación de los SLA sea justa, transparente y precisa, a la vez que mantiene plena alineación con los principios de gobierno establecidos por SUTEL y CTPN-M.

Todas las mediciones de SLA diferidos serán:

- Claramente identificadas dentro del tablero de reportería y reportes mensuales de SLA
- Totalmente trazables y auditables dentro de NPCDB y los registros de gestión de SLA
- Respaladas por justificación documentada y evidencia operativa
- Trasladas al período de reportería próximo aplicable en coordinación con CTPN-M y SUTEL.

La GUI del Tablero de SLA de TNPC descrita en la Sección 6.1 ofrecerá visibilidad completa de:

- Indicadores de SLA diferidos
- Motivo del diferimiento
- Período operativo afectado
- Asignación al período de reportería siguiente
- Conciliación final y estado del cálculo

Esto asegura que todos los interesados tienen transparencia continua respecto de la aplicabilidad, cálculos diferidos y resolución posterior de los SLA.

El marco también garantiza que los SLA diferidos no impacten la integridad operativa ni oculten condiciones de servicios subyacentes. Todas las incidencias asociadas, eventos del sistema, datos de monitoreo y registros operativos estarán disponibles para análisis, revisión de gobierno y auditoría durante todo el período de contratación.

A través de un enfoque estructurado y regulado, TNPC asegura que la administración de SLA sea:

- Justa y precisa operativamente
- Transparente y auditable
- Totalmente alineada con los requerimientos de gobierno regulatorio
- Consistente con los objetivos de mejora continua y monitoreo de desempeño de servicio a largo plazo

Esta capacidad consolida aún más el marco de gestión integral de SLA de TNPC y respalda el gobierno operativo colaborativo entre TNS, SUTEL y CTPN-M durante todo el ciclo de vida de las operaciones del SIPN.

6.5 *En caso de que la aplicación de multas por concepto del %SLA sumadas durante la ejecución del contrato alcance un monto equivalente al 25% del costo total por concepto de cuota fija mensual por el periodo de contratación, se considera que el contratista incurre en un incumplimiento, por lo que se podrá valorar la rescisión del contrato por parte del CTPN-M sin responsabilidad para este comité .*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS reconoce la importancia crítica de mantener un estricto cumplimiento de todos los compromisos de los SLA establecidos por SUTEL y CTPN-M; y reconoce cabalmente que el incumplimiento persistente o significado de algún SLA puede constituir una violación contractual sustancial. Por ende, TNPC tiene una arquitectura y estructura operativas específicas para minimizar el riesgo operativo, evitar proactivamente las violaciones de SLA y mantener la disponibilidad e integridad del servicio continuo del SIPN durante todo el período de contratación.

La plataforma de TNPC utiliza un marco de gobierno operativo integral que combina:

- Arquitectura resiliente nativa en la nube, grado operadora, de AWS
- Monitoreo y observación en tiempo real de AWS CloudWatch
- Seguimiento y análisis centralizado de SLA
- Mecanismos de generación de alertas y escalada automática
- Infraestructura redundante y geográficamente resiliente

- Soporte del Centro de Operaciones de Red 24x7
- Controles operativos y mantenimiento preventivo proactivos
- Procesos estructurados de gestión de incidencias y problemas

Este modelo operativo está diseñado para garantizar que los indicadores de los SLA estén continuamente dentro de los umbrales contractuales; y que cualquier potencial degradación sea identificada y corregida proactivamente antes de que ocurra un impacto.

En caso desviación de un SLA, TNPC implementará un proceso estructurado de remediación y acciones correctivas, que incluye:

- Análisis operativo y respuesta inmediatos ante la incidencia
- Identificación de causa principal y evaluación del impacto
- Planes de acciones correctivas y preventivas
- Monitoreo continuo y validación de la efectividad de la remediación
- Reportes formales y transparencia ante SUTEL y CTPN-M

Todos los cálculos de SLA, incidencias, penalidades, acciones correctivas y métricas operativas serán totalmente transparentes y auditables mediante la GUI del Tablero de SLA de TNPC y el marco de reportería descrito en la Sección 6.1.

TNS reconoce además que si las penalidades acumuladas de SLA superan el umbral contractualmente definido de 25% de la cuota fija mensual, esta condición puede constituir una violación contractual supeditada a la evaluación de CTPN-M conforme al marco contractual y regulatorio. La estrategia operativa, arquitectura resiliente, capacidades de monitoreo proactivo y procesos de gobierno disciplinado de TNPC tienen específicamente el objetivo de evitar la ocurrencia de tales escenarios.

A través de un riguroso marco operativo, técnico y de gobierno, TNPC ofrecerá a SUTEL y CTPN-M una **plataforma del SIPN altamente confiable, resiliente y continuamente monitoreada** para asegurar el cumplimiento de los SLA a largo plazo, la excelencia operativa y la protección de la infraestructura crítica de la portabilidad numérica en Costa Rica.

6.6 *La responsabilidad y el seguimiento de los SLA recaerá sobre la ERPN seleccionada. La no presentación de los reportes faculta al CTPN-M a estimar discrecionalmente el porcentaje de cálculo.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNS reconoce cabalmente y acepta la responsabilidad de la medición, monitoreo, cálculos, seguimiento y reportería de todos los indicadores de los SLA asociados a las operaciones del SIPN en forma continua, durante todo el período de contratación. TNPC incorpora un marco de gobierno y gestión operativa de SLA, específicamente diseñado para garantizar que todas las obligaciones de los SLA sean continuamente monitoreadas, calculadas con precisión, reportadas con transparencia y totalmente auditables.

TNPC realizará seguimiento continuo de:

- Métricas de disponibilidad y tiempo en línea
- Temporizadores del proceso de portación
- Desempeño de la generación y entrega de NIP
- Tiempos de respuesta de soporte y resolución
- Disponibilidad del IVR y subsistema operativo

- Desempeño de la sincronización e integración
- Cumplimiento con la respuesta y escalada de incidencias

Todos los indicadores de SLA estarán disponibles a través de la GUI del Tablero de SLA de TNPC basada en roles y segura, descrita en la Sección 6.1, que ofrece a los miembros de CTPN-M y SUTEL visibilidad en tiempo real del desempeño actual, tendencias históricas, eventos operativos y estadísticas de cumplimiento de SLA durante todo el período de contratación.

Los reportes formales de SLA mensuales serán automáticamente generados y entregados en forma electrónica a los interesados autorizados en formatos configurables que incluyen PDF, XLSX y CSV. Estos reportes incluirán:

- Cálculos detallados de SLA
- Estadísticas operativas y análisis de KPI
- Resúmenes de incidencias y caídas del sistema
- Análisis de causa principal y acciones correctivas
- Comparación histórica y análisis de tendencias
- Estado de cumplimiento por categoría de SLA

El marco SLA de TNPC está diseñado con un sólido gobierno operativo y controles automáticos para garantizar que las obligaciones de reportería se cumplen con consistencia. Los flujos de trabajo de reportería automáticos, la recolección centralizada de datos, las verificaciones de validaciones operativas y los procesos de generación de reportes programados minimizan el riesgo de demoras o falta de reportes.

TNS reconoce que no presentar los reportes de SLA requeridos podrá facultar a que CTPN-M estime discrecionalmente los porcentajes de los cálculos de SLA conforme al marco contractual. Conforme a ello, el modelo de gobierno de TNPC enfatiza:

- Monitoreo continuo de SLA
- Generación automática de reportes
- Responsabilidad operativa
- Controles de validación multinivel
- Transparencia y capacidad de autoría totales

a fin de asegurar que todos los reportes de SLA se entregan con precisión y a tiempo.

A través de este marco operativo y de gobierno disciplinado, TNPC ofrece a SUTEL y CTPN-M una **capacidad de gestión de SLA altamente transparente, continuamente monitoreada y totalmente auditable** que garantiza la confianza operativa, cumplimiento regulatorio y excelencia de servicio a largo plazo durante todo el ciclo de vida de las operaciones del SIPN.

- 6.7** *Se exige de la aplicación del SLA las salidas de operación por causa de terceros, caso fortuito o fuerza mayor, debiendo ser estos casos debidamente documentados y demostrados ante el CTPN-M. Lo anterior no aplica para los sucesos o hechos que puedan ser evitables y aquellos producidos por la negligencia, impericia o culpa.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

El marco de gobierno de SLA de TNPC reconoce que determinados eventos excepcionales, fuera del alcance razonable de TNPC, podrían impactar las operaciones del SIPN y, por ende, podrían estar excluidas de la aplicación de SLA. Estos eventos son específicamente ocasionados por:

- Fallas o caídas del servicio de terceros
- Eventos de fuerza mayor
- Casos fortuitos o circunstancias externas extraordinarias

En tales situaciones, TNS asegurará que los eventos afectados sean **totalmente documentados, técnicamente analizados y formalmente informados** a CTPN-M y SUTEL a través del marco de reportería de SLA y la gestión de incidencias.

Para cualquier evento que sea propuesto como excluido de la aplicación de los SLA, TNPC ofrecerá:

- Reportes detallados de incidencias
- Documentación de análisis de causa principal
- Tiempos operativos y cronología de eventos
- Evaluación del impacto
- Evidencia técnica y registros de monitoreo sustentatorios
- Identificación de la dependencia externa o condición de fuerza mayor
- Acciones correctivas y preventivas implementadas, cuando corresponda

Todos dichos eventos serán totalmente visibles y auditables a través de la GUI del Tablero de SLA de TNPC y el marco de reportería, descrito en la Sección 6.1 para asegurar transparencia total y visibilidad del gobierno para CTPN-M y SUTEL.

TNS reconoce cabalmente y acepta que estas exclusiones **no se aplicarán** a incidencias, caídas del sistema, degradaciones o eventos operativos que resulten de:

- Negligencia
- Impericia
- Falla operativa
- No seguir los procedimientos operativos establecidos
- Condiciones prevenibles o controles inadecuados

Conforme a ello, la arquitectura y gestión operativa de TNPC minimizan los riesgos evitables a través de:

- Arquitectura resiliente nativa en la nube, grado operadora, de AWS
- Diseño del sistema redundante y tolerante a fallas
- Monitoreo y generación de alertas proactivas de AWS CloudWatch
- Mantenimiento preventivo y gobierno operativo

- Capacidades automáticas de recuperación ante fallas y desastres
- Soporte operativo y gestión de incidencias 24x7
- Control de cambio y gobierno de versiones estructurados

Este marco operativo está específicamente diseñado para prevenir las caídas del sistema que son evitables y para asegurar que los servicios del SIPN están continuamente disponibles, son seguros y cumplen con los compromisos de los SLA.

A través de un enfoque de gobierno disciplinado y transparente, TNPC asegura que todas las exclusiones de los SLA son:

- Correctamente justificadas
- Totalmente documentadas y auditables
- Se comunican con transparencia a CTPN-M y SUTEL
- Se gestionan conforme a las obligaciones contractuales y regulatorias

a la vez que se mantienen los más elevados estándares de responsabilidad operativa, resiliencia y excelencia de servicio durante todo el ciclo de vida de las operaciones del SIPN.

7 Causales de resolución contractual

Serán causales de resolución contractual anticipada, de forma unilateral y mediante acuerdo del CTPN-M, aquellos incumplimientos que, por su naturaleza material o por su reiteración, afecten o pongan en riesgo la continuidad, seguridad, integridad, disponibilidad o confiabilidad del Sistema Integral de Portabilidad Numérica (SIPN) según se citan a continuación.

- 7.1** *Incumplimiento en la fecha de inicio del SIPN en más de cinco (5) días desde la puesta de operación indicada en este pliego de condiciones.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado. TNS anticipa que mantendrá conversaciones posteriores con SUTEL a fin de alcanzar términos mutuamente convenidos para la resolución contractual.

- 7.2** *El incumplimiento en más de tres (3) ocasiones durante un periodo de seis (6) meses de los SLA o de las obligaciones de soporte.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado. TNS anticipa que mantendrá conversaciones posteriores con SUTEL a fin de alcanzar términos mutuamente convenidos para la resolución contractual.

- 7.3** *Que la aplicación de multas por concepto del %SLA sumadas durante la ejecución del contrato alcance un monto equivalente al 25% del costo total por concepto de cuota fija mensual por el periodo de contratación.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado. TNS anticipa que mantendrá conversaciones posteriores con SUTEL a fin de alcanzar términos mutuamente convenidos para la resolución contractual.

- 7.4** *La reiteración de incumplimientos operativos, técnicos o regulatorios que evidencien un patrón de ejecución deficiente en más de tres (3) ocasiones durante un periodo de seis (6) meses.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado. TNS anticipa que mantendrá conversaciones posteriores con SUTEL a fin de alcanzar términos mutuamente convenidos para la resolución contractual.

7.5 *La no realización o falla de implementación de mejoras, actualizaciones o evoluciones tecnológicas obligatorias en más de dos (2) ocasiones.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado. TNS anticipa que mantendrá conversaciones posteriores con SUTEL a fin de alcanzar términos mutuamente convenidos para la resolución contractual.

7.6 *La ocurrencia de incumplimientos materiales que afecten la continuidad, seguridad o integridad del SIPN cuya gravedad haya sido acreditada por el CTPN-M.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado. TNS anticipa que mantendrá conversaciones posteriores con SUTEL a fin de alcanzar términos mutuamente convenidos para la resolución contractual.

7.7 *El uso, tratamiento, acceso o divulgación no autorizada de la información del SIPN para fines distintos a los establecidos en el pliego de condiciones o los contratos suscritos, independientemente de que se genere o no un daño económico directo.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado. TNS anticipa que mantendrá conversaciones posteriores con SUTEL a fin de alcanzar términos mutuamente convenidos para la resolución contractual.

7.7.1 *Incumplimiento de la protección de la información o difusión de la información obtenida a través de las bases de datos del SIPN o incumplimiento del acuerdo de confidencialidad regulado en el punto 1.5.13 del presente pliego de condiciones.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado. TNS anticipa que mantendrá conversaciones posteriores con SUTEL a fin de alcanzar términos mutuamente convenidos para la resolución contractual.

7.8 *La cesión, subcontratación, transferencia o delegación total o parcial de las obligaciones contractuales sin la autorización previa y expresa del CTPN-M.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado. TNS anticipa que mantendrá conversaciones posteriores con SUTEL a fin de alcanzar términos mutuamente convenidos para la resolución contractual.

- 7.9** *Cualquier otra causa grave debidamente acreditada que haga inviable la continuidad del servicio determinado por el CTPN-M.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado. TNS anticipa que mantendrá conversaciones posteriores con SUTEL a fin de alcanzar términos mutuamente convenidos para la resolución contractual.

- 7.10** *En el caso de que se presente alguna de las causales anteriores de resolución contractual el Comité lo analizará y le trasladará los antecedentes, la motivación y la prueba con la que cuente para acreditar la falta por parte del contratista, para lo cual le brindará a este un plazo de 10 días hábiles para que se refiera al respecto, la respuesta del contratista será analizada por el Comité y se le brindará una respuesta final respecto a la imposición de la sanción correspondiente, según se establece en la sección 1.5.11 o la resolución anticipada del contrato.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado. TNS anticipa que mantendrá conversaciones posteriores con SUTEL a fin de alcanzar términos mutuamente convenidos para la resolución contractual.

8 Validación biométrica con prueba de vida (OPCIONAL)

- 8.1** *El SIPN deberá contar con un módulo opcional que permita la validación biométrica remota con algoritmos que permitan constatar que la persona que realiza la gestión está viva. En este respecto debe contar con mecanismos para no permitir intentos de fraude o suplantación de identidad.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC ofrece un **marco de validación biométrica remoto, seguro, escalable y totalmente integrado**, diseñado para garantizar la identidad del suscriptor, mejorar la seguridad transaccional, reducir el riesgo de fraude y soportar los procesos de portación digitales y seguros dentro del ecosistema del SIPN en Costa Rica. Este marco biométrico está totalmente integrado a la orquestación de los flujos de trabajo de TNPC, para permitir **validación de identidad en tiempo real, verificación pasiva de prueba de vida, extracción de identidad basada en OCR, validación de legitimidad de documento, protección contra suplantación de identidad, capacidad de auditoría centralizada y trazabilidad operativa** dentro de los procesos de portación.

La capacidad de validación biométrica soportará la integración segura con los flujos de trabajo del SIPN, que incluyen:

- Procesos de prevalidación existentes
- Validación de solicitud de portabilidad existente
- Procesos de verificación de identidad de nuevos suscriptores, tal como sea acordado y definido por SUTEL y CTPN-M.

Flujos de trabajo de validación biométrica de TNPC

El módulo biométrico está directamente integrado a los flujos de trabajo de orquestación y validación de transacciones de TNPC, a través de API seguras y el control centralizado de procesos gestionado por el Procesador de Mensajes de TNPC, el motor de validaciones y el marco de orquestación de flujos de trabajo.

1. Inicialización de la sesión del suscriptor

Cuando se requiere validación biométrica, TNPC inicia la sesión de verificación biométrica segura vinculada con una transacción de portación y MSISDN del suscriptor específico. El suscriptor podría acceder la interfaz biométrica con dispositivos comunes, que incluyen:

- Dispositivos móviles
- Tabletas
- Navegadores de escritorio con acceso a cámara

La sesión biométrica se asocia de manera singular a la referencia transaccional de TNPC y es totalmente auditable dentro del ciclo de vida de los flujos de trabajo del SIPN:

TNPC gestiona centralmente:

- Inicialización de la sesión
- Asociación con transacción
- Orquestación de flujos de trabajo de validación
- Gestión de timeout de sesión
- Continuación o rechazo de flujo de trabajo
- Registros de auditoría y seguimiento de marca de tiempo

2. Captura facial en vivo y validación de calidad en tiempo real

Se orienta al suscriptor para obtener una foto del rostro en vivo o una breve captura de video usando el dispositivo con cámara. TNPC ofrece **feedback de orientación y validación de la captura en tiempo real** para asegurar que la imagen cumple con los requerimientos de calidad de reconocimiento facial conforme a:

- ISO/IEC 19794-5
- ISO/IEC 39794-5
- ISO 30107-3
- Recomendaciones de la NIST

Validación de TNPC:

- Posicionamiento y centrado del rostro
- Orientación facial natural
- Calidad de iluminación
- Nitidez y enfoque de la imagen
- Calidad de retrato y resolución
- Contraste del fondo
- Visibilidad de ojos
- Expresión facial natural
- Alineación de la cabeza
- Ausencia de obstrucciones
- Posicionamiento horizontal del rostro
- Total visibilidad del rostro
- Autenticidad de la imagen

Los formatos de imagen soportados incluyen:

- JPEG (ISO/IEC 10918-1)
- JPEG-2000 (ISO/IEC 15444-1)
- PNG (ISO/IEC 15948:2003)

Si no se cumplen los mínimos umbrales de calidad, TNPC solicita una nueva captura de la imagen antes de continuar con el proceso de validación.

3. Procesamiento de documento de identidad con base en OCR

TNPC soporta la captura segura de una o múltiples imágenes del documento de identidad desde el dispositivo del suscriptor directamente.

El motor OCR de TNPC realiza lo siguiente:

- Normalización automática de la imagen del documento
- Corrección de brillo y contraste
- Reducción de ruido
- Corrección de inclinación y orientación
- Optimización de alineación del texto
- Extracción de información de identidad con OCR

4. Validación de la legitimidad del documento de identidad

TNPC valida la legitimidad del documento de identidad con mecanismos de validación de documento y análisis antifraude estándares de la industria.

El motor de validación realiza lo siguiente:

- Análisis de marcas de seguridad
- Detección de falsificación
- Análisis de alteración
- Detección de copia/fotocopia
- Verificación de consistencia de plantilla
- Validación de autenticidad del documento
- Análisis de integridad de la imagen

TNPC soporta la integración segura con los servicios aprobados de validación de documento y biometría, cuando sea requerido por SUTEL y CTPN-M.

Si la validación de la legitimidad del documento falla:

- Se bloquea el flujo de trabajo biométrico
- Se puede rechazar la transacción de portación
- Se puede escalar la transacción para revisión manual

de conformidad con las reglas de negocio configurables de TNPC.

5. Coincidencia biométrica facial

La imagen facial capturada se procesa a través de algoritmos de reconocimiento biométrico estándar de la industria y se compara contra la imagen facial contenida dentro del documento de identidad presentado.

El marco biométrico admite tecnologías que comúnmente se basan en:

- Algoritmos faciales incorporados en base a Convolutional Neural Network (CNN)
- Motores de reconocimiento alineados con NIST Face Recognition Vendor Test (FRVT)
- Marcos biométricos que cumplen con ISO/IEC 19794
- Modelos de puntuación de similitud facial asistidos por IA.

El motor biométrico calcula:

- Puntaje de confianza de similitud facial
- Confianza de coincidencia rostro a documento
- Indicadores de autenticidad de la imagen
- Indicadores de integridad de sesión

TNPC devuelve los resultados configurables de la validación, que incluyen:

- Coincidencia exitosa
- Sin coincidencia
- Se requiere revisión manual

en base a umbrales de confianza configurables definidos por SUTEL y CTPN-M.

6. Detección de prueba de vida pasiva (ISO 30107-3)

TNPC implementa la **verificación de prueba de vida pasiva en cumplimiento con ISO 30107-3 y en línea con las recomendaciones de NIST.**

El análisis de prueba de vida pasiva se realiza automáticamente sin requerir la interacción explícita del usuario y evalúa:

- Consistencia de la textura del rostro
- Análisis de profundidad y contorno
- Características naturales de la piel
- Consistencia del reflejo e iluminación
- Análisis de los micromovimientos faciales
- Indicadores de autenticidad de la imagen
- Validación de la fuente de captura
- Indicadores de integridad del dispositivo
- Señales de autenticidad de la sesión

El motor de prueba de vida de TNPC valida continuamente que:

- El usuario está físicamente presente
- La captura sea auténtica
- La sesión biométrica no sea manipulada
- El usuario esté en vivo durante la transacción

Si la verificación de prueba de vida falla:

- Se bloquea la transacción
- Se rechaza la sesión de validación
- Se pueden disparar flujos de trabajo de revisión manual
- Se pueden generar alertas de fraude dentro de TNPC.

7. Prevención de fraude y suplantación de identidad

TNPC incorpora mecanismos de prevención de fraude y suplantación de identidad de avanzada, diseñados para detectar y prevenir:

- Ataques de fotografías estáticas
- Suplantación de identidad con imagen impresa
- Ataques de repetición de pantalla
- Repetición de video registrado
- Contenido facial deepfake o generado por IA
- Intentos de identidad sintética
- Suplantación de identidad basada en máscara
- Feeds de cámara manipulados o inyectados

El análisis de prevención de fraude combina:

- Verificaciones de autenticidad del rostro
- Validación de prueba de vida
- Telemetría de sesión
- Análisis de consistencia de la imagen
- Verificación de integridad de la captura
- Indicadores de validación del dispositivo

Los indicadores de fraude pueden disparar:

- Rechazo automático
- Revisión operativa manual
- Escalada del flujo de trabajo
- Bloqueo de la transacción

de conformidad con las políticas operativas configurables de TNPC.

8. Puntaje biométrico y decisiones en el flujo de trabajo de TNPC

TNPC utiliza un motor centralizado de puntaje biométrico que combina:

- Puntaje de confianza de similitud facial
- Puntaje de validación de prueba de vida pasiva
- Verificación de legitimidad del documento
- Indicadores de fraude/suplantación de identidad
- Análisis de calidad de la imagen
- Validad de integridad de la sesión
- Indicadores de autenticidad del dispositivo
- Contexto transaccional

El puntaje de la validación biométrica se calcula con las políticas de puntuación ponderada configurables definidas por SUTEL y CTPN-M. Por ejemplo:

- Confianza en coincidencia facial: 40%
- Validación de prueba de vida pasiva: 30%
- Legitimidad de documento e indicadores de suplantación de identidad: 20%
- Calidad de imagen e integridad de sesión: 10%

El puntaje de validación combinado determina el resultado del flujo de trabajo:

- **Puntaje de alta confianza:** La transacción de portación procede en forma automática
- **Puntaje de confianza media:** Se pueden requerir validación adicional o revisión manual
- **Puntaje de baja confianza o detección de fraude:** Se bloquea, rechaza o escala el flujo de trabajo de portabilidad

Esto asegura que las solicitudes de portabilidad sospechosas o fraudulentas no proceden por los flujos de trabajo de TNPC, sin que medie una validación adecuada y autorización operativa.

9. Flujo de trabajo de TNPC e integración de validación

El módulo biométrico está directamente integrado a los flujos de trabajo y procesos de orquestación operativa de TNPC. Los resultados de la validación son procesados por el motor de flujos de trabajo de TNPC y se vinculan al ciclo de vida de la transacción de portación.

TNPC gestiona centralmente:

- Solicitudes de validación biométrica
- Orquestación de sesión
- Respuestas de validación
- Resultados de prueba de vida pasiva
- Puntaje de fraude
- Resultados de extracción por OCR
- Resultados de validación de documento
- Decisiones en el flujo de trabajo
- Continuación o rechazo de transacción

El resultado de la validación se incorpora directamente dentro de:

- Flujos de trabajo de prevalidación
- Validación de solicitud de portabilidad
- Flujos de trabajo de verificación de identidad del suscriptor

a fin de garantizar la consistencia de las políticas de aseguramiento de la identidad en todos los operadores/proveedores.

10. Seguridad y protección de datos

Todas las actividades biométricas, eventos de validación, marcas de tiempo, resultados de OCR, resultados de validación de documentos, indicadores de fraude, decisiones de los flujos de trabajo y acciones operativas son totalmente registradas y auditable dentro de TNPC a fin de asegurar:

- Transparencia operativa
- Cumplimiento regulatorio

- Trazabilidad forense
- Auditoría a largo plazo

El suscriptor real y el video/imagen de ID asociado no se almacenan en TNPC por motivos de seguridad.

11. Reportería y análisis operativo

TNPC ofrece reportes de validación biométrica mensuales que incluyen:

- Número de validaciones exitosas
- Validaciones rechazadas
- Desglose de rechazos de validaciones
- Estadísticas de falta de coincidencia de documentos
- Detección de documentos alterados/fraudulentos
- Resultados biométricos sin coincidencia
- Estadísticas de revisión manual
- Las validaciones se procesan como máximo en una hora
- Estadísticas de verificación de prueba de vida pasiva
- Estadísticas de intentos de suplantación de identidad/deepfake
- Análisis de rendimiento operativo

Los reportes estarán disponibles a través de los tableros de la **GUI segura y serán descargables en formatos PDF o XLSX.**

12. Gobierno, pruebas y mejora continua

El marco biométrico seguirá el mismo gobierno estructurado, validación de seguridad, pruebas operativas y ciclo de vida de implementación aplicados a todos los módulos operativos de TNPC. Las capacidades biométricas serán validadas dentro de los entornos de desarrollo y pruebas antes de la entrada en producción con la participación de SUTEL, CTPN-M y los operadores/proveedores, según corresponda.

TNPC también soportará mejoras continuas a:

- Algoritmos biométricos
- Detección de prueba de vida pasiva
- Extracción por OCR
- Validación de legitimidad del documento
- Modelos de detección de fraude
- Prevención de deepfake
- Puntaje biométrico asistido por IA

de acuerdo con:

- Mejores prácticas de la industria
- Normas ISO
- Recomendaciones de NIST
- Requerimientos regulatorios establecidos por SUTEL y CTPN-M

A través de un marco de validación biométrica de avanzada, TNPC ofrece a Costa Rica una **capacidad de verificación de identidad biométrica segura, que cumple con los estándares, es resistente al fraude, escalable y está lista para el futuro**, totalmente integrada a los flujos de trabajo operativos del SIPN.

8.2 *Se requiere que el SIPN pueda realizar validaciones biométricas remotas (no presenciales) con prueba de vida automáticas de la identidad del usuario.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC permite a los suscriptores completar la **validación biométrica totalmente remota directo desde sus dispositivos personales** para eliminar la necesidad de verificación presencial, a la vez que mantiene una sólida garantía de la identidad y los controles de prevención de fraude en todo los procesos de portación del SIPN.

El marco biométrico de TNPC incorpora **verificación de prueba de vida pasiva automática** para confirmar que el suscriptor que realiza la transacción está físicamente presente durante la sesión de validación y que no intenta imitar la identidad a través de fotos, ni son repeticiones de pantallas, videos grabados, identidades sintéticas ni contenido por deepfake.

El proceso de validación de prueba de vida funciona de forma transparente durante el flujo de trabajo biométrico y evalúa continuamente:

- Indicadores de autenticidad facial
- Características naturales de la textura de la piel
- Consistencia profunda y validación de contorno
- Patrones de iluminación y reflejo
- Integridad de la captura y consistencia de la imagen
- Señales de autenticidad de la sesión y del dispositivo

TNPC realiza estas validaciones en tiempo real durante la sesión de captura biométrica, sin requerir una interacción complicada con el usuario, a fin de garantizar una experiencia de usuario sencilla y amigable, a la vez que mantiene una sólida protección contra la suplantación de identidad.

El flujo de trabajo de validación biométrica está totalmente integrado a los procesos de orquestación de transacciones y gestión de decisiones de TNPC. Los resultados de la validación son centralmente procesados y asociados a la correspondiente transacción de portación del SIPN, lo cual permite a TNPC:

- Aprobar las transacciones válidas
- Escalar las validaciones sospechosas para revisión manual
- Bloquear las transacciones que no pasan la prueba de vida o tienen indicadores de suplantación de identidad
- Generar alteras operativas y registros de auditoría

Todos los eventos de validación biométrica, resultados de verificación de prueba de vida, decisiones de flujos de trabajo, marcas de tiempo e indicadores de fraude son totalmente registrados y auditables dentro de TNPC a fin de asegurar transparencia operativa, trazabilidad y cumplimiento regulatorio.

A través de este marco integrado de validación remota, TNPC ofrece a Costa Rica una **capacidad de verificación biométrica remota, segura, sin inconvenientes, que cumple con los estándares**, que garantiza la identidad del suscriptor, a la vez que protege los procesos de portación del SIPN contra intentos de fraude y suplantación de identidad.

8.3 *El servicio de validación biométrica remota (no presencial) se realizará a través del dispositivo utilizado por el usuario final para acceder a la plataforma de Portabilidad.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC permite que la validación biométrica se ejecute directamente dentro del flujo de interacción digital del SIPN, con el uso del dispositivo de acceso del suscriptor, a fin de permitir que el proceso biométrico se complete como parte de la misma sesión de la transacción, sin requerir redireccionamiento a canales de verificación física externos.

El módulo biométrico está diseñado para admitir:

- Cámaras de dispositivos en parte frontal o trasera
- Flujos de trabajo de captura segura en base a navegadores
- Condiciones adaptativas de red y ancho de banda
- Flujos de interacción responsivos con el usuario
- Continuidad de la sesión en toda la plataforma

TNPC ajusta dinámicamente el flujo de trabajo de la captura biométrica conforme a las características del dispositivo detectado, las capacidades de la cámara, orientación de pantalla y calidad de conexión a fin de optimizar la precisión de la validación y la usabilidad del suscriptor.

El marco de validación también incorpora:

- Correlación de sesión del dispositivo con transacción del SIPN
- Controles de integridad de sesión de captura
- Validación de compatibilidad de navegador y dispositivo
- Estabilización de captura en tiempo real
- Manejo automático de reintento y recuperación
- Continuidad de sesión segura durante escenarios de conectividad interrumpida

Para mejorar la usabilidad del suscriptor y la calidad biométrica, TNPC ofrece:

- Asistencia en la alineación dinámica de la captura
- Evaluación automática del umbral de calidad
- Indicadores de posicionamiento en tiempo real
- Pauta de calidad ambiental
- Feedback progresivo de validación de captura

El flujo de trabajo biométrico se optimiza para minimizar el esfuerzo del suscriptor, a la vez que asegura que la captura resultante cumpla con los requerimientos de reconocimiento facial, OCR y validación de prueba de vida definidos por SUTEL y CTPN-M.

Todas las interacciones biométricas en base a dispositivos se asocian en forma segura con la transacción correspondiente del SIPN y se mantienen dentro del marco de auditoría y validación de TNPC, a fin de garantizar total trazabilidad operativa y cumplimiento regulatorio.

- 8.4** *La ERPN seleccionada deberá presentar un informe mensual de los resultados para las validaciones que realizó el cual indique la cantidad de validaciones exitosas, validaciones rechazadas (con su respectivo desglose como alteración de documentos o persona no concuerda, entre otros), validaciones que requirieron una revisión manual. También deberá incluir un informe que permita determinar la cantidad máxima de validaciones que realizó en 1 hora durante el periodo.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC ofrece **reportes de validación biométrica integrales mensuales** que contienen estadísticas operativas detalladas, validación, análisis de fraude y rendimiento asociadas con las actividades de verificación biométrica ejecutadas dentro de la plataforma del SIPN.

El marco de reportería está totalmente integrado al motor de orquestación biométrica de TNPC, los flujos de validaciones, marco de auditoría y repositorio central de reportería, lo cual permite reportes precisos y totalmente auditables de todas las actividades de las transacciones biométricas.

Los reportes mensuales incluyen, como mínimo:

- Número total de sesiones de validación biométrica
- Número de validaciones exitosas
- Número de validaciones rechazadas
- Desglose de causas de rechazo
- Estadísticas de falta de coincidencia de documentos
- Resultados de validaciones de personas no coincidentes
- Estadísticas de detección de documentos alterados o fraudulentos
- Fallas en las verificaciones de prueba de vida
- Estadísticas de detección de deepfake/suplantación de identidad
- Número de validaciones que requirieron revisión manual
- Resultados de las revisiones manuales

TNPC también brinda un reporte de desempeño operativo dedicado que identifica:

- Número máximo de validaciones biométricas validadas en un período de 1 hora
- Estadísticas de procesamiento en hora pico

El motor de reportería agrega los datos directamente desde los registros de transacciones biométricas de TNPC, los eventos de orquestación de flujos de trabajo, los resultados del procesamiento de OCR, los resultados de las verificaciones de prueba de vida, los motores de puntaje de fraude y los registros de auditoría a fin de garantizar una completa precisión, trazabilidad y transparencia regulatoria.

Los usuarios autorizados de SUTEL y CTPN-M podrán acceder estos reportes a través de:

- Tableros seguros basados en GUI
- Reportes PDF descargables y capacidades de exportación a XLSX

El marco de reportería también admite:

- Análisis comparativo en base al operador
- Estadísticas de monitoreo de fraude

Todos los reportes de validación biométrica y los análisis asociados se conservan en forma segura dentro de TNPC y se mantienen totalmente auditables durante todo el período de contratación.

A través de esta capacidad de reportes biométricos integrales, TNPC asegura **visibilidad operativa completa, desempeño mensurable de la validación biométrica, transparencia en el análisis de fraude y reportes regulatorios integrales** para SUTEL y CTPN-M.

8.5 *La ERP seleccionada contabilizará una transacción de validación biométrica como una sesión en la que se realice uno o más procesos de revisión de datos personales o de identidad independientemente de si el proceso se completó o no dentro de dicha sesión.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC gestionará y registrará cada transacción de validación biométrica como una **sola sesión biométrica**, asociada con la correspondiente transacción de portación del SIPN y el flujo de trabajo de verificación de identidad del suscriptor.

La sesión biométrica se define como cualquier interacción de validación en que se inicia una o más actividades de biometría, datos personales, documento de identidad, OCR, prueba de vida o verificación de identidad, independientemente de si el proceso de validación se completa al final, interrumpe, rechaza, abandona, escala o finaliza con éxito dentro de la sesión.

El motor de orquestación biométrica de TNPC realizará el seguimiento y mantendrá centralmente:

- Identificador único de sesión biométrica
- Referencia de transacción asociada del SIPN
- Marcas de tiempo de inicio y fin de sesión
- Asociación con MSISDN del suscriptor
- Intentos de validación de documento de identidad
- Actividades de extracción por OCR
- Eventos de coincidencia biométrica facial
- Actividades de validación de prueba de vida pasiva
- Eventos de detección de fraude/suplantación de identidad
- Resultados de validaciones
- Disparadores de revisiones manuales
- Interrupción de sesión o eventos de timeout
- Resultados finales del flujo de trabajo

El marco de gestión de la sesión asegura que todas las actividades biométricas son totalmente trazables y auditables durante todo el ciclo de vida de validación de la portación. Incluso si el suscriptor sale del proceso, experimenta una interrupción de la conexión, falla la validación o abandona la sesión antes de completarse, TNPC conserva todo el histórico operativo y los registros de validación asociados a la sesión biométrica.

El motor de flujos de trabajo de TNPC también soporta:

- Controles de continuidad de la sesión
- Manejo automático de timeout
- Prevención de duplicación de sesión

- Gestión de recuperación de sesión
- Políticas de reintento y nueva presentación
- Correlación histórica de la sesión
- Monitoreo de fraude durante los múltiples intentos de validación

La información de la sesión biométrica se almacena en forma segura y conserva dentro de TNPC conforme a los requerimientos regulatorios, operativos, de auditoría y reportería establecidos por SUTEL y CTPN-M.

A través de la capacidad de gestión centralizada de sesión biométrica, TNPC asegura **completa trazabilidad operativa, contabilidad precisa de transacciones, transparencia en la validación y gobierno de flujos de trabajo biométricos consistentes** en todo el ecosistema del SIPN en Costa Rica.

- 8.6** *El servicio de biometría en conjunto con la comparación del documento de identidad deberá permitir validar la correspondencia entre ambos, validar que el usuario no está fallecido, realizar la prueba de vida (conocida como Liveness en inglés) y evitar todo tipo de fraudes de suplantación de identidad (como el deepfake).*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

- 8.7** *Según corresponda, el servicio de validación biométrica con prueba de vida obtendrá el consentimiento del usuario para utiliza una fotografía de su rostro para compararlo con el documento capturado. Según el Código Nacional de Tecnologías Digitales del MICITT (Ministerio de Ciencia, Tecnología y Telecomunicaciones) del 2024, el oferente deberá señalar la forma en la cual cumple o supera las recomendaciones para la captura de retratos según la normativa ISO/IEC 19794-5 y Estructuras de datos ISO/IEC 39794-5. El sistema de captura deberá brindar retroalimentación en tiempo real al usuario para garantizar que la fotografía permita llevar el proceso de reconocimiento facial. Se deberá considerar lo siguiente:*

- 8.7.1** *Prueba de vida*

- 8.7.1.1** *Debe ser “Pasiva” y cumplir con los estándares del NIST y el ISO 30107-3.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC asegura que el proceso de validación biométrica se ejecute de manera segura, transparente, en cumplimiento de los estándares y con el consentimiento del usuario de conformidad con el Código Nacional de Tecnologías Digitales del MICITT (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones) de 2024 y los estándares biométricos internacionalmente reconocidos.

Antes de iniciar cualquier captura biométrica o proceso de comparación de identidad, TNPC solicitará al suscriptor que preste su **consentimiento explícito** para autorizar el uso de:

- Imágenes del rostro
- Imágenes del documento de identidad
- Procesamiento de comparación biométrica
- Verificación de prueba de vida
- Flujos de trabajo de validación de identidad

El proceso de consentimiento será integrado directamente al flujo de trabajo de validación biométrica y se registrará en forma segura en los registros de auditoría de TNPC junto con la correspondiente:

- Marca de tiempo
- Identificador de sesión
- Referencia transaccional
- Acuse de recibo del suscriptor
- Estado del flujo de trabajo de validación

El marco biométrico de TNPC está diseñado para cumplir o superar:

- **ISO/IEC 19794-5** estándares de datos de imágenes del rostro
- **ISO/IEC 39794-5** estándares de estructura de datos biométricos
- **ISO 30107-3** requerimientos de detección de prueba de vida pasiva
- **Recomendaciones de reconocimiento facial y prueba de vida de NIST**

El motor de captura y validación de TNPC evalúa continuamente la calidad de la imagen y ofrece **feedback en tiempo real al suscriptor** a fin de asegurar que la imagen capturada cumple con los requerimientos de reconocimiento biométrico antes de continuar con el proceso.

El feedback de validación en tiempo real incluye:

- Pauta de posicionamiento del rostro
- Validación de nitidez de imagen
- Recomendaciones de iluminación y visibilidad
- Instrucciones de alineación de la cabeza
- Evaluación del contraste del fondo
- Verificación de la visibilidad de los ojos
- Validación de resolución y enfoque
- Confirmación de calidad de captura

Esta pauta en tiempo real mejora la precisión del reconocimiento biométrico, a la vez que reduce los intentos de validación fallidos y mejora la experiencia total del suscriptor.

TNPC implementa la **verificación de prueba de vida pasiva en cumplimiento de ISO 30107-3 y en línea con las recomendaciones de NIST**. La validación de prueba de vida pasiva funciona automáticamente sin requerir una interacción complicada con el usuario y analiza continuamente:

- Textura facial natural
- Consistencia de profundidad y contorno
- Autenticidad del reflejo e iluminación
- Patrones de los micromovimientos faciales
- Integridad de la fuente de captura
- Indicadores de autenticidad de la imagen
- Señales de integridad de la sesión y del dispositivo

El marco de prueba de vida pasiva está específicamente diseñado para que:

- El suscriptor esté físicamente presente
- La captura biométrica sea auténtica
- El usuario esté en vivo durante la sesión
- No ocurran intentos de suplantación de identidad ni repeticiones

TNPC también incorpora mecanismos contra la suplantación de identidad para detectar y prevenir:

- Ataques de fotografías estáticas
- Suplantación de identidad con imagen impresa
- Ataques de repetición de pantalla
- Repetición de video registrado
- Contenido deepfake o generado por IA
- Intentos de identidad sintética
- Feeds de cámara manipulados o inyectados

Todos los eventos de validación biométrica, resultados de prueba de vida, acuse de recibo de consentimiento, validaciones de calidad de imagen, indicadores de fraude y decisiones de flujos de trabajo se registran en forma completa y son auditables dentro de TNPC.

A través de este marco de validación biométrica que cumple con los estándares, TNPC ofrece a Costa Rica una **capacidad de verificación de identidad remota segura, con privacidad, resistente al fraude y altamente confiable**, totalmente alineada con los requerimientos de MICITT, normas ISO y mejores prácticas biométricas internacionales.

8.7.1.1.1 Formato de la foto

8.7.1.1.1.1. *La fotografía debe ser a color, centrada y enfocada, para su formato se puede utilizar una de las siguientes codificaciones:*

- a. *Formato JPEG (ISO/IEC 10918-1)*
- b. *Formato JPEG-2000 (ISO/IEC 15444-1)*
- c. *Formato PNG (ISO/IEC 15948:2003)*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC soporta captura de imágenes biométricas utilizando **imágenes faciales correctamente enfocadas, de alta calidad, a color, centradas** en cumplimiento con las normas ISO aplicables. El marco biométrico admite los siguientes formatos de procesamiento de validación de identidad y reconocimiento facial:

- JPEG (ISO/IEC 10918-1)
- JPEG-2000 (ISO/IEC 15444-1)
- PNG (ISO/IEC 15948:2003)

TNPC valida continuamente la calidad de la imagen durante la captura a fin de asegurar que las imágenes presentadas cumplen con los requerimientos de reconocimiento biométrico, procesamiento de OCR y verificación de prueba de vida pasiva.

8.7.1.1.2 **Calidad de la fotografía**

8.7.1.1.2.1. La fotografía tiene que ser neutral en cuanto al color y el reflejo natural del color de la piel, para lograr una foto de calidad no debe haber saturación, todos los canales RGB deben tener al menos siete bits de variación en la intensidad, es decir, que abarque un rango de al menos 128 valores únicos en la región de la imagen.

8.7.1.1.2.2. Todas las fotografías deben tener el enfoque y profundidad suficientes, la cámara debe ser capaz de representar con precisión los detalles faciales finos como arrugas y lunares.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC valida que todas las imágenes biométricas mantengan el **tono natural de la piel, calidad de color balanceada y suficiente variación de intensidad RGB** a fin de posibilitar el reconocimiento facial y verificación de prueba de vida pasivos.

El motor de captura biométrica realiza automáticamente:

- Análisis de intensidad y saturación RGB
- Validación de brillo y contraste
- Verificación de balance de color
- Análisis de nitidez y enfoque de la imagen
- Verificaciones de calidad de los detalles del rostro
- Detección de borrosidad y ruido

durante el proceso de captura de imagen a fin de asegurar que la imagen presentada cumple los umbrales mínimos de calidad requeridos para el análisis de coincidencia biométrica y contra la suplantación de identidad.

TNPC también valida que las imágenes estén **correctamente enfocadas, con alta resolución y suficientes detalles** para identificar claramente las características del rostro como líneas finas, contornos y características de la piel requeridas para el procesamiento confiable de reconocimiento biométrico y prevención de fraude. Si no se cumplen los umbrales de calidad de imagen, TNPC ofrece feedback en tiempo real y solicita al suscriptor que vuelva a realizar la captura de la imagen antes de continuar con la validación.

8.7.1.1.3 **Posición del rostro con respecto de la cámara**

8.7.1.1.3.1. La foto tiene que mostrar a la persona mirando directamente al lente de la cámara, la fotografía tiene que guardar el aspecto natural del rostro.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC valida que el suscriptor esté **mirando directamente al lente de la cámara con un aspecto natural del rostro** para garantizar el reconocimiento biométrico y verificación de prueba de vida pasivos.

El motor de captura biométrica realiza automáticamente:

- Validación de la alineación del rostro
- Análisis de orientación de la cabeza
- Verificación de la dirección de los ojos
- Detección de pose natural

y ofrece orientación en tiempo real si el suscriptor no posa correctamente antes de continuar con el procesamiento biométrico.

8.7.1.1.4 Posición y aspecto del rostro

8.7.1.1.4.1. *La imagen en la fotografía debe reflejar la cabeza entera y la parte alta del cuello, los lados derecho e izquierdo del rostro deben estar completamente visibles. La persona fotografiada debe mirar directamente el lente de la cámara, la expresión del rostro debe ser natural y los labios deben estar cerrados. El rostro debe estar mirando fijo el lente de la cámara, la posición de la cabeza no puede estar torcida, no puede estar de perfil, no puede tener inclinaciones hacia arriba o abajo, debe estar en una posición horizontal con respecto del lente de la cámara.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC valida que la imagen capturada muestre el **rostro completo, cabeza completa, zona superior del cuello y visibilidad total de ambos lados del rostro**, con el suscriptor mirando directamente al lente de la cámara con una expresión facial natural y los labios cerrados.

El motor de captura biométrica realiza automáticamente:

- Análisis de posición e inclinación de la cabeza
- Validación de rostro centrado
- Detección de perfil y ángulo
- Verificación de alineación horizontal
- Análisis de visibilidad facial

para asegurar que las imágenes de perfil, con excesiva inclinación de la cabeza y las capturas que no estén correctamente alineadas sean rechazadas antes de continuar con el procesamiento biométrico.

8.7.1.1.5 Dirección y visibilidad de los ojos

8.7.1.1.5.1. *Los ojos deben mirar directamente hacia el lente de la cámara, ambos ojos deben de abrirse de forma natural, claramente visibles, no forzarse al abrirlos, no pueden estar cubiertos por cabello.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC valida que ambos ojos estén **naturalmente abiertos, claramente visibles y miren directamente al lente de la cámara**, sin obstrucción del cabello, sombras ni accesorios para garantizar el reconocimiento biométrico y la verificación de prueba de vida pasiva en forma precisa.

El motor de captura biométrica realiza automáticamente:

- Detección de posición y mirada de los ojos
- Análisis de visibilidad de los ojos
- Detección de obstrucción
- Validación de orientación del rostro

y ofrece orientación en tiempo real si la visibilidad de los ojos o los requerimientos de alineación no son satisfactorios antes de continuar con el procesamiento biométrico.

8.7.1.1.6 Brillo y contraste

8.7.1.1.6.1. *El rostro en todas las partes tiene que ser reflejado de manera nítida y con el contraste adecuado, en general el retrato debe tener brillo y buen contraste entre cara, cabello y fondo.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC valida que la imagen facial capturada mantenga **clara visibilidad, brillo balanceado y contraste adecuado** entre el rostro, cabello y fondo para el reconocimiento biométrico y verificación de prueba de vida en forma precisa.

El motor de captura biométrica realiza automáticamente:

- Análisis de brillo y contraste
- Detección de sombras y reflejos
- Validación de visibilidad del rostro
- Verificaciones de diferenciación del fondo

y ofrece orientación en tiempo real si las condiciones de iluminación o contraste no cumplen con los umbrales de calidad biométrica requeridos antes de continuar con el procesamiento de validación.

8.7.1.1.7 La iluminación (Luz)

8.7.1.1.7.1. *El rostro debe estar bien iluminado, se tienen que evitar reflejos, sombras en el rostro y el efecto de ojos rojos. No se utilizarán filtros de polarización lineal delante de la lente de la cámara, ya que interfieren con las cámaras de enfoque automático y reducen o eliminan la piel, información de textura que podría ser utilizada por los algoritmos de comparación de imágenes faciales.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC valida que la imagen facial capturada esté correctamente iluminada con la iluminación balanceada y clara visibilidad del rostro para el reconocimiento biométrico y verificación de prueba de vida en forma precisa.

El motor de captura biométrica realiza automáticamente:

- Análisis de consistencia de la iluminación
- Detección de reflejos y sombras
- Detección de ojo rojo
- Validación de textura del rostro
- Verificaciones de visibilidad detallada de la piel

para asegurar que los reflejos, sombras excesivas, brillo o distorsiones de iluminación no impacten en la calidad del procesamiento biométrico. TNPC también valida que las condiciones de captura de la imagen conserven la información de la textura natural del rostro requerida para una comparación confiable del rostro y para el análisis contra la suplantación de identidad.

8.7.1.1.8 Personas con anteojos

8.7.1.1.8.1. Los ojos tienen que estar bien visibles, el borde de los cristales y los marcos no pueden cubrir los ojos, los anteojos no pueden tener cristales de color u oscuros, los cristales no pueden reflejar la luz, no se pueden utilizar gafas de sol o gafas con filtros de polarización, se aplica una excepción cuando el sujeto afirma razón médica.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC valida que ambos ojos estén **totalmente visibles y sin obstrucciones** durante la captura biométrica para el reconocimiento facial y verificación de prueba de vida en forma precisa.

El motor de captura biométrica realiza automáticamente:

- Análisis de visibilidad de los ojos
- Detección de brillo y reflejos
- Validación de obstrucción de marcos
- Detección de lentes oscuras
- Verificaciones de visibilidad de marca facial

para garantizar que los anteojos de sol, lentes muy oscuras, anteojos polarizados o marcos que obstruyen los ojos sean rechazados antes de continuar con el procesamiento biométrico. Se pueden adaptar las excepciones de uso de anteojos por prescripción médica conforme a las políticas operativas configurables definidas por SUTEL y CTPN-M.

8.7.1.1.9 Cubiertas de la cabeza

8.7.1.1.9.1. La persona fotografiada no puede tener la cabeza cubierta salvo sea por razones religiosas, pero inclusive en esos casos debe ser visible sin distorsión ni sombras, desde la corona hasta la base de la barbilla, desde el punto de contacto superior entre la oreja izquierda y la cara, desde el punto de contacto superior entre la oreja derecha y cara, desde borde medio entre pelo y frente.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC valida que el rostro del suscriptor esté **totalmente visible desde la corona hasta la base de la barbilla y en ambos lados del rostro** para el reconocimiento biométrico y la verificación de prueba de vida en forma precisa.

El motor de captura biométrica realiza automáticamente:

- Análisis de visibilidad facial
- Detección de sombras y obstrucciones
- Validación de cubierta de cabeza
- Verificación de marcas y límites del rostro

para asegurar que las cubiertas de cabeza no interfieren con el procesamiento biométrico.

Para adaptaciones religiosas, TNPC ofrecerá al suscriptor opciones para indicar el **uso religioso de cubierta de cabeza** durante el flujo de trabajo biométrico. En tales casos, el sistema continuará con la validación para asegurar que las zonas requeridas del rostro permanecen claramente visibles y cumplen con los requerimientos definidos de calidad biométrica.

8.7.1.1.10 Accesorios faciales

8.7.1.1.10.1. La ornamentación facial que oscurece el rostro no es permitida, es permitida aquella que no interfiera en el rostro.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC valida que los accesorios u ornamentación facial no **obstruyan, oscurezcan ni interfieran con las zonas críticas del rostro** requeridas para el reconocimiento biométrico y verificación de prueba de vida en forma precisa.

El motor de captura biométrica realiza automáticamente:

- Detección de obstrucción facial
- Análisis de sombras y cobertura
- Validación de visibilidad de marca facial
- Verificaciones de interferencia de accesorios

para asegurar que los accesorios permitidos no impacten en la calidad de reconocimiento facial, verificación de prueba de vida ni con el análisis contra la suplantación de identidad antes de continuar con el procesamiento biométrico.

8.7.1.1.11 Dimensiones del retrato y ubicación de la cabeza

8.7.1.1.11.1. La cabeza debe estar centrada en el retrato, como se describe, la imagen debe estar entre el 74-80% de la foto, con respecto de la línea horizontal ocular. La distancia entre el borde izquierdo y el punto medio de la cara debe estar entre 45-55% y la distancia vertical entre el borde superior y el centro de la cara debe estar entre el 30- 50% del centro de la boca. Los puntos característicos referidos se describen en ISO/IEC 14496-2.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC valida que la imagen facial **esté correctamente centrada, sea proporcionada y esté alineada con el marco de captura** conforme a ISO/IEC 14496-2 y los requerimientos de posicionamiento biométrico aplicables.

El motor de captura biométrica realiza automáticamente:

- Validación de cabeza centrada
- Análisis de proporciones faciales
- Verificaciones de alineación de la línea ocular
- Verificación de posicionamiento y límites del rostro
- Validación de relación horizontal y vertical

para asegurar que el posicionamiento del rostro, tamaño de la cabeza y alineación de la imagen cumplen con los umbrales requeridos de reconocimiento biométrico y verificación de prueba de vida antes de continuar con el procesamiento.

- 8.7.1.2** *Según corresponda, el servicio deberá obtener el consentimiento del usuario para el inicio de su gestión de portabilidad numérica y contar con la capacidad para obtener una o varias imágenes claras de su documento de identificación (según corresponda) que le permita al servicio no sólo hacer la lectura y completado de la información correspondiente vía OCR sino hacer una comparación fehaciente con la persona que realiza el proceso. Los oferentes deberán acreditar la forma en la cual cumplen o superan las siguientes características para el servicio:*
- 8.7.1.2.1** *El servicio de captura de documentos deberá permitir la obtención de los datos de identificación vía OCR para que los datos personales no tengan que ser ingresados por el usuario.*
- 8.7.1.2.2** *Información como el/los números(s) telefónico(s) a registrar y el correo electrónico deberán ser ingresados de manera manual por el usuario.*
- 8.7.1.2.3** *Calidad de imagen:*
- a) Alta resolución: La resolución recomendada para imágenes WEB es de 72 píxeles por pulgada (ppp). El peso ideal de las imágenes es de unos 200-300 kb, y el tamaño del lado largo no debe exceder los 1200 píxeles.*
 - b) Relación de contraste y brillo que permita distinguir los caracteres del fondo.*
 - c) Eliminar el ruido de la imagen para facilitar la legibilidad para el algoritmo de OCR.*
 - d) Corregir la inclinación y orientación de la imagen de modo que el texto quede correctamente alineado.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC ofrece un **marco de captura de documento basado en OCR seguro e inteligente** que está directamente integrado a los flujos biométricos de portación a fin de permitir la extracción automática de la identidad, verificación del documento y garantizar la identidad del suscriptor.

El servicio de captura de documentos extrae automáticamente la información de identidad del documento de identidad presentado, usando la tecnología de OCR, eliminando la necesidad de que el suscriptor ingrese la información de identidad personal en forma manual durante el proceso de portación. El suscriptor puede manualmente proporcionar solo la información operativa adicional, cuando sea requerido, tal como:

- Número de teléfono
- Dirección de correo electrónico

TNPC valida continuamente la calidad de la imagen del documento durante la captura y ofrece feedback en tiempo real para asegurar que la imagen presentada cumpla con los requerimientos del OCR y de procesamiento biométrico.

El motor de validación de imágenes de TNPC realiza automáticamente:

- Validación de imagen de alta resolución
- Optimización de brillo y contraste
- Verificaciones de visibilidad de caracteres del fondo
- Reducción de ruido para legibilidad de OCR
- Corrección automática de inclinación y orientación
- Detección de borrosidad y enfoque
- Validación de límites y alineación del documento

TNPC valida que las imágenes capturadas del documento cumplan con los umbrales requeridos de calidad de imagen:

- Calidad de imagen web mínima recomendada 72 ppp
- Resolución y tamaño óptimos de imagen
- Lectura y contraste del texto adecuados
- Orientación correcta de la imagen
- Contenido de documento claro y legible

Si no se cumplen los umbrales de confianza del OCR, TNPC ofrece orientación inmediata y solicita al suscriptor que vuelva a realizar la captura del documento antes de continuar con el procesamiento de validación.

Los resultados de extracción por OCR, validaciones de calidad de imagen, eventos de procesamiento de documentos y las decisiones en el flujo de trabajo asociados se gestionan y auditan centralmente en TNPC a fin de asegurar:

- Trazabilidad operativa
- Extracción confiable por OCR
- Validación segura de la identidad
- Cumplimiento regulatorio
- Calidad consistente del flujo de trabajo biométrico

A través de este marco integrado de OCR y validación de calidad de imagen, TNPC ofrece a Costa Rica una **capacidad de captura de identidad digital con alta precisión, que cumple con los estándares y es amigable**; y está totalmente integrada a los flujos de trabajo de portación del SIPN.

8.7.1.3 *El servicio deberá ser capaz de hacer la verificación de legitimidad de los documentos de identificación capturados. Deberá verificar si los documentos están alterados de alguna manera considerando las marcas de seguridad según el tipo de documento a validar y la práctica de la industria para descartar si se trata de alguna falsificación o fotocopia.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC ofrece un **marco de validación de la legitimidad del documento de identidad de avanzada**, diseñado para verificar que los documentos de identidad presentados son auténticos, inalterados y válidos antes de continuar con el procesamiento de coincidencia biométrica y portación.

El motor de validación de documentos de TNPC realiza automáticamente:

- Detección de falsificación y alteraciones
- Identificación de copia/fotocopia
- Validación de consistencia de la plantilla del documento
- Análisis de integridad de la imagen
- Verificaciones de consistencia de texto y representación
- Validación de confianza en OCR
- Detección de manipulación de imagen

El marco de validación analiza:

- Consistencia del tamaño de letra y representación
- Patrones del fondo
- Artefactos de la imagen
- Indicadores de adulteración
- Anomalías en impresión y escaneo
- Consistencia de textura y resolución

a fin de identificar documentos de identidad potencialmente fraudulentos, modificados, duplicados o falsos en base a las prácticas de verificación de documento estándares de industria.

Si se detectan indicadores sospechosos o inconsistencias en los documentos, TNPC puede:

- Rechazar la validación
- Escalar la transacción para revisión manual
- Solicitar recaptura del documento
- Bloquear el flujo de trabajo de portación

en base a políticas operativas configurables definidas por SUTEL y CTPN-M.

Todos los eventos de validación de legitimidad del documento, indicadores de fraude, resultados de OCR, resultados de validaciones, marcas de tiempo y decisiones en el flujo de trabajo se registran y auditan centralmente dentro de TNPC.

A través de esta capacidad de validación de legitimidad del documento, TNPC ofrece a Costa Rica un **marco de validación de identidad seguro, en cumplimiento con los estándares y resistente al fraude**, que reduce significativamente el riesgo de uso de documentos de identidad falsos, alterados o duplicados dentro de las transacciones de portación del SIPN.

8.7.1.4 *La Contratista deberá incluir como parte del servicio, las actualizaciones y mejoras que apliquen sobre los algoritmos de biometría con prueba de vida, verificación de documentos y obtención de datos por OCR según las mejores prácticas de la industria.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

TNPC incluirá **actualizaciones y mejoras continuas a las capacidades de reconocimiento biométrico, detección de prueba de vida pasiva, procesamiento de OCR, validación de legitimidad del documento y contra la suplantación de identidad**, en línea con las mejores prácticas de la industria, los requerimientos regulatorios y los estándares de ciberseguridad en constante evolución.

El marco biométrico de TNPC soporta la mejora continua de:

- Algoritmos de coincidencia biométrico
- Modelos de detección de prueba de vida pasiva
- Mecanismos de detección de deepfake y suplantación de identidad
- Calidad de precisión y extracción del OCR
- Validación de autenticidad del documento
- Motores de puntaje de detección de fraude y riesgos
- Optimización de calidad y captura de imágenes

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

TNPC evalúa continuamente las amenazas biométricas, técnicas de fraude y ataques de identidad generados por IA que surgen y los patrones de falsificación de documentos en constante evolución, a fin de consolidar la precisión de la validación y seguridad de las transacciones a lo largo del sistema del SIPN.

Las mejoras aplicables y las actualizaciones de algoritmos se incorporarán al marco controlado de gestión de gobierno y versiones de TNPC para asegurar:

- Estabilidad operativa
- Retrocompatibilidad
- Cumplimiento regulatorio
- Mejora continua de seguridad
- Mínima interrupción operativa

Todas las mejoras serán validadas dentro de los entornos de desarrollo y pruebas antes de la entrada en producción y seguirán los mismos procesos estructurados de pruebas, auditorías y aprobaciones operativas aplicadas a todas las actualizaciones de la plataforma de TNPC.

A través del marco de mejora continua, TNPC garantiza que el servicio de validación biométrica sea **moderno, seguro, resistente al fraude, cumpla con los estándares y esté alineado con las prácticas biométricas y de verificación de identidad líderes de la industria** a través de las operaciones del ciclo de vida completo del SIPN.

9 Requisitos de admisibilidad de la oferta

El oferente deberá cumplir, como mínimo, con todos los requisitos determinados en el presente pliego de condiciones. Según lo anterior, se establecen los siguientes requisitos de admisibilidad.

- 1.5.17.1.** Su oferta debe indicar mediante la leyenda: “Entendemos, Aceptamos y Cumplimos” a cada uno de los ítems de los requisitos indicados en el presente pliego de condiciones. Mediante lo anterior, declara su compromiso con cada uno de los puntos respondidos.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

- 1.5.17.2.** Presentación de dos ofertas económicas independientes para dos periodos: 5 años y 7 años.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado. Por favor consultar la Propuesta Comercial de TNS (nombre del archivo: TNS_SUTEL_Respuesta Comercial ERPN).

- 1.5.17.3.** Documentación que acredite, al menos, 10 años de constituida y con experiencia en sistemas para portabilidad numérica con operadores/proveedores y/o reguladores de telefonía móvil.

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Consulte el Anexo 2 (Cartas de Referencias de Operación) y Anexo 3 (Cartas de Referencia de Migración).

Contamos con amplia experiencia como Entidad de Referencia de Portabilidad Numérica, también denominada Organismo de Administración de Portabilidad, Administrador de Base de Datos de Portabilidad o Clearinghouse.

Los países en los que hemos implementado y administrado la ERPN son:

- Grecia desde 2004 a la actualidad
- Sudáfrica desde 2006 a la actualidad
- Pakistán desde 2007 a la actualidad
- Malaysia desde 2008 a la actualidad
- Chile desde 2011 a la actualidad
- India desde 2011 a la actualidad
- Argentina desde 2012 a la actualidad
- Emiratos Árabes Unidos desde 2013 a la actualidad
- Estados Unidos de América desde 2018 a la actualidad
- Vietnam desde 2018 a la actualidad
- México desde 2008 a 2019
- Tailandia desde 2010 a 2018

- Nigeria desde 2013 a 2020
- Perú desde 2014 a 2019

1.5.17.4. *Acreditar haber operado con éxito como Entidad de Referencia de Portabilidad Numérica centralizada por un periodo mínimo de tres (3) años en al menos tres (3) países (al menos 1 deberá ser en Latinoamérica) en los últimos cinco (5) años.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Consulte el Anexo 2 (*Cartas de Referencias de Operación*) y Anexo 3 (*Cartas de Referencia de Migración*).

TNS es el líder del mercado mundial de soluciones de Portabilidad Numérica (PN), que soportan servicios de portabilidad numérica fija y móvil para suscriptores. Ofrecemos una solución de Portabilidad Numérica integral y de punta a punta; somos el único proveedor con habilidades complementarias ofrecidas en la capacitación y consultoría de PN, sistemas de software y servicios administrados. Los sistemas de PN de TNS están implantados en más países que cualquier otro proveedor, por lo tanto, se minimiza el riesgo de implantación tanto para el país como para sus operadores.

entrega de software a tiempo

100% de entrega de software a tiempo



Las soluciones de Portabilidad Numérica de TNS consta de dos importantes componentes: el TruNumber Portability Clearinghouse con Servicios Administrados y el TruNumber Portability Gateway.

Referencias de Number Portability Clearinghouse de TNS

El producto insignia de Portabilidad Numérica es **TruNumber Portability Clearinghouse (TNPC)**, un sistema centralizado al cual se conectan operadores móviles y/o fijos para portar números de teléfono de los suscriptores, de forma tal que, los suscriptores puedan retener su número cuando cambian de operador. TNPC es una plataforma de hardware y software con interfaces y procesamiento de mensajes e incluye una Base de Datos Centralizada de Referencia, que sirve como repositorio para todos los números portados en un país; y un histórico de todas las transacciones relacionadas con un número portado.

TNS también brinda **Servicios Administrados** para su TNPC. Los data centers de vanguardia primarios y de recuperación ante desastres alojan la plataforma de hardware y software que ejecuta la aplicación TNPC, y personal experimentado ofrece administración y monitoreo del sistema, soporte de mesa de ayuda, soporte de mantenimiento y copia de seguridad de datos para ayudar a garantizar la disponibilidad continua de los servicios de portación a los operadores y sus clientes.

TNS tiene ocho (8) implantaciones de TNPC. A continuación, se presenta una lista de las implementaciones de TNPC de TNS:

2017: Portabilidad Numérica Móvil en Vietnam

- La Autoridad de Telecomunicaciones de Vietnam (VNTA) seleccionó el TNPC de TNS para prestar servicios a 5 operadores móviles de Vietnam. El sistema TNPC fue lanzado con éxito en 2018.

2017: Portabilidad Numérica Móvil en Argentina con Servicios Administrados

- La Secretaría de Comunicaciones de Argentina, SECOM seleccionó el TNPC de TNS para atender a los operadores móviles de Argentina. La implementación del sistema TNPC se completó y el servicio de PNM fue lanzado en marzo de 2011. El servicio ha sido prestado por TNS sin interrupciones.

2015: Portabilidad Numérica Móvil y Fija en Chile con Servicios Administrados

- El Ministerio de Transporte y Telecomunicaciones de Chile seleccionó al TNPC de TNS para atender a los operadores móviles y fijos de Chile en agosto de 2011. El sistema TNPC fue implementado y lanzado con éxito en diciembre de 2011. El servicio ha sido prestado por TNS sin interrupciones.

2010: Portabilidad Numérica Móvil en Emiratos Árabes Unidos

- La Autoridad Regulatoria de Telecomunicaciones (TRA) seleccionó el TNPC de TNS para atender a los operadores móviles en Emiratos Árabes Unidos. El sistema TNPC de TNS se encuentra en producción; y el servicio ha sido prestado por TNS sin interrupciones.

2009: Portabilidad Numérica Móvil en India

- El Ministerio de Comunicaciones y el Departamento de Tecnología de la Información de las Telecomunicaciones (DoT) seleccionó a TNS para ofrecer servicios de PN móvil en la Zona del Sudeste a los operadores móviles de India. El sistema TNPC de TNS está siendo utilizado para implementar el Clearinghouse de PNM (MCH) en la Zona del Sudeste. El sistema TNPC de TNS fue lanzado en enero de 2011. El servicio ha sido prestado por TNS sin interrupciones.

2007: Portabilidad Numérica Móvil en Malaysia

- La Comisión de Comunicaciones y Multimedia de Malaysia (MCMC) seleccionó el TNPC de TNS para atender a operadores móviles en Malasia. La NP móvil fue lanzada en octubre de 2008. El servicio ha sido prestado por TNS sin interrupciones.

2006: Portabilidad Numérica Móvil en Sudáfrica

- A principios de 2006, TNS recibió la adjudicación de un contrato por su socio local Saab Grintek para brindar el sistema TNPC al consorcio de operadores móviles en la República de Sudáfrica. El servicio fue lanzado a fines de 2006. En abril de 2010, se agregó la Portabilidad Numérica Fija a la solución. El servicio ha sido prestado por TNS sin interrupciones.

2003: Portabilidad Numérica Fija y Móvil en Grecia con Servicios Administrados

- La Comisión Helénica de Comunicaciones y Correo (EETT) adjudicó un contrato a TNS para brindar servicios PN fijos y móviles a operadores fijos y móviles en Grecia. El sistema TNPC de TNS entró en producción a comienzos de 2004. En marzo de 2014, EETT renovó el contrato del TNPC para continuar con la prestación de servicios de PN. El servicio ha sido prestado por TNS sin interrupciones.

Referencias de TruNumber Portability Gateway de TNS

TNS **Number Portability Gateway (TNPG)** es un sistema ubicado en el entorno del operador que realiza funciones de gestión de flujos de trabajo dentro del entorno del operador para soportar la portación de números fijos y móviles. Brinda interfaces para procesar solicitudes de portabilidad del suscriptor desde las operaciones back-end y sistemas de red del operador, las pasa al Clearinghouse y coordina las actualizaciones de números portados y datos de enrutamiento del Clearinghouse a los sistemas back-end en el entorno del operador local, para permitir el enrutamiento preciso de llamadas hacia números portados.

TNS ha implantado TNPG en más países y atiende a más operadores que cualquier otro proveedor. A continuación se presenta una lista de implementaciones de TNPG de TNS:

2015: Portabilidad Numérica Móvil y Fija en Túnez

- Tunisie Telecom seleccionó a TNS para ofrecer un TNPG que funcione como interfaz con el Clearinghouse de PN en Túnez una vez que esté implementado. El NPG fue lanzado con éxito en 2016.

2012: Portabilidad Numérica Móvil en Nigeria

- Etisalat y Glo seleccionaron a TNS para brindar un TNPG que funcione como interfaz con el Clearinghouse de PNM en Nigeria y permita la prestación de servicios de PNM a sus suscriptores. Los TNPG entraron en producción en abril de 2013.

2011: Portabilidad Numérica Móvil en Argentina

- Nextel Argentina seleccionó a TNS para ofrecer un TNPG que funcione como interfaz con el Clearinghouse de PN en Argentina una vez implementado.

2011: Portabilidad Numérica Móvil y Fija en Chile

- VTR y Nextel Chile seleccionaron a TNS para brindar un TNPG que funcione como interfaz de TNPC de TNS para permitir la prestación de servicios de PN a sus suscriptores.

2010: Portabilidad Numérica Móvil en Emiratos Árabes Unidos

- du adjudicó a TNS un contrato para brindar un TNPG que funcione como interfaz de TNPC de TNS que atiende a los operadores móviles en EAU.

2009: Portabilidad Numérica Móvil en India

- Vodafone, Ideal Cellular y Aircel adjudicaron individualmente a iconectiv contratos para brindar NPG que hagan interfaz con el TNPC con el fin de posibilitar la prestación de sus servicios Portabilidad Numérica Móvil a sus suscriptores móviles. Airtel adjudicó a TNS un contrato para ofrecer activación del TNPG para hacer interfaz con TNPC de TNS a fin de permitir el enrutamiento correcto de llamadas y SMS/MMS a sus suscriptores móviles.

2008: Portabilidad Numérica Fija y Móvil en México

- Telmex, AT&T Mexico y Telcel adjudicaron individualmente a iconectiv contratos para brindar un TNPG en interfaz con el Clearinghouse de México, a fin de posibilitar la prestación de servicios de PNM a los suscriptores fijos y móviles.

2007, 1997: Portabilidad Numérica Fija y Móvil en Canadá

- El software del Gateway de Portabilidad Numérica móvil de TNS es el motor detrás de la Oficina de Servicios que procesa solicitudes de PN móvil de operadores en Canadá. Entre los operadores móviles canadienses que utilizan el sistema del Gateway de TNS podemos mencionar a Bell Canada, Bell Mobility, Fido, MTS Allstream Inc. (MTS), NorthernTel, Rogers Wireless, SaskTel, TBayTel, Telebec y TELUS.
- El Gateway de Portabilidad Numérica fija de TNS es utilizado por los tres (3) operadores más grandes de Canadá: Bell Canada, Telus y MTS Allstream.

2002-3, 1997: Portabilidad Numérica Fija y Móvil en EE.UU.

- El Gateway de Portabilidad Numérica móvil de TNS fue el primero en llegar al mercado de EE.UU. Los operadores móviles líderes de EE.UU. utilizan nuestro Gateway de Portabilidad Numérica para el procesamiento de portaciones. Nuestro software procesa más del 90% de todas las solicitudes de portabilidad en EE.UU. Las solicitudes de portabilidad de 85 operadores son procesadas por la Oficina de Servicios cuyo motor de software es el Gateway de Portabilidad Numérica de TNS.
- El Gateway de PN fija de TNS procesó la primera portación en vivo de un número en EE.UU. y es utilizado por los operadores más grandes en EE.UU., incluyendo Verizon.

1.5.17.4.1. *Demostrar que alguno de los anteriores haya tenido un volumen de transacciones superior a 1.200.000 gestiones de portabilidad por año.¹*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Consulte el Anexo 2 (*Cartas de Referencias de Operación*) y Anexo 3 (*Cartas de Referencia de Migración*).

Las cartas de referencia de cada país indican la cantidad de volumen de portaciones que el sistema de TNPC ha gestionado y procesado a través de los años en operación en cada país.

1.5.17.5. *Declaración jurada de que el oferente no tiene vínculos económicos, propiedad o control por parte de algún operador/proveedor de telecomunicaciones de Costa Rica.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Consulte el Anexo 4 (*Declaración jurada de que el oferente no tiene vínculos económicos, propiedad o control por parte de algún operador/proveedor de telecomunicaciones de Costa Rica*).

1.5.17.6. El oferente deberá acreditar que cuenta con la certificación ISO/IEC 27001 debidamente vigente. El adjudicatario deberá entregar anualmente un reporte de auditoría con recomendaciones de mejora.

1.5.17.6.1. Las siguientes certificaciones son deseables:

- a) ISO/IEC 25010
- b) ISO/IEC 42010
- c) ISO/IEC 12207
- d) ISO/IEC 9001
- e) SOC2

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Certificaciones ISO 27001



CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título



iconectiv, LLC
Certificate Number: ISMS-IC-072924

| iconectiv, LLC | |
|--|--|
| IN-SCOPE LOCATION HQ: 100 Somerset Corporate Boulevard, Bridgewater, New Jersey 08807 United States of America | REGISTERED ACTIVITY Corporate Operations, ISMS Management, and Software Development |

400 N Ashley Drive, Suite 1025, Tampa, FL 32602

888.702.5446

info@align.com

A-LIGN.com

Certificado Número: ISMS-IC-072924

CERTIFICADO DE REGISTRO

Sistema de Gestión de Seguridad de la Información

ISO/IEC 27001:2022

iconectiv, LLC

A-LIGN Compliance and Security, Inc. certifica que la organización opera como un Sistema de Gestión de Seguridad de la Información (SGSI) que cumple con los requisitos de ISO/IEC 27001:2022. El alcance y los límites del SGSI son los siguientes:

El Sistema de Gestión de Seguridad de la Información (SGSI) de Iconectiv, conforme a ISO/IEC 27001:2022, ha implementado controles de seguridad adecuados para proteger la confidencialidad, integridad y disponibilidad de los activos de información de Iconectiv. El alcance contempla el diseño, desarrollo, implementación y mantenimiento de los entornos de Soluciones de Información, Administrador de Portabilidad Numérica Local -Centro de Administración de Portabilidad Numérica (LNPA-NPAC, en inglés) y Corporativo.

| | | | |
|--|----------------|----------------------------------|---------------------|
| Certificado: | ISMS-IC-072924 | Fecha de Certificación Original: | 29 de julio de 2024 |
| Versión | 1.1 | Fecha de Vencimiento: | 29 de julio de 2027 |
| Declaración de Aplicabilidad: Versión 1.2 (7 de abril de 2025) | | Fecha de Emisión: | 18 de julio de 2025 |

Logo de ISO 27001 – ANAB – IAF

Autorizado por:

Stephanie Oyler

Vicepresidenta Ejecutiva de Servicio de Constatación

El presente certificado es propiedad de A-LIGN Compliance and Security, Inc. ("A-LIGN") y es legalmente vinculante conforme a acuerdos ejecutables. El presente certificado se refiere al Sistema de Gestión de Seguridad de la Información de la organización y los requisitos de ISO/IEC 27001:2002, tal como están definidos en el alcance; y no implicarán de modo alguno la certificación de los productos, procesos o servicios de la organización (dentro y fuera del alcance). El número de certificado, marca en el cuerpo del mismo y marca de acreditación no serán usados en los productos ni utilizados junto con documentos relativos a los productos, procesos o servicios de la organización. A-LIGN tomará medidas frente a uso incorrecto o engañoso del certificado, estado de certificación o marcas. Para validar este certificado, contactarse con A-LIGN.

400 N Ashley Drive, Suite 1325, Tampa, FL 32602 888.702.5446 info@a-lign.com A-LIGN.com

Logo de A-ALIGN

iconectiv, LLC

Certificado Número: ISMS-IC-072924

iconectiv, LLC

UBICACIÓN DENTRO DEL ALCANCE

ACTIVIDAD REGISTRADA

Sede central: 100 Somerset Corporate Boulevard,
Bridgewater, Nueva Jersey 08807
Estados Unidos de América

Operaciones corporativas, Gestión de SGSI
y Desarrollo de Software.

400 N Ashley Drive, Suite 1325, Tampa, FL 32602 888.702.5446 info@a-lign.com A-LIGN.com

This is a true and complete translation into Spanish of the source document written in English which I had before me. The translation is digitally signed by Maria Laura Rosenzweig, Certified Translator, Commission 4091, VOLUME 12, FOLIO 403. In Buenos Aires, on this 15th day of September, 2025.

Lo que antecede es traducción fiel y completa al idioma español del documento fuente redactado en idioma inglés que tuve a la vista y al cual me remito. La traducción está firmada digitalmente por María Laura Rosenzweig, Traductora Pública, Matrícula 4091, TOMO 12, FOLIO 403. En Buenos Aires, a los 15 días de septiembre de 2025.-

Maria Laura Rosenzwaig

Firmado digitalmente por ROSENZWAIG María Laura
 DN: C=AR, O=Consejo Autónomo de Buenos Aires, OU=Secretaría de
 Tecnologías de Gestión, OU=Ministerio de Gestión Pública,
 OU=Oficina Nacional de Tecnologías de Información, OU=Secretaría de
 Gestión de Procesos, SERIALNUMBER=227.88888887,
 OU=Autoridad Certificada de Firma Digital
 Razón: María Laura Rosenzwaig - Traductora Pública de Inglés -
 Certified English Translator
 Fecha: 2016.06.24 13:52:00 -03

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

- 1.5.17.7.** *Demostrar haber realizado, al menos, un (1) proceso de migración exitosa de sistemas existentes hacia su propia plataforma, sin interrupción del servicio y con preservación de la integridad histórica de los datos. Brindar la información pertinente a cualquier otro proceso de migración exitoso. Esta deberá ser acreditada por parte del regulador del país correspondiente y validada por los miembros del CTPN-M.*

Respuesta de TNS:

Entendemos, Aceptamos y Cumplimos con el requerimiento arriba indicado.

Consulte el anexo 1 (Caso de Estudio : *Implementación de la Portabilidad Numérica Móvil y Fija en Perú*) y Anexo 3 (Cartas de Referencia de Migración).

TNS presenta las siguientes pruebas de experiencias previas exitosas en la migración de procesos de portación desarrollados por terceros y que se encuentran en producción.

- Perú en 2014, de Informática El Corte Inglés, fue la primera migración realizada a nivel mundial y se realizó en forma efectiva y sin problemas técnicos, con el apoyo del regulador peruano (OSIPTEL). Consultar documento adjunto.
- EE.UU. en 2018, la migración fue realizada por Neustar, utilizando también las mejores prácticas aprendidas de Perú. Esta migración fue la más grande en función del volumen y también la completamos sin ningún problema técnico.

En resumen, cabe mencionar que es necesario coordinar con el Comité de Portabilidad la información mínima requerida como establecen los reglamentos; y que el proveedor saliente entregue una copia histórica de estos datos y después proporcione las actualizaciones diarias para mantener la nueva base de datos actualizada hasta el día del lanzamiento de la nueva plataforma.

Además para que la integración sea lo más fluida posible, es necesario contar con las definiciones de las interfaces para que la integración con la nueva ERPN y los operadores telefónicos no requiera ninguna modificación.

10 Notificaciones

Esta respuesta al pliego de condiciones es para fines informativos solamente y no constituye un contrato ni una oferta de contrato. Es posible que las descripciones de productos incluidas en la presente propuesta sean generales y deban ajustarse para satisfacer los requerimientos específicos de la SUTEL.

Este documento y la información confidencial que contiene serán usados por la Sutel solo para considerar un posible acuerdo comercial con TNS y para ningún otro fin; y serán distribuidos, enviados o puestos a disposición solamente de las personas autorizadas que deban tomar conocimiento dentro de la SUTEL, pero no de terceros, salvo con el consentimiento previo por escrito de TNS.

11 Marcas Registradas

Copyright 2026 de Transaction Network Services, Inc.

El logo de TNS y las demás marcas registradas, marcas de servicio y diseños son marcas comerciales, registradas o no, de Transaction Network Services, Inc. y sus subsidiarias en Estados Unidos y países extranjeros. Todas las demás marcas comerciales son propiedad de sus respectivos dueños.

12 Anexos

Esta sección contiene una descripción de los documentos presentados que constituyen nuestra respuesta completa:

Anexo 1 – Caso de Estudio : *Implementación de la Portabilidad Numérica Móvil y Fija en Perú*

Anexo 2 – Cartas de Referencias de Operacion

Anexo 3 – Cartas de Referencia de Migracion

Anexo 4 – Declaración jurada de que el oferente no tiene vínculos económicos, propiedad o control por parte de algún operador/proveedor de telecomunicaciones de Costa Rica.

Anexo 1 – Caso de Estudio : Implementación de la Portabilidad Numérica Móvil y Fija en Perú



Caso de Estudio

Implementación de la Portabilidad Numérica Móvil y Fija en Perú



Cómo iconectiv Perú reemplazó al Administrador de PNM existente y lanzó la PNF en tiempo récord

La Portabilidad Numérica Móvil (PNM) se lanzó originalmente en Perú en enero de 2010, a través de un procedimiento gratuito para los consumidores, y con un plazo máximo para el trámite de portabilidad de hasta siete días (07) que incluía la presentación de documentación de parte de los usuarios para solicitar cambiarse de empresa operadora, así como procedimientos de validación manuales por parte del Administrador, no lográndose los resultados esperados, debido, entre otros, al tiempo que podría tomar el referido trámite así como al nivel de información que tenía el usuario sobre este mecanismo de competencia.

En dicho contexto, a fin de hacer que la portabilidad numérica sea más fácil para el consumidor y promover el desarrollo de un mercado de telecomunicaciones pujante y competitivo, el regulador de telecomunicaciones de Perú, OSIPTEL, aprobó en diciembre de 2013 la nueva reglamentación que

RESUMEN EJECUTIVO

Panorama general de la Portabilidad Numérica en Perú:

- La PNM fue originalmente lanzada en 2010
- PNM con resultados obtenidos por debajo de los esperados. Falta de información de los consumidores, y largos tiempos de portación de hasta siete (07) días

Requerimientos y desafíos

- Reducir el tiempo máximo de portación de 7 días a 24 horas
- Reemplazar la documentación impresa por la Consulta Previa en línea
- Cronograma ajustado para los lanzamientos de PNM y PNF
- Facilitar la portabilidad numérica al menor costo posible para los concesionarios

Solución

- iconectiv implementó su solución Number Portability Clearinghouse líder en la industria para PNM y PNF en tiempo récord
- La solución soporta la nueva Consulta Previa en línea, y la Base de Datos Alojada de Validación
- Permite a los pequeños concesionarios acceder al sistema de PN en forma rentable

Resultados

- Mejora en la competencia y opciones para los consumidores
- Proceso de portación más fácil para el usuario
- Reducción de los tiempos de portación a 24 horas
- Acceso rentable de los concesionarios al sistema de PN y funciones de soporte

Un mercado de telecomunicaciones en constante cambio en Perú

El mercado de telecomunicaciones peruano tiene más de 30 millones de abonados del servicio móvil y fijo. Movistar y Claro son los líderes del mercado tanto en servicios móviles como fijos, y Entel Perú (ex Nextel) es el tercer concesionario móvil.

Las áreas de foco clave de OSIPTEL, el regulador de telecomunicaciones de Perú, son promover la competencia y mejorar la calidad del servicio. La introducción de servicios de PNM más fáciles para el usuario y el lanzamiento reciente de la PNF forman parte de este esfuerzo.

El mercado móvil de Perú es reconocido por su potencial. El ingreso reciente de Viettel bajo la marca Bitel como el cuarto concesionario móvil, ayudado por la portabilidad numérica, marca el comienzo de un nuevo y emocionante capítulo en el mercado de las telecomunicaciones de Perú.



CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título



Caso de Estudio

reduce el tiempo de portación a un día para portaciones móviles, y elimina la presentación de documentación adicional a los usuarios, realizándose las validaciones de los requisitos para poder portarse en línea. La reglamentación también requería la implementación de la Portabilidad Numérica Fija (PNF) para julio de 2014.

Luego de publicar un nuevo concurso para PNM y PNF, OSIPTEL seleccionó a iconectiv Perú S.A.C. ("iconectiv")¹ en marzo de 2014 para la implementación y administración de los sistemas de PNM y PNF. A pesar de los plazos ajustados, la introducción de nuevas prestaciones, y las preocupaciones de los concesionarios del servicio fijo respecto del costo de implementación, iconectiv pudo trabajar con todos los interesados de la industria para implementar un sistema conjunto de PNM y PNF en tan sólo tres meses. En julio de 2014, iconectiv asumió con éxito la administración del servicio de PNM existente del consorcio IECISA-INDRA, y lanzó el nuevo servicio de PNF a tiempo, cumpliendo con todos los requerimientos del regulador.

El Desafío

Cuando en marzo de 2014 OSIPTEL nombró a iconectiv Perú como el nuevo administrador de la portabilidad numérica a partir de julio de 2014, fue el comienzo de un período intenso para la compañía. iconectiv enfrentó una serie de desafíos:

- Un cronograma ajustado de tres meses para la implementación del sistema, la integración de los concesionarios, y la realización de pruebas en pos de garantizar un lanzamiento comercial sin inconvenientes
- La migración de los datos de PNM existentes del proveedor anterior, y la transición íntegra del servicio de PNM sin interrupciones
- La reducción significativa del tiempo de portación de 7 días a 24 horas

- La incorporación de una nueva consulta en línea, o proceso de Consulta Previa

La Consulta Previa evita que los consumidores deban presentar documentación impresa en el punto de venta cuando solicitan la portabilidad. También minimiza el riesgo de rechazo de las solicitudes de portabilidad.

"Trabajar con iconectiv ha sido una grata experiencia durante todo el proceso de implementación de la Base de Datos Centralizada Principal de Portabilidad Numérica en el servicio público móvil y en el servicio público de telefonía fija, e inclusive durante el período de pruebas".

"Resaltamos la experiencia demostrada y la total disposición brindada para solucionar las eventualidades presentadas, con la flexibilidad y celeridad que ameritaba, no sólo en el proceso mismo de implementación de la base de datos, sino en especial para lograr que el proceso de migración de la portabilidad en el servicio público móvil sea ejecutado cumpliéndose con los plazos inicialmente programados".

Opinión oficial de OSIPTEL sobre su experiencia de trabajar con iconectiv Perú S.A.C.



¹ Iconectiv Perú S.A.C. es una subsidiaria totalmente controlada de Telcordia Technologies, Inc., que opera como iconectiv.



Caso de Estudio

iconectiv también tuvo que trabajar en paralelo con todos los concesionarios del servicio fijo de Perú en la implementación, pruebas, y lanzamiento del nuevo servicio de PNF al tiempo que se garantizó una solución altamente rentable.

La Solución

iconectiv implantó su solución de Number Portability Clearinghouse líder en el mundo, que actualmente se utiliza en 16 países, incluyendo Argentina, Chile, México, India, Turquía, Nigeria, Sudáfrica, Tailandia, y Malasia. Number Portability Clearinghouse se ha mejorado continuamente a través de los años, con la incorporación de las mejores prácticas, y los requerimientos de portabilidad numérica de países de todo el mundo.

La solución de iconectiv Perú, robusta y probada en el campo, cuenta con las siguientes características clave:

- Soporta tanto la PNM como la PNF en una versión del software
- Se aloja en forma remota para reducir costos y aprovechar las instalaciones de clearinghouse de portabilidad numérica existentes de iconectiv

- Incluye una base de datos centralizada para almacenar datos de portabilidad numérica, temporizadores de mensajes, y una interfaz gráfica de usuario para los concesionarios pequeños, el regulador y la administración del sistema

El sistema también soporta la función de Consulta Previa en línea. Cuando un cliente ingresa a una tienda para cambiar de concesionario, el concesionario anterior (la red del cedente) recibe una consulta en línea para verificar la información del abonado. La red del cedente debe responder dentro de los 120 segundos. El sistema de portabilidad numérica monitorea e informa las respuestas al regulador, a fin de garantizar que el concesionario cumple con las reglas de portabilidad numérica. Si la red del cedente no responde dentro de los 120 segundos, la portación aún puede proceder por defecto, pero el sistema registra el incidente y, eventualmente, puede dar lugar a una multa sustancial para la red del cedente.

Para abordar las preocupaciones de los concesionarios que no contaban con una interfaz de servicios web Simple Object Access Protocol (SOAP) para la prestación de consultas en línea, iconectiv desarrolló la función de Base de Datos Alojada de Validación en pos de ahorrar costos de implementación innecesarios.

| Plazos | |
|--|-----------------------------------|
| Anuncio de Adjudicación | 17 de marzo de 2014 |
| Definición de los Requerimientos de Software | 18 de marzo - 18 de abril de 2014 |
| Instalación del Hardware/Software de Terceros Requeridos | 21 de abril - 12 de mayo de 2014 |
| Implementación y Documentación del Software | 27 de mayo - 20 de junio de 2014 |
| Aceptación | 2-26 de junio de 2014 |
| Capacitación | 23-30 de junio de 2014 |
| Establecimiento de Mesa de Ayuda y Data Center | 2 de junio de 2014 |
| Pruebas de la Industria | 1-11 de julio de 2014 |
| Entrada en producción Móviles | 16 de julio de 2014 |
| Entrada en producción Fijas | 26 de julio de 2014 |



Caso de Estudio

Hacer el trabajo

Las capacidades técnicas líderes de la industria de iconectiv sumadas a las metodologías de gestión de proyectos, y décadas de vasta experiencia en la implantación de soluciones de portabilidad numérica de iconectiv fueron, sin dudas, cruciales a la hora de cumplir con los exigentes plazos requeridos por OSIPTEL.

Garantizar una transición de PNM sin inconvenientes

iconectiv reunió un equipo técnico con grandes habilidades de gestión de proyectos y comunicación. El equipo pudo trabajar directamente con el regulador y los concesionarios para desarrollar los requerimientos y la solución correcta para Perú en base a las condiciones del mercado local. Dado que ya existía un sistema de PNM anterior, iconectiv trabajó estrechamente con los concesionarios para minimizar el impacto en sus gateways de portabilidad numérica existentes, y hacer que la transición al nuevo sistema de PNM fuese lo más fluida posible. La compañía programó reuniones de estado del proyecto en forma regular con los concesionarios y OSIPTEL para intercambiar información y garantizar que todos los interesados comprendieran y estuviesen preparados para las próximas actividades. La migración de los datos de PNM del proveedor anterior al sistema de PNM nuevo de iconectiv fue una tarea clave. Exigió convenir los formatos de entrega y diversas iteraciones para

garantizar que la migración funcionase conforme a lo previsto.

Optimización del desempeño del sistema de PNM y Soporte al Cliente

La implementación de la portabilidad numérica no es sólo un cambio cultural sino también un cambio técnico que afecta a toda la industria. Escuchando con atención a los concesionarios, el equipo de iconectiv pudo saber qué funcionaba y qué no funcionaba tan bien con el sistema de PNM anterior, y luego propuso mejoras. Por ejemplo, una mejora importante fue la interfaz gráfica de usuario general y el desempeño al consultar un número telefónico. Con la aplicación anterior podía llevar un minuto o más consultar un número, mientras que la solución de iconectiv devuelve una respuesta en segundos. Otra mejora fue la implementación de una mesa de ayuda 24x7 a la cual los concesionarios pueden acceder por correo electrónico o por teléfono. Luego de la puesta en producción, se convirtió en la primera fuente de soporte al concesionario.



Caso de Estudio

Resultados y beneficios

La transición al nuevo sistema de PNM de iconectiv se realizó sin inconvenientes. El 15 de julio de 2014 por la mañana, iconectiv recibió los datos de PNM del proveedor anterior, migró los datos al nuevo sistema, y comenzó con éxito el nuevo servicio de PNM el 16 de julio de 2014. El 26 de julio de 2014 siguió el lanzamiento exitoso del servicio de PNF de iconectiv.

Los servicios mejorados de PNM y nuevos de PNF contribuyen al desarrollo de un mercado de telecomunicaciones competitivo y dinámico en Perú. Un proceso de portación más fácil para el usuario con tiempos de portación más rápidos significa que los consumidores pueden portar sus números en forma efectiva con sólo una visita a la tienda, y sin tener que llevar ninguna documentación impresa.

"Trabajar con iconectiv fue una experiencia muy buena, se tuvo muy buena documentación y todo estaba bien organizado y preparado, lo cual nos ayudó a implementar fácilmente los sistemas desde nuestro lado. A pesar que no tuvimos la oportunidad de asistir a las capacitaciones presenciales, la buena documentación y apoyo técnico fueron fundamentales para sacar adelante el sistema de portabilidad.

"Personal bien entrenado, mucha experiencia en este tipo de trabajo, buena infraestructura tecnológica", buena organización y planeación.

"Agradecerles su paciencia y tiempo en ayudarnos en cada uno de nuestras dificultades en la hora del desarrollo y pruebas".

Concesionario de Perú

Prestaciones y beneficios de Number Portability Clearinghouse

| | |
|--|--|
| Reducción del tiempo de portación de 7 días a 24 horas | Facilita el proceso de portación a los consumidores. Requiere sólo una visita a la tienda del concesionario. |
| Consulta Previa en Línea | Simplifica la portación a los consumidores. Elimina la necesidad de presentar documentación impresa. |
| Base de Datos Alojada de Validación | Ahorra costos de implementación a los concesionarios. Elimina la necesidad de desarrollar nuevas interfaces web. |
| Sistema de portabilidad numérica alojado en forma remota | Reduce los costos para los concesionarios y los consumidores. Aprovecha las instalaciones del sistema de PN de iconectiv existentes. |
| Interfaz gráfica de usuario mejorada | Fácil para el usuario. Ahorra tiempo y reduce el potencial de error para el usuario. |
| Consulta de número más rápida | Facilita la consulta de números. Ahorra tiempo y costos de empleados. |
| Mesa de ayuda 24x7 mejorada | Mejora la eficiencia y calidad de todo el servicio. |

Acerca de iconectiv Perú S.A.C.

iconectiv Perú S.A.C. es una subsidiaria totalmente controlada de Telcordia Technologies, Inc., que opera como iconectiv. iconectiv desarrolla soluciones líderes del mercado que permiten a los operadores interconectar redes, dispositivos y aplicaciones críticas al mercado global de las telecomunicaciones en constante evolución. Las soluciones poderosas de interconexión y base de datos de iconectiv para la industria de las telecomunicaciones incluyen los clearinghouses de portabilidad numérica, servicios de gestión de información de red, servicios de mensajería móvil, registros de dispositivos móviles antirrobo, bases de datos de administración de espectro, y otros servicios de información de interconexión.

Para más información acerca de iconectiv, contáctese con su ejecutivo de cuentas local, o comuníquese al:

+1 732.699.6800
info@iconectiv.com
www.iconectiv.com

Copyright ©2014 iconectiv
Todos los derechos reservados.
MC-NP-CS-001S_Peru

5

Anexo 2 – Cartas de Referencias de Operación

Comité de Portabilidad Numérica República Argentina (COPON)

Ciudad Autónoma Buenos Aires, 14 de Mayo 2026

Señores

**Superintendencia de Telecomunicación
Costa Rica**

PABLO FRANCISCO ARANCEDO, en mi calidad de Coordinador Ejecutivo y representante del Comité de Portabilidad Numérica de la República Argentina ("COPON"), CERTIFICO: que la sociedad Administradora de la Portabilidad Argentina S.A. ("APA"), subsidiaria de Iconectiv, LLC ("Iconectiv") en octubre de 2011 resultó adjudicataria y celebró contrato con los licenciatarios de servicios de comunicaciones móviles para actuar como administradora de la Base de Datos Centralizada de Portabilidad Numérica en la República Argentina. En mayo del 2021, resultó nuevamente adjudicataria del segundo proceso de licitación para la administración centralizada de la Base de Datos de Portabilidad Numérica en la República Argentina, celebrando nuevo contrato con los licenciatarios de servicios de comunicaciones móvil y fijos.

El servicio de Portabilidad Numérica móvil de APA (en base al esquema All Call Query) opera en forma regular y continua desde su lanzamiento comercial en marzo del 2012 hasta la fecha. En Septiembre del año 2022 se inició a la portabilidad numérica del servicio de telefonía fija.

Desde el inicio del servicio de administración centralizada se procesaron más de 32,6 millones de solicitudes de portación, completándose más de 27,7 millones de portaciones móviles y fijas con la atención de más de 75 millones de móviles y fijos para 45 Prestadores de Servicios Portables de Argentina.



Pablo F. Arancedo

Coordinador Ejecutivo

**Comité Portabilidad Numérica
(COPON)**

Marcelo T. de Alvear 636 piso 9º
Ciudad Autónoma Buenos Aires
República Argentina

011-4311-7999

Santiago de Chile, 14 de Mayo de 2026

Señores
Superintendencia de Telecomunicaciones
Costa Rica

De nuestra consideración:

El propósito de esta carta es acreditar que el Comité Representativo de la Portabilidad Numérica de Chile adjudicó con fecha 5 de agosto de 2011, el 28 de octubre de 2015, el 3 de febrero de 2020 y el 24 de Noviembre del 2025, en sendas licitaciones, como Organismo Administrador de la Portabilidad Numérica para telefonía fija y móvil en nuestro país a la empresa Telcordia Technologies, inc., entidad nacional de Transaction Network Services ("TNS").

Por la presente acreditamos que TNS implementó con éxito el Sistema de Gestión de la Portabilidad basado en su solución TruNumber Clearinghouse de Portabilidad Numérica. La primera fase de la solución pasó a producción el día 5 de diciembre de 2011 para telefonía fija en el Norte de Chile, y luego, a partir del día 16 de enero de 2012, para la telefonía móvil en todo el país. Luego de adjudicada la segunda licitación, el 8 de agosto de 2016 se realizó la migración de los datos a la nueva plataforma de manera exitosa, para posteriormente dar inicio a la portabilidad completa el 5 de septiembre de 2016, luego, el 26 de octubre de 2020 se puso en marcha el tercer ciclo de operación del OAP y este 4 de junio del 2026 se iniciará la operación del cuarto ciclo. Estos hitos se cumplieron según lo establecido en las distintas bases de la licitación adjudicadas por este Comité.

Actualmente, el Sistema de Gestión de la Portabilidad Numérica de Telcordia ha gestionado satisfactoriamente hasta la fecha, al cierre del mes de abril del 2026 la portación de más 43,1 millones de números telefónicos fijos, móviles, voz sobre IP y rural en todo el territorio nacional, procesando más de 250 millones de transacciones, prestando sus servicios a 112 operadores de servicios de telefonía, que a su vez atienden a un universo aproximado de 31 millones de suscriptores telefónicos. De acuerdo con la

regulación aplicable en la materia en Chile, el método de portabilidad implementado es All Call Query ("ACQ"). Además, TNS, en su plataforma de portabilidad numérica para Chile administra la Base de Datos de IMEI Bloqueados y la Base de Datos de Números de Emergencia para toda la industria de Telefonía de Chile.

El objeto de los servicios proporcionados por TNS incluye el diseño, implementación, operación, seguridad, mantenimiento, e integridad de la Base de Datos de Portabilidad Numérica. Estos servicios han sido brindados de manera ininterrumpida hasta la fecha, y han estado en operación continua desde su introducción el día 05 de diciembre de 2011.

Atentamente,

Powered by  Firma electrónica avanzada
DANIEL ENRIQUE
GUROVICH CAMHI
2026.05.22 11:06:27 -0400

Daniel Gurovich

Secretario Ejecutivo

Comité Representativo de Portabilidad Numérica de Chile

dgurovich@gya.cl



13 May 2026
166A Kifissias Avenue & Sofokleous Str.
15126 Marousi, Athens,
Greece

Attention: To whom it may concern.

Dear Sir or Madam,

Subject: Reference Letter for iconectiv, LLC

I, Angelos Noulas, General Manager and CTO of the company, Nevapark, herewith certify that iconectiv, LLC ("iconectiv"), serves as the solution and support provider for the Number Portability Clearinghouse ("NPC") in the Greece.

iconectiv and Nevapark, as system integrator, entered into a contract on **17th July 2003** for iconectiv (then called Telcordia) to provide the solution for mobile and fixed number portability (MNP & FNP) in Greece. This letter aims to certify that iconectiv has successfully implemented the MNP and FNP and the solution became operational on **1st April 2004**.

Since **1st April 2004** and until the end of **April 2026**, the number of total fixed and mobile successfully serviced by the iconectiv FNP and MNP solution has reached **18.8 million** ports, serving **58** fixed and mobile network operators and roughly **10.1 million** fixed and mobile subscribers. The average mobile ports per month are around **65,000**.

The iconectiv number portability solution, has been in continuous operation since its introduction, and while it has undergone software upgrades and hardware replacement for almost two (2) decades, it was never offline during such tasks, due to careful planning and meticulous execution.

The services provided by iconectiv include consulting on design, software development, software installation and 3rd level support of the FNP & MNP solution.

Yours faithfully,

For and on behalf of
Nevapark

Angelos Noulas
General Manager and CTO
F: +30 210 94 20 049
M: +30 697 72 77 554
noulas@nevapark.com

www.nevapark.com

1

166A Kifissias Avenue & Sofokleous Str.
15126 Marousi
Athens, Greece



13 de mayo de 2026
166A Kifissias Avenue & Sofokleous Str.
15126 Marousi, Atenas,
Grecia

Atención: A quien corresponda:

De nuestra consideración:

Asunto: Carta de referencia para iconectiv, LLC

Yo, Angelos Noulas, Gerente General y CTO de la compañía Nevapark, certifico por la presente que iconectiv, LLC ("iconectiv") actúa como proveedor de la solución y soporte para el Clearinghouse de Portabilidad Numérica ("NPC") de Grecia.

TNS y Nevapark, como integrador de sistemas, celebraron un contrato el **17 de julio de 2003** para que iconectiv (en ese entonces Telcordia) brindara la solución para la portabilidad numérica fija y móvil (PNF y PNM) en Grecia. La presente carta tiene por objeto certificar que iconectiv implementó la PNM y PNF con éxito; y que la solución inició sus operaciones el **1 de abril de 2004**.

Desde el **1 de abril de 2004** hasta fines de **abril de 2026**, la cantidad total de portaciones fijas y móviles cursadas con éxito por la solución de PNF y PNM de iconectiv alcanzaron **18,8 millones** de portaciones, atendiendo a **58** operadores de redes fijas y móviles; y cerca de **10,1 millones** de suscriptores fijos y móviles. El promedio mensual de portaciones móviles es de aproximadamente **65.000**.

La solución de portabilidad numérica de iconectiv se mantuvo en continua operación desde su introducción, y si bien se realizaron actualizaciones de software y reemplazos de hardware durante las últimas dos (2) décadas, nunca estuvo offline durante esas tareas, gracias a una planificación cuidadosa y una ejecución metódica.

Los servicios prestados por iconectiv incluyen consultoría sobre diseño, desarrollo de software, instalación de software y soporte de tercer nivel para la solución de PNF y MNP.

Atentamente.

En nombre y representación de
Nevapark

Angelos Noulas
Gerente General y CTO
F: +30 210 94 20 049
M: +30 697 72 77 554 noulas@nevapark.com

www.nevapark.com

1

166A Kifissias Avenue & Sofokleous Str.
15126 Marousi
Atenas, Grecia

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título



5 September 2025

Building 25, 5 Bauhinia Street
Highveld
Centurion
South Africa
0081

Attention: To whom it may concern.

Dear Sir or Madam,

Subject: Reference Letter for iconectiv, LLC.

I, Suraj Ramlall, General Manager and CTO of the company, SGT Solutions (Pty) Ltd, ("SGTS"), herewith certify that iconectiv, LLC ("iconectiv"), serves as the solution and support provider for the Number Portability Clearinghouse Central Reference Database ("CRDB") in the Republic of South Africa.

iconectiv and SGT, as system integrator, entered into a contract on 10 April 2006 for iconectiv (then called Telcordia) to provide the solution for the CRDB for mobile number portability (MNP) in South Africa. This letter aims to certify that iconectiv has successfully implemented the CRDB and the solution became operational on 10 November 2006.

Since November 2006 and until the end of August 2025, the number of mobile ports successfully serviced by the iconectiv CRDB has reached 14 575 922 ports, serving 5 mobile network operators and roughly 125 million mobile subscribers. The average mobile ports per month are around 65 071.

The iconectiv number portability solution, CRDB, has been in continuous operation since its introduction, and while it has undergone software upgrades and hardware replacement for almost two (2) decades, it was never offline during such tasks, due to careful planning and meticulous execution.

The services provided by iconectiv include consulting on design, software development, software installation and 3rd level support of the CRDB solution. In accordance with the regulation in South Africa, the mode of portability implemented by iconectiv is All Call Query ("ACQ").

Yours faithfully,

For and on behalf of
SGT Solutions (Pty) Ltd

Suraj Ramlall
General Manager
SGT Solutions (Pty) Ltd
Work: +27 12 672 8000
Mobile: +27 82 565 6068
e-mail: sramlall@sgtsolutions.co.za

Digitally signed by sramlall@sgtsolutions.co.za
DN: cn=sramlall@sgtsolutions.co.za
Reason: I am approving this document
Location: Centurion
Date: 2025-09-05 15:56+02:00

| | | | | |
|--|---|--|--|---|
| SGT Solutions (Pty) Ltd Reg No 1963/006462/07 | Directors AB Amod, Dr AV Scholtz W Mc Lachlan, AJ Mekan | T: +27 (0) 12 672 8000 F: +27 (0) 12 672 8301 sgtinfo@sgtsolutions.co.za www.sgtsolutions.co.za | Business Address BLD 25 5 Bauhinia Street Highveld, Centurion 0169 | Postal Address PO Box 11212 Swartkops 0051 |
|--|---|--|--|---|



SOLUTIONS

5 de setiembre de 2025

Building 25, 5 Bauhinia Street
Highveld
Centurion
Sudáfrica
0081

Atención: A quien corresponda:
De nuestra consideración:

Asunto: Carta de Referencia para iconectiv, LLC

Yo, Suraj Ramlall, Gerente General y CTO de la compañía SGT Solutions (Pty) Ltd ("SGTS"), por la presente certifico que iconectiv, LLC ("iconectiv") actúa como proveedor de soluciones y soporte para la Base de Datos Central de Referencia ("CRDB") del Clearinghouse de Portabilidad Numérica en la República de Sudáfrica.

iconectiv y SGT, como integrador de sistemas, celebraron un contrato el 10 de abril de 2006 para que iconectiv (en ese entonces Telcordia) brindara la solución para la CRDB de portabilidad numérica móvil (PNM) de Sudáfrica. La presente carta tiene por objeto certificar que iconectiv implementó la CRDB con éxito y que la solución inició sus operaciones el 10 de noviembre de 2006.

Desde noviembre de 2006 hasta fines de agosto de 2025, la cantidad de portaciones móviles atendidas con éxito a través de la CRDB de iconectiv alcanzaron 14.575.922, atendiendo a 5 operadores de redes móviles y casi 125 millones de suscriptores móviles. El promedio mensual de portaciones móviles es de aproximadamente 65.071.

La solución de portabilidad numérica de iconectiv, CRDB, se mantuvo en continua operación desde su introducción, y si bien se realizaron actualizaciones de software y reemplazos de hardware durante las dos (2) últimas décadas, nunca estuvo offline durante esas tareas, gracias a una planificación cuidadosa y una ejecución meticulosa.

Los servicios prestados por iconectiv incluyen consultoría sobre diseño, desarrollo de software, instalación de software y soporte de tercer nivel para la solución CRDB. De acuerdo con la regulación de Sudáfrica, el método de portabilidad implementado por iconectiv es All Call Query ("ACQ").

Atentamente.

En nombre y representación de
SGT Solutions (Pty) Ltd


Suraj Ramlall
Gerente General
SGT Solutions (Pty) Ltd
Teléfono comercial: +27 12 672 8000
Móvil: +27 82 565 6068
Correo electrónico: sramlall@sgtsolutions.co.za

Firmado digitalmente por sramlall@sgtsolutions.co.za
DN: cn=sramlall@sgtsolutions.co.za
Motivo: Aprobación de documento
Ubicación: Centurion
Fecha: 2025-09-05 15:56:02.00

Directores:
AB Amod, Dr AV Scholtz W Mc Lachlan, AJ Makan

SGT Solutions (Pty) Ltd
Reg. N° 1963/008462/07

T: +27 (0) 12 672 8000
F: +27 (0) 12 672 8301
sgtinfo@sgtsolutions.co.za
www.sgtsolutions.co.za

Domicilio comercial
BLD 25 5 Bauhinia Street
Highveld, Centurion
0169

Código postal
PO Box 11212
Swarthkops
0061

This is a true and complete translation into Spanish of the source document written in English which I had before me. The translation is digitally signed by María Laura Rosenzwaig, Certified Translator, Commission 4091, VOLUME 12, FOLIO 403. In Buenos Aires, on this 18th day of September, 2025. -----

Lo que antecede es traducción fiel y completa al idioma español del documento fuente redactado en idioma inglés que tuve a la vista y al cual me remito. La traducción está firmada digitalmente por María Laura Rosenzwaig, Traductora Pública, Matrícula 4091, TOMO 12, FOLIO 403. En Buenos Aires, a los 18 días de septiembre de 2025.-

María Laura Rosenzwaig

Firmado digitalmente por ROSENZWAIG María Laura
DN: C=AR, S=Ciudad Autónoma de Buenos Aires, OU=Subsecretaría de Tecnologías de Gestión, OU=Secretaría de Gestión Pública, OU=Oficina Nacional de Tecnologías de Información, O=Jefatura de Gabinete de Ministros, SERIALNUMBER=CUIT 30680604572, CN=Autoridad Certificante de Firma Digital
Razon: María Laura Rosenzwaig - Traductora Pública de Inglés - Certified English Translator
Fecha: jueves, 18 de septiembre de 2025 17:26:36

Anexo 3 – Cartas de Referencia de Migración



PERÚ

Presidencia
del Consejo de Ministros

Organismo Supervisor
de Inversión Privada en
Telecomunicaciones



Decenio de la Igualdad de Oportunidades para Mujeres y Hombres
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho".

Lima, 22 de enero de 2024

C. 00045-GG/2024

SEÑORA
ANGIE FORD
SR. ACCOUNT DIRECTOR - LATAM | ICONECTIV
ICONECTIV PERÚ S.A.C.
100 SOMERSET CORPORATE PLACE BLVD
BRIDGEWATER, NEW JERSEY 08807
UNITED STATES OF AMERICA.-

Ref.: Su solicitud registrada el 12 de enero de 2024

De mi consideración:

Me dirijo a usted con relación a la comunicación de la referencia, mediante la cual su representada solicitó la emisión de una constancia respecto a la prestación de servicios de Administrador de la Base de Datos Centralizada Principal de Portabilidad Numérica de los Servicios Públicos de Telefonía Fija y Móvil del Perú, realizada en el periodo 2014 - 2019.

Al respecto, sírvase encontrar adjunto a la presente lo solicitado, para los fines que considere pertinente.

Sin otro particular, quedo de usted.

Atentamente,

Firmado digitalmente por:
CIFUENTES
CASTAÑEDA Sergio
Enrique FAU
20216072155 soft

SERGIO ENRIQUE CIFUENTES CASTAÑEDA
GERENTE GENERAL
GERENCIA GENERAL

Adj. Lo indicado.



**BICENTENARIO
DEL PERÚ
2021 - 2024**

CALLE DE LA PROSA 136 – SA
MESA DE PARTES VIRTUAL:

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Organismo Supervisor de la Inversión Privada en Telecomunicaciones, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web:
url: <https://serviciosweb.osiptel.gob.pe/ValidarDocumento> Clave: 20230637TSY2

<https://serviciosweb.osiptel.gob.pe/MesaPartesVirtual/login.aspx>



www.osiptel.gob.pe

CONFIDENCIAL – ACCESO RESTRINGIDO.
Ver restricciones de confidencialidad en la página de título

Don **SERGIO ENRIQUE CIFUENTES CASTAÑEDA**, con DNI número 10134272, número de teléfono +511 2251313, en calidad de Gerente General del Organismo Supervisor de Inversión Privada en Telecomunicaciones (en lo sucesivo, Osiptel), y con domicilio a efectos de notificaciones en la República del Perú en la Calle de la Prosa N° 136 – San Borja, Lima;

CERTIFICA

PRIMERO.- Que, con fecha 3 de enero de 2014, se instaló el Comité de Portabilidad, conforme a lo indicado en el Reglamento de Portabilidad Numérica en el Servicio Público Móvil y el Servicio de Telefonía Fija, aprobado por Resolución de Consejo Directivo N° 166-2013-CD/OSIPTEL, para la selección de la entidad que administrará la respectiva base de datos de portabilidad numérica.

La entidad administradora seleccionada tiene por función el diseño, implementación, operación, seguridad, mantenimiento y cautela de la integridad de la Base de Datos para la implementación de la portabilidad numérica en el modelo *All Call Query* tanto para la telefonía fija como móvil.

SEGUNDO.- Que, a partir del 17 de marzo de 2014, Iconectiv Perú S.A.C., subsidiaria de Telcordia Technologies, Inc en su calidad de entidad administradora seleccionada, brindó servicios como Administrador de la Base de Datos Centralizada Principal de Portabilidad Numérica hasta el 31 de marzo de 2019, fecha en que expiró su contrato.

TERCERO.- Que, Iconectiv Perú S.A.C. puso en operación la mencionada Base de Datos el 16 de julio de 2014, permitiendo de este modo el cumplimiento de las fechas y disposiciones definidas por el Estado Peruano para el relanzamiento de la portabilidad numérica en el servicio público móvil (16 de julio de 2014), y el inicio de la portabilidad numérica en el servicio de telefonía fija (26 de julio de 2014); en ese sentido, Iconectiv Perú S.A.C. cumplió con la implementación en los tiempos requeridos establecidos en las bases del concurso.

Asimismo, la base de datos desarrollada por Iconectiv Perú S.A.C. para el sistema de portabilidad, implicó el cambio de procesos manuales por validaciones en línea (tiempo real), reduciendo el plazo de portación de 7 días a 24 horas. Así también, la referida empresa efectuó la migración de la integridad de los datos de portabilidad numérica generados durante el período comprendido entre enero de 2010 a junio de 2014¹, hacia la Base de Datos desarrollada con el nuevo sistema.

CUARTO.- Que, durante el periodo en que Iconectiv Perú S.A.C. brindó sus servicios, la Base de Datos antes referida ha atendido un total acumulado de 16 668 947 portaciones del servicio móvil y 163 552 portaciones del servicio fijo.

Se extiende el presente documento a solicitud de la parte interesada para los fines que estime pertinente.

En Lima, a los 18 días de enero de 2024.


SERGIO ENRIQUE CIFUENTES CASTAÑEDA
GERENTE GENERAL

¹ Base de datos que fue administrada por el Consorcio C.E.I., integrado por Informática El Corte Inglés S.A., Everis Spain S.L. e Indra Perú S.A.



September 12, 2025

Attention: To whom it may concern

Dear Sir or Madam,

Subject: Reference Letter for iconectiv, LLC

I, Teresa Patton, NAPM LLC Co-Chair, on behalf of The North American Portability Management LLC (NAPM LLC), certify that iconectiv, LLC (iconectiv), serves as the Local Number Portability Administrator (LNPA) in all seven United States service regions. iconectiv manages the nation's Number Portability Administration Center (NPAC) on behalf of The North American Portability Management LLC (NAPM LLC), which provides oversight of the nation's number portability system under the authority of the Federal Communications Commission (FCC).

NAPM LLC entered into a contract with iconectiv in August 2016. Final transition was completed in May 2018. The transition to iconectiv as the LNPA involved thousands of stakeholders across government and the private sector, and the multi-year project successfully completed on schedule and as planned.

As the Local Number Portability Administrator (LNPA), iconectiv maintains the database of ported phone numbers and handles hundreds of thousands of daily porting transactions in the U.S. The U.S. Number Portability Administration Center (NPAC) contains about 1 billion phone numbers for roughly 1,600 service providers and allows consumers to keep their phone numbers when switching carriers, promoting competition and consumer choice. While exact daily or monthly statistical reports from the NPAC are not publicly available, the high volume of transactions underscores the system's vital role in telecommunications.

The NPAC has been in continuous operation since its introduction. Through careful planning and meticulous execution, software and hardware upgrades are done during industry scheduled maintenance windows so as to maintain the high availability of the system.

The services provided by iconectiv including consulting on design, software development, security compliance and customer service support.

Sincerely,

Teresa Patton



12 de septiembre de 2025

Atención: A quien corresponda:

De nuestra consideración:

Asunto: Carta de referencia para iconectiv, LLC

Yo, Teresa Patton, Presidenta Conjunta de NAPM LLC, en nombre de The North American Portability Management LLC (NAPM LLC), certifico que iconectiv, LLC (iconectiv), actúa como Administrador de Portabilidad Numérica Local (LNPA, en inglés) en todas las siete regiones de servicio en Estados Unidos. iconectiv gestiona el Centro de Administración de Portabilidad Numérica (NPAC, en inglés) de la nación en nombre de The North American Portability Management LLC (NAPM LLC), quien supervisa el sistema de portabilidad numérica de la nación, bajo la autoridad de la Comisión Federal de Comunicaciones (FCC, en inglés).

NAPM LLC celebró un contrato con iconectiv en agosto de 2016. La transición final se completó en mayo de 2018. La transición hacia iconectiv en calidad de Administrador de Portabilidad Numérica Local involucró a miles de interesados de todo el gobierno y el sector privado; y el proyecto plurianual se completó con éxito, conforme al cronograma y tal como se planificó.

Como Administrador de Portabilidad Numérica Local (LNPA), iconectiv mantiene la base de datos de números portados y maneja cientos de miles de transacciones de portabilidad a diario en el Centro de Portabilidad Numérica Local (NPAC) de Estados Unidos, que contiene cerca de mil millones de números telefónicos para casi 1.600 proveedores de servicio; y permite que los consumidores mantengan sus números telefónicos cuando cambian de operadora, lo cual promueve la competencia y que el cliente pueda elegir. Si bien los informes estadísticos diarios o mensuales exactos de NPAC no están públicamente disponibles, el alto volumen de transacciones pone de relieve el rol fundamental del sistema en las telecomunicaciones.

NPAC se encuentra en funcionamiento continuo desde su introducción. A través de una planificación cuidadosa y una ejecución meticulosa, las actualizaciones de software y hardware se realizan durante las ventanas de mantenimiento programadas de la industria, a fin de mantener una alta disponibilidad del sistema.

Los servicios prestados por iconectiv incluyen consultoría sobre diseño, desarrollo de software, cumplimiento regulatorio y soporte de atención al cliente.

Atentamente.

Teresa Patton



This is a true and complete translation into Spanish of the source document written in English which I had before me. The translation is digitally signed by María Laura Rosenzwaig, Certified Translator, Commission 4091, VOLUME 12, FOLIO 403. In Buenos Aires, on this 12th day of September, 2025.

Lo que antecede es traducción fiel y completa al idioma español del documento fuente redactado en idioma inglés que tuve a la vista y al cual me remito. La traducción está firmada digitalmente por María Laura Rosenzwaig, Traductora Pública, Matrícula 4091, TOMO 12, FOLIO 403. En Buenos Aires, a los 12 días de septiembre de 2025.-

María Laura Rosenzwaig

Firmado digitalmente por ROSENZWAIG María Laura
DN: C=AR, S=Ciudad Autónoma de Buenos Aires, OU=Subsecretaría de Tecnologías de Gestión, OU=Secretaría de Gestión Pública, OU=Oficina Nacional de Tecnologías de Información, O=Jefatura de Gabinete de Ministros, SERIALNUMBER=CUIT 30680604572, CN=Autoridad Certificante de Firma Digital
Razon: María Laura Rosenzwaig - Traductora Pública de Inglés -
Certified English Translator
Fecha: viernes, 12 de septiembre de 2025 11:42:16

Anexo 4 – Declaración jurada de que el oferente no tiene vínculos económicos, propiedad o control por parte de algún operador/proveedor de telecomunicaciones de Costa Rica.

DECLARACIÓN JURADA CLÁUSULA 1.5.17.5.

El suscrito, James T. McLaughlin, mayor de edad, casada, abogada, Estado Unidos, con domicilio en 4411 Eastwood Court, Fairfax, Virginia, 22032 USA, portador(a) del pasaporte número 596236761, en mi condición de General Counsel de **TRANSACTION NETWORK SERVICES, INC.** ("la Compañía), sociedad constituida y existente de conformidad con las leyes del Estado de Delaware, Estados Unidos, con domicilio social en The Corporation Trust Company, 1209 Orange Street, Wilmington, Condado de New Castle, Delaware 19801, Estados Unidos, compañía oferente dentro del procedimiento de licitación promovido por la Superintendencia de Telecomunicaciones (SUTEL) denominado "**PORTABILIDAD NUMÉRICA PARA LA CONTINUIDAD, EL DESARROLLO Y LA OPERACIÓN DEL SISTEMA INTEGRADO DE PORTABILIDAD NUMÉRICA**", con facultades suficientes para este acto y apercibido(a) de la gravedad y de las consecuencias legales que me acarrearía el delito de perjurio y falso testimonio, DECLARO BAJO LA FE DEL JURAMENTO:

ÚNICO: Que la compañía **TRANSACTION NETWORK SERVICES, INC.** no tiene vínculos económicos, de propiedad o de control, directos ni indirectos, con ningún operador o proveedor de telecomunicaciones en Costa Rica, de conformidad con lo establecido en la cláusula 1.5.17.5. del pliego de condiciones de la licitación de referencia. Es todo.

En fe de lo anterior, firmo en London, United Kingdom, el 28 de Mayo de 2026.

x 

James T. McLaughlin

General Counsel and Secretary, Transaction Network Services, Inc.