

inetum.™



Propuesta Técnica

**Implementación de la
Portabilidad Numérica
en Costa Rica**





Índice

Definiciones y acrónimos	6
1 Introducción	8
1.1 Resumen Ejecutivo	10
1.2 ¿Por qué Inetum?	11
1.3 Referencias de Portabilidad por país.....	12
2 Requerimientos funcionales	35
2.1 Proceso 00 – Proceso de generación y envío de NIP	36
2.1.1 Descripción del proceso.....	36
2.1.2 Interacción de mensajes	38
2.1.3 Diagramas de actividad	40
2.2 Proceso 02 – Proceso de consultas de prevalidación	43
2.2.1 Descripción del proceso.....	43
2.2.2 Interacción de mensajes	44
2.2.3 Diagramas de actividad	50
2.3 Proceso 01 – Proceso de portabilidad.....	53
2.3.1 Descripción del proceso.....	53
2.3.2 Interacción de mensajes	54
2.3.3 Diagramas de actividad	60
2.4 Proceso 03 – Proceso de cancelación de portabilidad	62
2.4.1 Descripción del proceso.....	62
2.4.2 Interacción de mensajes	62
2.4.3 Diagramas de actividad	63
2.5 Proceso 04 – Proceso de repatriación.....	66
2.5.1 Descripción del proceso.....	66
2.5.2 Interacción de mensajes	66
2.5.3 Diagramas de actividad	67
2.6 Proceso 05 – Proceso de sincronización con la ERPN	68
2.6.1 Descripción del proceso.....	68
2.6.2 Interacción de mensajes	69
2.6.3 Diagramas de actividad	70



2.7	Subproceso de error detectado por la ERPN	70
2.7.1	Descripción del proceso.....	70
2.7.2	Interacción de mensajes	71
2.7.3	Diagramas de actividad	71
3	Requerimientos No-Funcionales	72
3.1	Alta Disponibilidad.....	72
3.2	Disaster Recovery Service.....	73
3.2.1	Capa de datos: Oracle Data Guard	73
3.2.2	Capa de aplicación: Oracle Kubernetes Engine DR	74
3.2.3	Operación conjunta Data Guard + OKE DR.....	74
3.3	Escalabilidad.....	75
3.3.1	Escalabilidad horizontal basada en microservicios y OKE	75
3.3.2	Escalabilidad de la infraestructura: OCI Compute Worker Nodes.....	75
3.3.3	Escalabilidad vertical controlada	76
3.3.4	Escalabilidad integrada con el DRS.....	76
3.4	Flexibilidad	76
4	Infraestructura.....	77
4.1	Alojamiento de las aplicaciones	77
4.1.1	Características Data Centers de Oracle Cloud Infrastructure	78
4.2	Comunicaciones.....	81
4.2.1	Canales de comunicación.....	81
4.2.2	Canal de comunicación para integración	82
4.2.3	Protocolos de comunicación	84
4.3	Arquitectura general de la solución	89
5	Metodología de Implementación y Aceptación.....	91
5.1	Propuesta general de implementación.....	91
5.1.1	Metodología de Implementación	92
5.1.2	Estrategia de pruebas	94
5.1.3	Tipos de pruebas	95
5.1.4	Severidad de los errores durante las pruebas	96
5.1.5	Gestión de incidencias durante el período de pruebas.....	97
5.2	Aceptación del Sistema	97



5.2.1	Pruebas de Desarrollo.....	98
5.2.2	Aceptación	98
5.2.3	Aceptaciones Posteriores (Incorporación de nuevos Operadores)	99
5.2.4	Pruebas con terceros	99
5.3	Capacitación.....	99
5.4	Equipo de trabajo.....	101
6	Requerimientos de Operación	105
6.1	Seguridad	105
6.1.1	Descripción General	105
6.1.2	Política de Seguridad de la Información	106
6.1.3	Aspectos organizativos para la seguridad	107
6.1.4	Seguridad ligada a los recursos humanos	107
6.1.5	Gestión de Comunicaciones y operaciones.....	108
6.1.6	Adquisición, desarrollo y mantenimiento de sistemas de información	109
6.1.7	Gestión de incidentes de seguridad.....	110
6.1.8	Gestión de continuidad del Negocio.....	112
6.1.9	Conformidad o Cumplimiento.....	112
6.2	Respaldo y recuperación de la información.....	113
6.3	Actualización y mantenimiento del Sistema	113
6.3.1	Actualización y Mantenimiento del HW.....	114
6.3.2	Actualización y Mantenimiento del SW	115
6.3.3	Actualización y Mantenimiento de Portaflow	117
6.3.4	Procedimiento de actuación ante actualizaciones y mantenimientos..	118
6.4	Soporte Técnico.....	119
6.5	Gestión de incidencias de la operación.....	123
6.5.1	Definición de incidente.....	123
6.5.2	Base de Datos Información de contactos.....	123
6.5.3	Herramienta de gestión de incidentes	124
6.5.4	Definición del Proceso de Gestión de Incidentes.....	133
6.5.5	Niveles de Severidad.....	141
6.5.6	Acuerdo de Niveles de Servicio (SLA) de la mesa de ayuda	142
6.5.7	Protocolo de Emergencia ante caída prolongada del sistema de un	



Operador Donante.....	142
7 Biometría.....	142
7.1 Introducción	142
7.2 Proceso de validación biométrica	143
7.3 Prueba de vida	148
7.4 Fotografía	150
7.5 Consentimiento	151
7.6 OCR.....	152
7.7 Verificación de legitimidad.....	152



Definiciones y acrónimos

Se presentan los siguientes conceptos y acrónimos:

- **All Call Query (ACQ):** esquema de enrutamiento en el que, de previo al establecimiento de una comunicación, el proveedor que la origina debe consultar una base de datos operativa y obtener información que le permita enrutarla al proveedor destinatario.
- **Base de Datos Administrativa (NP-DB):** Base de datos administrada por la ERPN, que contiene como mínimo la información necesaria para el enrutamiento de comunicaciones hacia números portados, y que se actualiza de conformidad con el Proceso de Portación.
- **Base de Datos Operativa (BDO):** base de datos administrada por un determinado operador o proveedor de servicios de telecomunicaciones, que contiene la información necesaria para el enrutamiento de las comunicaciones hacia números portados, la cual es obtenida y actualizada desde la NP-DB.
- **CTPN (Comité Técnico de Portabilidad):** órgano permanente de carácter consultivo de la Sutel y conformado por todos los operadores y proveedores de servicios de telecomunicaciones móviles a los cuales se les han asignado recursos de numeración, los cuales están obligados a implementar la Portabilidad Numérica Móvil en Costa Rica.
- **Datacenter:** centro de datos.
- **Entidad de Referencia de Portabilidad Numérica (ERPN):** empresa que tendrá a su cargo la implementación, operación, mantenimiento, continuidad, mejoras y administración de todo el SIPN.
- **GAA:** Grupo de Apoyo Administrativo.
- **GAT:** Grupo de Apoyo Técnico.
- **GUI:** según sus siglas en inglés, *Graphical User Interface*, interfaz gráfica de usuario.
- **Interfaz Estándar:** es aquella que hace uso de algún protocolo de la industria de telecomunicaciones reconocido internacionalmente, de manera que permita el intercambio entre dos o más sistemas o componentes de hardware.
- **IVR:** según sus siglas en inglés, *Interactive Voice Recording*, sistema de atención interactivo para llamadas de voz.



- **LDI:** Larga Distancia Internacional.
- **MSISDN:** según sus siglas en inglés, *Mobile Station Integrated Services Digital Network*.
- **NIP:** número único asignado por la ERPN a un número telefónico, que permite la asociación entre el número telefónico a portarse y el solicitante. El NIP de portación podrá ser de tipo individual o grupal en el caso de solicitudes múltiples de portación.
- **Oferente:** empresa interesada en participar del presente proceso de selección, con el propósito de convertirse en la ERPN en Costa Rica.
- **OMV:** Operador de red Móvil Virtual.
- **Operador/Proveedor Donante:** operador o proveedor de redes y servicios de telecomunicaciones desde el cual es portado un determinado número como resultado del proceso de portación.
- **Operador/Proveedor Receptor:** operador o proveedor de servicios de telecomunicaciones hacia el cual es portado un determinado número como resultado del proceso de cambio.
- **Operador/Proveedor:** persona física o jurídica, pública o privada, que explota redes de telecomunicaciones móviles con la debida concesión o autorización, las cuales podrán prestar servicios de telecomunicaciones disponibles al público en general.
- **OR:** según sus siglas en inglés, *Onward Routing*, esquema de enrutamiento mediante el cual el proveedor que origina una llamada en su red siempre la enruta hacia la red del proveedor asignatario del número de destino, y en el caso que la llamada tenga como destino un abonado de una red diferente a la de dicho proveedor, éste último deberá realizar la consulta a la BDO para determinar la información de enrutamiento apropiada y encaminarla en forma directa hacia la red correcta de destino.
- **Portabilidad Numérica:** posibilidad del usuario de conservar su número telefónico sin deterioro de la calidad y confiabilidad, en el evento que cambie de operador o proveedor de redes y servicios de telecomunicaciones.
- **RN:** según sus siglas en inglés, *Routing Number*, número de enrutamiento de red.
- **RPO:** según sus siglas en inglés, *Recovery Point Objective*, métrica crítica de continuidad de negocio que define la cantidad máxima de pérdida de datos aceptable después de una interrupción.



- **RTO:** según sus siglas en inglés, *Recovery Time Objective*, métrica crítica de continuidad de negocio que define la velocidad o tiempo de recuperación del sistema.
- **SIPN:** Sistema Integral de Portabilidad Numérica.
- **SLA:** según sus siglas en inglés, *Service Level Agreement*, Acuerdo de Nivel de Servicio.
- **SMSC:** según sus siglas en inglés, *Short Message Service Center*, Centro de Servicios de Mensajería Corta.
- **Sutel:** Superintendencia de Telecomunicaciones.
- **Ventana de Cambio:** período definido para realizar las portaciones programadas, durante el cual los números a portarse se desactivan en el operador o proveedor donante y se activan en el operador o proveedor receptor.

1 Introducción

El objetivo del presente documento es dar respuesta técnicamente al proceso de selección a la Entidad de Referencia de Portabilidad Numérica (ERPN), para la continuidad, implementación, operación, mantenimiento, mejoras y administración del Sistema Integral de Portabilidad Numérica (SIPN) en Costa Rica. Lo anterior con el fin de asegurar el cumplimiento del derecho de los usuarios finales de conservar su número telefónico tal y como lo dispone la Ley General de Telecomunicaciones, Ley Número 8642, en su artículo 45 inciso 17): *“17) Mantener los números de teléfono sin menoscabar la calidad, confiabilidad o conveniencia cuando cambie entre proveedores de servicio similares”*.

Adicionalmente el artículo 89 del Reglamento sobre el régimen de Protección al Usuario Final (RPUF) establece que *“Los operadores/proveedores que cuenten con recurso numérico del Plan Nacional de Numeración asignado por la Sutel, se encuentran en la obligación de garantizar la implementación, operación y administración de la Portabilidad Numérica, mediante el uso del esquema de consulta de cada llamada, para el tráfico telefónico local y el enrutamiento indirecto, para las llamadas internacionales, y deben asegurar el correcto funcionamiento de ambos esquemas”* y declara que el incumplimiento de esta habilitación técnica podrá considerarse como una infracción tipificada en la Ley General de Telecomunicaciones, Ley Número 8642.

En referencia a la portabilidad numérica para servicios de telefonía móvil, se deben considerar lo dispuesto en las normativas regulatorias aplicables a portabilidad numérica emitidas por el Consejo de la Sutel definidas mediante la resolución RCS-319-2014, RCS-



027-2021 y acuerdos 029-017-2023 y 021-067-2024.

En virtud de dar respuesta a las “**ESPECIFICACIONES Y REQUISITOS PARA LA SELECCIÓN DE LA ENTIDAD DE REFERENCIA DE PORTABILIDAD NUMÉRICA PARA LA CONTINUIDAD, EL DESARROLLO Y LA OPERACIÓN DEL SISTEMA INTEGRADO DE PORTABILIDAD NUMÉRICA**”, INETUM como Administrador del ERPN se sujetará, además de lo establecido en el contrato a suscribir, a lo siguiente:

- Diseñar, implementar, operar y mantener la Entidad de Referencia de Portabilidad, así como prestar el servicio de administración de esta, bajo los términos y condiciones solicitadas en las Bases y la normativa aplicable.
- Establecer y/o desarrollar todas las medidas que sean necesarias para permitir que la Entidad de Referencia de Portabilidad quede completamente instalada, opere y se conecte a las distintas redes, plataformas y sistemas actualmente en funcionamiento del operador, en condiciones operativas y técnicas (parámetros de calidad de servicio y seguridad, entre otros) establecidos para cumplir con las presentes Bases del Concurso y la normativa aplicable.
- Asegurar que el funcionamiento de la Entidad de Referencia de Portabilidad sea interoperable con todos los operadores de telefonía, y se encuentre permanente y continuamente disponible, de manera segura, flexible para modificaciones y actualizaciones, escalable, con capacidad para registros de incidencia, acciones y procesos simultáneos, interfaces y protocolos abiertos.
- Dimensionar la Entidad de Referencia de Portabilidad, en modo tal que asegure el manejo y atención oportuna de todas las solicitudes de portabilidad recibidas diariamente, en forma simultánea, según lo establecido en las Bases del Concurso y la normativa aplicable.
- Cumplir en todo momento con la Resolución de Portabilidad y las Especificaciones Operativas para la Implementación de la Portabilidad Numérica.
- Mantener informado al Comité de Portabilidad, los Prestadores de Servicios de Telecomunicaciones y a la SUTEL de los hechos y eventos que por su impacto en el servicio resulten relevantes.

INETUM cuenta con un sistema, denominado **Portaflow 3.0**, que da cumplimiento a todos requerimientos funcionales solicitados en las Bases del Concurso, tal como se irá describiendo a lo largo del documento.

1.1 Resumen Ejecutivo



INETUM España SA es una compañía de servicios ágil que proporciona servicios y soluciones digitales y un grupo global que ayuda a compañías e instituciones a aprovechar al máximo el flow digital. En un contexto de continuo movimiento, en el que las necesidades y los usos se reinventan constantemente, el grupo INETUM se compromete con todos esos actores a innovar, seguir adaptándose y mantenerse a la vanguardia. Con su perfil multi-experto, INETUM ofrece a sus clientes una combinación única de proximidad, organización sectorial y soluciones de calidad industrial.

Presente en más de 26 países, el Grupo tiene cerca de 27.000 empleados y en 2024 generó unos ingresos de 2.400 millones de euros.

Nuestra estrategia se basa en 3 pilares

- Proximidad - Confianza - Agilidad
- Industrialización - Automatización
- Innovación - Soluciones de negocio

Un Líder regional

Global & Local: Top 5 en casi todos nuestros países

Multi-especialista: Soluciones de negocio vertical para apoyar la estrategia de nuestros clientes

Innovación: Impulsor para potenciar nuestra propuesta de valor.



Soluciones de negocio

Digital Customer Experience | CRM – ECOMMERCE – CUSTOMER PORTALS

Finance & Operation Performance | ERP –SCM –BILLING – EPM – ECM – PLM

Digital Employee Experience | DIGITAL WORKPLACE – HCM –PAYROLL –DIGITAL CULTURE

Soluciones de software

Sector Público | Seguros | Salud | Tiempo y Actividades | Gestión Documental | Supply Chain
| Detección del fraude

Partners estratégicos

SAP, Microsoft, Oracle, Salesforce

AWS, IBM, Sage, HRAccess

PTC, Siemens, Dassault

Certificaciones

ISO 9001 | ISO 14001 | CMMI v1.3 DEV -3 | ISO 20000-1 | ISO 27001

1.2 ¿Por qué Inetum?

Inetum presenta al Comité de Portabilidad de Costa Rica, a los Operadores de Servicios de Telecomunicaciones Móviles y a la SUTEL, la más completa, robusta y experimentada solución de portabilidad numérica en Iberoamérica.

Nuestra experiencia probada permite una rápida implementación y garantiza el éxito de la solución ofrecida, la cual cuenta con más de 26 años de exitosa operación en España, así como otras implementaciones en países como República Dominicana, México, Colombia, Paraguay, Costa Rica, Perú, entre otras, siendo en Europa el primer caso exitoso de portabilidad centralizada, convirtiéndose en un referente tanto dentro de la Unión Europea como a nivel mundial.

La nueva arquitectura probada de la solución es de naturaleza no intrusiva, abierta y apegada a las normativas y estándares de las industrias de software y telefonía, garantizando una cómoda integración con la diversidad de sistemas usados por las prestadoras de servicio (back-end), así como flexibilidad para la escalabilidad futura y adecuación y personalización a necesidades específicas que pudieran surgir en el futuro fuera del marco de lo requerido actualmente.

Nuestra solución, al no ser de carácter intrusivo, no obliga ni condiciona a los Proveedores de Servicios de Telecomunicaciones a realizar ningún tipo de inversión obligada por la implementación de la Base de Datos Centralizada de Portabilidad.

A continuación, desglosamos nuestra propuesta técnica, detallando la arquitectura de hardware, software y comunicaciones, la alta disponibilidad de la plataforma, su seguridad,



escalabilidad y flexibilidad, el plan de transición, implementación y puesta en marcha, el alojamiento de los sistemas, la gestión de incidentes y estructura de soporte, los aspectos de seguridad, así como nuestras referencias en portabilidad y resultados en la Unión Europea.

Considerando que nuestra solución integral supera con creces las necesidades descritas a lo largo de las bases del concurso, nos sentimos con la confianza suficiente de poder ofrecer al Comité de Portabilidad nuestro compromiso para la implantación del SIPN dentro de los requerimientos, producto de nuestra experiencia en proyectos similares en la industria.

1.3 Referencias de Portabilidad por país

País	Referencia
ESPAÑA	
República Dominicana	
Perú	
Brasil	
México	
Colombia	
Panamá	
Argentina	



Chile	
Paraguay	
Costa Rica	
Honduras	
El Salvador	

Sistema Central Portabilidad España

Cliente	Comisión del Mercado de Telecomunicaciones
Proyecto	Portanet
Fecha	Desde el año 1999 hasta la actualidad
Descripción	Implantación del servicio denominado "Portabilidad Numérica en Redes Fijas y Móviles" creando para ello un ente denominado "Entidad de Referencia" la cual gestiona todos los procesos de portabilidad que se presenten. La Portabilidad Numérica consiste en permitir que un abonado telefónico pueda cambiar el servicio telefónico de un Operador a otro y mantener la numeración de su línea telefónica. El proyecto consiste en montar dos arquitecturas una de Producción en Clúster y otra de BRS (ubicadas en distintos centros de procesos de datos) más un desarrollo específico que se centra en un sistema de intercambio de mensajes entre los operadores involucrados en los procesos de portabilidad.
Actividades	<p>Análisis solución portabilidad</p> <p>Diseño, desarrollo e implementación de la solución de portabilidad central en España.</p> <p>Integración con los sistemas de los Operadores y sistemas internos de la Entidad de gestión Técnica</p> <p>Outsourcing. Del proyecto desde 1999 hasta la actualidad y con contrato vigente hasta año 2014.</p>
Resultados /	1.- Se consiguió que el 1 enero de 2000, la portabilidad en



Beneficios	<p>España fuese posible</p> <p>2.- Poner de acuerdo con más de 40 empresas con intereses distintos</p> <p>3.- Integración de los sistemas utilizando la última tecnología del mercado</p> <p>4.- Adaptación a las necesidades de los Operadores y la portabilidad en cada momento</p> <p>Creación de una entidad que administre la base de datos centralizada principal de la solución técnica denominada “All Call Query” – Consulta de Todas las Llamadas – para la portabilidad numérica en los servicios públicos móviles, móviles virtuales (OMVs) y fijos.</p>
Metodologías / Tecnologías	Metodología propia de INETUM y CMMI

Cliente de portabilidad: British Telecom España (BT)

Cliente	British Telecom España
Proyecto	Port@node
Fecha	Desde el año 2003 hasta la actualidad
Descripción	Implantación y evolución del sistema cliente de portabilidad de BT
Actividades	<p>Implantación cliente portabilidad</p> <p>Desarrollo constante de módulos para realizar integraciones con sistemas de información</p> <p>Mantenimientos preventivos, correctivos y evolutivos</p>
Resultados / Beneficios	<p>1.- Permitir a BT cumplir con la obligación de portabilidad.</p> <p>2.- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos</p> <p>3.- Lanzamiento de campañas de forma ágil</p> <p>4.- Cuadros de mando para el seguimiento de las campañas</p> <p>5.- Reducción de incidencias de provisión de red</p>
Metodologías /	Metodología propia de BT y CMMI



Tecnologías	
-------------	--

Cliente de portabilidad: Colt Telecom España

Cliente	Colt Telecom
Proyecto	Port@node
Fecha	Desde el año 2003 hasta la actualidad
Descripción	Implantación y evolución del sistema cliente de portabilidad de Colt Telecom
Actividades	Implantación cliente portabilidad Mantenimientos preventivos, correctivos y evolutivos Provisión de la central NORTEL
Resultados Beneficios	/ 1.- Permitir a Colt cumplir con la obligación de portabilidad. 2.- Reducción de incidencias de provisión de red
Metodologías Tecnologías	/ Metodología propia de Colt Telecom y CMMI

Cliente de portabilidad: France Telecom España (Orange)

Cliente	France Telecom España (Orange)
Proyecto	SGP-Sistema Gestión Portabilidad
Fecha	Desde año 2001 hasta la actualidad
Descripción	Junto a France Telecom INETUM administra, gestiona, desarrolla, implanta y mantiene los sistemas de portabilidad del Operador, así como las integraciones con todos los sistemas implicados Adicionalmente INETUM es la encargada de provisionar los números portados a los sistemas de red
Actividades	Implantación aplicación cliente portabilidad Desarrollo constante de módulos para realizar integraciones con sistemas de información Responsables de los proyectos de portabilidad dentro de France Telecom Mantenimientos preventivos, correctivos y evolutivos



		Soporte funcional a los usuarios de portabilidad Soporte 7X24 de los sistemas Integración módulo de provisión de Red Integración con la red móvil Integración con DataWareHouse
Resultados / Beneficios		1.- Permitir a France Telecom cumplir con la obligación de portabilidad. 2.- Gracias a la integración con otros sistemas France Telecom consigue reducir los tiempos y costos de todos SUS procesos internos. 3.- Lanzamiento de campañas de forma ágil 4.- Cuadros de mando para el seguimiento de las campañas 5.- Reducción de incidencias de provisión de red
Metodologías / Tecnologías		Metodología propia de France Telecom y CMMI

Cliente de portabilidad: Iberbanda (Grupo Movistar)

Cliente	Iberbanda
Proyecto	Portanode
Fecha	Desde año 2010 hasta la actualidad
Descripción	Desarrollo, implantación, mantenimiento correctivo y evolutivo de la aplicación de portabilidad numérica en redes fijas y móviles.
Actividades	Análisis de la Solución de Portabilidad. Análisis de las integraciones con sistemas de BackEnd. Diseño, desarrollo y mantenimiento del sistema. Integración con CRM Integración con sistema HPSA de provisión Integración con sistema IMS de provisión Integración con central de conmutación NORTEL
Resultados / Beneficios	1.- Permitir a Iberbanda cumplir con la obligación de portabilidad. 2.- Cuadros de trabajo y responsabilidades para poder



	distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos 3.- Lanzamiento de campañas de forma ágil 4.- Cuadros de mando para el seguimiento de las campañas 5.- Reducción de incidencias de provisión de red
Metodologías / Tecnologías	Metodología propia de INETUM y CMMI Java, Oracle, Servicios Web.

Cliente de portabilidad: Jazztel España

Cliente	Jazztel España
Proyecto	Port@node Gateway
Fecha	Desde el año 2010 hasta la actualidad
Descripción	Desarrollo, implantación, mantenimiento correctivo y evolutivo de la aplicación de portabilidad numérica en redes fijas y móviles.
Actividades	Análisis de la Solución de Portabilidad. Análisis de las integraciones con sistemas de BackEnd. Diseño, desarrollo y mantenimiento del sistema.
Resultados / Beneficios	1.- Permitir a Jazztel cumplir con la obligación de portabilidad. 2.- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos 3.- Lanzamiento de campañas de forma ágil 4.- Cuadros de mando para el seguimiento de las campañas 5.- Reducción de incidencias de provisión de red
Metodologías / Tecnologías	Metodología propia de INETUM CMMI Java, Oracle, JES (Sun Microsystems Java Enterprise System).

Cliente de portabilidad: Ono España



Cliente	ONO
Proyecto	SGP-Sistema gestión Portabilidad
Fecha	Desde año 2002 hasta 2010
Descripción	Implantación y evolución del sistema cliente de portabilidad de ONO. Unificación de más de 11 Operadoras sobre el sistema de gestión de portabilidad (SGP) producto de la fusión de las empresas que componen el actual ONO.
Actividades	Mantenimientos preventivos, correctivos y evolutivos Desarrollo interfaces con otros sistemas de información Integración con sistema de provisión de red Desarrollo de informes para usuarios
Resultados / Beneficios	1.- Permitir a ONO cumplir con la obligación de portabilidad. 2.- Centralizar la portabilidad de más de 11 operadores en una sola herramienta de gestión de portabilidad, reduciendo costes y optimizando los procesos de resolución de incidencias 3.- Cuadros de mando para el seguimiento de las portabilidades 4.- Reducción de incidencias de provisión de red
Metodologías / Tecnologías	Metodología propia de ONO y CMMI

Cliente de portabilidad: Telefónica Movistar España

Cliente	Telefónica Móviles de España
Proyecto	Port@node
Fecha	Desde el año 2007 hasta la actualidad
Descripción	Implantación del sistema cliente de portabilidad de Telefónica Móviles de España
Actividades	Implantación cliente portabilidad Mantenimientos preventivos, correctivos y evolutivos Desarrollo interfaces con otros sistemas de información Integración con sistema de provisión de red
Resultados /	1.- Permitir a Telefónica Móviles España cumplir con la



Beneficios		obligación de portabilidad. 2.- Integración con otros sistemas a través de Tuxedo 3.- Facilitar la provisión de red
Metodologías Tecnologías	/	Metodología propia del Grupo Telefónica y CMMI

Cliente de portabilidad: Verizon Business España

Cliente		Verizon Business España
Proyecto		Port@node Gateway
Fecha		Desde el año 2008 hasta la actualidad
Descripción		Implantación y evolución del sistema cliente de portabilidad de Verizon Business España
Actividades		Implantación cliente portabilidad Mantenimientos preventivos, correctivos y evolutivos
Resultados Beneficios	/	1.- Permitir a Verizon cumplir con la obligación de portabilidad. 2.- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos 3.- Lanzamiento de campañas de forma ágil 4.- Cuadros de mando para el seguimiento de las campañas 5.- Reducción de incidencias de provisión de red
Metodologías Tecnologías	/	Metodología propia de Verizon y CMMI

Cliente de portabilidad: Vodafone España

Cliente		Vodafone (Tele2 / Comunitel)
Proyecto		Port@node
Fecha		Desde el año 2003 como solución de portabilidad de Comunitel, hasta la actualidad implantada en Vodafone, pasando por Tele2.
Descripción		Implantación y evolución del sistema cliente de portabilidad de Comunitel. Adaptaciones posteriores con



	Tele2 y con Vodafone.
Actividades	Implantación cliente portabilidad. Desarrollo constante de módulos para realizar integraciones con sistemas de información. Integración con CRM. Mantenimientos preventivos, correctivos y evolutivos
Resultados / Beneficios	1.- Permitir al operador (en la actualidad Vodafone), cumplir con la obligación de portabilidad. 2.- Cuadros de mando para el seguimiento de las campañas 3.- Reducción de incidencias de provisión de red 4.- Optimización / automatización de los procesos de portabilidad reduciendo las incidencias de estas
Metodologías / Tecnologías	Metodología propia de Comunitel, Tele2, Vodafone y CMMI

Cliente de portabilidad: Embratel Brasil

Cliente	Embratel
Proyecto	Port@node Gateway & Integrator
Fecha	Desde el año 2008 a 2009
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación Brasileña
Actividades	Análisis modelo portabilidad brasileño Implantación cliente portabilidad e integración con los sistemas legacy del Operador Mantenimientos preventivos, correctivos y evolutivos
Resultados / Beneficios	1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador Brasileño. 2.- Análisis de impacto en los sistemas legacy del Operador. 3.- Lecciones aprendidas del modelo español 4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos



Metodologías / Tecnologías	Metodología propia de Embratel y CMMI
-------------------------------	---------------------------------------

Cliente de portabilidad: Cablecom/MetroRed México

Cliente	Cablecom/MetroRed
Proyecto	Port@node Gateway
Fecha	Año 2008
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación Mexicana
Actividades	Análisis modelo portabilidad mexicano Implantación cliente portabilidad Mantenimiento del sistema
Resultados / Beneficios	1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador Mexicano.
Metodologías / Tecnologías	Metodología propia de INETUM y CMMI

Sistema Central Portabilidad República Dominicana

Cliente	Instituto Dominicano de las Telecomunicaciones (Indotel) República Dominicana
Proyecto	SCP (Sistema Central Portabilidad)
Fecha	Desde el año 2009 hasta la actualidad
Descripción	Implantación Ente Central de Portabilidad de Fijo y de Móvil
Actividades	Análisis modelo portabilidad Implantación solución Portaflow de INETUM Mantenimiento del sistema a cinco años
Resultados / Beneficios	Establecer los procesos, procedimientos, requisitos y condiciones generales que deberán observarse al momento de la puesta en marcha de la facilidad de la Portabilidad Numérica correspondiente tanto a las prestadoras de servicios de redes fijas como de redes móviles; de igual manera, dichas especificaciones aplican tanto para la modalidad de servicio prepago como postpago. A su vez, se persigue obtener, el mínimo impacto posible en la calidad de servicio al usuario y



	<p>el mínimo tiempo en que el usuario que decida portarse a otro operador quede sin servicio.</p> <p>Creación de una entidad que administre la base de datos centralizada principal de la solución técnica denominada “All Call Query” – Consulta de Todas las Llamadas – para la portabilidad numérica en los servicios públicos fijos y móviles.</p>
Metodologías / Tecnologías	Metodología propia de INETUM y CMMI

Cliente de portabilidad: Tricom República Dominicana

Cliente	Tricom
Proyecto	Port@node Gateway & Integrator
Fecha	Desde el año 2009 hasta el 2016
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en República Dominicana
Actividades	<p>Análisis modelo portabilidad de República Dominicana</p> <p>Implantación cliente portabilidad e integración con los sistemas legacy del Operador (CRM, Billing, sistema de provisión a red y DataWareHouse)</p> <p>Mantenimientos preventivos, correctivos y evolutivos</p>
Resultados / Beneficios	<p>1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador Dominicana.</p> <p>2.- Análisis de impacto en los sistemas legacy del Operador.</p> <p>3.- Lecciones aprendidas del modelo español</p> <p>4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos</p>
Metodologías / Tecnologías	Metodología propia de Tricom y CMMI

Cliente de portabilidad: Orange Dominicana

Cliente	Orange Dominicana
Proyecto	Port@node Gateway & Integrator
Fecha	Desde el año 2009 hasta el 2016



Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en República Dominicana
Actividades	Análisis modelo portabilidad de República Dominicana Implantación cliente portabilidad e integración con los sistemas legacy del Operador (SMS database, CRM, Billing, sistema de provisión a red y DataWareHouse) Mantenimientos preventivos, correctivos y evolutivos
Resultados / Beneficios	1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador Dominicana. 2.- Análisis de impacto en los sistemas legacy del Operador. 3.- Lecciones aprendidas del modelo español 4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos
Metodologías / Tecnologías	Metodología propia de Orange y CMMI

Cliente de portabilidad: Claro Rep. Dominicana

Cliente	Claro
Proyecto	Port@node Gateway & Integrator
Fecha	Desde el año 2009 hasta la actualidad
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en República Dominicana
Actividades	Análisis modelo portabilidad de República Dominicana Implantación cliente portabilidad e integración con los sistemas legacy del Operador (CRM, sistema de asignación de números y provisión a red) Mantenimientos preventivos, correctivos y evolutivos
Resultados / Beneficios	1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador Dominicana. 2.- Análisis de impacto en los sistemas legacy del Operador. 3.- Lecciones aprendidas del modelo español 4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos,



	enfocado a clientes distintos
Metodologías / Tecnologías	Metodología propia de Claro y CMMI

Administrador de Base de Datos Centralizada Principal de Perú

Cliente	Nextel, Claro, Movistar.
Proyecto	ABDCP (Administrador de Base de Datos Centralizada Principal de Portabilidad)
Fecha	Desde el año 2010 hasta el año 2014. Desde 2018 hasta el año 2024
Descripción	Implantación Ente Central de Portabilidad de Móvil
Actividades	Análisis modelo portabilidad Implantación solución Portaflow de INETUM Mantenimiento del sistema a cinco años
Resultados / Beneficios	Creación de una entidad que administre la base de datos centralizada principal de la solución técnica denominada “All Call Query” – Consulta de Todas las Llamadas – para la portabilidad numérica en los servicios públicos móviles.
Metodologías / Tecnologías	Metodología propia de INETUM, PMP y CMMI

Cliente de portabilidad: Entel Perú

Cliente	Entel Perú
Proyecto	Port@node Gateway
Fecha	Desde el año 2010 hasta el 2024
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en el Perú
Actividades	Análisis modelo portabilidad del Perú Implantación cliente portabilidad e integración con los sistemas legacy del Operador (CRM, sistema de asignación de números y provisión a red) Mantenimientos preventivos, correctivos y evolutivos
Resultados /	1.- Permitir al cliente dar cumplimiento a los requisitos



Beneficios	solicitados por el ABDCP. 2.- Análisis de impacto en los sistemas legacy del Operador. 3.- Lecciones aprendidas del modelo español 4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos
Metodologías / Tecnologías	Metodología propia de Entel y CMMI

Sistema Central Portabilidad Colombia

Cliente	Movistar, Tigo, Claro, Avantel
Proyecto	ABD (Administrador Base de Datos de Portabilidad)
Fecha	Desde el año 2010 hasta el 2024
Descripción	Implantación Ente Central de Portabilidad Móvil
Actividades	Análisis modelo portabilidad Implantación solución Portaflow de INETUM Mantenimiento del sistema a cinco años
Resultados / Beneficios	Establecer los procesos, procedimientos, requisitos y condiciones generales que deberán observarse al momento de la puesta en marcha de la facilidad de la Portabilidad Numérica correspondiente tanto a las prestadoras de servicios de redes fijas como móviles y prestadores de servicios móviles virtuales (OMVs); de igual manera, dichas especificaciones aplican tanto para la modalidad de servicio prepago como pospago. A su vez, se persigue obtener, el mínimo impacto posible en la calidad de servicio al usuario y el mínimo tiempo en que el usuario que decida portarse a otro operador quede sin servicio. Creación de una entidad que administre la base de datos centralizada principal de la solución técnica denominada “All Call Query” – Consulta de Todas las Llamadas – para la portabilidad numérica en los servicios públicos fijos y móviles.
Metodologías / Tecnologías	Metodología propia de INETUM y CMMI



Sistema Registro de Terminales Móviles Colombia

Cliente	Movistar, Tigo, Claro, Avantel
Proyecto	SRTM (Sistema de Registro de Terminales Móviles)
Fecha	Desde el año 2012 a la actualidad
Descripción	Implantación Base de Datos centralizada de terminales móviles robados
Actividades	Análisis modelo centralizado de registro de terminales móviles Implantación solución STRM de INETUM Mantenimiento del sistema a cinco años
Resultados / Beneficios	Establecer un modelo técnico, los aspectos operativos y las reglas para la implementación, carga y actualización de las bases de datos positiva y negativa para la restricción de la operación en las redes de telecomunicaciones móviles de los equipos terminales móviles reportados como hurtados y/o extraviados
Metodologías / Tecnologías	Metodología propia de INETUM y CMMI

Cliente de portabilidad: Claro Colombia

Cliente	Claro Colombia
Proyecto	Port@node Gateway & Integrator
Fecha	Año 2011
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en República de Colombia
Actividades	Análisis modelo portabilidad de República de Colombia Implantación cliente portabilidad e integración con los sistemas legacy del Operador (CRM, sistema de asignación de números y provisión a red) Mantenimientos preventivos, correctivos y evolutivos
Resultados / Beneficios	1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador de Colombia. 2.- Análisis de impacto en los sistemas legacy del Operador. 3.- Lecciones aprendidas del modelo español 4- Cuadros de trabajo y responsabilidades para poder



	distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos
Metodologías / Tecnologías	Metodología propia de Claro y CMMI

Cliente de portabilidad: Tigo Colombia

Cliente	Tigo Colombia
Proyecto	Port@node Gateway & Integrator
Fecha	Desde el año 2017 hasta la actualidad
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en Colombia Migración del sistema actual de portabilidad del operador a la plataforma Port@node
Actividades	Implantación cliente portabilidad e integración con los sistemas Back-End del Operador (CRM, provisión plataforma prepago / pospago, fijo / móvil y provisión a red) Mantenimientos preventivos, correctivos y evolutivos
Resultados / Beneficios	1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador de Colombia 2.- Análisis de impacto en los sistemas back-end del Operador. 3.- Migración del sistema actual del operador 4.- Integración con los operadores móviles virtuales 5.- Lecciones aprendidas del modelo español 6- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos
Metodologías / Tecnologías	Metodología propia de Tigo y CMMI

Cliente de portabilidad: Claro Panama

Cliente	Claro Panamá
---------	--------------



Proyecto	Port@node Gateway & Integrator
Fecha	Desde el año 2011 hasta 2021
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en Panamá
Actividades	Análisis modelo portabilidad de Panamá Implantación cliente portabilidad e integración con los sistemas legacy del Operador (CRM, sistema de asignación de números y provisión a red) Mantenimientos preventivos, correctivos y evolutivos
Resultados / Beneficios	1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador de Panamá. 2.- Análisis de impacto en los sistemas legacy del Operador. 3.- Lecciones aprendidas del modelo español 4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos
Metodologías / Tecnologías	Metodología propia de Claro y CMMI

Cliente de portabilidad: Claro Argentina

Cliente	Claro Argentina
Proyecto	Port@node Gateway & Integrator
Fecha	Desde el año 2011 hasta la actualidad
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en Argentina
Actividades	Análisis modelo portabilidad de Argentina Implantación cliente portabilidad e integración con los sistemas legacy del Operador (CRM y provisión a red) Mantenimientos preventivos, correctivos y evolutivos
Resultados / Beneficios	1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador de Argentina. 2.- Análisis de impacto en los sistemas legacy del Operador. 3.- Lecciones aprendidas del modelo español



	4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos
Metodologías / Tecnologías	Metodología propia de Claro y CMMI

Cliente de portabilidad: Entel / Entel PCS

Cliente	Entel y Entel PCS
Proyecto	Port@node Gateway Multioperador
Fecha	Año 2011 hasta 2020
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en Chile
Actividades	Análisis modelo portabilidad de Chile Implantación cliente portabilidad e integración con los sistemas legacy del Operador Mantenimientos preventivos, correctivos y evolutivos
Resultados / Beneficios	1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador de Chile. 2.- Análisis de impacto en los sistemas legacy del Operador. 3.- Lecciones aprendidas del modelo español 4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos
Metodologías / Tecnologías	Metodología propia de Entel y CMMI

Sistema Central Portabilidad Paraguay

Cliente	Claro, Personal, Tigo y Vox
Proyecto	EAPN (Administrador Base de Datos de Portabilidad)
Fecha	Desde el 30 de noviembre de 2012 hasta la actualidad
Descripción	Implantación Ente Central de Portabilidad Móvil
Actividades	Análisis modelo portabilidad Implantación solución Portaflow de INETUM



	Mantenimiento del sistema a cuatro años
Resultados / Beneficios	<p>Establecer los procesos, procedimientos, requisitos y condiciones generales que deberán observarse al momento de la puesta en marcha de la facilidad de la Portabilidad Numérica correspondiente a las prestadoras de servicios de redes móviles; de igual manera, dichas especificaciones aplican tanto para la modalidad de servicio prepago como postpago. A su vez, se persigue obtener, el mínimo impacto posible en la calidad de servicio al usuario y el mínimo tiempo en que el usuario que decida portarse a otro prestador quede sin servicio.</p> <p>Creación de una entidad que administre la base de datos centralizada principal de la solución técnica denominada "All Call Query" – Consulta de Todas las Llamadas – para la portabilidad numérica en los servicios públicos móviles.</p>
Metodologías / Tecnologías	Metodología propia de INETUM y CMMI

Cliente de portabilidad: Claro Paraguay

Cliente	Claro Paraguay
Proyecto	Port@node Gateway & Integrator
Fecha	Año 2012 hasta la actualidad
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en Paraguay
Actividades	<p>Análisis modelo portabilidad de Paraguay</p> <p>Implantación cliente portabilidad e integración con los sistemas legacy del Operador (CRM y provisión a red)</p> <p>Mantenimientos preventivos, correctivos y evolutivos</p>
Resultados / Beneficios	<p>1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador de Paraguay.</p> <p>2.- Análisis de impacto en los sistemas legacy del Operador.</p> <p>3.- Lecciones aprendidas del modelo español</p> <p>4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos</p>



Metodologías / Tecnologías	Metodología propia de Claro y CMMI
----------------------------	------------------------------------

Cliente de portabilidad: Vox

Cliente	Vox
Proyecto	Port@node Gateway & Integrator
Fecha	Año 2012
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en Paraguay
Actividades	Análisis modelo portabilidad de Paraguay Implantación cliente portabilidad e integración con los sistemas legacy del Operador (CRM y provisión a red) Mantenimientos preventivos, correctivos y evolutivos
Resultados / Beneficios	1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador de Paraguay. 2.- Análisis de impacto en los sistemas legacy del Operador. 3.- Lecciones aprendidas del modelo español 4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos
Metodologías / Tecnologías	Metodología propia de Vox y CMMI

Sistema Central Portabilidad Costa Rica

Cliente	Claro, Telefónica, ICE, TuyoMóvil y FullMóvil
Proyecto	ERPN (Entidad de Referencia de Portabilidad Numérica)
Fecha	Desde el 26 de agosto de 2013
Descripción	Implantación Ente Central de Portabilidad Móvil
Actividades	Análisis modelo portabilidad Implantación solución Portaflow de INETUM Mantenimiento del sistema a siete años
Resultados / Beneficios	Establecer los procesos, procedimientos, requisitos y condiciones generales que deberán observarse al momento



	<p>de la puesta en marcha de la facilidad de la Portabilidad Numérica correspondiente a las prestadoras de servicios de redes móviles y prestadores de servicios móviles virtuales (OMVs); de igual manera, dichas especificaciones aplican tanto para la modalidad de servicio prepago como pospago. A su vez, se persigue obtener, el mínimo impacto posible en la calidad de servicio al usuario y el mínimo tiempo en que el usuario que decida portarse a otro prestador quede sin servicio.</p> <p>Creación de una entidad que administre la base de datos centralizada principal de la solución técnica denominada “All Call Query” – Consulta de Todas las Llamadas – para la portabilidad numérica en los servicios públicos móviles.</p>
Metodologías / Tecnologías	Metodología propia de INETUM y CMMI

Cliente de portabilidad: Claro Costa Rica

Cliente	Claro Costa Rica
Proyecto	Port@node Gateway & Integrator
Fecha	Año 2013
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en Costa Rica
Actividades	<p>Análisis modelo portabilidad de Costa Rica</p> <p>Implantación cliente portabilidad e integración con los sistemas legacy del Operador (CRM, provisión plataforma prepago y pospago y provisión a red)</p> <p>Mantenimientos preventivos, correctivos y evolutivos</p>
Resultados / Beneficios	<p>1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador de Costa Rica.</p> <p>2.- Análisis de impacto en los sistemas legacy del Operador.</p> <p>3.- Lecciones aprendidas del modelo español</p> <p>4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos</p>
Metodologías /	Metodología propia de Claro y CMMI



Tecnologías	
-------------	--

Cliente de portabilidad: TuyoMóvil

Cliente	Tuyomovil
Proyecto	Port@node Gateway Cloud
Fecha	Año 2013 hasta 2019
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en Costa Rica en servicio "Cloud"
Actividades	Análisis modelo portabilidad de Costa Rica Implantación cliente portabilidad en servicio "Cloud" Mantenimientos preventivos, correctivos y evolutivos
Resultados / Beneficios	1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador de Costa Rica. 2.- Uso del sistema en la nube. 3.- Lecciones aprendidas del modelo español 4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos
Metodologías / Tecnologías	Metodología propia de INETUM y CMMI
Información de contacto	Oscar Chon León, responsable del proyecto Email: oscar.chon@tuyomovil.com

Cliente de portabilidad: Claro Honduras

Cliente	Claro Honduras
Proyecto	Port@node Gateway & Integrator
Fecha	Año 2014 hasta la actualidad
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en Honduras
Actividades	Análisis modelo portabilidad de Honduras Implantación cliente portabilidad e integración con los sistemas legacy del Operador (CRM, provisión plataforma prepago y pospago y provisión a red)



	Mantenimientos preventivos, correctivos y evolutivos
Resultados / Beneficios	1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador de Honduras. 2.- Análisis de impacto en los sistemas legacy del Operador. 3.- Lecciones aprendidas del modelo español 4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos
Metodologías / Tecnologías	Metodología propia de Claro y CMMI

Cliente de portabilidad: Claro El Salvador

Cliente	Claro El Salvador
Proyecto	Port@node Gateway & Integrator
Fecha	Año 2015
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en El Salvador
Actividades	Análisis modelo portabilidad de El Salvador Implantación cliente portabilidad e integración con los sistemas Back-End del Operador (CRM, provisión plataforma prepago / pospago, fijo / móvil y provisión a red) Mantenimientos preventivos, correctivos y evolutivos
Resultados / Beneficios	1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador de El Salvador. 2.- Análisis de impacto en los sistemas back-end del Operador. 3.- Lecciones aprendidas del modelo español 4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos
Metodologías / Tecnologías	Metodología propia de Claro y CMMI

Cliente de portabilidad: Tigo El Salvador



Cliente	Tigo El Salvador
Proyecto	Port@node Gateway & Integrator
Fecha	Año 2015 hasta la actualidad
Descripción	Implantación sistema global de Portabilidad para cumplimiento Regulación en El Salvador
Actividades	Análisis modelo portabilidad de El Salvador Implantación cliente portabilidad e integración con los sistemas Back-End del Operador (CRM, provisión plataforma prepago / pospago, fijo / móvil y provisión a red) Mantenimientos preventivos, correctivos y evolutivos
Resultados / Beneficios	1.- Permitir al cliente dar cumplimiento a los requisitos solicitados por el Ente Regulador de El Salvador. 2.- Análisis de impacto en los sistemas back-end del Operador. 3.- Lecciones aprendidas del modelo español 4- Cuadros de trabajo y responsabilidades para poder distribuir el trabajo de portabilidad entre varios equipos, enfocado a clientes distintos
Metodologías / Tecnologías	Metodología propia de Tigo y CMMI

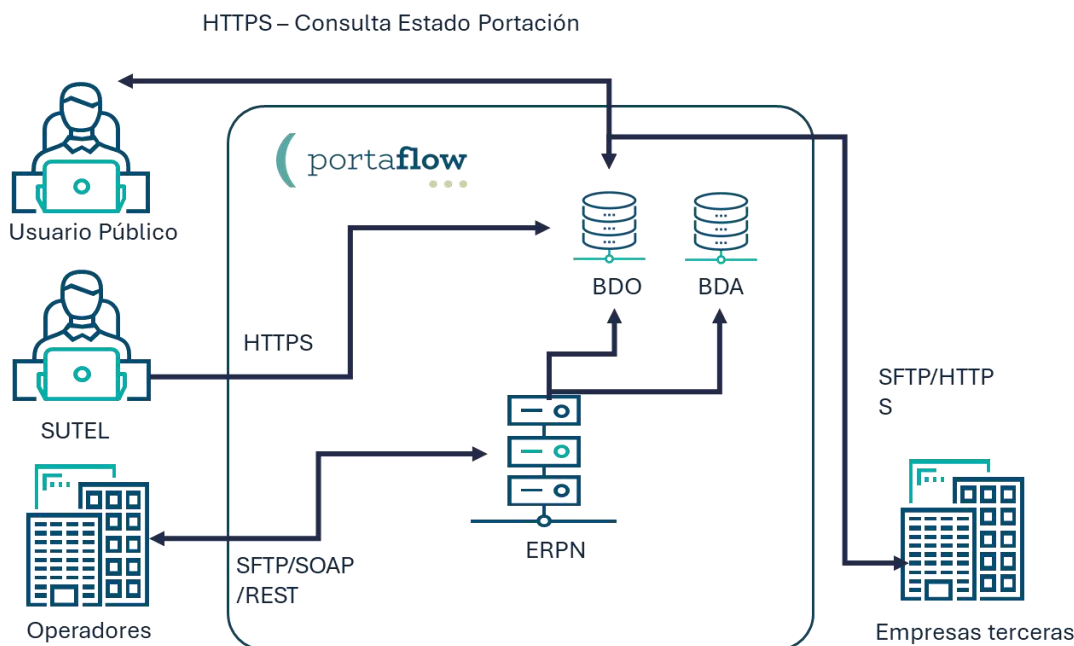
2 Requerimientos funcionales

El ERP, a través del producto **Portaflow 3.0** contará con las funcionalidades necesarias que aseguren el correcto funcionamiento de los procesos de portabilidad de acuerdo con lo especificado en el **"Manual de Interfaces con mejoras.docx"** y **"Manual de Interfaces y Procesos.pdf"**

En todos los casos, Portaflow interactuará en forma automática con los componentes de software dispuestos por los operadores para estos procesos.

Todos los valores o plazos establecidos en las Bases Técnicas serán configurables y podrán modificarse a solicitud del CTPN durante la ejecución del contrato, independientemente de que se encuentre expresamente especificado.

El siguiente diagrama muestra a alto nivel el sistema propuesto para dar una solución centralizada, integral y completa a los requerimientos de la Portabilidad numérica en Costa Rica.



El sistema propuesto por INETUM que ofrece todos estos servicios recibe el nombre de **Portaflow 3.0**.

El producto **Portaflow** resuelve toda la lógica de negocio definida en la especificación técnica en lo relativo a todos los procesos de portabilidad, gestionando, no solo la coherencia entre los mensajes, sino también el tratamiento de todos los temporizadores, objeciones, manejo de errores y/o excepciones, y otras actividades tales como, llegado el caso, ejecutar auditorías sobre los procesos, mantener la relación con otras bases de datos y procesos que puedan llegar a encadenarse, etc.

Portaflow genera trazas de log sobre todas las acciones realizadas en el tratamiento de los mensajes, gestión de los procesos de portabilidad y almacenamiento en base de datos, permitiendo hacer un seguimiento detallado de todos los eventos sucedidos, así como la captura y el manejo de excepciones y errores, notificando los mismos a quien corresponda.

El sistema dispone además de una interfaz de administración mediante la cual se podrán configurar aquellos parámetros que definan el comportamiento del sistema, así como el nivel de detalle de los logs que se generan.

2.1 Proceso 00 - Proceso de generación y envío de NIP

2.1.1 Descripción del proceso

Es el proceso mediante el cual la ERP'N genera un NIP a solicitud del operador receptor cuando un usuario desea portar su número. Posteriormente el NIP es entregado al usuario a través de la red del operador donante.

La solicitud deberá incluir un número único de proceso que generará el receptor y que



identificará a todos los mensajes asociados al proceso.

Portaflow será capaz de recibir solicitudes de generación de NIP y validar el contenido de las mismas según el formato definido en los términos de referencia, y además se encargará de administrar y controlar las vigencias de los NIPs.

La validez del NIP es de 24 horas laborales o hasta que la solicitud de portabilidad es entregada al operador donante, lo que antes suceda. Si la solicitud de portabilidad es rechazada por el donante, el receptor podrá usar el mismo NIP una segunda vez, no obstante, el número de veces que podrá ser usado el NIP tras el rechazo del donante será un parámetro configurable.

Se permitirá la portabilidad de un mismo número en el último año calendario hasta un límite de veces que será configurable en Portaflow, si se solicita un NIP una vez más, la solicitud será rechazada

Portaflow generará trazas de log sobre todas las acciones realizadas en la recepción de solicitudes, generación de NIP y almacenamiento en base de datos, permitiendo hacer un seguimiento detallado de todos los eventos sucedidos, así como la captura y el manejo de excepciones y errores, notificando los mismos a quien corresponda.

Una vez validada la solicitud de generación de NIP, Portaflow generará de forma aleatoria un número compuesto de un número configurable de dígitos, que inicialmente será igual a 4 dígitos y no se permitirá al usuario solicitar un nuevo NIP para otro trámite de portación sin haber finalizado el primer trámite.

Portaflow entregará a la red del operador donante el NIP para que este sea enviado al usuario vía SMS. Para la entrega de los SMS, cada operador móvil establecerá un enlace vía Internet, y se realizará mediante protocolo SMPP (Short Message Peer-to-Peer Protocol).

En caso de que Portaflow no reciba acuse de recibo del SMSC proveniente de la red del operador donante, en el lapso de cinco (5) minutos realizará dos (2) reintentos adicionales, y si superados los reintentos se continúa sin poder entregar el SMS a la red de operador donante o se continúa sin recibir el ack, Portaflow intentará el envío del NIP a través de la red del receptor hasta 3 veces. En caso de no conseguir tampoco entregar el NIP a la red del receptor, el abonado deberá utilizar el IVR para obtener el NIP.

Los NIPs quedarán almacenados en espera de recibir la solicitud de portabilidad del Proveedor Receptor hasta tanto finalice su vigencia.

El NIP enviado al usuario deberá ser posteriormente indicado en la solicitud de portabilidad que el operador receptor envíe a la ERPN.

El texto SMS a enviar tendrá el siguiente formato: "Su código de portabilidad es: [xxxx], con vencimiento [dd/mm/yyyy hh:mm], para el prestador [nombre]"

Para las solicitudes de portabilidad múltiples (varias numeraciones) el receptor deberá indicar en la solicitud de generación de NIP a qué número quiere que sea enviado el SMS, este número será el que posteriormente se indique como número asociado al NIP grupal



en la solicitud de portabilidad. Portaflow generará un NIP individual para cada uno de los números contenidos en la solicitud con la misma vigencia que el NIP grupal

Obtención del NIP a través del IVR

Cuando el usuario no haya recibido el NIP mediante un SMS, podrá realizar la consulta mediante el IVR. El diagrama de flujo constará de los siguientes procesos:

1. El usuario deberá llamar desde la línea que tiene el número telefónico utilizado en la solicitud de NIP, y desde el cual desea conocerlo a través del IVR. En caso de empresas se deberá hacer la llamada desde el número para el que se solicitó el NIP
2. El IVR detectará el número de teléfono originador de la llamada y realizará una consulta al ERPN para dicho número mediante el servicio web que estará disponible
3. Si tiene un NIP vigente, se lo dirá al usuario dándole la oportunidad de repetírselo. En ambos casos finaliza la llamada.
4. Si no tiene un NIP vigente, informará al usuario de ello y finalizará la llamada.

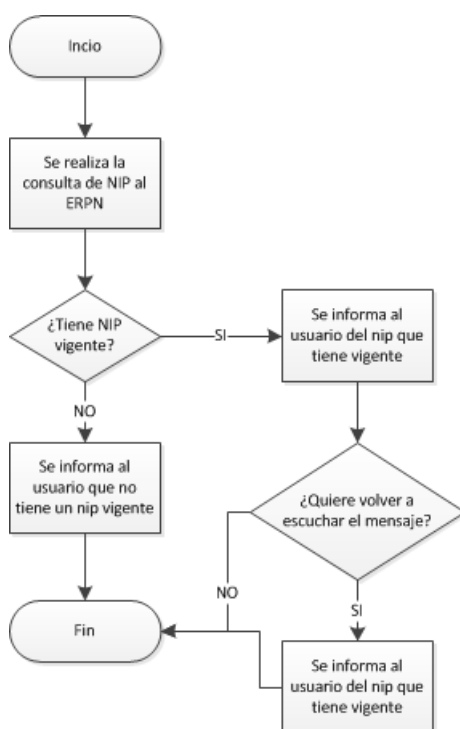


Figura 1 – Diagrama de flujo de la consulta del NIP

2.1.2 Interacción de mensajes

1. El prestador receptor enviará a la ERPN un mensaje 0001 de solicitud de generación de NIP, indicando la numeración a portar.
2. La ERPN realizará las siguientes validaciones a la solicitud para cada línea incluida en la



solicitud:

- La línea existe
- La numeración no está portada al operador receptor
- La línea no está involucrada en ningún trámite de portabilidad
- No existe un NIP ya vigente para el número
- El operador donante indicado en la solicitud es el correcto
- El número para el que se solicita el NIP está incluido en la lista de números a portar
- No existen líneas duplicadas
- El número no se ha portado más del límite de veces permitido en el último año calendario

Si la solicitud no es válida

1. La ERPN enviará al operador receptor un mensaje de respuesta 0090 indicando todas las causas de rechazo asociadas a cada número rechazado.
2. La ERPN cancelará el proceso de generación y envío de NIP

Si la solicitud es válida

1. La ERPN generará un NIP de 4 dígitos, y lo almacenará en la base de datos de NIPs durante el tiempo definido en el temporizador TNIP de vigencia de NIPs. Una vez superado este plazo, el NIP será eliminado de la base de datos de NIPs vigentes.
2. La ERPN enviará el NIP al número indicado en la solicitud, al centro de mensajes del prestador donante para que el mismo remita dicho NIP al usuario vía SMS.

Si el NIP no puede entregarse al prestador donante o el operador donante no devuelve el ack

1. En caso de error de envío a la red del operador donante, habrá hasta 3 reintentos dentro de los 2 minutos desde la generación del NIP. Superados los reintentos se probará el envío del SMS a la red del receptor. Si aun así no se pudiera entregar el SMS, la ERPN le enviará un mensaje 0002 al prestador receptor indicando error en el envío del mensaje.

Si el NIP se entregó correctamente al prestador donante o al prestador receptor

1. La ERPN enviará al prestador receptor un mensaje 0002 indicando aceptación de generación y confirmación de envío de NIP, indicando el operador al que fue entregado el SMS (operador donante o receptor), la fecha de generación del NIP y la fecha y la hora de fin de vigencia del NIP
2. El receptor podrá solicitar el envío de NIP al usuario mediante un mensaje 0003 o bien con un mensaje 0001 siempre dentro de la vigencia del NIP



Si la respuesta de confirmación de entrega de NIP (0002) no puede enviarse al prestador receptor

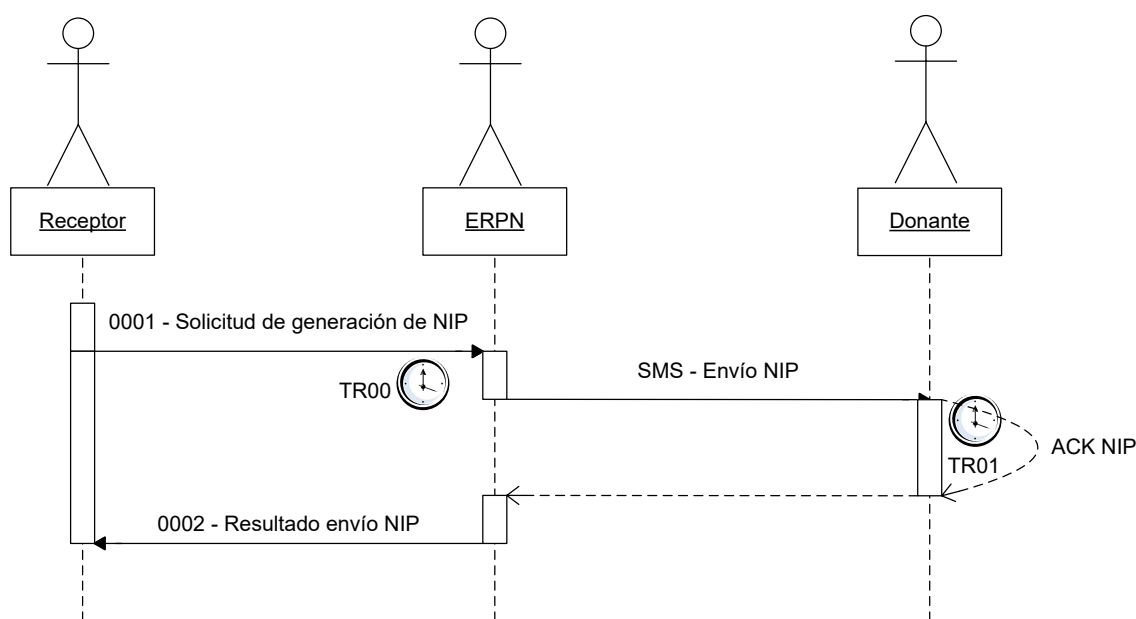
1. Ante un fallo en la entrega de los mensajes por problemas en la comunicación o porque el sistema del operador no esté disponible, la ERPN siempre reenviará X veces cada mensaje con un tiempo de espera entre reintentos.
2. El NIP continuará siendo vigente hasta su fecha de vencimiento o hasta que la solicitud de portabilidad sea entregada al operador donante, lo que antes suceda.
3. El operador receptor podrá solicitar el envío del NIP mediante el mensaje 0003 o el mensaje 0001.

Si el usuario no recibe el NIP o lo recibió, pero lo perdió

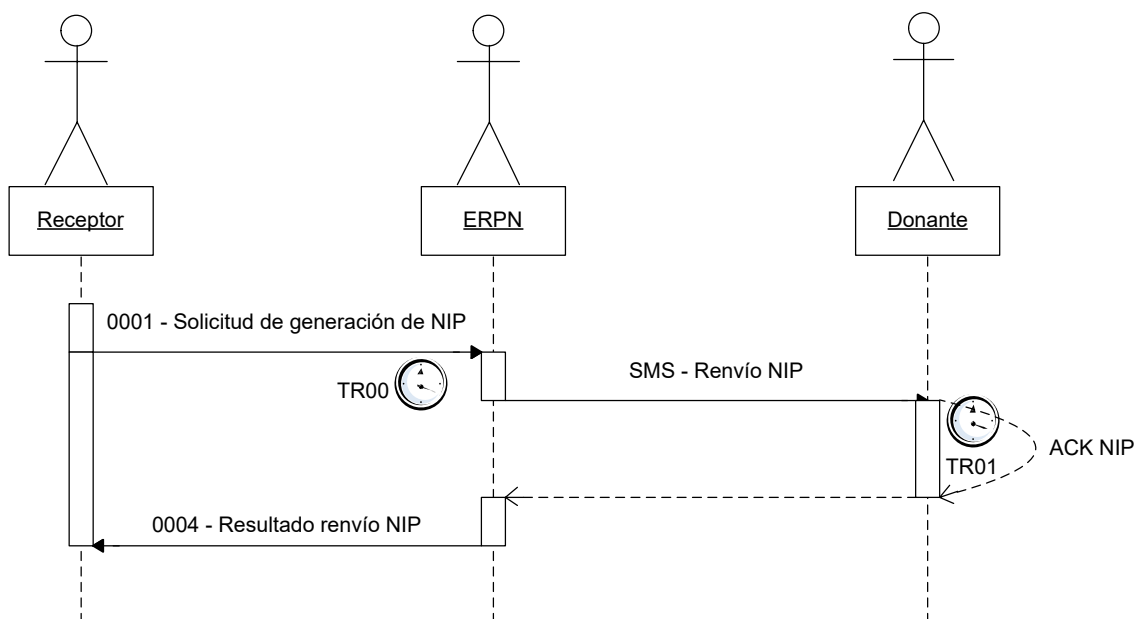
1. El operador receptor podrá solicitar el envío del NIP mediante el mensaje 0003 o el mensaje 0001
2. La ERPN reenviará el NIP a la red del operador donante siguiendo el mismo proceso que para el envío del NIP, es decir, en caso de error en la entrega o no recibir el ack, se probará el envío con la red del operador receptor
3. La ERPN enviará al operador receptor un mensaje 0004 confirmando el envío del NIP, indicando el operador al que entregó el SMS (operador donante o receptor), la fecha de envío y la fecha y hora de fin de vigencia del NIP

2.1.3 Diagramas de actividad

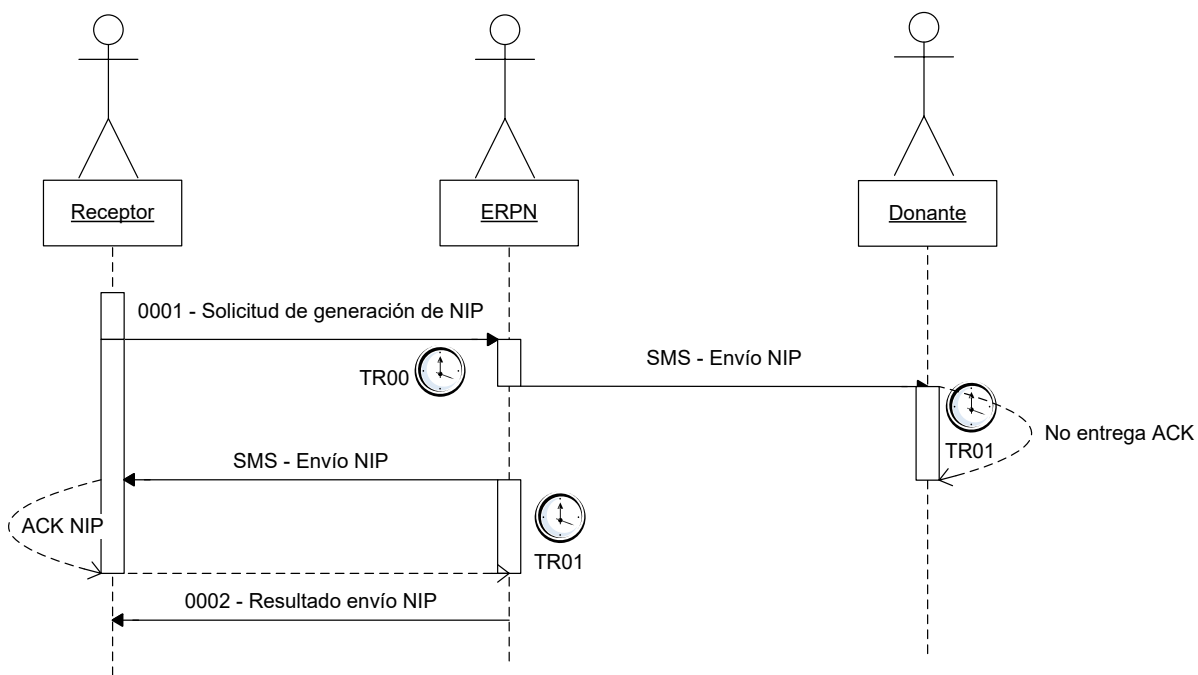
Solicitud de generación y envío de NIP



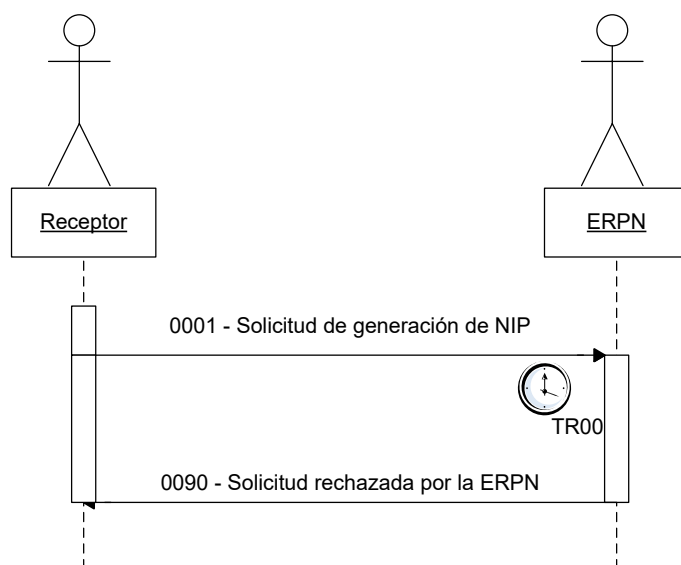
Flujo sin NIP Vigente sin errores ni rechazos



Flujo con NIP Vigente sin errores ni rechazos

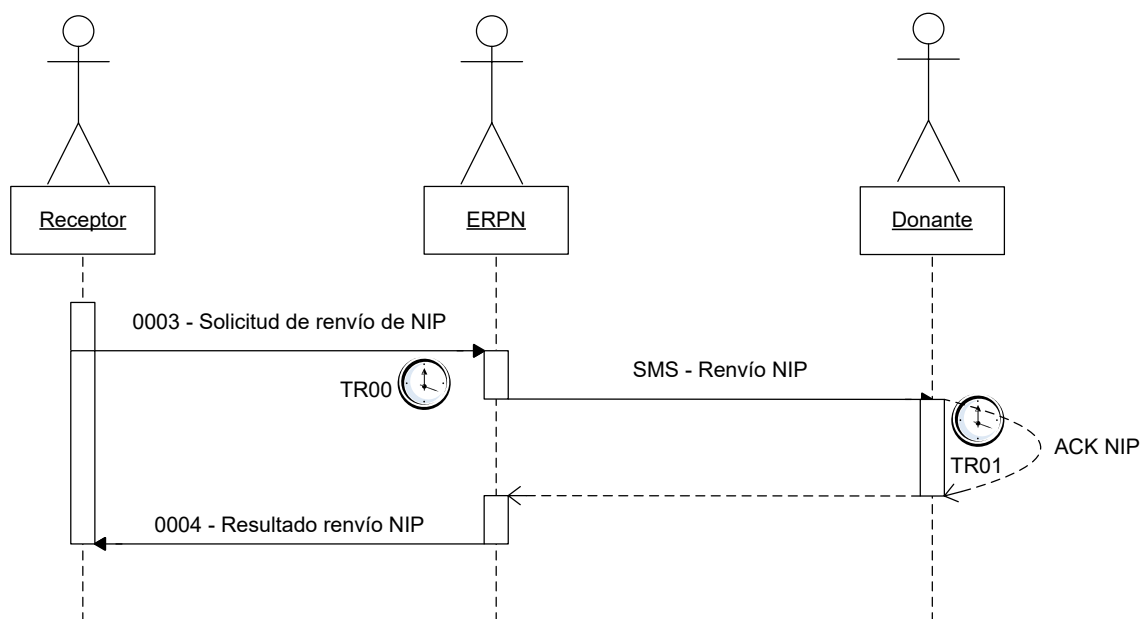


Flujo con error de envío de SMS al operador donante

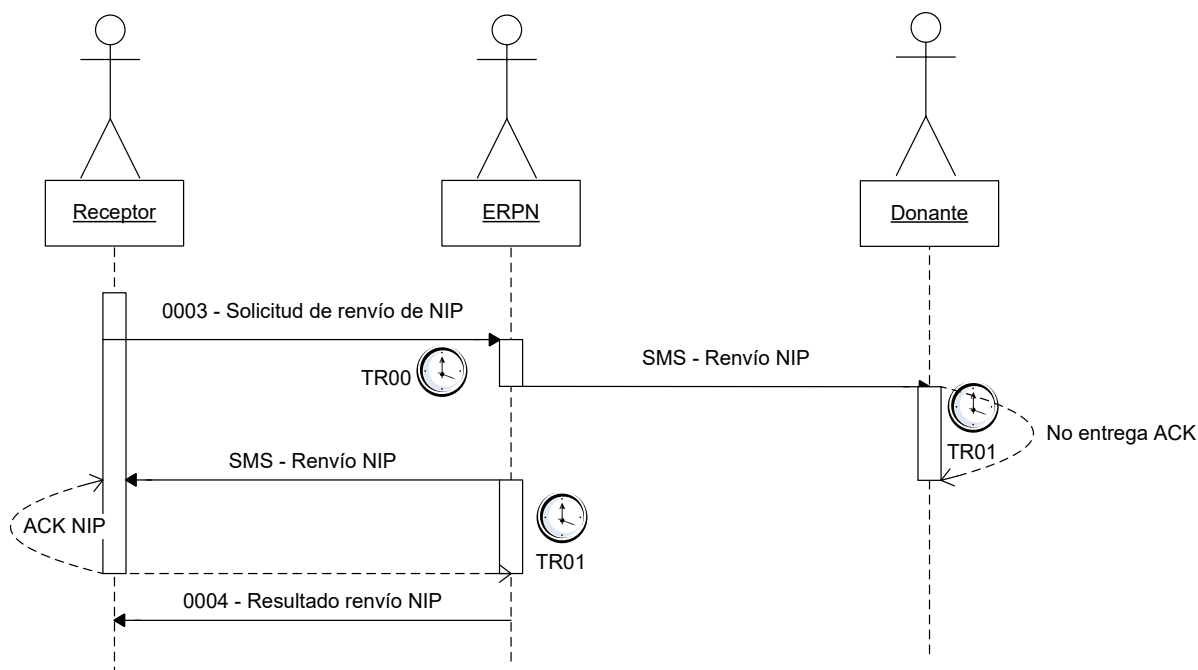


Flujo con rechazo de la ERPN

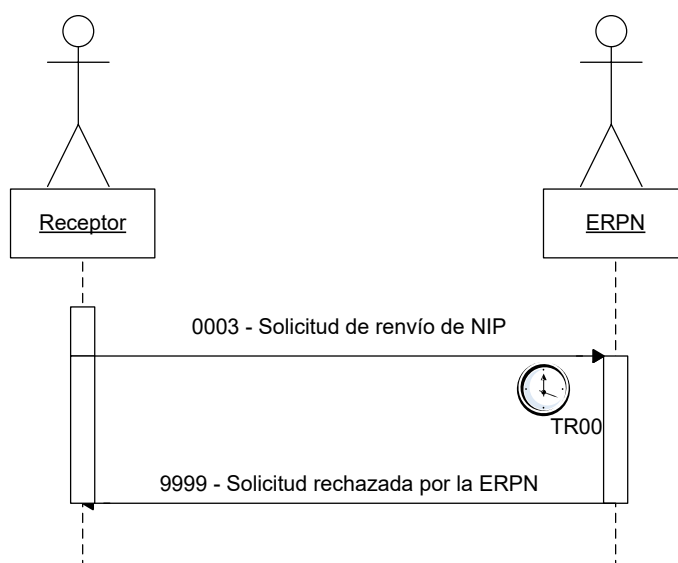
Solicitud envío de NIP



Flujo sin errores ni rechazos



Flujo con error de envío de SMS al operador donante



Flujo con rechazo de la ERPN

2.2 Proceso 02 – Proceso de consultas de prevalidación

2.2.1 Descripción del proceso

Portaflow permitirá realizar, tras una solicitud de Generación y Entrega de NIP, la realización de consultas mediante las cuales los operadores o proveedores receptores solicitan información específica de los requisitos para portar el número asociado al NIP generado, pero este proceso no necesariamente se deberá convertir en una solicitud de portabilidad.

Existirán dos tipos de consulta de prevalidación:



- Consulta de prevalidación automática de proceso en curso
- Consulta de prevalidación al operador donante de datos del abonado

2.2.2 Interacción de mensajes

2.2.2.1 Consulta automática de proceso en curso

1. El prestador receptor enviará a la ERPN un mensaje 2001 de consulta automática de proceso en curso.
2. La ERPN realizará las siguientes validaciones para cada número de teléfono incluido en la consulta:
 - La línea existe
 - Existe un NIP vigente para el número y operador receptor y es el indicado en la consulta

Si la solicitud no es válida

1. La ERPN enviará al operador receptor un mensaje de respuesta 2090 indicando todos los números que no cumplen alguna validación y todas las causas de rechazo asociadas a cada número rechazado. El mensaje de rechazo deberá ser enviado dentro del plazo TR20 contado a partir de la recepción de la consulta

Si la solicitud es válida

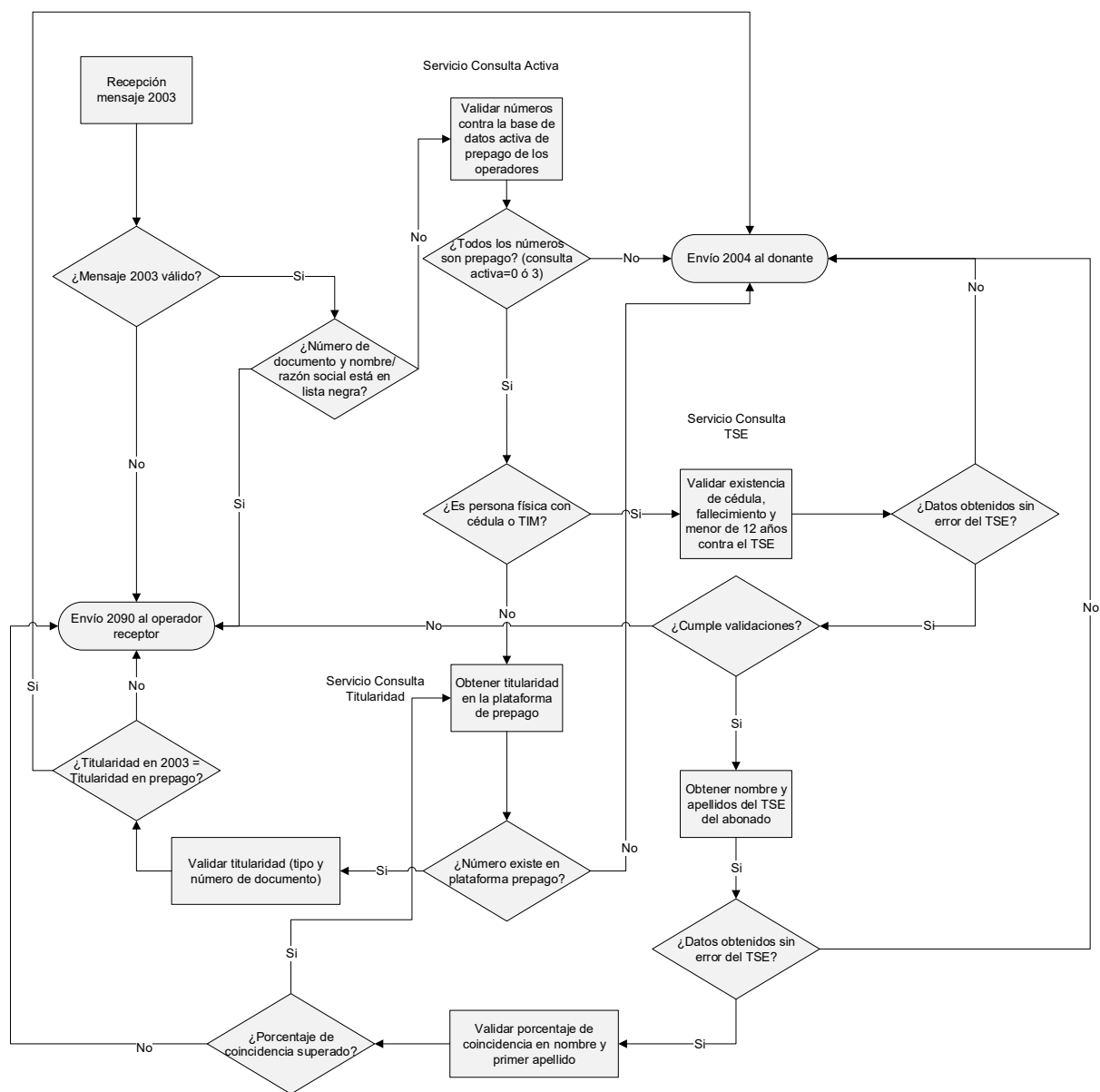
1. La ERPN enviará al operador un mensaje 2002 de respuesta automática de proceso en curso indicando al operador si existe o no proceso en curso para las numeraciones incluidas en la consulta. El mensaje de respuesta deberá ser enviado dentro del plazo TR20 contado a partir de la recepción de la consulta

2.2.2.2 Consulta al operador donante de datos del abonado

Dando cumplimiento al requerimiento de integración de portabilidad con los sistemas de registro de prepago y del TSE para el caso de Cédulas o TIM y con el sistema de Migración y Extranjería para el caso de DIMEX, el flujo a seguir será el siguiente (los servicios se describen en el apartado **Anexo V. Servicios de integración con registro de prepago, TSE y Migración y Extranjería**):

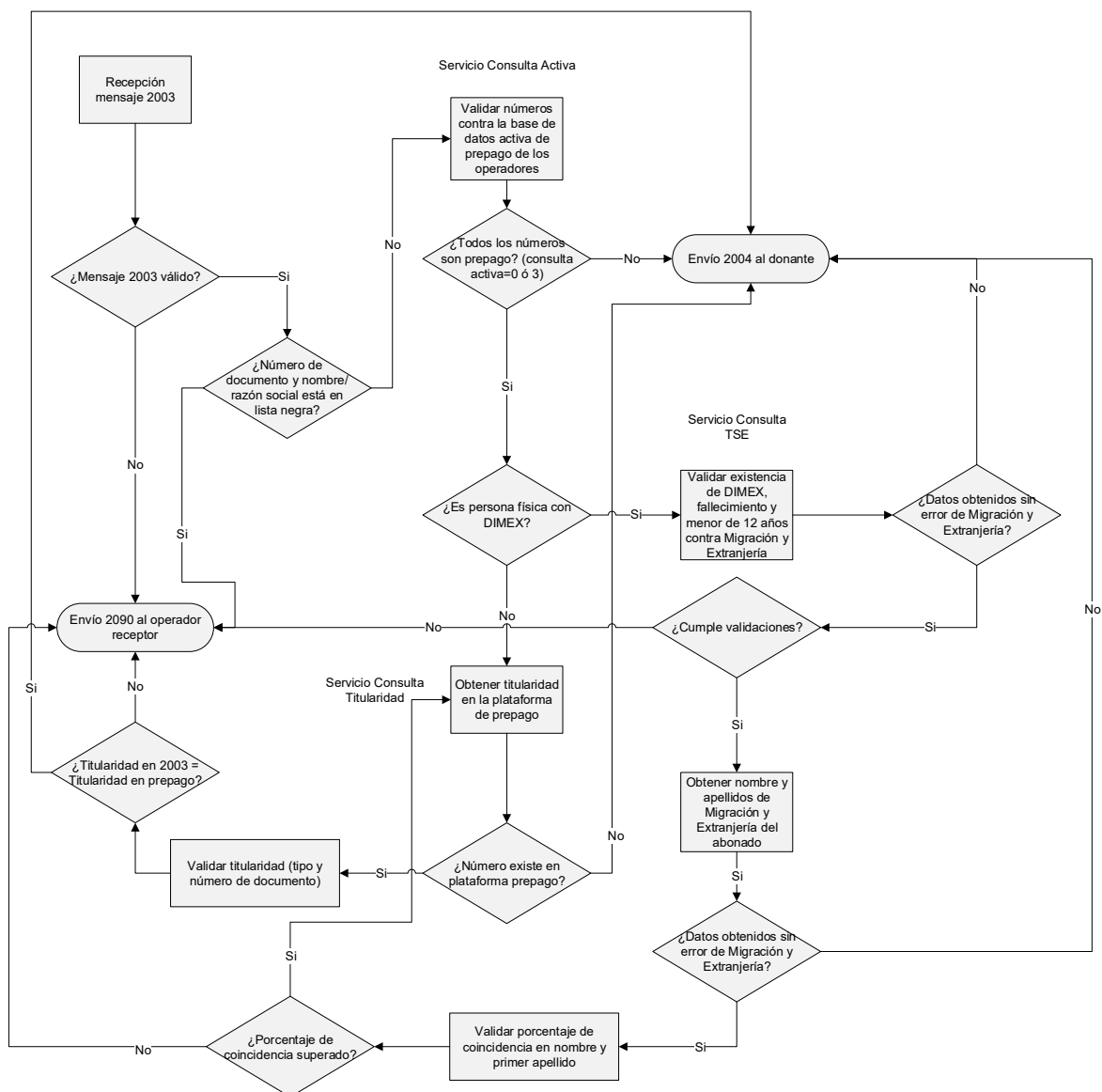


Flujo para cédula y TIM





Flujo para DIMEX



Se debe tener en cuenta que la validación de titularidad en la ERPN se basa en las siguientes premisas:

Personas físicas:

- campos de nombre y/o apellidos no estén vacíos, contengan caracteres numéricos, caracteres especiales o secuencias de caracteres que no correspondan a un nombre (Ejemplos: NO-PER; A!\$4%2#2%).
- campos de número de identificación que cumplan con lo siguiente:
 - Cédula de identidad para adulto únicamente números y con 9 dígitos sin guiones ni espacios entre sí.
 - Documento TIM para menores, únicamente con números y con 9 dígitos sin guiones ni espacios entre sí.



- Cédula de residencia DIMEX únicamente con números y con 12 dígitos sin guiones ni espacios entre sí.
- Pasaporte: deberá poseer longitud variable de máximo 20 caracteres, de carácter alfanumérico y no permitirá el uso de caracteres especiales

Personas jurídicas:

- a. el campo de nombre o razón social podrá aceptar caracteres alfanuméricos y especiales (es el único caso que acepta la introducción de caracteres especiales (¡"#\$%&=*+?))
- b. El campo de cédula jurídica únicamente podrá admitir números y deberá mantener el siguiente formato de 10 caracteres, siempre respetando que el primer carácter sea un "dos", un "tres" o un "cuatro": 2/3/4TTTCCCCC, sin guiones ni espacios entre sí.

En general, la ERPN contará con una "Lista negra" que contemplará todas las casuísticas que podrán presentarse en cuanto a patrones irregulares que sean detectados por los operadores y que sean aprobados por el CTPN. Como ejemplos iniciales puede citarse: una cédula compuesta por 9 ceros (000000000), 9 unos (111111111), 9 dos (222222222), así sucesivamente. Un pasaporte que posea un único carácter (A, c, l, O,... entre otros). Cédulas jurídicas con patrones como (3000000000, 3111111111, entre otros)

Estas reglas se irán expandiendo conforme se vayan requiriendo. Para tales efectos, los patrones irregulares serán enviados por parte de los operadores al correo portabilidad@sutel.go.cr. En caso de no recibirse observaciones/comentarios por parte de los operadores en un plazo de 1 día hábil se tendrá por aceptado el nuevo patrón, el cual será comunicado al proveedor para su inclusión en la Lista Negra.

La ERPN eliminará espacios al inicio y al final de los campos de nombre y primer y segundo apellido en las gestiones que envían los operadores

1. El prestador receptor enviará a la ERPN un mensaje 2003 de consulta al operador donante de datos del abonado.
2. La ERPN realizará las siguientes validaciones para cada número de teléfono incluido en la consulta:
 - La línea existe
 - Existe un NIP vigente para el número y operador receptor y es el indicado en la consulta
 - El operador donante indicado en la consulta es correcto
 - La numeración no se encuentra ya portada al operador receptor
 - La línea no está involucrada en ningún trámite de portabilidad en curso



- Si es prepago, cumple con las validaciones de formato en el nombre y número de documento

Si la solicitud no es válida

1. La ERPN enviará al operador receptor un mensaje de respuesta 2090 indicando todos los números que no cumplen alguna validación y todas las causas de rechazo asociadas a cada número rechazado. El mensaje de rechazo deberá ser enviado dentro del plazo TR21 contado a partir de la recepción de la consulta

Si la solicitud es válida y no es prepago

1. La ERPN replicará la consulta al operador donante mediante el mensaje 2004 y activará el temporizador TR22. La réplica al operador donante deberá ser enviada dentro del plazo TR21 contado a partir de la recepción de la consulta
2. El operador donante deberá enviar la respuesta a la consulta de datos del abonado mediante el mensaje 2005

Si la solicitud es válida y es prepago

1. En caso de persona física con cédula o TIM, la ERPN validará primero en el TSE si la persona es menor de 12 años o ha fallecido. Si es persona física con tipo de documento DIMEX la ERPN realizará la validación en Migración y Extranjería
2. En caso contrario la ERPN consultará el tipo y número de documento en la plataforma de prepago de SUTEL

Si la persona es menor de 12 años o ha fallecido o no existe la cédula

1. La ERPN enviará al operador receptor un mensaje de respuesta 2090 indicando la causa de rechazo. El mensaje de rechazo deberá ser enviado dentro del plazo TR21 contado a partir de la recepción de la consulta

Si la persona es mayor de 12 años y no ha fallecido y existe la cédula

1. La ERPN consulta la titularidad en el TSE y valida nombre y primer apellido

Si la solicitud no supera las validaciones de titularidad contra el TSE

1. La ERPN enviará al operador receptor un mensaje de respuesta 2090 indicando la causa de rechazo. El mensaje de rechazo deberá ser enviado dentro del plazo TR21 contado a partir de la recepción de la consulta

Si la solicitud supera las validaciones de titularidad contra el TSE

1. La ERPN consultará el tipo y número de documento en la plataforma de prepago de SUTEL



Si los números no están registrados en la plataforma de SUTEL

1. La ERPN replicará la consulta al operador donante mediante el mensaje 2004 incluyendo el nombre y apellidos obtenidos del TSE (solo en caso de persona física con cédula o TIM) o de Migración y Extranjería (solo en caso de persona física con DIMEX) y activará el temporizador TR22 (ver Temporizadores del proceso). La réplica al operador donante deberá ser enviada dentro del plazo TR21 contado a partir de la recepción de la consulta
2. El operador donante deberá enviar la respuesta a la consulta de datos del abonado mediante el mensaje 2005

Si los números están registrados en la plataforma prepago de SUTEL

1. La ERPN validará que el tipo y número de documento de la consulta del receptor coincidan con los datos de prepago

Si la titularidad no coincide con los datos de la plataforma prepago de SUTEL

1. La ERPN enviará al operador receptor un mensaje de respuesta 2090 indicando la causa de rechazo y los datos de titularidad obtenidos de la plataforma prepago de SUTEL (tipo y número de documento en caso de pasaporte y nombre/razón social para cualquier tipo de documento). El mensaje de rechazo deberá ser enviado dentro del plazo TR21 contado a partir de la recepción de la consulta

Si la titularidad en SUTEL coincide con los datos de la consulta del receptor

1. La ERPN replicará la consulta al operador donante mediante el mensaje 2004 incluyendo el nombre y apellidos obtenidos del TSE (solo en caso de persona física con cédula o TIM) o de Migración y Extranjería (solo en caso de persona física con DIMEX) y activará el temporizador TR22. La réplica al operador donante deberá ser enviada dentro del plazo TR21 contado a partir de la recepción de la consulta
2. El operador donante deberá enviar la respuesta a la consulta de datos del abonado mediante el mensaje 2005

Si los servicios de consulta del donante de la plataforma prepago de SUTEL o del TSE no estuvieran disponibles

1. La ERPN replicará la consulta al operador donante mediante el mensaje 2004 con los datos del receptor y activará el temporizador TR22. La réplica al operador donante deberá ser enviada dentro del plazo TR21 contado a partir de la recepción de la consulta
2. El operador donante deberá enviar la respuesta a la consulta de datos del abonado mediante el mensaje 2005



Si el operador donante no responde en el plazo TR22

3. La ERPN desactivará el temporizador TR22 y enviará un mensaje 2006 al operador receptor indicando que no se ha recibido respuesta del operador donante
4. NOTA: en caso de existir una incidencia técnica en el operador donante, éste deberá notificar a la ERPN dicho inconveniente y deberá responder a través de la GUI de la ERPN siempre que sea posible.

Si el operador donante responde en el plazo TR22

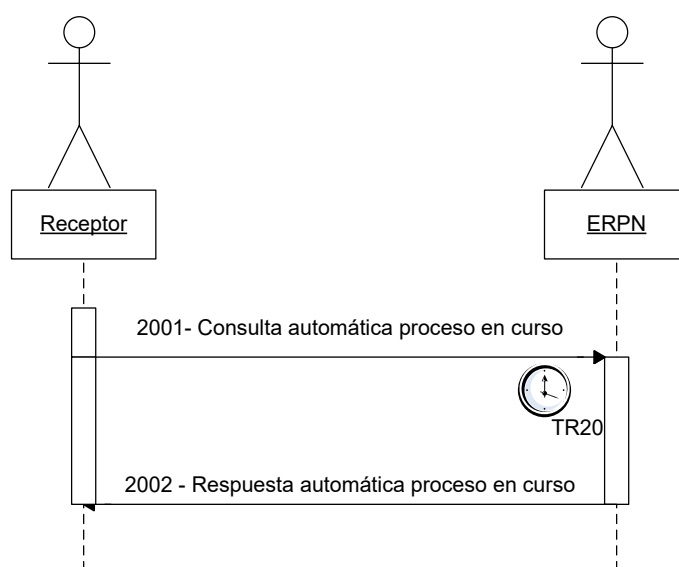
1. La ERPN desactivará el temporizador TR22 y replicará el mensaje 2006 al operador receptor indicando que se ha recibido respuesta del operador donante

Si alguno de los mensajes no puede entregarse al operador

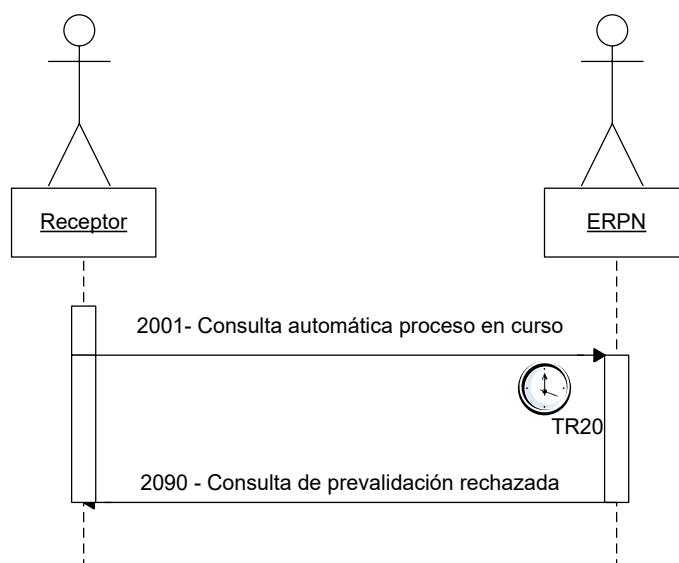
1. Ante un fallo en la entrega de los mensajes por problemas en la comunicación o porque el sistema del operador no esté disponible, la ERPN siempre reenviará X veces cada mensaje con un tiempo de espera entre reintentos y siempre dentro del plazo que se tiene para cumplir los SLAs. Si finalmente no consigue entregar el mensaje 2004 al operador donante o el 2006 al receptor, la ERPN generará y enviará un mensaje de error 9999 al prestador receptor indicando el error en la entrega del mensaje y cancelando el proceso .
2. El operador receptor podrá enviar de nuevo la consulta a la ERPN.

2.2.3 Diagramas de actividad

Consulta automática de proceso en curso

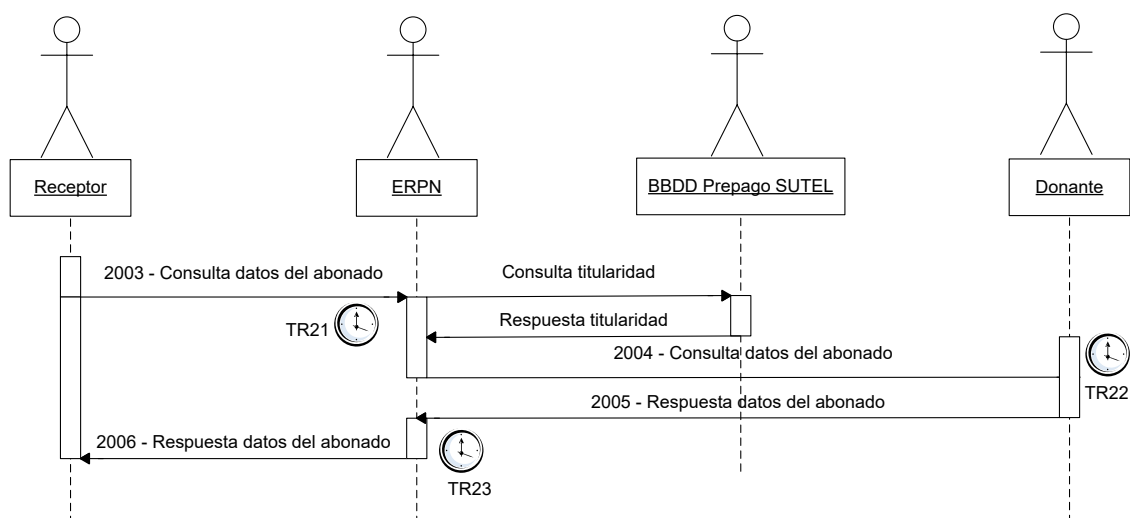


Flujo sin errores ni rechazos

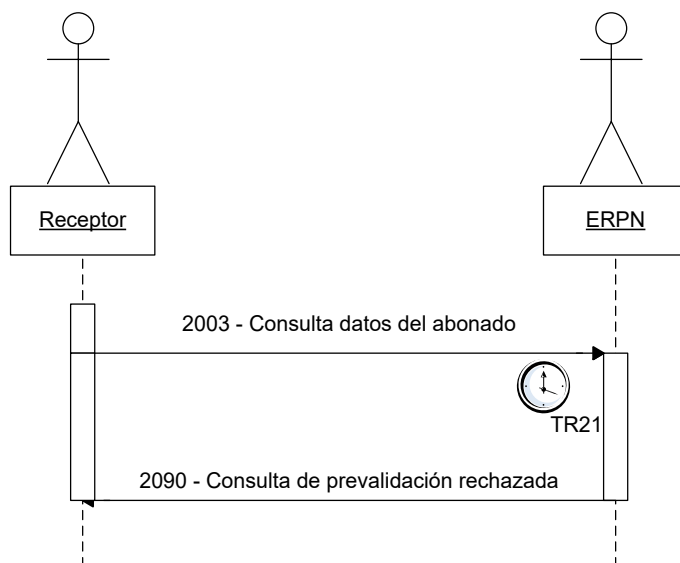


Flujo con rechazo de la ERP

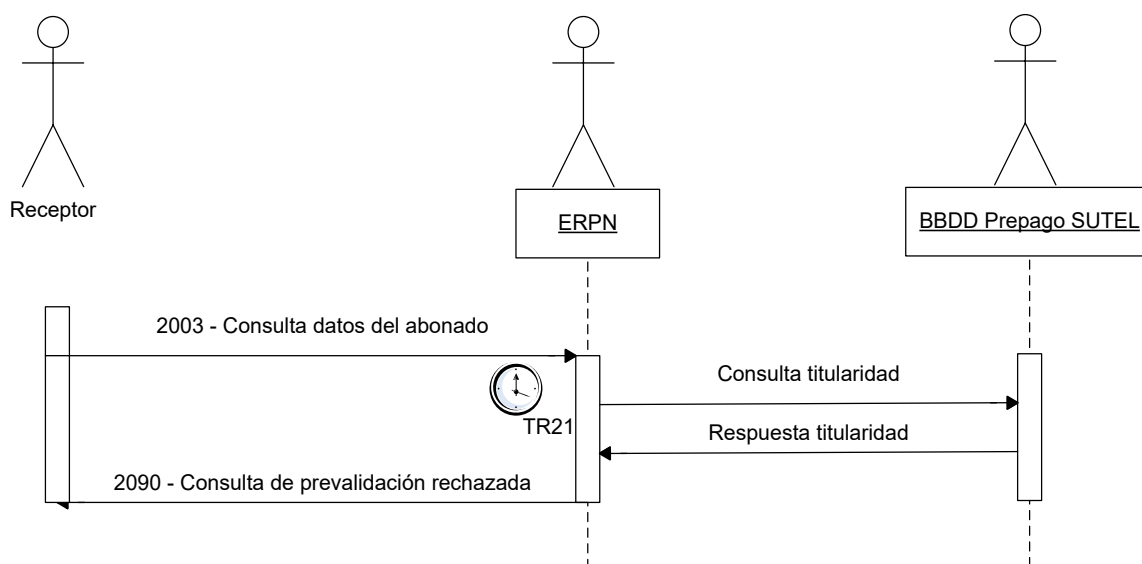
2.2.3.1 Consulta al operador donante de datos del abonado



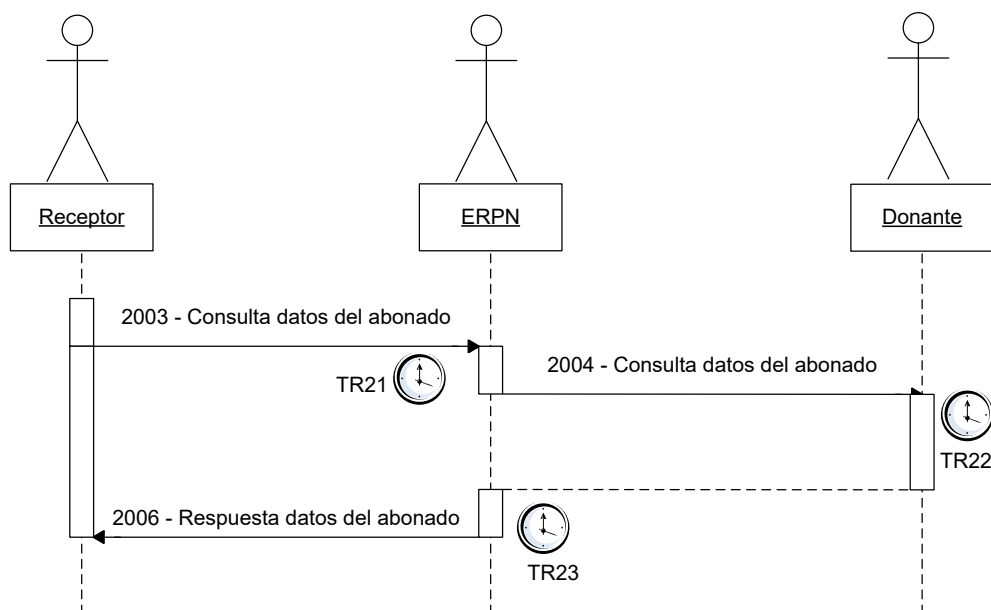
Flujo sin errores ni rechazos



Flujo con rechazo de la ERPN



Flujo con rechazo de la ERPN por titularidad incorrecta



Flujo sin respuesta del operador donante

2.3 Proceso 01 – Proceso de portabilidad

2.3.1 Descripción del proceso

El proceso de portabilidad es el proceso por el que el abonado titular de una numeración causa baja en el prestador que le provee el servicio (prestador donante) y solicita simultáneamente el alta del servicio en otro prestador (prestador receptor) conservando dicha numeración. A lo largo del documento este proceso también es denominado como Solicitud de Portabilidad.

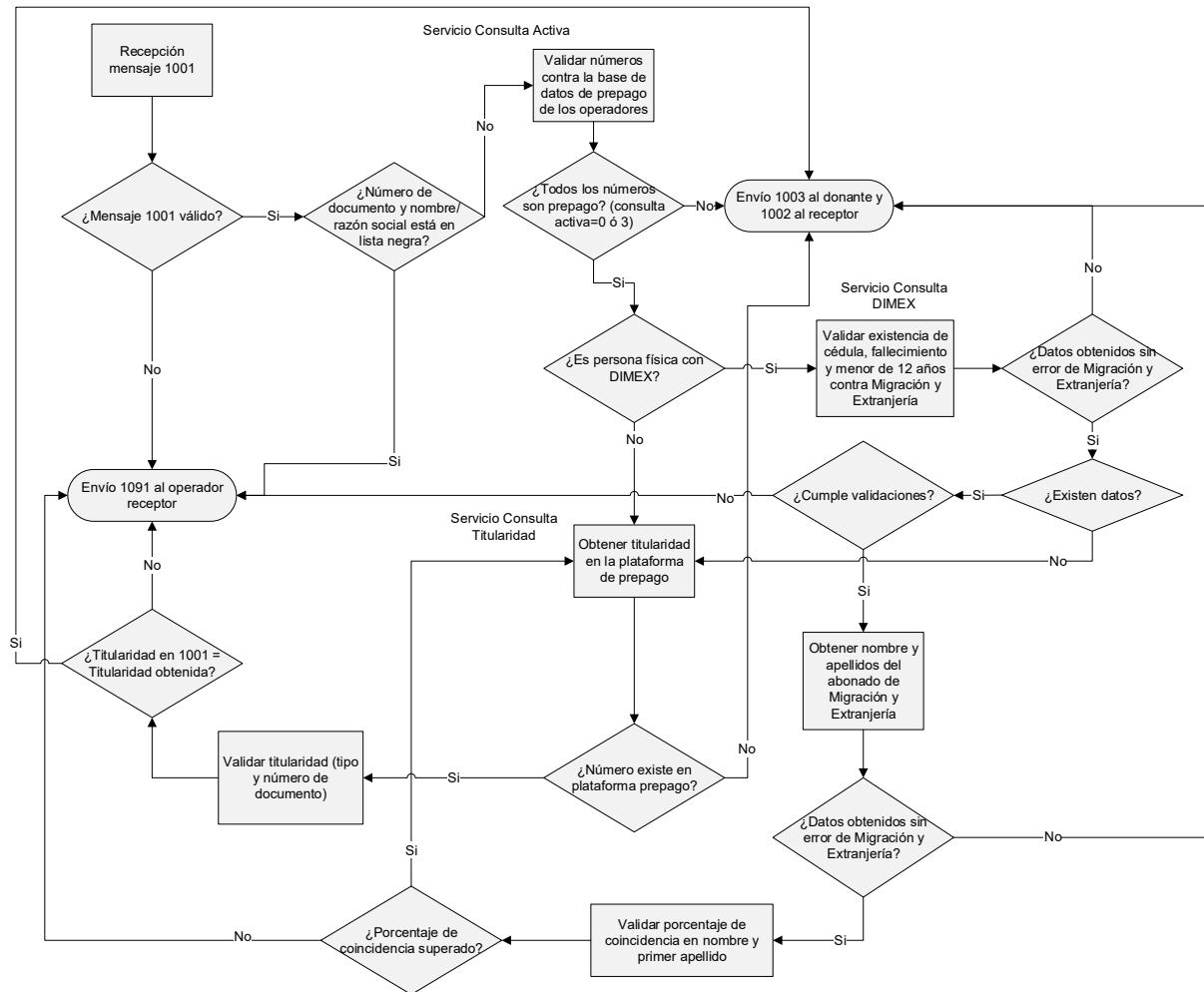
Si el prestador receptor de la numeración fuera el prestador donante inicial, es decir el propietario, una vez concluido el proceso de cambio dicha numeración tendrá, a todos los efectos, la consideración de numeración no portada, por lo cual la numeración será eliminada de la base de datos de números portados.

Se debe establecer para la portación una fecha programada que deberá ser conocida por todos los prestadores para realizar los cambios oportunos en la red. A esta fecha se la denomina Ventana de Cambio, y deberá ser una fecha aprobada por la ERPN y que cumpla con los plazos definidos.

La solicitud deberá incluir un número único de proceso que generará el receptor y que identificará a todos los mensajes asociados al proceso.

En el caso de trámites de portaciones múltiples, tanto la ERPN como el operador o proveedor receptor y el operador o proveedor donante, gestionarán la portación de cada número del conjunto como individual, de manera que se deberá verificar el rechazo o aprobación para cada número a ser portado de conformidad con las razones de rechazo justificadas indicadas en el pliego de condiciones y en el presente documento. De esta forma, rechazos

Flujo para DIMEX



Se debe tener en cuenta que la validación de titularidad en la ERPN se basa en las siguientes premisas:

Personas físicas:

- campos de nombre y/o apellidos no estén vacíos, contengan caracteres numéricos, caracteres especiales o secuencias de caracteres que no correspondan a un nombre (Ejemplos: NO-PER; A!\$4%2#2%).
- campos de número de identificación que cumplan con lo siguiente:
 - Cédula de identidad para adulto únicamente números y con 9 dígitos sin guiones ni espacios entre sí.
 - Documento TIM para menores, únicamente con números y con 9 dígitos sin guiones ni espacios entre sí.
 - Cédula de residencia DIMEX únicamente con números y con 12 dígitos sin guiones ni espacios entre sí.



- Pasaporte: deberá poseer longitud variable de máximo 20 caracteres, de carácter alfanumérico y no permitirá el uso de caracteres especiales

Personas jurídicas:

- a. el campo de nombre o razón social podrá aceptar caracteres alfanuméricos y especiales (es el único caso que acepta la introducción de caracteres especiales (¡"#\$%&=+?))
- b. El campo de cédula jurídica únicamente podrá admitir números y deberá mantener el siguiente formato de 10 caracteres, siempre respetando que el primer carácter sea un "dos", un "tres" o un "cuatro": 2/3/4TTTCCCCC, sin guiones ni espacios entre sí.

En general, la ERPN contará con una "Lista negra" que contemplará todas las casuísticas que podrán presentarse en cuanto a patrones irregulares que sean detectados por los operadores y que sean aprobados por el CTPN. Como ejemplos iniciales puede citarse: una cédula compuesta por 9 ceros (000000000), 9 unos (111111111), 9 dos (222222222), así sucesivamente. Un pasaporte que posea un único carácter (A, c, l, O,... entre otros). Cédulas jurídicas con patrones como (3000000000, 3111111111, entre otros)

Estas reglas se irán expandiendo conforme se vayan requiriendo. Para tales efectos, los patrones irregulares serán enviados por parte de los operadores al correo portabilidad@sutel.go.cr. En caso de no recibirse observaciones/comentarios por parte de los operadores en un plazo de 1 día hábil se tendrá por aceptado el nuevo patrón, el cual será comunicado a INETUM para su inclusión en la Lista Negra

La ERPN eliminará espacios al inicio y al final de los campos de nombre y primer y segundo apellido en las gestiones que envían los operadores

1. El prestador receptor enviará a la ERPN un mensaje 1001 de solicitud de portabilidad indicando los datos requeridos.
2. La ERPN realizará las siguientes validaciones a la solicitud para cada una de las líneas incluidas en la solicitud:
 - La línea existe
 - La numeración no se encuentra ya portada al operador receptor
 - La línea no está involucrada en ningún trámite de portabilidad ni de repatriación
 - Existe un NIP vigente para el número y operador receptor y es el indicado en la solicitud de portabilidad
 - La solicitud contiene los datos necesarios en función del tipo de usuario y servicio
 - El operador donante indicado en la solicitud es el correcto



- No existen líneas duplicadas en la solicitud
- Si es prepago, cumple con las validaciones de formato en el nombre y número de documento

Si la solicitud no es válida

1. La ERPN enviará un mensaje 1091 al prestador receptor indicando todas las numeraciones rechazadas y sus causas de rechazo
2. La ERPN cerrará el proceso de portabilidad y el receptor deberá iniciar otro nuevo proceso subsanando las causas de rechazo

Si la solicitud es válida y no es prepago

1. La ERPN enviará un mensaje 1002 al operador receptor y replicará la solicitud al operador donante mediante un mensaje 1003
2. El prestador donante deberá validar los datos del mensaje 1003 y enviar una respuesta de aceptación o rechazo en el mensaje 1004 dentro del plazo establecido

Si la solicitud es válida y es prepago

1. En caso de persona física con cédula, DIMEX o TIM, la ERPN validará primero en el TSE si la persona es menor de 12 años o ha fallecido
2. En caso contrario la ERPN consultará el tipo y número de documento en la plataforma de prepago de SUTEL

Si la persona es menor de 12 años o ha fallecido o no existe la cédula

1. La ERPN enviará al operador receptor un mensaje de respuesta 1091 indicando la causa de rechazo.

Si la persona es mayor de 12 años y no ha fallecido y existe la cédula

1. La ERPN consulta la titularidad en el TSE/Extranjería (Ver apartado Anexo V. Servicios de integración con registro de prepago y TSE/Extranjería) y valida nombre y primer apellido

Si la solicitud no supera las validaciones de titularidad contra el TSE/Extranjería

1. La ERPN enviará al operador receptor un mensaje de respuesta 1091 indicando la causa de rechazo. En caso de DIMEX, si no existe en la base de datos de extranjería se consulta el tipo y número de documento en la plataforma de prepago de SUTEL

Si la solicitud supera las validaciones de titularidad contra el TSE/Extranjería

1. La ERPN consultará el tipo y número de documento en la plataforma de prepago de



SUTEL

Si los números no están registrados en la plataforma de SUTEL

1. La ERPN enviará un mensaje 1002 al prestador receptor indicando que todas las validaciones fueron superadas con éxito, añadiendo a dicho mensaje el campo de fecha de ventana calculada de forma automática dentro del plazo máximo de portación
2. La ERPN replicará la solicitud al operador donante mediante un mensaje 1003 incluyendo el nombre y apellidos obtenidos del TSE (solo en caso de persona física con cédula, DIMEX o TIM)
3. El prestador donante deberá validar los datos del mensaje 1003 y enviar una respuesta de aceptación o rechazo en el mensaje 1004 dentro del plazo establecido.

Si los números están registrados en la plataforma prepago de SUTEL

1. La ERPN validará que el tipo y número de documento de la solicitud del receptor coincidan con los datos de prepago

Si las validaciones de titularidad contra prepago no son superadas

1. La ERPN enviará al operador receptor un mensaje de respuesta 1091 indicando la causa de rechazo.
2. La ERPN cerrará el proceso de portabilidad y el receptor deberá iniciar otro nuevo proceso subsanando las causas de rechazo

Si las validaciones de titularidad contra prepago son superadas

1. La ERPN enviará un mensaje 1002 al prestador receptor indicando que todas las validaciones fueron superadas con éxito, añadiendo a dicho mensaje el campo de fecha de ventana calculada de forma automática dentro del plazo máximo de portación
2. La ERPN replicará la solicitud al operador donante mediante un mensaje 1003 incluyendo el nombre y apellidos obtenidos del TSE (solo en caso de persona física con cédula, DIMEX o TIM)
3. El prestador donante deberá validar los datos del mensaje 1003 y enviar una respuesta de aceptación o rechazo en el mensaje 1004 dentro del plazo establecido

Si los servicios de consulta del donante, de la plataforma prepago de SUTEL o del TSE/Extranjería no estuvieran disponibles

1. La ERPN enviará un mensaje 1002 al prestador receptor indicando que todas las validaciones fueron superadas con éxito, añadiendo a dicho mensaje el campo de fecha de ventana calculada de forma automática dentro del plazo máximo de portación



2. La ERPN replicará la solicitud al operador donante mediante un mensaje 1003
3. El prestador donante deberá validar los datos del mensaje 1003 y enviar una respuesta de aceptación o rechazo en el mensaje 1004 dentro del plazo establecido

Si la respuesta del operador donante es de aceptación

1. La ERPN generará y enviará al operador donante y receptor un mensaje 1005 indicando que la numeración se encuentra lista para ser programada la ventana de cambio
2. El operador receptor podrá opcionalmente reprogramar la ventana de cambio mediante el mensaje 1006 dentro del plazo TR14. Si el receptor no enviara la programación dentro del plazo definido para ello, la ventana de cambio programada será la contenida en el mensaje 1002.
3. La ERPN incluirá la numeración en el fichero de portabilidades diarias del día de la ventana de cambio
4. La ERPN enviará a receptor y operador donante un mensaje de confirmación 1007 con la ventana de cambio programada final
5. La ERPN programará la actualización de la base de datos de números portados durante la ventana de cambio

Si el operador donante envía respuesta de rechazo

1. La ERPN enviará el mensaje 1092 al prestador receptor y al prestador donante indicando todas las numeraciones rechazadas con sus correspondientes causas de rechazo.
2. La ERPN cerrará el proceso de portabilidad para las numeraciones rechazadas. Si algunas numeraciones son aceptadas o no rechazadas se continuará con el proceso de portación para las mismas con el mensaje 1005 hacia receptor y donante

Si el operador donante no envía la respuesta en el plazo estipulado

1. La ERPN generará y enviará al operador donante y receptor un mensaje 1005 indicando que la numeración se encuentra lista para ser programada la ventana de cambio
2. El operador receptor podrá opcionalmente reprogramar la ventana de cambio mediante el mensaje 1006 dentro del plazo TR14. Si el receptor no enviara la programación dentro del plazo definido para ello, la ventana de cambio programada será la contenida en el mensaje 1002.
3. La ERPN incluirá la numeración en el fichero de portabilidades diarias del día de la ventana de cambio



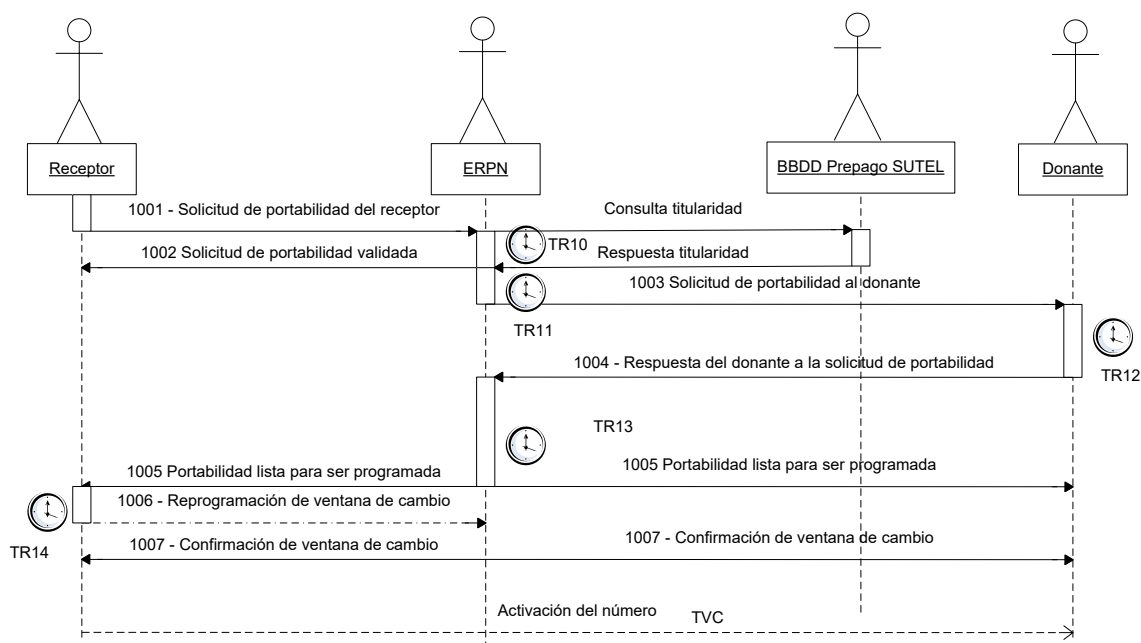
4. La ERPN enviará a receptor y donante un mensaje de confirmación 1007 con la ventana de cambio programada final
5. La ERPN programará la actualización de la base de datos de números portados durante la ventana de cambio

Si La ERPN no consigue entregar algún mensaje al operador por fallo en la comunicación o sistema de operador no disponible

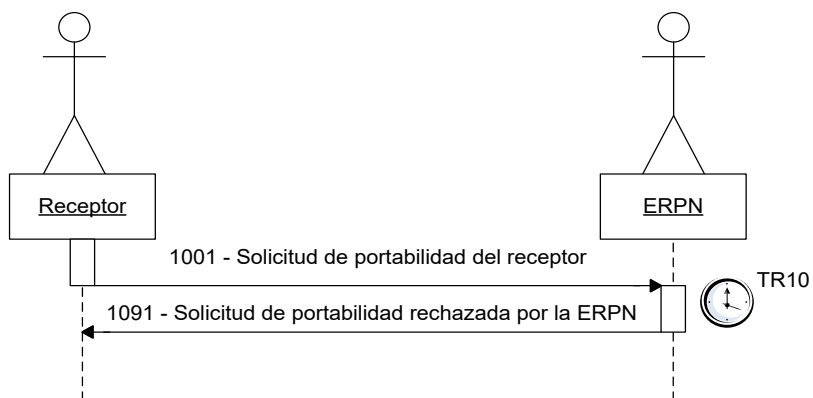
1. La ERPN ante un fallo de entrega de mensaje siempre reintentará X veces (configurable) el envío de dicho mensaje. Si finalmente no consigue entregar dicho mensaje se generará un mensaje de error por fallo de entrega 9999 el cual enviará a ambos operadores, pero el proceso no será cancelado (ver apartado 5.7 Subproceso de error detectado por la ERPN)
2. Un operador que no reciba en los tiempos establecidos el mensaje de la ERPN deberá cerrar el proceso para iniciar uno nuevo.
3. Si la ERPN no puede entregar el mensaje de solicitud de portabilidad lista para ser programada (mensaje 1005) o cualquier mensaje posterior al mismo, se continuará con el proceso de portación.

2.3.3 Diagramas de actividad

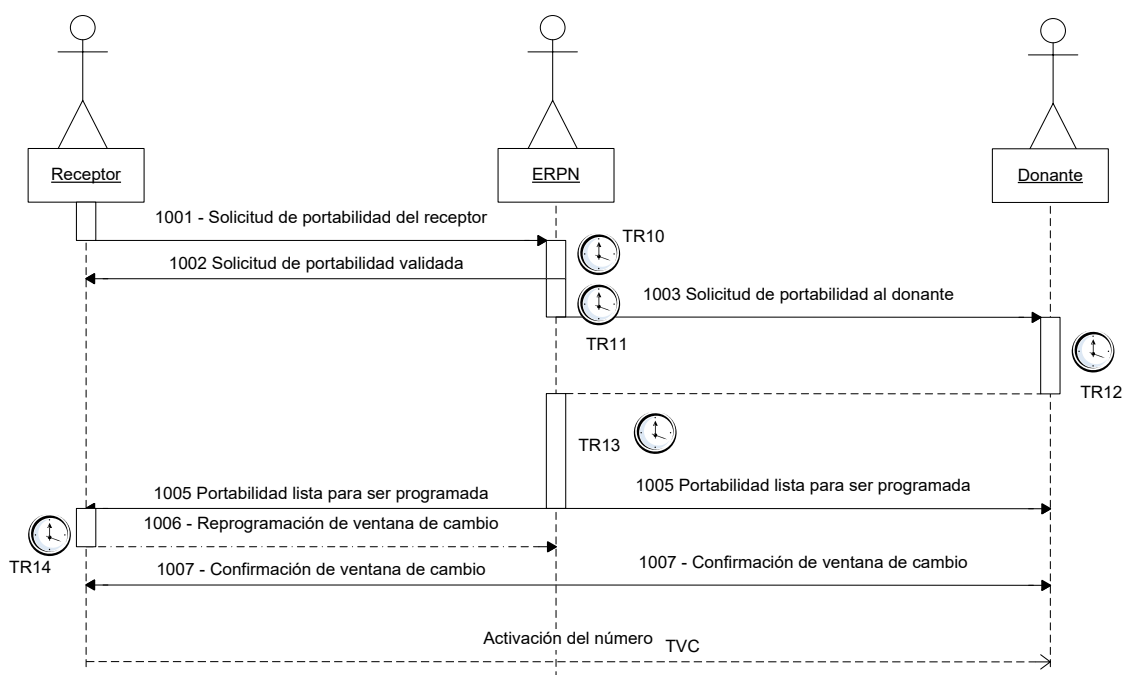
A continuación, se muestran los diagramas de actividad del proceso de solicitud de portabilidad.



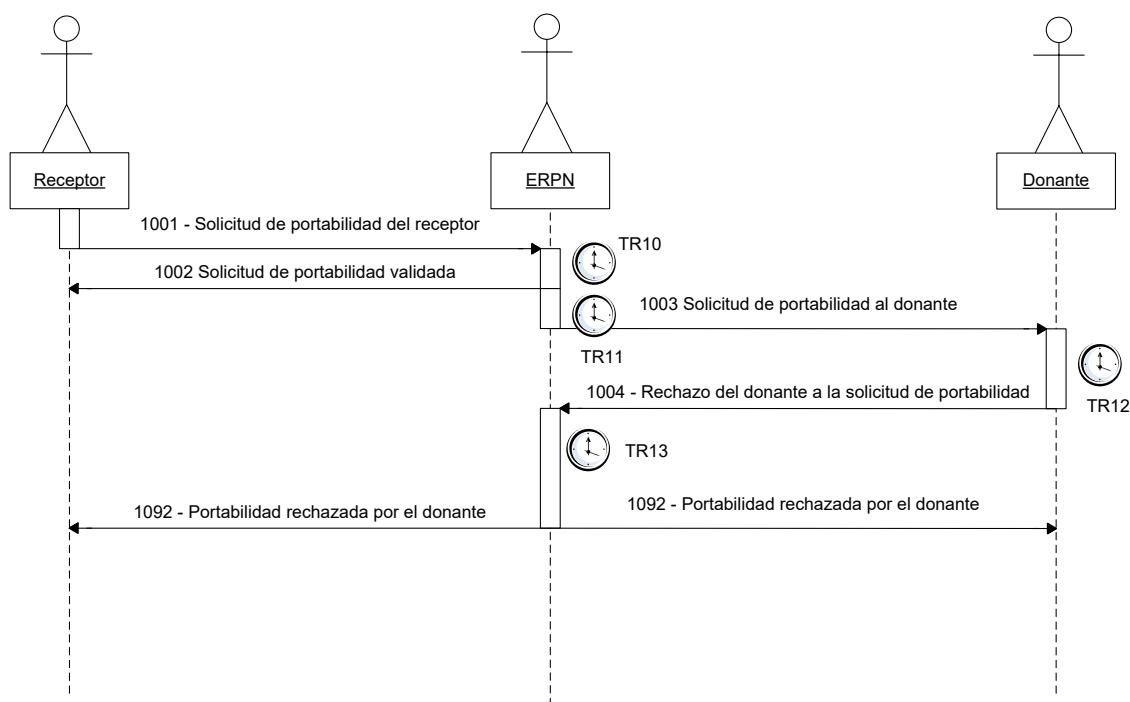
Flujo sin errores ni rechazos



Flujo con rechazo de la ERPN



Flujo sin respuesta del operador donante



Flujo con rechazo del operador donante

2.4 Proceso 03 – Proceso de cancelación de portabilidad

2.4.1 Descripción del proceso

Es el proceso mediante el cual se cancela una solicitud de portación que haya sido aceptada por el operador o proveedor donante y que aún esté pendiente de activación.

La cancelación podrá ser llevada a cabo bien por la SUTEL por razones de interés público o bien por el receptor cuando éste cuente con el consentimiento expreso del usuario a desistir del trámite.

La solicitud de cancelación permitirá adjuntar evidencia documental, en el caso de ser iniciada por el receptor el documento adjunto será obligatorio. Para la nomenclatura de los documentos de soporte que han de adjuntarse se seguirá el siguiente formato:

OOOOYYYYMMDDHHCCNNNNN.xxx donde:

OOOOYYYYMMDDHHCCNNNNN será el identificador de proceso asociado al mensaje que contiene los documentos adjuntos.

Los valores permitidos para xxx serán los siguientes: **jpg, jpeg, txt, tiff, pdf, gif y png**.

Se permitirá un máximo de 5 Mb para el documento adjunto.

2.4.2 Interacción de mensajes

1. La SUTEL/receptor enviará a la ERPN un mensaje 3001 de solicitud de cancelación de portabilidad indicando los datos requeridos.



2. La ERPN realizará las siguientes validaciones sobre la solicitud:
 - La portabilidad es cancelable, es decir, ya se encuentra aceptada y pendiente de la ejecución de la ventana de cambio

Si la solicitud no es válida

1. La ERPN enviará a la SUTEL/receptor un mensaje de rechazo de cancelación 3090 indicando la causa de rechazo

Si la solicitud es válida

1. La ERPN renvía el mensaje de solicitud de cancelación 3002 al operador donante
2. El operador donante envía un mensaje de respuesta de cancelación 3003 a la ERPN en el plazo establecido
3. La ERPN replica el mensaje 3004 de respuesta a la SUTEL y al operador receptor y cancela proceso de portabilidad dejando la numeración en su estado anterior

Si el operador donante no responde en plazo

1. La ERPN genera el mensaje de respuesta 3004 y lo envía a la SUTEL y a los operadores donante y receptor
2. La ERPN cancela proceso de portabilidad dejando la numeración en su estado anterior

Si la ERPN no consigue entregar algún mensaje por fallo en la comunicación o sistema del destinatario no disponible

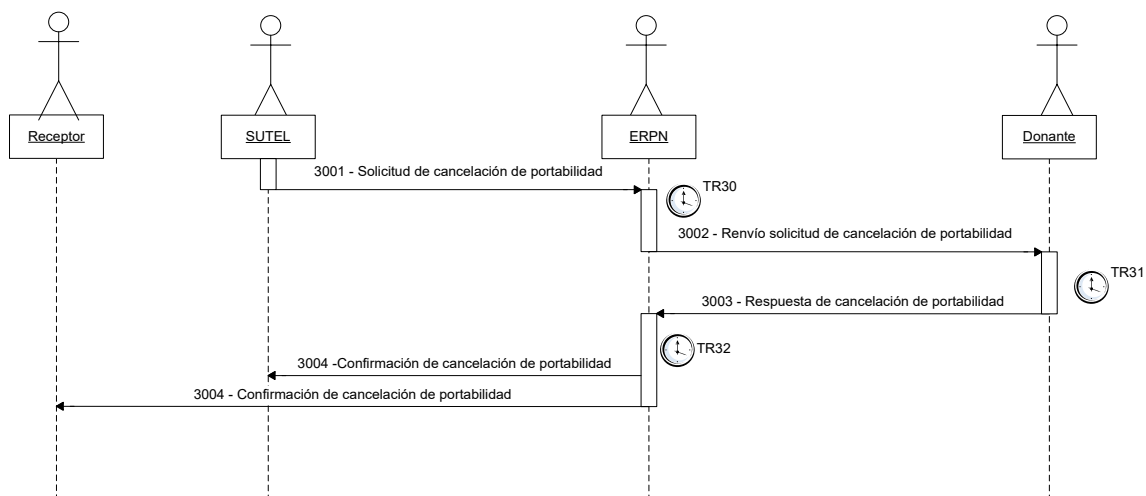
1. Ante un fallo en la entrega de los mensajes por problemas en la comunicación o porque el sistema del operador/SUTEL no esté disponible, la ERPN siempre renviará X veces cada mensaje con un tiempo de espera entre reintentos y siempre dentro del plazo que se tiene para cumplir los SLAs. Si finalmente no consigue entregar el mensaje 3004 a la SUTEL/operadores, la ERPN generará y enviará un mensaje de error 9999 a la SUTEL y a los operadores receptor y donante indicando el error en la entrega del mensaje y cancelando el proceso (ver apartado 5.7 Subproceso de error detectado por la ERPN)
2. La SUTEL/receptor deberá volver a enviar la solicitud de cancelación a la ERPN.

2.4.3 Diagramas de actividad

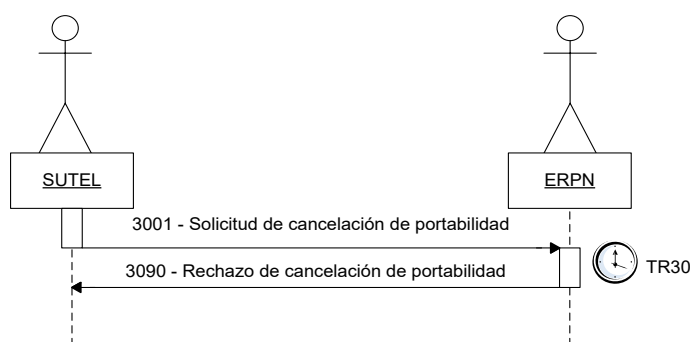
A continuación, se muestran los diagramas de actividad del proceso de cancelación de portabilidad.



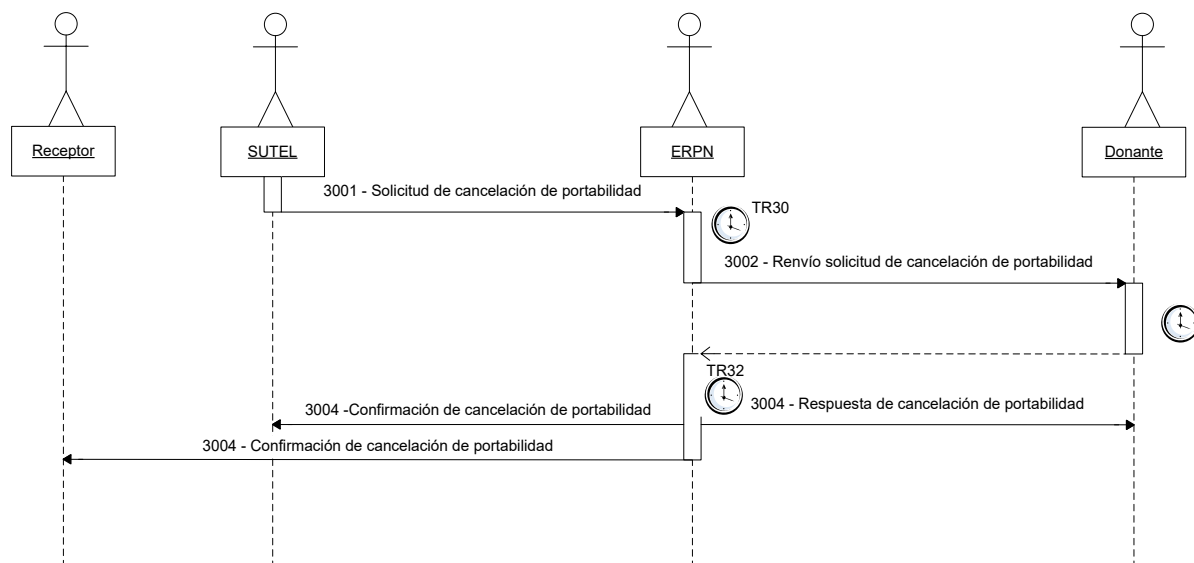
Cancelación iniciada por la SUTEL



Flujo sin errores ni rechazos



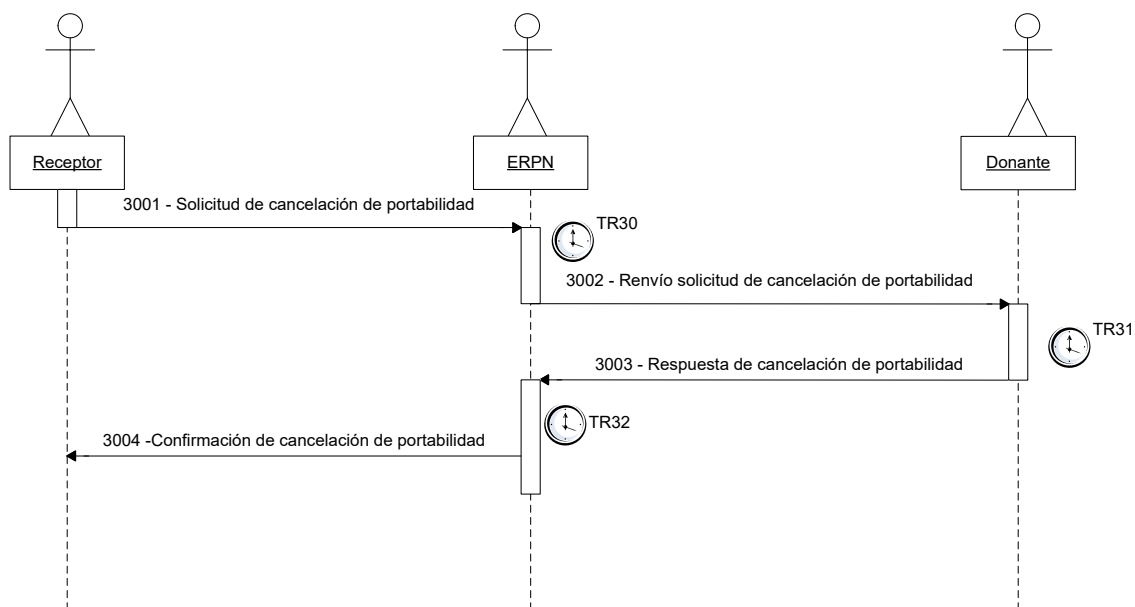
Flujo con rechazo de la ERPN



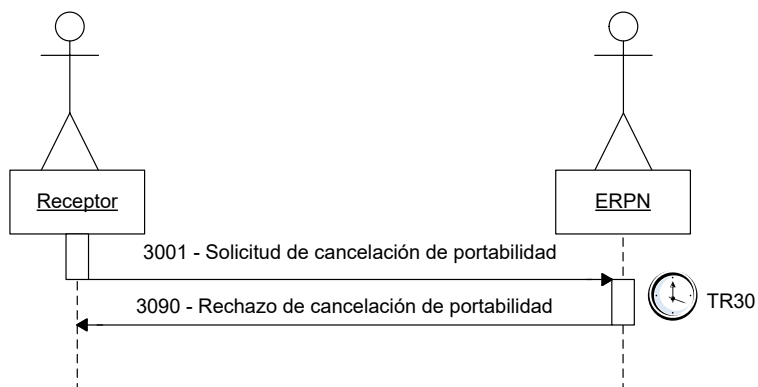
Flujo sin respuesta del operador donante



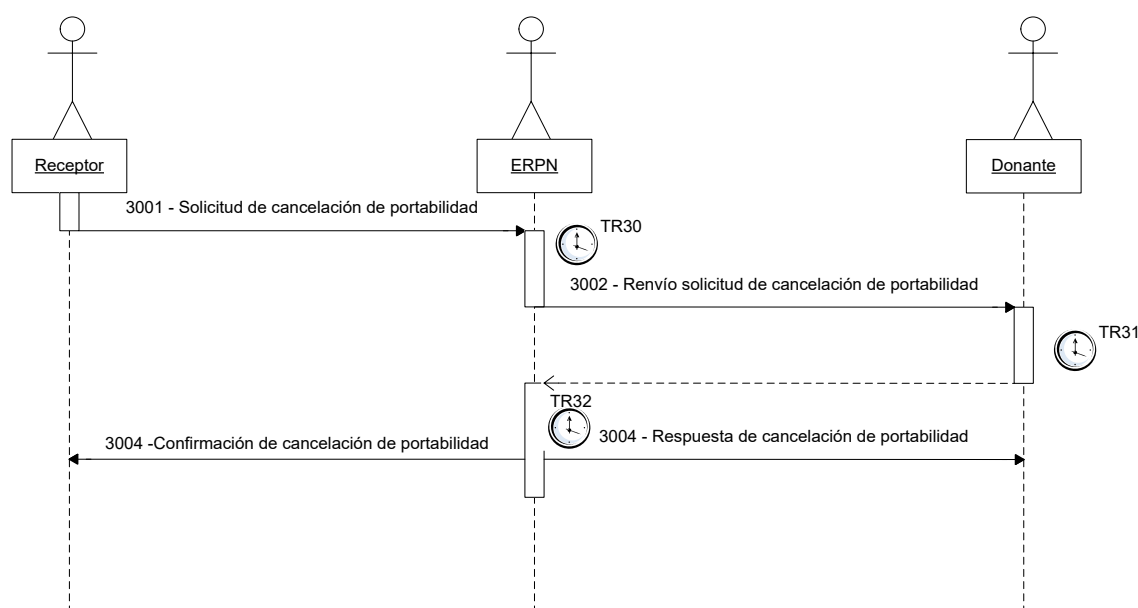
Cancelación iniciada por el receptor



Flujo sin errores ni rechazos



Flujo con rechazo de la ERP



Flujo sin respuesta del operador donante

2.5 Proceso 04 – Proceso de repatriación

2.5.1 Descripción del proceso

Este proceso permite a un usuario que ha sido portado finalizar su relación contractual con el operador o proveedor donde el número portado esté activo (último operador o proveedor receptor), o que dichos servicios sean finalizados por causas fortuitas (muerte del suscriptor) o debido a la liquidación o suspensión definitiva del servicio por falta de pago. Para tales efectos, el operador o proveedor donde el número portado esté activo deberá generar una solicitud de repatriación de número hacia la ERPN.

Una vez finalizado el proceso con éxito, la numeración pasará al operador asignatario de la misma.

Para tales efectos, el operador o proveedor donde el número portado esté activo deberá generar una solicitud de repatriación de número hacia Portaflow.

Portaflow validará la solicitud del operador o proveedor receptor, posteriormente identificará el proveedor que originalmente era poseedor del recurso numérico asignado y por último devolverá ese número a dicho operador o proveedor

2.5.2 Interacción de mensajes

1. El prestador receptor enviará a la ERPN un mensaje 4001 de solicitud de repatriación que contenga los números a retornar
2. La ERPN validará cada uno de los números contenidos en el mensaje:
 - El número indicado existe y pertenece a algún operador
 - El número no se encuentra en trámite de portabilidad



- El operador solicitante es el último operador receptor del número
- El número se encuentra portado

Si algún número no es válido

1. La ERPN enviará al receptor un mensaje 4090 de rechazo que contenga los números rechazados y las causas de rechazo correspondientes a cada uno de ellos

Si los números son válidos

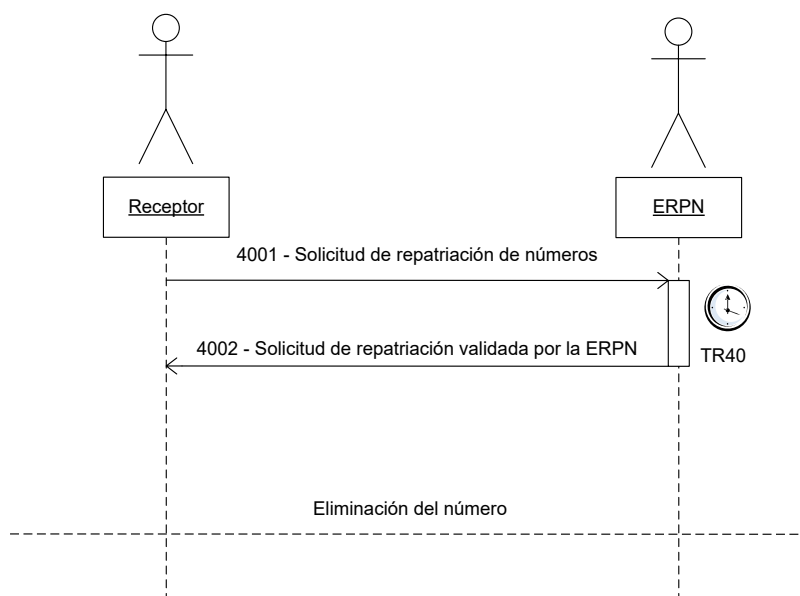
1. La ERPN generará un mensaje 4002 de respuesta para el receptor que contenga los números válidos
2. La ERPN incluirá esas numeraciones en el fichero de números repatriado para la ventana hábil más próxima
3. La ERPN programará la eliminación de los números de la base de datos de números portados durante la ventana de repatriación

Si la ERPN no consigue entregar el mensaje de confirmación por fallo en la comunicación o sistema del destinatario no disponible

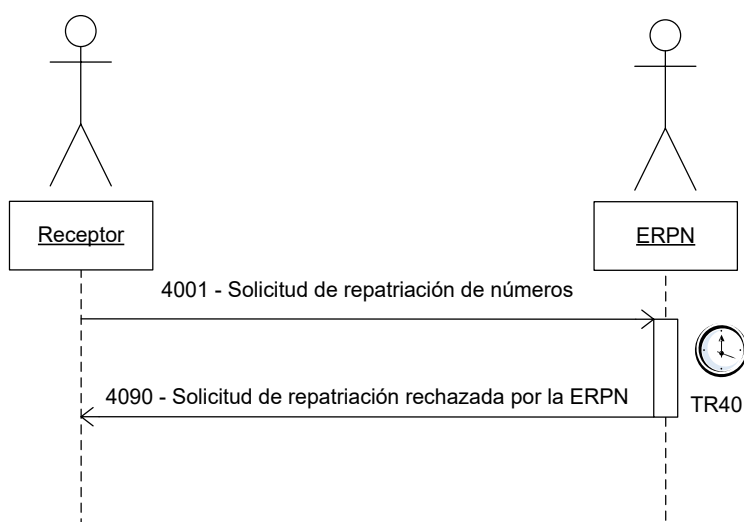
1. Ante un fallo en la entrega de los mensajes por problemas en la comunicación o porque el sistema del operador no esté disponible, la ERPN siempre reenviará X veces cada mensaje con un tiempo de espera entre reintentos y siempre dentro del plazo que se tiene para cumplir los SLAs. Si finalmente no consigue entregar el mensaje 4002 al receptor, la ERPN continuará con el proceso de repatriación incluyendo las numeraciones validadas en el fichero de números repatriados y activará la programación de la ventana de repatriación

2.5.3 Diagramas de actividad

A continuación, se muestran los diagramas de actividad del proceso de repatriación de número al operador asignatario.



Flujo sin errores ni rechazos



Flujo con rechazo de la ERPN

2.6 Proceso 05 – Proceso de sincronización con la ERPN

2.6.1 Descripción del proceso

El subproceso especial de sincronización con la ERPN será invocado cuando un operador necesite sincronizar su base de datos operativa con la base de datos administrativa, por razones diferentes a la actualización regular de nuevos números portados y de números portados cancelados. Esto se puede llevar a cabo de dos formas:

- Descarga completa de la base de datos.
- Descarga incremental de la base de datos.

Típicamente se requiere una descarga completa cuando se trata de un nuevo proveedor



de redes y servicios.

Una descarga incremental se requerirá cuando la base de datos operativa de un proveedor sale de operación y necesita recuperar la información perdida.

En función del tipo de sincronización, la información contenida en los ficheros será:

- Descarga completa: contiene todos los números que se encuentran actualmente portados en la NP-DB
- Descarga incremental: contiene todas las numeraciones portadas en un intervalo de fechas en la ERPN y que actualmente siguen portadas

La generación del fichero comenzará a la finalización de la jornada laboral, es decir a las 24:00 horas, y quedará disponible a las 02:00 horas para ser descargado por el operador. Si un operador requiriese de forma urgente el contenido de la base de datos de números portados, deberá solicitarlo a la mesa de ayuda mediante la apertura de una incidencia.

Los archivos se mantendrán a disposición de los operadores un número N configurable de días que en inicio será 10.

2.6.2 Interacción de mensajes

1. Prestador envía mensaje 5001 indicando tipo de sincronización (incremental o completa)
2. La ERPN realizará las siguientes validaciones a la solicitud:
 - Si el tipo es Completa los campos de Fecha Inicio y Fecha Fin deberán estar vacíos
 - Si el tipo es Incremental los campos de Fecha Inicio y Fecha Fin deberán estar completados
 - Si el tipo es Incremental el valor de **Fecha Inicio** debe ser menor que el valor de **Fecha Fin**

Si la solicitud no es válida

1. La ERPN enviará al operador receptor un mensaje de respuesta 5090 indicando rechazo y la causa del mismo.
2. La ERPN cerrará el proceso de sincronización

Si la solicitud es válida

1. La ERPN generará un fichero cuyo contenido será la información de numeraciones solicitadas por el prestador
2. Una vez finalizado el fichero, la ERPN enviará el mensaje de respuesta 5002 indicando aceptación y la ruta donde se encuentra el fichero generado
3. El prestador se descargará el fichero por SFTP y actualizará su base de datos local.

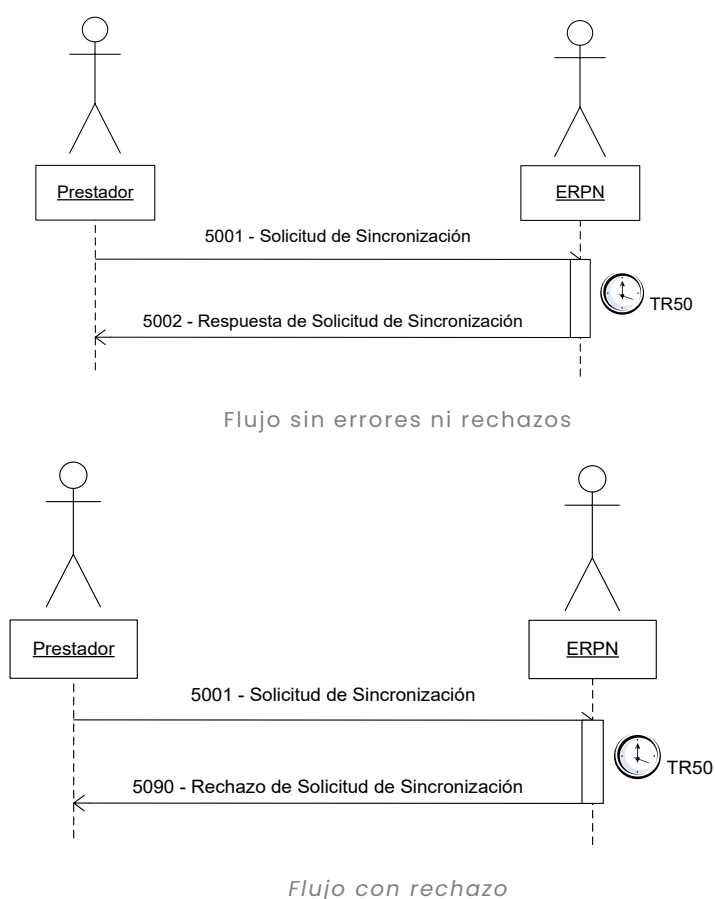


Si La ERPN no consigue entregar algún mensaje al operador por fallo en la comunicación o sistema de operador no disponible

1. La ERPN ante un fallo de entrega de mensaje siempre reintentará X veces (configurable) el envío de dicho mensaje. Si finalmente no consigue entregar dicho mensaje se generará un mensaje de error por fallo de entrega 9999 el cual enviará a ambos operadores para la cancelación del proceso.
2. Un operador que no reciba en los tiempos establecidos el mensaje de la ERPN deberá cerrar el proceso para iniciar uno nuevo.

2.6.3 Diagramas de actividad

A continuación, se muestran los diagramas de actividad del proceso de sincronización con la ERPN.



2.7 Subproceso de error detectado por la ERPN

2.7.1 Descripción del proceso

Cuando exista un proceso en curso, del tipo que sea, la ERPN puede detectar que existe un error debido a distintas causas, como puede ser un mensaje fuera de secuencia, error en el contenido de los mensajes, etc.



En este caso, la ERPN iniciará el proceso de error detectado, el cual consiste en notificar a los prestadores implicados en el proceso dicho error y su causa, lo que implica:

- Renvío del mensaje que provocó el error en caso de que el error tenga su origen en el mensaje enviado por el operador
- Cancelación del proceso, en caso de que el error sea producido en el sistema de la ERPN (causa ERROR00000) y no sea enviando un mensaje 0002, 0004, 1002, 1003, 1005, 1007 o 4002 o tratando un mensaje 1006 o 1004
- Notificación de un error de tratamiento o envío de mensaje (causa ERROR00000) que no cancela el proceso, si no que continúa el flujo con el siguiente mensaje, esto es, enviando un mensaje 0002, 0004, 1002, 1005, 1007 o 4002 o tratando un mensaje 1006 o 1004

La ERPN usará este mensaje de error para solicitar el envío de mensajes erróneos sólo para aquellos que no inician proceso, es decir:

- Proceso de solicitud de generación y envío de NIP: mensaje 0003
- Proceso de consultas de prevalidación: mensaje 2005
- Proceso de solicitud de portabilidad: mensajes 1004, 1006
- Proceso de cancelación de portabilidad: mensaje 3003

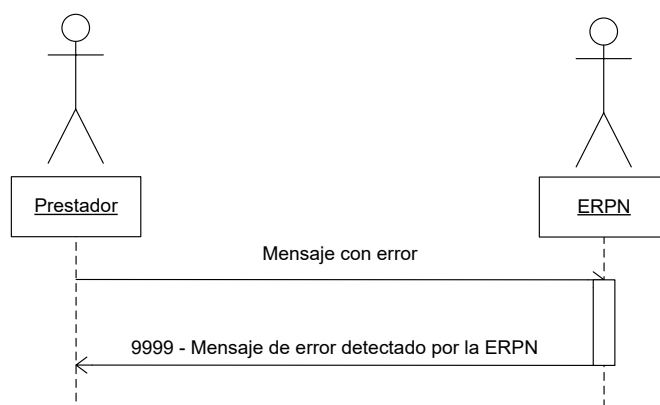
Para los mensajes que inician proceso se usará el correspondiente mensaje de cancelación por validaciones (0090, 2090, 1091, 2091, 3090, etc.).

2.7.2 Interacción de mensajes

1. El operador envía un mensaje con error a la ERPN
2. La ERPN detecta el error y envía un mensaje 9999 indicando la/s causa/s al operador que envió el mensaje erróneo

2.7.3 Diagramas de actividad

A continuación, se muestran los diagramas de actividad del proceso de error detectado por la ERPN.



Flujo de notificación de error

3 Requerimientos No-Funcionales

3.1 Alta Disponibilidad

Dado que la aplicación será desplegada en un entorno de **Oracle Cloud Infrastructure (OCI)**, utilizando **Oracle Kubernetes Engine (OKE)** sobre **OCI Compute Worker Nodes**, INETUM garantiza la continuidad de los servicios necesarios para la correcta implementación y operación de la solución de portabilidad, alineándose con los requisitos de alta disponibilidad y niveles de servicio comprometidos.

Con el objetivo de minimizar los riesgos que puedan afectar a la continuidad operativa, la **Portaflow 3.0** se apoya en una **arquitectura orientada a microservicios**, principio ya aplicado por INETUM en sistemas de misión crítica de portabilidad, donde la disponibilidad continua del servicio es un requisito esencial.

La adopción de **Kubernetes** como plataforma de orquestación permite:

- **Desacoplar** funcionalmente los componentes de la solución, desplegando cada servicio de negocio como un microservicio independiente.
- **Aislar fallos:** una incidencia en un microservicio no impacta en el resto de la plataforma, reduciendo el riesgo de indisponibilidad global.
- **Escalabilidad horizontal nativa**, permitiendo incrementar o reducir dinámicamente el número de instancias de cada microservicio en función de la carga de trabajo, principio alineado con los modelos de escalabilidad horizontal descritos en las propuestas técnicas de INETUM.
- **Actualizaciones sin interrupción del servicio**, mediante despliegues controlados (rolling updates), evitando paradas programadas y manteniendo los SLA comprometidos.

La plataforma se apoya en **Worker Nodes**, distribuidos de forma redundante, lo que permite:



- **Alta disponibilidad a nivel de infraestructura**, evitando puntos únicos de fallo.
- **Reubicación automática de cargas** en caso de indisponibilidad de un nodo, gracias a los mecanismos de Kubernetes.
- **Optimización de recursos**, adaptando la capacidad de cómputo a las necesidades reales del sistema en cada momento.

Este enfoque es coherente con los principios de **arquitectura de alta disponibilidad y continuidad del servicio** ya definidos por INETUM, donde la infraestructura está diseñada para seguir prestando el servicio incluso ante fallos de componentes individuales.

La combinación de **arquitectura de microservicios, orquestación mediante Kubernetes y nodos de cómputo redundados en OCI** permite garantizar que:

- Los servicios de portabilidad estarán disponibles **24x7**, conforme a los SLA establecidos.
- La solución podrá **absorber incrementos de carga** sin degradar el rendimiento.
- Se reducen significativamente los riesgos asociados a interrupciones del servicio, cumpliendo con los objetivos de continuidad operativa exigidos para sistemas críticos de portabilidad numérica.

3.2 Disaster Recovery Service

Con el objetivo de garantizar la continuidad del servicio ante eventos de contingencia mayor, la solución contempla la implantación de un Centro de Recuperación ante Desastres (**DRS**) en un segundo datacenter, físicamente independiente del principal. Este DRS se apoya en la combinación de Oracle Data Guard para la capa de datos y Oracle Kubernetes Engine Disaster Recovery (OKE DR) para la capa de servicios y aplicaciones.

Este enfoque está alineado con los modelos de redundancia geográfica, continuidad operativa y cumplimiento de SLA que INETUM ha definido previamente para sistemas críticos de portabilidad, donde la infraestructura secundaria es capaz de asumir la totalidad del servicio sin impacto relevante en la operación.

3.2.1 Capa de datos: Oracle Data Guard

La base de datos del sistema se protege mediante **Oracle Data Guard**, configurado entre el datacenter principal y el datacenter de contingencia, lo que permite:

- **Replicación en tiempo casi real** de la información desde la base de datos primaria hacia la base de datos standby, con **RPO = 0 y RTO < 15 minutos**.
- **Protección frente a fallos del sitio principal**, asegurando la integridad y consistencia de los datos.
- **Conmutación controlada (switchover/failover)** hacia el entorno DRS en caso de indisponibilidad del entorno principal.



- **Reducción del RPO**, al mantener las bases de datos sincronizadas mediante réplicas en caliente, práctica ya empleada por INETUM en sus arquitecturas de alta disponibilidad.

Este mecanismo asegura que la información crítica de portabilidad esté disponible en el sitio secundario y pueda ser utilizada de forma inmediata tras la activación del DRS.

3.2.2 Capa de aplicación: Oracle Kubernetes Engine DR

Para la capa de servicios, la solución utiliza **Oracle Kubernetes Engine (OKE) con capacidades de Disaster Recovery**, desplegando un **cluster Kubernetes en el datacenter secundario**, preparado para asumir la operación cuando sea necesario. Este esquema permite:

- **Replicación de la configuración del cluster**, incluyendo definiciones de microservicios, despliegues y políticas de escalado.
- **Arquitectura activa/pasiva o warm standby**, donde el entorno DR puede mantenerse sincronizado y listo para activación.
- **Reanudación rápida de los servicios**, minimizando el tiempo de indisponibilidad percibido por los operadores y sistemas externos.
- **Coherencia con la arquitectura de microservicios**, permitiendo que los componentes de la aplicación se levanten de forma controlada y ordenada en el entorno DRS.

Este modelo refuerza la capacidad de la plataforma para mantener la operación incluso ante una caída completa del datacenter principal, cumpliendo con los objetivos de continuidad definidos en los SLA del servicio.

3.2.3 Operación conjunta Data Guard + OKE DR

La integración de **Data Guard** y **OKE DR** permite una estrategia de recuperación integral:

- La **base de datos standby** en el DRS garantiza la disponibilidad inmediata de la información.
- El **cluster OKE de contingencia** permite desplegar los microservicios contra dicha base de datos, restableciendo la funcionalidad completa del sistema.
- La **conmutación entre sitios** se realiza sin pérdida de información relevante y sin necesidad de rediseños de la arquitectura.
- El sistema mantiene la **capacidad de cumplir los niveles de servicio comprometidos**, incluso en escenarios de desastre mayor.

Este enfoque reproduce el modelo de redundancia geográfica completa que INETUM aplica en otras soluciones de portabilidad, donde ambos sitios están preparados para prestar el servicio en condiciones equivalentes.



3.3 Escalabilidad

La solución propuesta ha sido diseñada para garantizar una escalabilidad flexible y controlada, permitiendo adaptarse de forma progresiva al crecimiento del servicio, al aumento del volumen de transacciones de portabilidad y a la incorporación de nuevos operadores o funcionalidades, todo ello sin afectar a la disponibilidad ni a los niveles de servicio comprometidos.

Este principio de escalabilidad constituye uno de los pilares fundamentales de la arquitectura de **INETUM** en sistemas críticos de portabilidad, donde la plataforma debe evolucionar de forma acompasada al crecimiento del negocio y a las exigencias regulatorias.

3.3.1 Escalabilidad horizontal basada en microservicios y OKE

La adopción de una **arquitectura orientada a microservicios**, desplegada sobre **Oracle Kubernetes Engine (OKE)**, permite una **escalabilidad horizontal nativa**, basada en los siguientes aspectos:

- **Escalado independiente por servicio**, incrementando o reduciendo el número de réplicas de cada microservicio en función de la carga real.
- **Ajuste dinámico de capacidad**, respondiendo a picos de demanda en procesos críticos como validaciones, portaciones masivas o ventanas de cambio.
- **Distribución equilibrada de la carga**, gracias a los mecanismos de balanceo propios de Kubernetes.
- **Ausencia de impacto global**, ya que el escalado de un microservicio no afecta al resto de componentes de la plataforma.

Este modelo permite absorber incrementos de carga de forma gradual y eficiente, manteniendo los tiempos de respuesta y la estabilidad del sistema, tal como se establece en las arquitecturas escalables descritas por INETUM.

3.3.2 Escalabilidad de la infraestructura: OCI Compute Worker Nodes

La capa de infraestructura se apoya en **OCI Compute Worker Nodes**, lo que posibilita:

- **Crecimiento horizontal del cluster Kubernetes**, incorporando nuevos nodos de cómputo cuando la demanda lo requiera.
- **Optimización de recursos**, ajustando CPU, memoria y capacidad de proceso sin necesidad de rediseñar la arquitectura.
- **Acompañamiento del crecimiento del servicio**, manteniendo un coste marginal controlado frente al coste inicial de la plataforma.

Este enfoque permite que la plataforma evolucione de forma progresiva, garantizando que la infraestructura soporte el aumento de carga derivado del crecimiento del sistema de



portabilidad .

3.3.3 Escalabilidad vertical controlada

De forma complementaria a la escalabilidad horizontal, la solución admite **escalabilidad vertical** cuando sea necesario, mediante:

- Incremento de recursos de cómputo (CPU, memoria) en los nodos existentes.
- Ajustes de configuración en componentes concretos que requieran mayor capacidad de proceso.
- Optimización de parámetros de ejecución para mantener el rendimiento en escenarios de alta demanda.

La combinación de escalabilidad horizontal y vertical permite seleccionar en cada momento la estrategia más eficiente, garantizando el cumplimiento de los SLA establecidos.

3.3.4 Escalabilidad integrada con el DRS

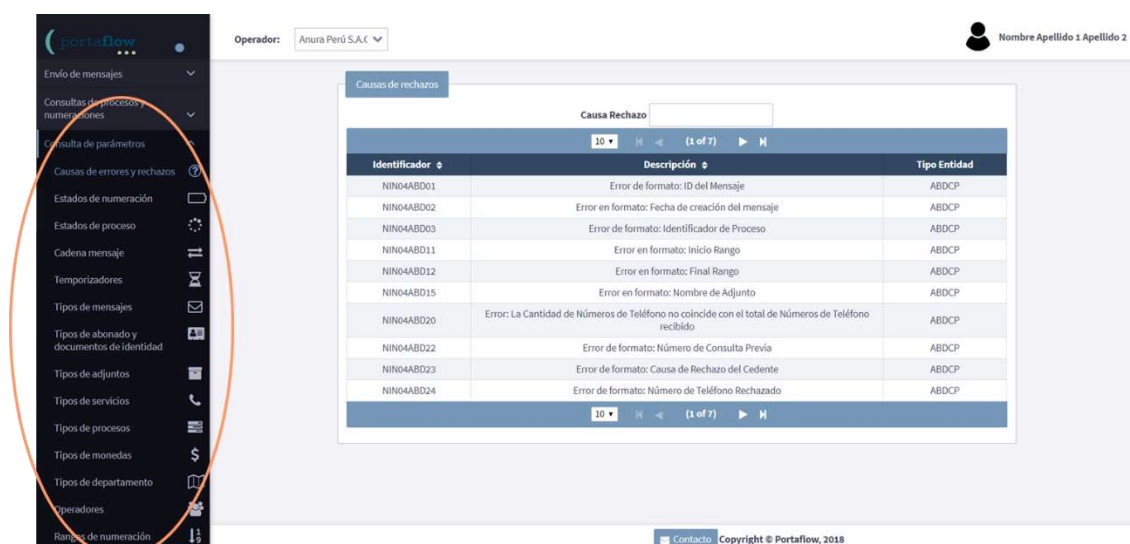
El esquema de **Disaster Recovery (Data Guard + OKE DR)** se encuentra alineado con el modelo de escalabilidad de la solución, de forma que:

- El **cluster OKE del sitio de contingencia** puede escalar de manera equivalente al entorno principal.
- La **base de datos standby**, protegida mediante Data Guard, está dimensionada para asumir el volumen de carga del entorno productivo.
- La activación del DRS no supone pérdida de capacidad ni degradación del servicio.

3.4 Flexibilidad

El sistema propuesto **Portaflow 3.0** permite realizar las modificaciones que se identifiquen como necesarias como resultado de la experiencia de la implementación y operación de la portabilidad. Al ser un desarrollo en **JAVA** cuenta con la facilidad de realizar cambios de forma sencilla y rápida. En todos los países donde INETUM es administrador, han surgido modificaciones regulatorias producto de la experiencia y necesidad de incorporar nuevas funcionalidades para adaptarse al desarrollo y crecimiento del mercado, en todas ellas hemos cumplido con lo solicitado y en los tiempos acordados con los operadores.

Portaflow 3.0 es parametrizable en el ámbito operativo, de tal manera que sus componentes pueden ser configurados de acuerdo con los procesos y procedimientos cuya modificación sea necesario efectuar a través del tiempo. Además, la parametrización se puede realizar en caliente sin afectación de servicio.



Pantalla de configuración de parámetros

4 Infraestructura

4.1 Alojamiento de las aplicaciones

Las aplicaciones que conforman el **Sistema Integral de Portabilidad Numérica (SIPN)** y los sistemas de soporte asociados a la **Entidad de Referencia de Portabilidad Numérica (ERPN)** se alojarán en una infraestructura cloud de primer nivel, basada en **Oracle Cloud Infrastructure (OCI)**, garantizando en todo momento los niveles de seguridad, disponibilidad, continuidad operativa y escalabilidad requeridos por la normativa y el pliego de condiciones.

Infraestructura principal (Producción)

El entorno principal de producción se implantará en la **región de OCI en México**, seleccionada por su proximidad geográfica a Costa Rica, su baja latencia y su cumplimiento con estándares internacionales de seguridad y operación. Esta infraestructura alojará todos los componentes críticos del SIPN, incluyendo:

- Plataformas de aplicaciones y servicios web.
- Bases de datos de portabilidad (NP-DB) y repositorios asociados.
- Servicios de integración con operadores, proveedores y SUTEL.
- Portales web, APIs y sistemas de gestión y monitorización.

La arquitectura se diseñará bajo un esquema de **Alta Disponibilidad**, con distribución de cargas, redundancia de componentes y tolerancia a fallos, de forma que la indisponibilidad de un elemento no afecte a la continuidad del servicio, cumpliendo con la operación **24x7x365** exigida en el pliego.



Infraestructura de contingencia y Recuperación ante Desastres (DRS)

De acuerdo con los requisitos establecidos para infraestructuras en la nube, se dispondrá de un **entorno de contingencia geográficamente separado**, ubicado en la **región de OCI en Colombia**, que actuará como **sitio de Recuperación ante Desastres (DRS)**.

Este entorno contará con:

- Replicación continua y segura de los datos y sistemas críticos desde la región principal.
- Capacidad de activación controlada en caso de desastre mayor o indisponibilidad prolongada del sitio principal.
- Infraestructura dimensionada para garantizar la continuidad del servicio sin pérdida de información.

El esquema de DRS permitirá cumplir con los objetivos de **Recuperación ante Fallos**, asegurando la integridad de la información y la reanudación del servicio conforme a los compromisos de **RTO < 15 minutos y RPO = 0** definidos en la oferta técnica, tal y como exige el pliego en caso de uso de infraestructura cloud.

Seguridad y cumplimiento

La solución de alojamiento contempla medidas avanzadas de seguridad, entre ellas:

- Cifrado de la información en tránsito y en reposo.
- Segregación de entornos (QA y producción).
- Control de accesos basado en roles y perfiles.
- Monitorización continua y registro de eventos de seguridad.

Todo ello garantiza la **confidencialidad, integridad y disponibilidad** de la información gestionada por el SIPN, en cumplimiento de las obligaciones establecidas para la ERPN y de la regulación de portabilidad numérica vigente en Costa Rica.

Escalabilidad y sostenibilidad

El uso de OCI permite una **escalabilidad elástica**, facilitando la adaptación de la plataforma a incrementos de carga, nuevos operadores o cambios regulatorios, sin impacto en la operación del servicio. Asimismo, el modelo cloud optimiza los costes operativos y asegura la vigencia tecnológica durante todo el período de prestación del servicio.

4.1.1 Características Data Centers de Oracle Cloud Infrastructure

La infraestructura de **Oracle Cloud Infrastructure (OCI)** en México forma parte de la red global de regiones cloud de Oracle, diseñada bajo un modelo homogéneo de seguridad, operación y control, aplicable a todas las regiones OCI y auditado de forma independiente.



A continuación, se describen las principales características del datacenter

Seguridad Física y de Entorno

Oracle implementa **controles de seguridad física multinivel** en todos los data centers de OCI, incluida la región de México. Estos controles incluyen:

- Instalaciones de acceso restringido, no públicas.
- Perímetros protegidos con vigilancia física continua.
- Sistemas de detección de intrusión y control perimetral.
- Acceso limitado exclusivamente a personal autorizado de Oracle.

Cabe destacar que Oracle **no publica ubicaciones exactas ni detalles arquitectónicos de sus data centers por motivos de seguridad**, política que aplica también a la región de México.

Seguridad Lógica

OCI aplica un **modelo de seguridad lógica “defense in depth”**, común a todas sus regiones:

- Aislamiento estricto entre clientes (tenancy isolation).
- Segmentación de red mediante Virtual Cloud Networks (VCN).
- Firewalls virtuales y listas de seguridad configurables.
- Protección a nivel de hipervisor y plano de control independiente del plano de datos.

Control de Accesos

El control de accesos en OCI se basa en:

- **Identity and Access Management (IAM)** centralizado.
- Autenticación fuerte y control de privilegios mínimos.
- Separación de funciones administrativas.
- Registro y auditoría de accesos y acciones (OCI Audit).

Sistema de Control de Incendios

Oracle declara que todos sus data centers OCI cuentan con:

- Sistemas automáticos de **detección temprana de incendios**.
- Sistemas de **supresión de incendios adecuados a entornos TI**, diseñados para minimizar daños a los equipos.
- Procedimientos operativos de emergencia documentados.



Energía eléctrica

Las regiones OCI, incluida México, están diseñadas con:

- Fuentes de energía redundantes.
- Sistemas de respaldo (UPS y generación auxiliar).
- Diseño orientado a alta disponibilidad.

Climatización

Los data centers OCI utilizan sistemas de climatización diseñados para:

- Mantener condiciones térmicas adecuadas para equipamiento TI.
- Redundancia en los sistemas de refrigeración.
- Monitorización continua de temperatura y humedad.

Administración y supervisión

La operación de los data centers OCI se realiza por:

- Equipos especializados de Oracle.
- Procedimientos estandarizados de operación y respuesta ante incidentes.
- Separación entre personal de operación física y personal de administración cloud.

La administración sigue **políticas corporativas globales de Oracle**, auditadas regularmente.

Monitoreo de infraestructura

Oracle mantiene **monitorización continua 24x7** de su infraestructura cloud:

- Supervisión de estado de hardware y servicios.
- Detección proactiva de incidencias.
- Gestión de eventos y alertas internas.

Mantenimiento preventivo

OCI aplica planes de:

- Mantenimiento preventivo del hardware.
- Sustitución planificada de componentes.
- Actualizaciones sin impacto para los clientes, siempre que es técnicamente posible.

Las tareas de mantenimiento se realizan conforme a procedimientos internos y políticas de continuidad de servicio.



Estándares

Los datacenters de oracle (OCI) están diseñados conforme a buenas prácticas de data centers de misión crítica y certificados bajo estándares internacionales

- ISO/IEC 27001 (Seguridad de la Información)
- ISO/IEC 27017 (Seguridad en la nube)
- ISO/IEC 27018 (Protección de datos personales en cloud)
- SOC 1, SOC 2 y SOC 3

Protección de Datos Personales

Oracle establece contractualmente que:

- Los datos del cliente **permanecen bajo control del cliente**.
- El tratamiento de datos cumple con estándares internacionales de protección de datos.
- OCI ofrece mecanismos de cifrado, control de acceso y auditoría.

4.2 Comunicaciones

4.2.1 Canales de comunicación

La interacción entre los operadores y terceros autorizados que así lo soliciten con el SIPN será a través de integración por web services, por archivos o a través de un aplicativo web.

Será elección de las operadores y terceros autorizados que así lo soliciten determinar cuál de los medios utiliza, teniendo el ERPN que soportar todos los medios de comunicación mencionados.

Independientemente de los canales de comunicación, todos ellos estarán cifrados y autenticados en los casos en que corresponda, utilizando protocolos estándares de uso por la industria.

Todos los módulos de la solución de portabilidad disponen de seguridad, verificando en todo momento la identidad y perfil de la persona que intenta acceder al sistema, limitando, según el perfil, el acceso a la información, así como a la funcionalidad del ERPN, evitando así el acceso no autorizado y/o malintencionado al sistema.

Igualmente, los accesos hacia el ERPN desde cada uno de los proveedores se controlan y restringen a través de la infraestructura de seguridad disponible en el ERPN, estableciéndose la plena identificación de las conexiones origen y destino.

- Acceso **SOAP/REST**: la seguridad en Web Services está basada en varios conceptos:
 - **Identificación y autenticación**: Verificación de la identidad de un usuario, proceso o dispositivo, a menudo como prerrequisito para permitir el acceso



a los recursos en un sistema de información.

- **Autorización:** El permiso de utilización de un recurso, asignado de forma directa o indirecta por una aplicación o por el dueño del sistema
- **Integridad:** La propiedad de que los datos no han sido alterados por alguien no autorizado mientras se almacenan, se procesan o están en tránsito.
- **No repudio:** Seguridad de que el remitente de la información obtiene pruebas de la recepción de la información por parte del destinatario, y que el destinatario obtiene pruebas de la identidad del remitente, de forma que ninguno pueda negar posteriormente el procesamiento de la información.

El protocolo HTTPS está definido como HTTP sobre SSL/TLS. SSL/TLS proporciona seguridad a nivel de socket, encriptado toda comunicación sobre una conexión TCP particular, asignando inmediatamente a una comunicación seguridad sin alterar la misma.

- **Acceso a la GUI por HTTPS:** se destacan los principales mecanismos ofrecidos en este sentido:
 - **Encriptación:** El emisor obtendrá las garantías de que los datos, encriptados antes de ser transmitidos sólo serán desencriptados por el receptor deseado.
 - **Autenticación:** El receptor asegurará que los datos recibidos realmente provienen del emisor apropiado.
 - **No repudio:** Tanto el emisor como el receptor asegurarán que la otra parte no podrá posteriormente rechazar la transacción intentando que un tercero les represente fraudulentamente.
 - **Control de acceso al sistema:** Como cualquier sistema convencional de proceso de información, se asegura que los usuarios tienen los permisos necesarios para visualizar o cambiar los datos con los que están autorizados para trabajar.
- **Acceso por SFTP:** para la descarga de ficheros diarios: el protocolo SFTP está definido como FTP sobre SSL/TLS. SSL/TLS proporciona seguridad a nivel de socket, encriptando toda comunicación sobre una conexión TCP particular, asignando inmediatamente a una comunicación seguridad sin alterar la misma.

Portaflow registrará cualquier actividad de modificación o borrado, y cuenta con los mecanismos necesarios para asegurar la integridad de dichos registros.

4.2.2 Canal de comunicación para integración

Se considera la provisión de los servicios del Sistema Integral de Portabilidad Numérica (SIPN) mediante la utilización de la **red pública de Internet**, garantizando en todo momento la **seguridad, confidencialidad e integridad de las transacciones**, de conformidad con lo establecido en el pliego de condiciones de la ERPN y la normativa vigente aplicable.



La arquitectura de comunicaciones se soporta sobre **Oracle Cloud Infrastructure (OCI)**, utilizando mecanismos estándar y ampliamente probados de seguridad de red, cifrado y control de accesos, que permiten la interconexión segura con operadores, proveedores y terceros autorizados.

Seguridad de las comunicaciones

Todas las comunicaciones que se realicen a través de Internet se protegerán mediante:

- **Cifrado de las comunicaciones** utilizando protocolos seguros estándar de la industria (por ejemplo, TLS/IPsec).
- **Aislamiento de red** mediante Virtual Cloud Networks (VCN) en OCI, con segmentación lógica de los distintos entornos (producción, pruebas y desarrollo).
- **Controles de acceso a nivel de red**, limitando los orígenes y destinos permitidos mediante listas de seguridad y políticas de red.

Estos mecanismos garantizan que las transacciones realizadas entre el SIPN y los distintos actores se efectúen de forma segura, aun utilizando la red pública de Internet, cumpliendo con los requisitos de confidencialidad e integridad exigidos por el pliego.

Capacidad y ancho de banda

La infraestructura desplegada en OCI dispone de la **capacidad de red necesaria para soportar el ancho de banda requerido por los prestadores**, permitiendo:

- Escalabilidad dinámica de los recursos de red en función de la carga.
- Soporte simultáneo de múltiples conexiones entrantes desde operadores y terceros.
- Operación continua del servicio bajo esquemas de alta disponibilidad.

El modelo cloud de OCI permite adaptar la capacidad de red a las necesidades operativas del SIPN sin impacto en la continuidad del servicio.

Conectividad mediante VPN

INETUM pone a disposición de los operadores, proveedores y terceros autorizados la **posibilidad de conexión segura mediante VPN**, utilizando los servicios de red de OCI.

Estas conexiones VPN podrán configurarse de acuerdo con las necesidades específicas de cada entidad, contemplando los siguientes escenarios:

- **VPN site-to-site**, para la interconexión permanente entre las infraestructuras de los operadores o terceros y el entorno del SIPN en OCI.
- **VPN cliente-servidor (remote access)**, para accesos controlados de usuarios o sistemas específicos que así lo requieran.

Las VPN se implementarán utilizando **tecnologías estándar de la industria**, con cifrado fuerte y autenticación, garantizando que el acceso a los sistemas del SIPN se realice



exclusivamente por entidades autorizadas y bajo condiciones de seguridad adecuadas.

Flexibilidad y control

La arquitectura propuesta permite:

- Incorporar nuevos operadores o terceros de forma ágil.
- Ajustar los esquemas de conectividad según las decisiones del CTPN-M o la SUTEL.
- Mantener un control centralizado de las comunicaciones y accesos, alineado con los principios de seguridad definidos en el pliego de condiciones.

4.2.3 Protocolos de comunicación

A continuación, se presentan los protocolos e interfaces que el sistema debe facilitar para la conexión de los operadores, la SUTEL y demás entidades que deban acceder SIPN.

El sistema **Portaflow 3.0** incorpora varias interfaces de comunicación con los Proveedores, ofreciendo una serie de protocolos estandarizados que permiten el intercambio seguro de información entre los proveedores y el ABD resolviendo así otros de los servicios que debe de ofrecer el ERPN para cumplir eficientemente con las funciones requeridas en las especificaciones de portabilidad.

Los interfaces de comunicación son los siguientes:

- Interfaz Web
- Interfaz SOAP/REST
- Interfaz FTP/SFTP

A continuación, se enuncian y resumen cada uno de los sub-módulos que comprende este sistema.

4.2.3.1 Interfaz Web

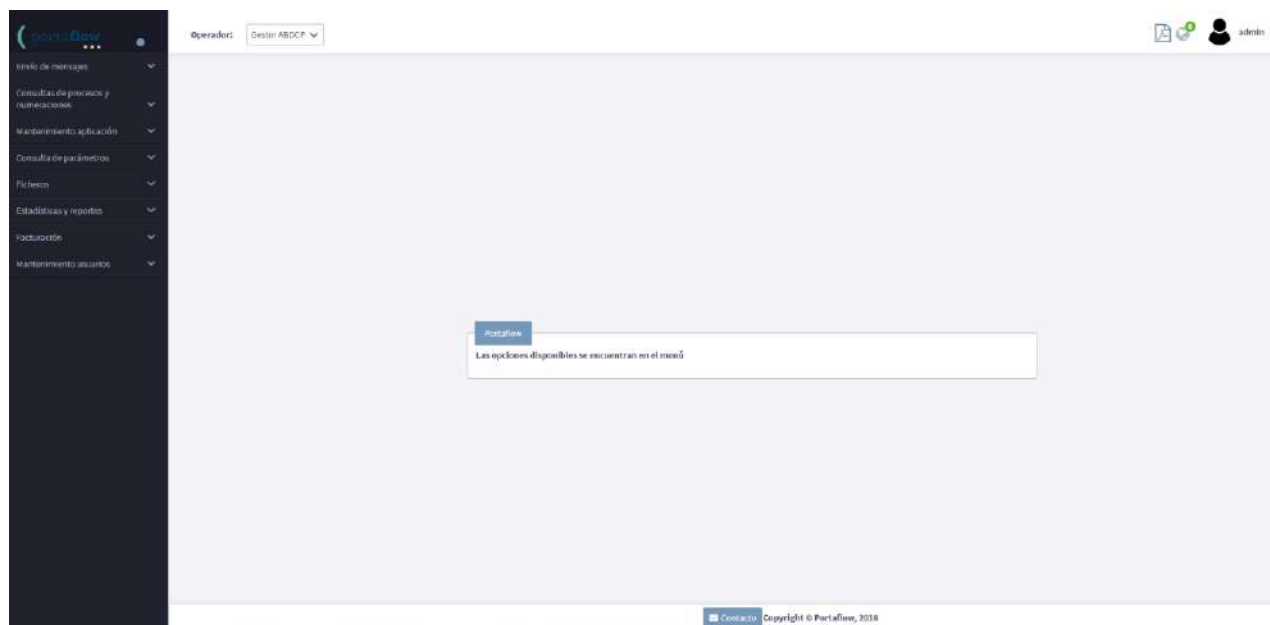
Portaflow 3.0 dispone de una interfaz web que permitirá acceder al sistema del ERPN a los operadores y a la Sutel.

Las funcionalidades de este interfaz web son las siguientes:

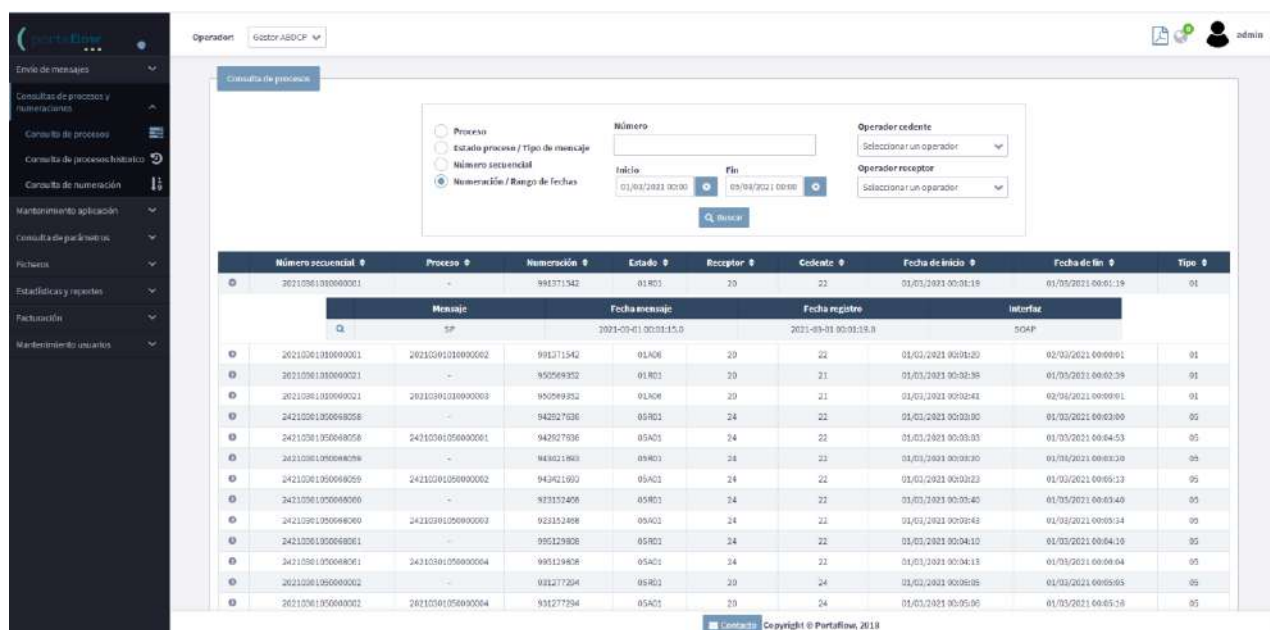
- **Consola de mensajes:** permitirá a los OSTM llevar a cabo la ejecución de los procesos de portabilidad, para ello existen formularios de envío y recepción de todos los mensajes.
- **Consultas sobre estados de números, procesos de portabilidad y mensajería asociada**
- **Reportes y estadísticas** de portabilidades.
- Reportes de transacciones a facturar
- Acceso a la documentación y los manuales del proyecto.

- Configuración y mantenimiento del sistema por parte de los administradores. Se podrán configurar parámetros del sistema, tales como tipos de mensajes, códigos de proveedores, temporizadores, feriados, etc. El administrador del sistema podrá realizar desde la web de Portaflow la gestión de usuarios y perfiles.

A continuación, se muestran varias pantallas de la interfaz web de Portaflow.













Pantalla Principal de la interfaz Web de la aplicación



Pantalla de Consultas sobre Procesos de Portabilidad

Operador: gestor ABDCP

Temperizaciones

Identificador	Descripción	Mínimo	Máximo	Calendario	Unidad	Opciones
TAP	Activación del pago de deuda	0	0	Laboral	Días	 
TPVC	Tiempo de fin de la ventana de cambio	0	0	Laboral	Minutos	 
TPP	Programación de la portabilidad	0	30	Laboral	Días	 
TRABO	Tiempo de respuesta del ABDCP	30	30	Natural	Segundos	 
TRC	Tiempo máximo de respuesta por parte del cedente	2	2	Natural	Minutos	 

[+ Nuevo temperizador](#)

Alcance

Nombre	Descripción	Fórmula	Hora
AlarmA0106	Activación del pago de deuda	MAXTAP	22:00:00
AlarmA0104	Ejecución de portabilidad clientes esporádicos	MAXTPC	06:00:00
AlarmA0501	Tiempo límite de respuesta del cedente	MAXTRC	
AlarmA0106	Ejecución de portabilidad	MAXTPC	08:00:00
AlarmA0102	Programación de portabilidad fijos	MAXTPP	22:00:00

[Contacto](#) Copyright © Portaflow, 2018

Pantalla de Consulta y Envío de Mensajes de Portabilidad por la Web

Operador: gestor ABDCP

Receptor

[Consulta de Mensajes](#) [Consulta Previa](#) [Solicitud de Portabilidad](#) [Solicitud de Retorno](#)

Datos del solicitante

Operador receptor: gestor ABDCP

Tipo documento * Seleccione un tipo

Documento de identificación *

Operador cedente * Seleccione un tipo

Departamento * Seleccione un tipo

Nombre del contacto

Email del contacto

Teléfono de contacto

Fax del contacto

Número de consulta previa

Tipo de cliente * Seleccione un tipo

Tipo de servicio * Seleccione un tipo

Observaciones

[Enviar](#)

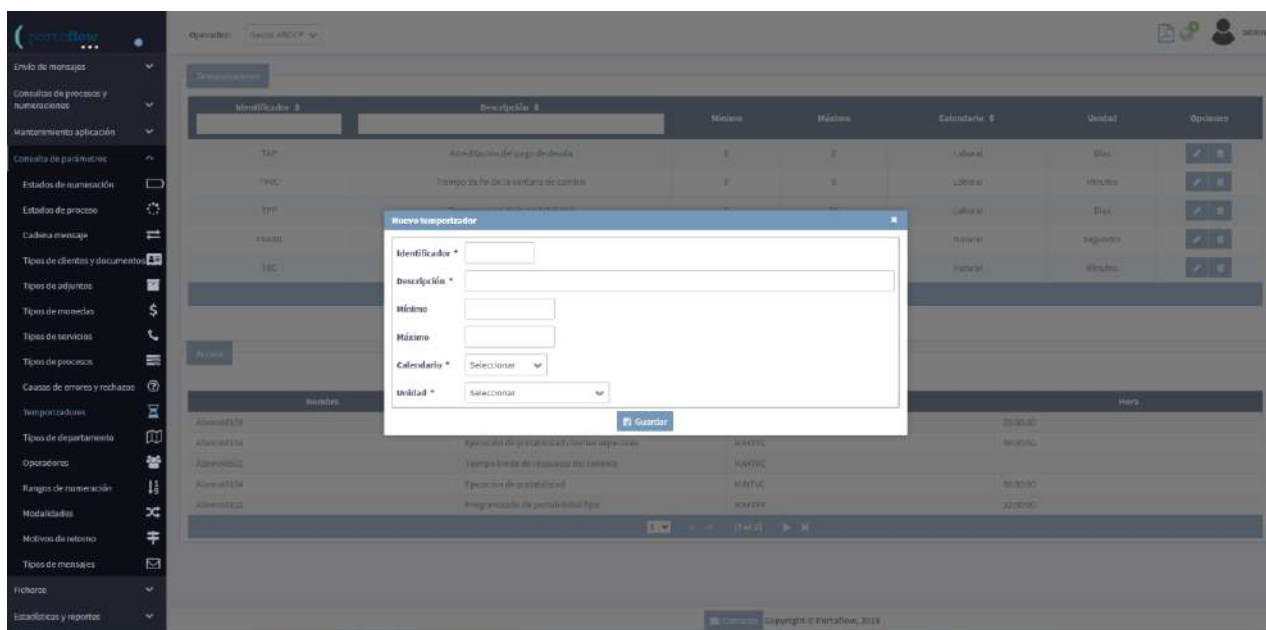
Numéricas

Número	Modulador cedente	Modulador receptor	Opciones
No hay numeraciones			

[Carga Bchero](#) [+ Eliminar](#) [Iniciar](#) [Cancelar](#)

[Contacto](#) Copyright © Portaflow, 2018

Pantalla Formulario de un mensaje de solicitud de portabilidad



4.2.3.2 Interfaz SOAP/REST

La solución propuesta se fundamenta en una arquitectura orientada a servicios (SOA), que facilita la integración de los distintos sistemas de los operadores y proveedores de servicios de telecomunicaciones con el sistema central de la ERPN, garantizando interoperabilidad, escalabilidad y neutralidad tecnológica.

Servicios Web SOAP y REST

- **Servicios Web SOAP**, utilizados principalmente para los procesos críticos de portabilidad definidos en el Manual de Interfaces y Procesos, con contratos de servicio formalizados mediante WSDL, esquemas XML normalizados y control estricto de mensajes y errores.
- **Servicios REST**, orientados a operaciones de consulta, integración flexible y servicios auxiliares, manteniendo igualmente mecanismos de autenticación, autorización y cifrado de las comunicaciones.

Ambos tipos de servicios se exponen mediante **canales seguros HTTPS**, garantizando la confidencialidad e integridad de la información intercambiada.



Seguridad, autenticación y trazabilidad

Con independencia del protocolo utilizado (SOAP o REST), **todos y cada uno de los accesos al sistema estarán debidamente registrados**, con la finalidad de realizar un seguimiento exhaustivo de los mensajes intercambiados entre los operadores y el sistema de la ERPN, tal y como exige el pliego de condiciones.

El uso de **certificados digitales** y credenciales de acceso permite:

- Autenticar de forma inequívoca a los agentes que intervienen en los procesos de portabilidad.
- Garantizar la seguridad transaccional extremo a extremo.
- Proveer mecanismos sólidos de **no repudio** y auditoría.

Gestión centralizada de los mensajes de portabilidad

El sistema central de la ERPN es el encargado de **recibir, validar, procesar y enviar todos los mensajes asociados a los procesos de portabilidad**, actuando como punto único de orquestación de los intercambios de información con la Base de Datos Centralizada de Portabilidad y con los sistemas de los operadores.

El sistema opera en **modo on-line**, resolviendo todas las emisiones y recepciones de mensajes que apliquen sobre los procesos de portabilidad definidos por la regulación vigente.

Validación, acuses de recibo y control de errores

Cuando el sistema de la ERPN recibe un mensaje de portabilidad, valida que el remitente corresponda a un operador o proveedor debidamente dado de alta en el sistema. Una vez recibido y validado el mensaje, se devuelve al remitente un **acuse de recibo**, que confirma la correcta recepción del mismo.

El sistema gestiona internamente la ejecución de las acciones asociadas a cada mensaje y realiza el **envío de los mensajes de portabilidad generados** a los destinatarios correspondientes.

Registro de eventos y auditoría

El sistema genera **trazas de log detalladas** sobre todas las acciones realizadas durante la recepción y el envío de mensajes, incluyendo:

- Envío y recepción de mensajes SOAP y REST.
- Gestión de acuses de recibo.
- Registro de errores, excepciones y eventos relevantes.
- Notificación de incidencias a las partes correspondientes.

Estos registros permiten un seguimiento completo de los eventos del sistema y constituyen



la base para la **resolución de disputas, la gestión de incidencias y la auditoría de los procesos de portabilidad**, conforme a los requisitos del pliego ERPN.

Interfaces de configuración y administración

El sistema dispone de una **interfaz web de administración**, desde la cual se pueden:

- Configurar los operadores y proveedores que interactúan con el sistema.
- Gestionar el alta, baja o modificación de participantes.
- Definir parámetros operativos y horarios de funcionamiento.
- Configurar el nivel de detalle de los registros de log.
- Consultar los mensajes intercambiados entre la ERPN y los operadores.

Esta interfaz permite una gestión centralizada, controlada y auditable del sistema, alineada con las funciones que debe desempeñar la ERPN durante toda la operación del SIPN.

4.2.3.3 Interfaz SFTP y API para descarga de ficheros

Si bien el intercambio de mensajes de portabilidad se realiza mediante los protocolos de Servicios Web seguros (SOAP y REST sobre HTTPS), para los casos en los que sea necesario el intercambio de ficheros o la descarga de archivos generados por el ERPN, dicho intercambio se podrá llevar a cabo mediante el protocolo SFTP (Secure File Transfer Protocol), de acuerdo con las prácticas habituales del SIPN y lo establecido en el Manual de Interfaces y Procesos o bien mediante un API con autenticación de acuerdo a las mejoras propuestas.

El uso de SFTP permite realizar el intercambio de archivos de forma eficiente, robusta y segura, proporcionando un canal cifrado extremo a extremo que garantiza la confidencialidad e integridad de la información, aun cuando el transporte se realice a través de la red pública de Internet.

4.3 Arquitectura general de la solución

INETUM suministrará **Portaflow 3.0** con una arquitectura e infraestructura tecnológica necesaria para la correcta ejecución del servicio, garantizando las siguientes premisas:

- Alta disponibilidad
- Confiabilidad
- Escalabilidad.
- Extensibilidad
- Flexibilidad
- Fiabilidad y seguridad
- Mecanismos robustos de acceso



- Proporcionar integridad referencial
- Integridad de datos
- Transaccionalidad
- Exportable a otras bases de datos

Basándose en la criticidad de los sistemas involucrados, se incluye el suministro de una solución integral para la Seguridad de todos los sistemas.

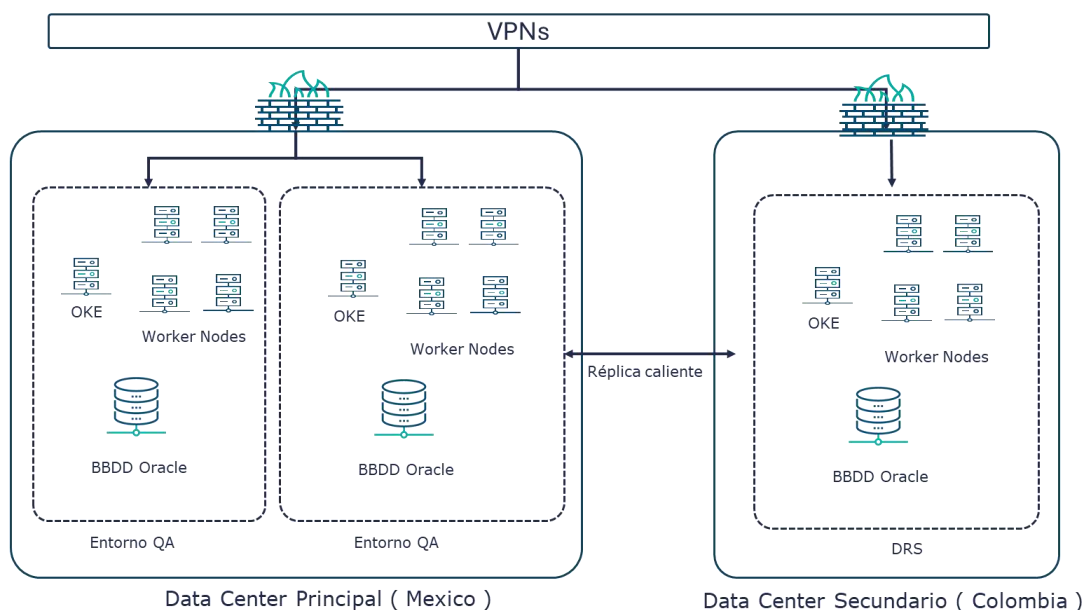
Para la elaboración de la arquitectura de la solución integral de seguridad nos hemos basado en tres conceptos, a nuestro entender, fundamentales: la **alta disponibilidad**, la **seguridad** y la **escalabilidad** de la solución.

En referencia a la **alta disponibilidad** y redundancia, tenemos que aclarar que la propuesta ofrece una plataforma en redundancia sobre sus elementos de front-end y back-end de modo que no exista punto único de fallo en la plataforma.

En cuanto a **seguridad** hemos dotado a la plataforma de una doble capa de seguridad mediante un doble nivel de cortafuegos que separan la parte del “front-end” o zona de acceso público Web, de la zona del “back-end” o zona donde se encuentran los datos confidenciales de los usuarios y del cliente.

Sobre el tema de la **escalabilidad** queremos hacer un especial hincapié en el diseño de la solución que permite la escalabilidad vertical y la horizontal. O sea, ampliar los sistemas existentes en caso de necesidad mediante una escalabilidad vertical con mayores recursos (disco, memoria, cpu, etc.) y habilitar la posibilidad de un crecimiento horizontal.

A continuación, se muestra el diagrama de la arquitectura propuesta para dar solución a las necesidades de portabilidad numérica en Costa Rica:





5 Metodología de Implementación y Aceptación

5.1 Propuesta general de implementación

El marco metodológico que se seguirá en todas las fases del proyecto será el que define el **PMBok** del **Project Management Institute (PMI)**, ya que el responsable del proyecto estará certificado en PMP. Se establecerá una PMO (oficina de proyectos), la cual velará por la buena marcha del proyecto, gestionando al equipo de trabajo, alcance y plazos, y coordinando con los operadores las distintas actividades.

Se mantendrán reuniones semanales de seguimiento en las que se entregará el avance del proyecto y se revisarán los puntos que estén pendientes de cerrar, así como exponer nuevos hitos y tareas.

Tras la firma del último contrato se realizará la primera reunión de seguimiento junto al Comité de Portabilidad en la que se presentará el responsable del proyecto quien coordinará y sustentará todas las actividades y entregables asociados al contrato.

Además, se hará entrega del documento Plan de Implementación o plan de Proyecto que contendrá toda la planificación a nivel global del proyecto. Dicho documento se irá ajustando según se vaya avanzando el proyecto y contendrán entre otros los siguientes planes:

- Plan de Implantación
- Plan de Pruebas
- Plan de Comunicaciones
- Plan de Capacitación
- Plan de Puesta en Operación

Tras dicha primera reunión se establecerá la siguiente en un plazo de una semana con el fin de que todos los operadores puedan realizar una revisión sobre la documentación entregada en la primera reunión, y debatir la misma con el fin de adoptar los acuerdos que puedan llegar a presentarse, así como adaptar/modificar lo que sea requerido para aprobar dicha documentación. A partir de ahí se realizarán reportes semanales sobre el avance del proyecto con el Comité de Portabilidad.

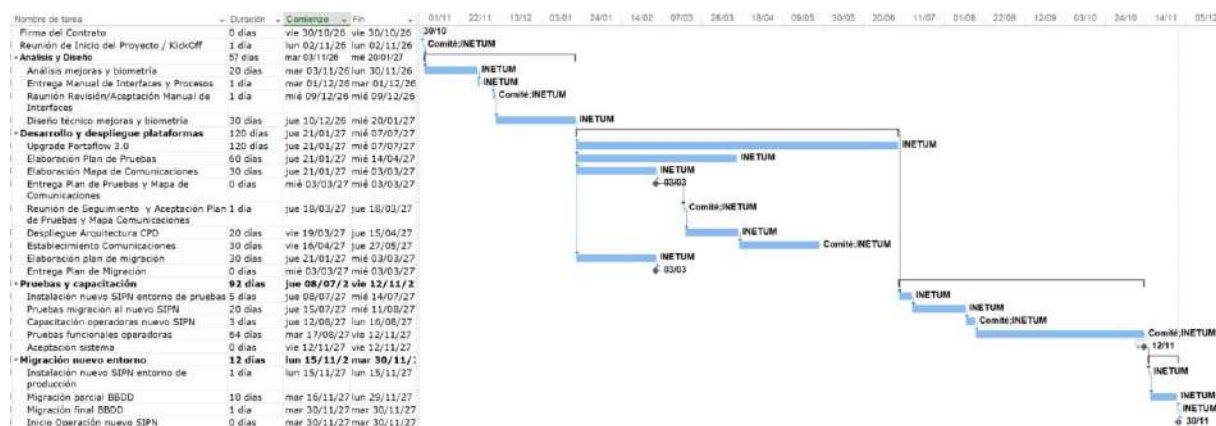
Si bien se adjunta a la presente **propuesta una planificación** de todas y cada una de las actividades que se han de desarrollar en el proyecto de implantación, INETUM asegura el cumplimiento de las fechas enunciadas en el mismo, y por dicha razón brinda las garantías suficientes como para poder afirmar el cumplimiento de los plazos existentes en el pliego



de condiciones, teniendo como hitos principales las siguientes fechas:

- Fechas de Implementación del sistema: Inicio el 30 de octubre de 2026
- Inicio Ejecución de Pruebas: 18 de agosto de 2027
- Puesta en producción e inicio de operaciones: 30 de noviembre de 2027.

A continuación, se presenta una planificación detallada sobre la implementación del sistema:



La planificación aquí descrita se presenta a título de propuesta inicial y podrá ser modificada o ajustada en función de las necesidades del proyecto, previo consenso y aprobación del Comité.

5.1.1 Metodología de Implementación

En los siguientes apartados se definen las diferentes fases upgrade del SIPN en Costa Rica que INETUM llevará a cabo.

5.1.1.1 Análisis y Diseño de Portaflow

Con la adjudicación del ERP, el equipo experto en portabilidad de INETUM realizará un análisis y diseño para adaptar el sistema **Portaflow 3.0** a las especificaciones del ERP de Costa Rica tomando como premisa el “Manual de Interfaces y Procesos.pdf” y “Manual de Interfaces con mejoras.docx”.

A partir de dicho análisis se modificará el documento Manual de Interfaces y Procesos, el cual describirá todo el detalle técnico, interfaces con los operadores y otras entidades, formato de los ficheros a intercambiar, campos de los mensajes, casos de uso, etc.

Este documento será entregado al CTPN para su revisión interna y se mantendrán reuniones con los operadores para los comentarios, dudas y observaciones que se tengan sobre el documento, así como cerrar alcances y definiciones que deban ponerse de común acuerdo.

El Manual de Interfaces y Procesos permitirá a los operadores implementar sus sistemas de portabilidad y será imprescindible su aprobación final por parte del CTPN para poder iniciar



las adaptaciones del sistema **Portaflow 3.0**.

5.1.1.2 Desarrollo y disponibilidad de plataformas

INETUM tendrá como base de sus adaptaciones las últimas versiones actualizadas en cuanto a arquitectura, framework web, seguridad, rendimiento y otros.

Dentro de esta fase se comenzarán a acometer las modificaciones sobre la solución de portabilidad **Portaflow 3.0**, con el objetivo de amoldar la misma a las necesidades recopiladas en los requerimientos técnicos.

En paralelo se iniciará la elaboración detallada del documento Plan de Pruebas y el Mapa de Comunicaciones por parte de **INETUM**.

Ambos documentos se entregarán a los operadores para que analicen la información que contienen y propiciar el debate de éstos en la reunión que se convoque oportunamente.

Tras esa reunión, y tras la adopción de los acuerdos que llegado el caso correspondan, se procederá a la aprobación y aceptación de los citados documentos.

Todos los avances sobre cada una de estas actividades serán informados en las correspondientes reuniones de seguimiento del proyecto.

5.1.1.3 Establecimiento de plataformas y comunicaciones

En esta fase se establecerán las plataformas hardware y software base en cada uno de los entornos del ERP (QA, producción y contingencia), tras lo cual se iniciará la configuración de las comunicaciones.

INETUM se encargará de definir los mapas de comunicaciones y coordinará las ventanas necesarias con cada uno de los operadores durante las cuales se llevarán a cabo la configuración de los enlaces y las pruebas de conectividad, con un acompañamiento total desde el inicio de la tarea hasta su culminación, pudiendo determinar así la disponibilidad de las comunicaciones y los distintos servicios entre el SIPN y los operadores.

Finalizado el despliegue y configuración de los distintos entornos, y una vez haya terminado el desarrollo de las adaptaciones de **Portaflow 3.0**, INETUM procederá a instalar dicha solución en el entorno de pruebas.

Una vez más, todos los avances y circunstancias sobre cada una de estas actividades serán informados en las correspondientes reuniones de seguimiento del proyecto.

5.1.1.4 Capacitación

INETUM elaborará toda la documentación necesaria para llevar a cabo la capacitación técnica y administrativa a los operadores y la SUTEL.

INETUM impartirá un plan de capacitación que permita a los usuarios del sistema conocer toda la funcionalidad de las aplicaciones del SIPN.



5.1.1.5 Ejecución plan de pruebas

Con el sistema listo en el entorno de pruebas y el conocimiento adquirido en la capacitación se procederá a iniciar la fase de pruebas.

En la ejecución del plan de pruebas han de participar todos los operadores junto con el administrador de base de datos.

Toda incidencia que pueda llegar a presentarse durante la ejecución del plan de pruebas será informada por las vías que se definan a tales efectos oportunamente, esto es, a través de la plataforma **Mobydesk**, la cual estará activada desde el inicio de las pruebas, y serán resueltos por **INETUM**. Del mismo modo, cuando alguna incidencia aplique sobre los propios operadores, han de ser éstos quienes resuelvan las mismas para poder proseguir con su propio plan de pruebas.

Al final de este plan de pruebas se debe obtener un correcto funcionamiento de todos los aplicativos informáticos, tanto del **SIPN** como de los operadores.

El avance y circunstancias que se presenten sobre cada una de estas actividades han de ser informadas en las correspondientes reuniones de seguimiento del proyecto.

5.1.1.6 Puesta en producción

Con las pruebas realizadas se verificará el correcto funcionamiento del ERP. Una vez concluido el plan de pruebas y recibida la aceptación final del sistema por parte del CTPN, se realizará por parte de INETUM la preparación final del entorno de producción para disponer de éste en la fecha prevista para su salida a operación.

Tras la puesta en producción del sistema se activarán los servicios correspondientes a la propia explotación del sistema.

De más está decir que todas estas circunstancias, tareas y avances del propio proyecto han de ser tratadas e informadas en las correspondientes reuniones de seguimiento.

5.1.2 Estrategia de pruebas

INETUM elaborará un plan de pruebas detallado, el cual integrará todos los tipos de prueba que se han de llevar a cabo para certificar el sistema **Portaflow 3.0**. Este plan será revisado y consensuado con el CTPN. En el siguiente apartado se describen las distintas pruebas que se deberán ejecutar.

La metodología sugerida para la ejecución de las pruebas incluirá la supervisión de la ejecución de las mismas desde cada entidad implicada en las mismas (los operadores e INETUM) por personal de SUTEL para dar fe del cumplimiento o no de las mismas, durante todo el período de tiempo necesario para la ejecución de éstas.

Durante la ejecución del proyecto se definirá entre todas las partes el calendario detallado



de las pruebas a realizar, así como la duración de cada uno de los periodos para los distintos tipos de pruebas que se detallan a continuación.

5.1.3 Tipos de pruebas

El Plan de Pruebas contemplará la realización de ciertas pruebas sobre las infraestructuras hardware y de comunicaciones, verificación de la seguridad implantada, tanto sobre el perímetro donde residen los servidores como dentro de las salas de proceso de datos.

Desde el punto de vista software, se elaborará un plan que cubra la ejecución de pruebas unitarias sobre cada componente desarrollado, un bloque de pruebas de integración que permitan verificar la correcta integración entre los aplicativos de los operadores y el SIPN, una batería de pruebas con gran nivel de detalle de pruebas funcionales que garantice la funcionalidad de todos los procesos de portabilidad definidos y una batería de pruebas de sistema que permita analizar y verificar un correcto funcionamiento del sistema en su conjunto.

En dicho plan estarán incluidas las siguientes pruebas:

- Pruebas Funcionales
 - Pruebas unitarias internas
 - Pruebas funcionales de los procesos de portación
 - Pruebas de interfaces e integración con los operadores
 - Pruebas de consultas y reportes de las bases de datos
- Pruebas no funcionales
 - Pruebas de Concurrencia y Alta disponibilidad
 - Pruebas de carga y rendimiento
 - Pruebas de seguridad

Todas ellas serán necesarias para validar y aceptar el sistema por parte de todos los usuarios de este.

Pruebas Funcionales

Son las encargadas de verificar el correcto funcionamiento del SIPN desde un punto de vista funcional y de su integración con los sistemas de los operadores.

Las pruebas realizadas dentro de este bloque incluyen las unitarias de desarrollo sobre los componentes del sistema **Portaflow 3.0**. Comprenden también las pruebas de los operadores que realizarán de forma individual usando para ello el operador real y el operador virtual según los escenarios descritos en el plan de pruebas del SIPN, usando de esta forma todas las interfaces disponibles, WEB, SOAP/REST y SFTP.

Los escenarios para estas pruebas funcionales abarcan todas las posibles casuísticas que



se puedan dar dentro de todos los procesos de portabilidad contemplados en la presente oferta.

Adicionalmente se probarán todas las consultas y reportes e información que se puede obtener a través de la interfaz web de **Portaflow 3.0**.

Pruebas no funcionales

Estas pruebas se realizarán sobre el entorno productivo, con el objeto no solo de auditar la seguridad de este sino también de verificar que el rendimiento del mismo es acorde a las necesidades del proyecto.

También se incluirán pruebas de concurrencia, balanceo y alta disponibilidad, para ello se realizarán envíos masivos de solicitudes de portación y se simulará la caída de uno de los nodos para verificar la continuidad de negocio sin pérdida de información ni afectación del servicio

5.1.4 Severidad de los errores durante las pruebas

INETUM hará entrega a los operadores de una matriz de pruebas que deberá ir siendo completada por estos durante las pruebas con el resultado de estas. Cuando una prueba no resulte satisfactoria deberá ser abierto un ticket a través de la herramienta de la mesa de ayuda del ERPN, entregando todas las evidencias y datos utilizados durante la ejecución de la prueba, el número de ticket deberá ser registrado en la matriz para seguimiento de la resolución.

Semanalmente los operadores deberán hacer entrega de los resultados al ERPN para que este pueda realizar un informe consolidado del status y avance de la ejecución de las pruebas.

Se deberá establecer un método de evaluación del resultado de las pruebas que establezca claramente la severidad de la falla y el tiempo máximo de resolución, de acuerdo con la siguiente tabla:

Severidad	Consecuencia	Tiempo máximo de resolución
Bloqueante	La falla es bloqueante para continuar el proceso de pruebas	2 días
Alta	La falla no es bloqueante, no impide continuar el proceso de pruebas, pero no cumple con el requerimiento definido, debería tener prioridad alta en su resolución	4 días
Media	La falla no es alta, no impide continuar el proceso de pruebas, pero no cumple completamente con el requerimiento definido, se tiene un camino alternativo para cumplir el requerimiento. La prioridad de resolución es media, depende de la disponibilidad de desarrollo	15 días
Baja	La falla refiere a aspectos estéticos, mejoras sugeridas, no a aspectos de funcionalidad. La prioridad de resolución es baja, depende de la	Nuevo release



	disponibilidad de desarrollo	
--	------------------------------	--

5.1.5 Gestión de incidencias durante el período de pruebas

Desde el día de inicio de la ejecución de las pruebas, **INETUM** facilitará el acceso a su herramienta de mesa de ayuda a todas las personas encargadas de realizar las pruebas sobre el sistema del ERPN. Además, se facilitará un buzón de correo electrónico como soporte adicional.

Cualquier incidencia o consulta que se tenga en la ejecución y resultado de las pruebas realizadas deberá ser reportada por los medios indicados. **INETUM** analizará la severidad de la incidencia y procederá al análisis y resolución de esta, informando al usuario de la fecha en la que será desplegada la solución.

Una vez desplegada la solución procederá a cerrar el ticket. **INETUM** garantiza e incluso mejora los tiempos de resolución indicadas en la tabla del apartado anterior.

El equipo de desarrollo realizará pruebas internas previamente antes de dar por solucionada la incidencia. Diariamente se establecerán ventanas de despliegue incluyendo la solución de todas aquellas incidencias que hayan sido resueltas, cuyo horario será establecido fuera de la jornada laboral para no interferir en la tarea de los operadores.

5.2 Aceptación del Sistema

La aceptación final del Sistema requerirá del cumplimiento de determinadas fases de implementación que comprenden tanto el desarrollo de los sistemas, así como los distintos tipos de pruebas que se detallan a continuación:

- Desarrollos sobre el ERPN
- Pruebas de Desarrollo (funcionales y no funcionales)
- Aceptación del Sistema (pruebas de integración conjuntas entre ERPN y los operadores, funcionales y no funcionales)

Cabe mencionar que el plan de trabajo en detalle para cada una de estas fases, sus hitos y alcances, así como entregables y los criterios de aceptación de cada etapa serán propuestos al CTPN, quienes deberán aprobarlo previo al inicio de la fase de Desarrollo. Los plazos asignados para cada fase podrán ajustarse en menor medida de acuerdo con el plan de trabajo, siempre y cuando garanticen la fecha de inicio de operaciones establecida.



5.2.1 Pruebas de Desarrollo

En esta fase se validarán los desarrollos realizados por INETUM utilizando el entorno de pruebas.

Se entenderá por terminada esta fase si se cumplen los criterios de aceptación acordados y descritos en la siguiente tabla:

Tipo de Prueba	Pre-requisito	Quién Ejecuta	Quién Valida	Criterio aceptación
Pruebas Unitarias	Desarrollo Concluido	ERP	ERP	100% OK según los criterios acordados
Pruebas Funcionales Manuales de Sistema	Todos los desarrollos concluidos	ERP	Comité CTPN	100% OK según los criterios acordados
	Pruebas unitarias validadas	ERP	Comité CTPN	100% OK según los criterios acordados
	Ambiente de Test disponible	ERP	Comité CTPN	100% OK según los criterios acordados
Pruebas No Funcionales	Arquitectura e Infraestructura lista	ERP	Comité CTPN	100% OK según los criterios acordados

Como ya se ha mencionado anteriormente, INETUM entregará un Plan detallado de trabajo con cada una de las fases de pruebas que deberá seguirse para asegurar la correcta ejecución de éste, incluyendo un cronograma y la metodología a seguir.

5.2.2 Aceptación

Una vez finalizada la fase de Aceptación del sistema, se habilitará el entorno productivo para empezar la fase de aceptación final, incluyendo a usuarios finales para la ejecución de las pruebas UAT, conforme se establece en la siguiente tabla:

Tipo de Prueba	Quién Ejecuta	Quién Valida	Criterio aceptación
Pruebas de Integración entre el ERP y otros operadores	CTPN y ABD	CTPN	100% OK según los criterios acordados
Pruebas no funcionales	CTPN y ABD	CTPN	100% OK según los criterios acordados
Pruebas de UAT	CTPN y ABD	CTPN	100% OK según los criterios acordados

De común acuerdo entre INETUM y el CTPN se podrá aprobar la Aceptación Final y se definirán plazos de corrección para aquellos incidentes presentados.

Sin perjuicio de lo anterior, podrán existir aceptaciones parciales por tipo de servicio, de



común acuerdo entre INETUM y el CTPN.

5.2.3 Aceptaciones Posteriores (Incorporación de nuevos Operadores)

El procedimiento a seguir para las aceptaciones adicionales o posteriores de nuevos Operadores será el mismo descrito en las etapas detalladas anteriormente, a partir de la integración hasta la Aceptación Final.

5.2.4 Pruebas con terceros

INETUM garantiza que realizará pruebas con terceros habilitados por el CTPM y/o SUTEL, en el ambiente de pruebas sin impactar en la operación normal de los operadores.

5.3 Capacitación

INETUM impartirá un plan de capacitación que permita a los operadores conocer toda la funcionalidad de las aplicaciones del SIPN (Portaflow, Web usuario consulta, Mobydesk y demás).

Se procederá con la elaboración de los correspondientes manuales, se realizará la convocatoria a las sesiones formativas y se realizarán las mismas con un tiempo suficiente para que los asistentes tengan el conocimiento necesario de cara a la realización de las pruebas sobre el nuevo sistema, y posteriormente para su uso en modo productivo, siendo este de al menos 15 días de acuerdo con las bases técnicas

Idioma

Todos los planes de capacitación serán impartidos en idioma español.

Material

INETUM hará entrega a los asistentes al plan de capacitación de toda la documentación necesaria para un correcto desarrollo del curso a impartir.

Para ello, y en idioma español, se entregarán manuales y documentos adicionales que permitan dar a conocer no solo la solución informática desde un punto de vista teórico, sino también desde el punto de vista práctico, desarrollándose para ello ejercicios y demostraciones al respecto.

Asistentes

La convocatoria a los cursos se realizará con cada uno de los operadores, así como de la Sutel.

En principio se establecerá un dimensionamiento de asistentes a la misma de 50 personas por módulo de capacitación y por tanda, previéndose en inicio dos tandas de capacitación.

Si se requiere repetir la capacitación, o bien aumentar el número de asistentes a la misma, INETUM se reservará el derecho de cotizar el servicio.



Según el temario a impartir, será responsabilidad de cada OSTM identificar al recurso más idóneo para asistir a cada módulo del plan de capacitación.

Organización y convocatoria

La formación será impartida por un Consultor experto en portabilidad el cual estará a cargo de todo el temario, y será el responsable de llevar a buen fin el ciclo formativo no sólo desde el punto de vista teórico sino también práctico.

Se promoverá una reunión de seguimiento del proyecto en fecha cercana al inicio de las actividades formativas donde se ultimarán los detalles de la convocatoria.

El responsable del proyecto por parte de **INETUM** hará entrega de un documento que indicará, entre otras cosas, el mecanismo mediante el cual cada operadores deberá hacer llegar la relación de personas que asistirán al evento formativo con el objeto de que se pueda formalizar la convocatoria.

Temario de la capacitación

El temario del plan de capacitación se estructurará en dos módulos, el administrativo y el técnico, dando cumplimiento a lo exigido en el pliego de condiciones, siendo en principio 3 sesiones de 8 horas cada una para el módulo administrativo y 2 sesiones de 8 horas para el módulo técnico, no obstante, se podrá extender de común acuerdo entre el CTPN y el ERPN si se viese la necesidad.

Cada módulo tendrá la duración suficiente como para que se cubra todo el temario a tratar.

- Temario Módulo Administrativo.
 - Acceso y uso de la aplicación Portaflow.
 - Tramitación de procesos de portabilidad
 - Descarga de ficheros diarios
 - Consultas sobre procesos de portabilidad
 - Reportes y estadísticas
 - Mesa de ayuda del ERPN (Mobydesk)
 - Servicio de soporte y notificación de errores
- Temario Módulo Técnico.
 - Plataforma hardware y de comunicaciones del ERPN
 - Interfaces de comunicación y protocolos con el ERPN
 - Mesa de ayuda del ERPN (Mobydesk)



- Servicio de soporte y notificación de errores

Además de la capacitación inicial, **INETUM** incluye como valor añadido un plan de capacitación continua que contempla jornadas con la periodicidad que se defina y/o se requiera en cada caso.

El propósito de este plan no es otro que implementar una mejora continua de procesos, revisar aquellos aspectos de la operativa cotidiana de la portabilidad que son susceptibles de mejora, así como detectar nuevas funcionalidades que ayuden y simplifiquen la gestión de los procesos de portabilidad.

En estas jornadas **INETUM** propondrá soluciones en base a experiencias en otros países, dando a conocer las buenas prácticas de otros sistemas de portabilidad, e incluso analizando y diseñando posibles nuevas funcionalidades que puedan aportar beneficios tanto a los OSTM como a los usuarios finales.

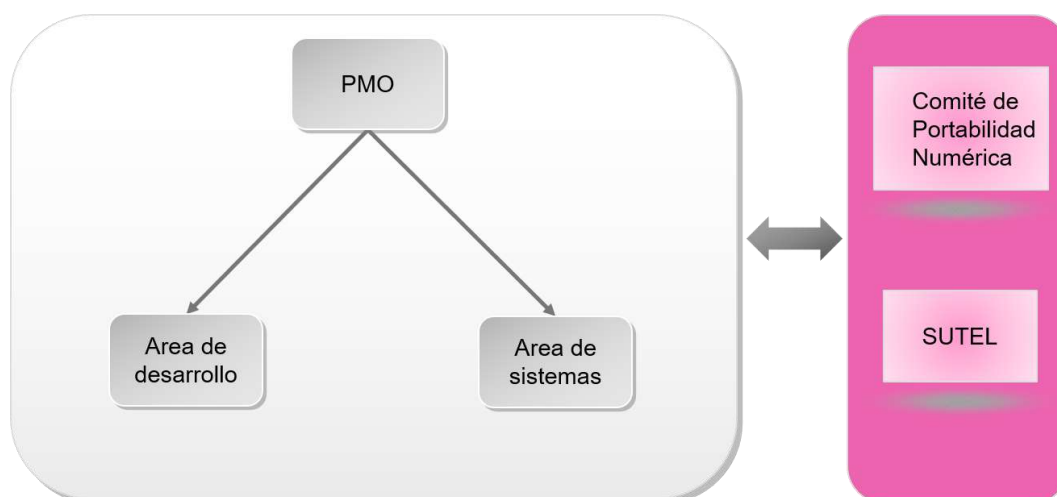
5.4 Equipo de trabajo

El equipo de trabajo que aportará INETUM al proyecto será multidisciplinar, vistas las distintas áreas que un proyecto de estas características tiene que cubrir.

Dentro del equipo participarán de forma puntal y permanente un equipo de profesionales. Algunos de ellos tendrán los conocimientos específicos para acometer sus tareas precisas, mientras que los recursos que deban cubrir los temas relativos a la portabilidad serán consultores expertos en esta materia y permanecerán asignados al proyecto durante toda la vigencia del servicio.

INETUM asegura que el equipo de trabajo involucrado en la implementación de la solución técnica, objeto de los términos de referencia establecidos en las condiciones generales de contratación, contará con la apropiada experiencia técnica, operativa y administrativa, así como con el entrenamiento necesario para su desarrollo, implementación, prueba y operación.

Con el fin de gestionar la ejecución del proyecto objeto del Contrato, el Gerente de Proyecto de INETUM será el punto de contacto principal con la SUTEL, el Comité Técnico de la Portabilidad Numérica y con los Prestadores que suscriban el respectivo contrato con la ERPN. El Gerente de Proyecto tendrá la misión de coordinar el desarrollo de todas las actividades relacionadas con la implementación de la solución y de la remisión de los correspondientes entregables que se deriven de las obligaciones contractuales adquiridas.



El esquema del equipo de trabajo se resume en la siguiente gráfica:

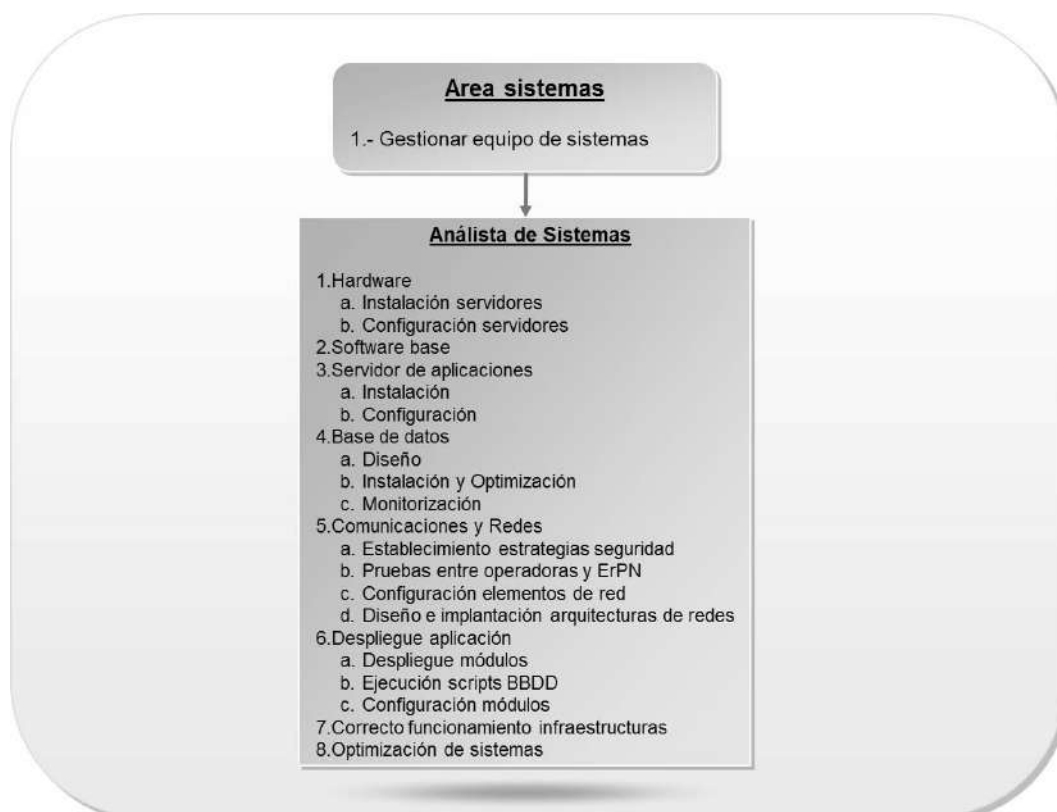


En las 3 áreas, en función de las necesidades que se vayan presentando en el proyecto, han de requerir la participación de ingenieros y/o consultores especialistas para la realización de tareas.

Entrando en profundidad en cada área, los roles y tareas dentro de cada una de ellas quedaría definido de la siguiente manera:



Dentro de la segunda área se tratarán todos los temas relacionados con sistemas:





Por último, y una vez puesto en producción el sistema de Administración de Portabilidad Numérica entra en juego el Área de soporte y operación:



El equipo de trabajo estará compuesto por miembros de INETUM ya conocidos por el Comité de Portabilidad Numérica, los cuales estuvieron prestando el servicio desde el inicio de la portabilidad numérica en Costa Rica:

- PMO: José Carlos Aljan y Patricia Sánchez Ortega
- 1 gerente de proyecto: José Carlos Aljan
- 1 analista funcional y orgánico: Alberto Bueno
- 2 analistas de sistemas: Carlos Javier Pérez Rodríguez y Biaggini Durán
- 5 ingenieros de desarrollo: Jose Luis Martínez, Carlos Javier Pérez Rodríguez, Iván Castrillo, Biaggini Durán y Alberto Bueno
- 2 técnicos de soporte: Jose Luis Martínez y Carlos Javier Pérez Rodríguez

Sin embargo, dadas las características del proyecto, y teniendo en cuenta la versatilidad de los componentes del equipo (producto de su amplia experiencia reflejada en las hojas de vida adjuntadas), los perfiles necesarios para llevar a buen término el desarrollo de este proyecto pueden ser cubiertos por personas capaces de asumir diferentes perfiles según las necesidades que el proyecto tenga.



6 Requerimientos de Operación

6.1 Seguridad

INETUM se compromete a guardar la más estricta confidencialidad sobre el contenido del contrato objeto de la presente propuesta de colaboración, así como los datos o información a la que pueda tener acceso o generar como consecuencia de la ejecución de este, pudiendo únicamente poner en conocimiento de terceros aquellos extremos que SUTEL y/o el Comité de portabilidad le autorice por escrito y a usar dicha información a los exclusivos fines de la ejecución del contrato.

INETUM pondrá en marcha una serie de **medidas dirigidas a garantizar la seguridad y confidencialidad** de los datos en los apartados que se resumen a continuación:

- Respecto a la propiedad de la información.
- En relación con la confidencialidad de los datos manejados.
- Relativas al personal asignado al proyecto

En cuanto al material disponible durante la ejecución del proyecto, INETUM designará una persona responsable de las relaciones con SUTEL y/o el Comité de portabilidad, a efectos del uso correcto del material y de la información a manejar.

INETUM manifiesta que cumplirá con los siguientes puntos:

- No enviará o distribuirá información confidencial a terceros, incluyendo empleados de INETUM que no requieran conocerla, diferentes de aquellos empleados autorizados expresamente por INETUM.
- No usará la información confidencial para su propio beneficio o para el beneficio de terceros.

6.1.1 Descripción General

El Grupo INETUM, con el fin de satisfacer mejor las expectativas de su mercado (Francia, Europa, América Latina, África, Oriente Medio), toma decisiones diferenciadoras con el fin de proporcionar un catálogo de soluciones y servicios de valor añadido, basados en la proximidad, la industrialización y la innovación.

- La proximidad tiene como objetivo fortalecer el acompañamiento de nuestros clientes, con un mayor conocimiento de su sector, y participar activamente en la economía local.
- La industrialización, punta de lanza de nuestro negocio, responde a los retos económicos de nuestros clientes en un contexto de fuerte transformación digital.
- La innovación, en el corazón de nuestro proyecto empresarial, se traduce en una



búsqueda constante de nuevas tecnologías basada en la experiencia del cliente y las mejores alianzas.

Nuestra ambición y el crecimiento de nuestras actividades, en línea con la evolución del mercado, están respaldados por nuestra dinámica de nuestros técnicos, nuestro desempeño empresarial y la eficacia en la integración de diferentes adquisiciones.

La confianza de nuestros clientes, fuerza impulsora de nuestro desarrollo, es una garantía de la calidad de nuestra estrategia y proyecto empresarial.

6.1.2 Política de Seguridad de la Información

En materia de Seguridad de la Información, nuestro objetivo es lograr un alto nivel de seguridad para nuestros clientes:

- Garantizar la seguridad de los activos de nuestros clientes: la información que nos confían debe ser protegida contra toda alteración, pérdida, daño, divulgación o acceso no autorizado.
- Establecer un justo equilibrio entre los costes organizacionales y económicos destinados a la mitigación del riesgo y el perjuicio que pueda ocasionar la materialización del riesgo en sí.
- Promover medidas de prevención para garantizar la seguridad de los datos personales y activos tanto de los clientes, como los corporativos.
- Fomentar una cultura de seguridad y privacidad en toda la organización.
- Gestionar los incidentes de seguridad con objeto de limitar los impactos para Inetum y nuestros clientes.

INETUM cuenta con las siguientes certificaciones en materia de Seguridad y Calidad de la Información:

- ISO-27001 (adjunto en la propuesta)
- ISO-9001 (adjunto en la propuesta)
- CMMI
- ISO-20000
- Tisax Assessment
- ISO-22301
- ISO-27701

En cualquier caso, todos sus datos se consideran confidenciales y se procesarán de acuerdo con el nivel adecuado de seguridad y ninguno de ellos se transfiere fuera de los países de la Unión Europea o si un país no cuenta con un nivel adecuado de datos personales.



6.1.3 Aspectos organizativos para la seguridad

Para administrar la seguridad de información dentro de la organización, INETUM asegurará lo siguiente:

- Cumplimiento de las medidas técnicas y organizativas previstas en la normativa de protección de datos personales.
- Designación de delegado de protección de datos personales.
- Participación de la Gerencia en Seguridad de Información o equivalente.
- Coordinación de seguridad de la Información.
- Asignación de responsabilidades de seguridad de la información
- Proceso de autorización para la instalación de procesamiento de información.
- Acuerdos de Confidencialidad
- Contacto con autoridades del SIPN
- Revisiones independientes de seguridad de información
- Identificación de riesgos relacionados con partes externas
- Directivas de seguridad en el trato con clientes
- Directivas de seguridad en acuerdos con terceras partes

6.1.4 Seguridad ligada a los recursos humanos

INETUM está comprometido a:

- Mantener y mejorar de forma continua la eficacia y la eficiencia del Sistema Integrado de Gestión evaluando los riesgos y oportunidades, objetivos y metas, a través de revisiones periódicas e implantando las medidas correctoras necesarias en caso de desviación de los objetivos marcados.
- Cumplir con la legislación vigente aplicable y otros requisitos suscritos voluntariamente por la organización en todos aquellos aspectos relativos a la calidad de nuestros productos y servicios, medio ambiente y seguridad de la información.
- Establecer mecanismos de interacción continua con el cliente a fin de conocer y canalizar sus necesidades y expectativas.
- Difundir esta política a las partes interesadas, promoviendo una actitud proactiva de todo el personal, a través de una participación activa basada en capacitaciones y concienciación adecuadas a sus requerimientos.
- Avalar, por parte de la Dirección, el suministro de los recursos y la delegación en los responsables de los sistemas de gestión, las funciones de formular el Sistema Integrado de Gestión, supervisar su implantación, asegurar su cumplimiento y



revisar su efectividad; para ello, dichos responsables quedan investidos con la suficiente y necesaria autoridad dentro de la organización.

6.1.5 Gestión de Comunicaciones y operaciones

Para asegurar la correcta y segura operación de las instalaciones de procesamiento de información, **INETUM** cuenta con:

- Procedimientos y responsabilidades operativas:

Los roles y tareas operativas deben estar definidas y documentadas mediante procedimientos que son revisados/actualizados de acuerdo con los cambios operativos

- Administración de servicios entregados por terceros
- Los terceros que participen conocerán y aplicarán todas las definiciones de seguridad de la información
- Aceptación y planificación de sistemas:
 - Existirá un proceso de verificación previo a los pasos de producción
 - Existirá un procedimiento de control de cambios con autorizaciones y registro
- Protección contra código malicioso

Tanto las estaciones de trabajo, notebooks como servidores disponen de un antivirus operativo y actualizado en todo momento.

- **Recuperación y Respaldos:**
 - Los respaldos serán administrados en áreas seguras, esto es, con control de acceso
 - Los medios dados de baja serán borrados de manera segura
 - Se establece una política de respaldo periódico de la información, que minimice los riesgos de pérdida frente a situaciones excepcionales, para lo cual los respaldos deben realizarse al menos una vez por día.
 - Existen procedimientos de recuperación, contingencia y continuidad operacional debidamente certificados por Auditorías.
 - Existen respaldos históricos disponibles durante el período de ejecución del contrato.
- **Administración de Seguridad:** se define el rol de administrador de seguridad a nivel de todos los componentes críticos de la solución.
- **Intercambio de Información:** El intercambio de información debe realizarse utilizando métodos de cifrados sólidos
- **Transacciones en línea:** Las transacciones en línea estarán cifradas con un método



sólido y debidamente autenticadas en los casos necesarios.

- **Monitoreo**

- Existirá un control tipo IPS, que permita detectar y tomar acciones ante código malicioso y ataques que perjudiquen la disponibilidad de los servicios.
- Se establecen controles con Firewalls, WAF's y prevención de ataques de denegación de servicios.
 - Se establece un monitoreo 7x24 que permita asegurar la disponibilidad y seguridad de los servicios. Este monitoreo incluye todos los componentes críticos de la solución.
 - Existe una sala de control 7x24

6.1.6 Adquisición, desarrollo y mantenimiento de sistemas de información

INETUM garantiza que la seguridad es una parte integral de los sistemas de información.

- Las aplicaciones y/o sistemas funcionarán publicando servicios del tipo web con cifrado (https), mediante intercambio de transacciones en línea vía WebServices SOAP, REST y con SFTP seguro para el intercambio de archivos con datos (para efectos de conciliación de datos).
- Sólo se publicarán los servicios requeridos para el funcionamiento del sistema.
- Existirá un proceso de autenticación y autorización de los usuarios/sistemas que utilizan las aplicaciones
- El sistema contará con doble factor de autenticación, al menos para las conexiones remotas, y sobre sistemas críticos.
- Existirá un sistema de administración de usuarios con diferentes roles y administración de roles
- Existirá un registro de las transacciones realizadas por al menos doce (12 meses, indicando el formato del log correspondiente.
- Procesamiento correcto en aplicaciones
 - La entrada de datos en los sistemas y aplicaciones contarán con mecanismos de validación para comprobar si son correctos y adecuados dentro de los rangos definidos para dichos datos.
 - Los sistemas incluirán controles internos de validación de datos para detectar cualquier corrupción de la información por errores de proceso o actos deliberados.
- El intercambio de información será cifrado en el servicio habilitado utilizando



criptografía sólida.

- Seguridad en los sistemas de archivos: Estarán definidos y aplicados distintos perfiles de acceso a los sistemas de archivos, diferenciando al menos permiso de lectura, escritura y ejecución.
- Seguridad en los ambientes
 - El ambiente de producción estará separado, por medidas de seguridad adecuadas, de los demás ambientes.
 - Se generarán datos de prueba distintos a los datos de producción. No se emplearán datos personales de producción salvo que hayan sido objeto de un previo proceso de anonimizar.
- Administración de vulnerabilidades técnicas
 - Se mantendrán al día, de acuerdo con la clasificación de severidad, las actualizaciones de seguridad declarada por los proveedores, los OSTM y la industria.
 - Se realizarán análisis de vulnerabilidades de forma periódica.
- El código de programación del sistema respetará las 10 principales reglas del Open Web Application Security Project ("OWASP"; Proyecto de seguridad de aplicaciones web abiertas).

6.1.7 Gestión de incidentes de seguridad

Para asegurar que los eventos de seguridad de información y las vulnerabilidades asociadas sean comunicadas de manera tal que permita tomar acciones correctivas oportunas, **INETUM** contempla lo siguiente:

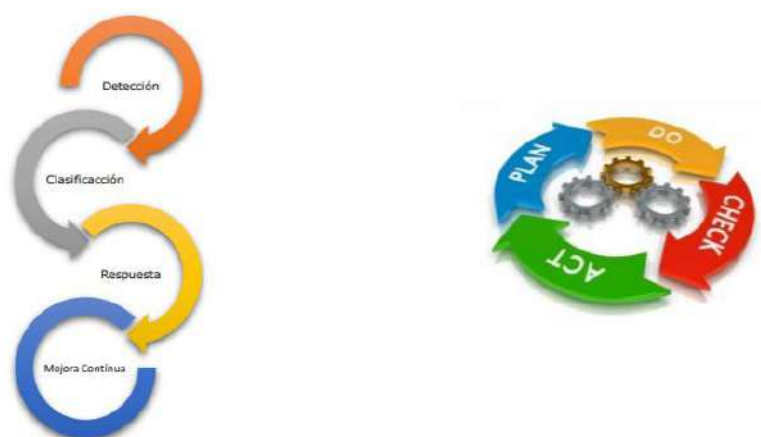
Reportar vulnerabilidades y eventos de seguridad

- Se debe mantener contacto con los proveedores e Industria para recibir las alertas de seguridad que implican actualización de software o elementos físicos.
- Debe existir una clasificación de los incidentes de seguridad.
- Debe existir registro de los incidentes de seguridad.

En caso de vulneración de seguridad que incida en la Protección de Datos Personales, INETUM se compromete a dar cumplimiento a las comunicaciones previstas en el Decreto Nro. 64/020.

- Administración y mejora de incidentes de seguridad de información: INETUM cuenta con una gestión de los incidentes de seguridad.

La gestión de incidentes forma parte de un proceso de mejora continua de la seguridad.



Las lecciones aprendidas de los incidentes de seguridad deben contribuir a la mejora en los procesos de gestión de incidentes.

Debe llevarse a cabo un análisis posterior al incidente como parte del ciclo de mejora continua PDCA (Plan, Do, Check, Act). Este análisis debe involucrar a todas las partes interesadas, las cuales deberán comprometerse a realizar las mejoras necesarias. Para esto se podrá formar un comité o se podrá organizar algún tipo de reunión que involucre a personas con capacidad para tomar decisiones.

INETUM establecerá responsabilidades y procedimientos que garanticen una respuesta rápida, efectiva y pertinente en caso de que se produzca un incidente de seguridad de la información.

INETUM pedirá a todos los empleados y personal externo que utilizan los servicios y sistemas de información que registren e informen de cualquier brecha de seguridad que observen o sospechen de su existencia.

Los eventos de seguridad de la información deben ser reportados lo antes posible, a través de los canales apropiados, por todo el personal.

Se definirá un proceso para:

- Evaluar los eventos de seguridad de la información.
- Decidir si debieran o no ser clasificados como incidentes de seguridad de la información.
- Responder a incidentes de seguridad de la información.

INETUM llevará a cabo un análisis de causa raíz y acumular el conocimiento adquirido siguiendo este análisis y la resolución de incidentes para reducir la probabilidad o impacto de nuevos incidentes.

INETUM define y aplica procedimientos de identificación, recolección, adquisición y protección de información que puede ser utilizada como evidencia cuando sea necesario.

Se implementará un sistema de escalado para manejar los incidentes más graves durante



una emergencia.

6.1.8 Gestión de continuidad del Negocio

El objetivo de esta gestión será:

- Asegurar que los compromisos contraídos con los clientes en términos de continuidad del servicio puedan cumplirse bajo cualquier circunstancia.
- Alcanzar los objetivos negociados en los acuerdos de servicio (SLA), es decir, garantizar el nivel de continuidad compatible con las necesidades de negocio.
- Asegurar estos objetivos, en particular para funciones críticas de negocio, identificadas en el SLA

Para evitar la interrupción de actividades de negocios y para proteger los procesos críticos de negocios de los efectos producidos por una falla mayor de sistemas de información o un desastre y asegurar su reconstitución oportuna, se contará con lo siguiente:

- Un sistema de Gestión del Riesgo y Continuidad de Negocios
- Diseño e implantación de planes de continuidad que incluyan seguridad de información
- Marco de trabajo para planificación de continuidad de negocios
- Pruebas, mantenimiento y reevaluación de planes de continuidad de negocios
- Arquitectura de Alta Disponibilidad.

6.1.9 Conformidad o Cumplimiento

Con respecto de cualquier ley, estatuto, regulación u obligación contractual y cualquier requerimiento de seguridad:

- Cumplimiento de los requerimientos legales, reglamentarios y contractuales que correspondan.
- Conformidad con la política, los estándares de seguridad, y conformidad con los requerimientos técnicos establecidos en estas Bases.
- Consideraciones de auditoría de sistemas
 - Se proporcionarán medios para verificar que se han cumplido los requisitos de seguridad.
 - Se indicará la periodicidad de las auditorías y comunicar sus resultados.
 - Los logs de auditoría estarán protegidos de modificaciones y deben existir controles para detectar si los mecanismos han sido violados y los logs han sufrido manipulación.



- INETUM registrará toda actividad que sea relevante para el trazado de las acciones implicadas en la portabilidad, en el cual se mantendrá:
 - el valor anterior
 - el valor actual
- fecha y hora (timestamp), que permita ordenar en el tiempo la ejecución de las diferentes transacciones.

6.2 Respaldo y recuperación de la información

Se implementará una **política integral de copias de seguridad** para toda la plataforma desplegada en **Oracle Cloud Infrastructure (OCI)**, con el objetivo de garantizar la **disponibilidad, integridad y recuperación de la información**, en cumplimiento de los requisitos de continuidad operativa exigidos a la ERPN.

La estrategia de respaldos se basará en la automatización de copias de seguridad, con los siguientes esquemas de ejecución y retención:

- **Backup diario incremental**, con una **retención de dos (2) semanas**.
- **Backup semanal completo**, con **retención mensual**.
- **Backup mensual completo**, con **retención anual**.

Los respaldos se gestionan mediante los **servicios nativos de backup de OCI**, apoyados en infraestructura de almacenamiento cloud de alta durabilidad y redundancia, eliminando la necesidad de medios físicos o magnéticos locales. Estos servicios permiten una gestión centralizada, segura y auditable de las copias de seguridad, así como su restauración controlada en caso de incidencias.

Las copias de seguridad se realizan de forma **automática y programada**, conforme a las políticas definidas, y se almacenan en ubicaciones seguras dentro de la región OCI correspondiente, garantizando la protección de la información y su disponibilidad ante fallos, errores operativos o requerimientos de recuperación.

Asimismo, **todas las operaciones de respaldo y restauración quedan debidamente registradas**, permitiendo su seguimiento y auditoría, en línea con los principios de trazabilidad y control exigidos para la operación del Sistema Integral de Portabilidad Numérica (SIPN).

6.3 Actualización y mantenimiento del Sistema

Todo sistema que se precie como tal, y mucho más aquellos como éste considerados sistemas de misión crítica sufren a lo largo de su vida una serie de tareas que consisten en realizar actualizaciones y mantenimientos que garanticen su correcto funcionamiento.

INETUM ejecutará las actividades de mantenimiento en las ventanas que se establezcan, siempre fuera de la jornada laboral, domingos o feriados. Todos los operadores serán



informados de las actividades de mantenimiento programadas con una antelación de al menos 10 días hábiles.

Hemos de diferenciar para detallar el presente apartado, 3 (tres) grandes módulos sobre los cuales el sistema recibirá actualizaciones y mantenimientos.

El primer se corresponde con el **hardware** utilizado en el proyecto que, gracias a su mantenimiento y actualización, entre otras cosas, garantizará que sus prestaciones y rendimiento se mantengan inalterables en todo momento.

El siguiente punto se refiere a todas las **infraestructuras software** utilizadas en el proyecto, entendiendo por éstas, al software base utilizado para una correcta explotación de la/s aplicación/es de portabilidad, así como a la disponibilidad de otros servicios como pueden ser la mensajería, la gestión de un directorio, el gestor de base de datos entre otros.

Para concluir, el último punto a desarrollar dentro de la presente propuesta se corresponde con las actividades que deben de realizarse sobre las propias aplicaciones de portabilidad, las cuales en su régimen de mejora reciben actualizaciones y mantenimientos de forma acorde a su ciclo de vida.

6.3.1 Actualización y Mantenimiento del HW

En la solución propuesta, basada en **Oracle Cloud Infrastructure (OCI)**, las actividades de **actualización y mantenimiento del hardware** subyacente a la plataforma del Sistema Integral de Portabilidad Numérica (SIPN) son gestionadas íntegramente por el proveedor de infraestructura cloud, de acuerdo con sus políticas operativas y de continuidad del servicio.

OCI proporciona una infraestructura **estandarizada, redundada y de alta disponibilidad**, en la que las tareas de mantenimiento preventivo, correctivo y de renovación tecnológica del hardware se realizan de forma planificada y controlada, minimizando cualquier impacto sobre los servicios desplegados.

Las operaciones de mantenimiento del hardware incluyen, entre otros aspectos:

- Sustitución de componentes defectuosos o en fin de vida.
- Actualización progresiva de la infraestructura física.
- Mejora continua de las capacidades de cómputo, red y almacenamiento.
- Aplicación de buenas prácticas de operación en centros de datos de misión crítica.

Estas tareas se ejecutan siguiendo procedimientos internos del proveedor cloud, diseñados para **garantizar la continuidad del servicio**, apoyándose en arquitecturas tolerantes a fallos y en mecanismos de redundancia que permiten mantener la operación del SIPN sin interrupciones apreciables.

Desde el punto de vista de la ERPN, el modelo cloud de OCI permite **desacoplar la operación del servicio de la gestión del hardware**, evitando la necesidad de planificar intervenciones



físicas, gestionar inventarios o realizar renovaciones tecnológicas, y asegurando en todo momento la **vigencia tecnológica** de la plataforma durante el periodo de prestación del servicio, conforme a lo requerido en el pliego de condiciones.

6.3.2 Actualización y Mantenimiento del SW

Tareas Preventivas

De forma diaria se realizarán todas las tareas de **prevención** sobre el software base utilizada en el proyecto, estas tareas de revisión y prevención consisten en chequear sobre el software desplegado revisiones desde todo punto de vista para que se pueda garantizar el nivel de servicio requerido en las bases del presente concurso.

Dentro de estas tareas se encuentra la verificación de que no se requiere instalar ninguna actualización sobre los mismos, que desde el punto de vista base de datos, la misma cuenta con espacio suficiente como para alojar la información a almacenar a lo largo de la jornada laboral en curso, que no existe problema alguno con los parámetros y configuración de los servicios desplegados y en funcionamiento, y un largo etcétera que cubre de manera preventiva todos los aspectos que pueden llegar a presentarse sobre el software desplegado.

Tareas Correctivas

Es posible que durante el uso del software base del proyecto, se presenten sobre estos problemas de variada índole, ante su detección, los fallos se han de reportar de forma inmediata para obtener su pronta solución.

Para ello no sólo se apelará a la experiencia que los profesionales de **INETUM** tienen en la materia, sino que también se ha de abrir incidencia a los propios fabricantes del software afectado a través de los contratos de mantenimiento y soporte que se mantendrán vigentes con cada uno de ellos.

Las presentes incidencias básicamente cuentan con dos posibles vías de solución, la primera de ellas es, si se conoce el origen y solución del problema, ante este tipo de situación, se actuará de la forma que proceda a aplicar con la mejor de las prácticas la solución que corresponda, dando así por solventada la incidencia.

La restante vía de solución se presenta ante el supuesto caso en que la solución definitiva se dilate en el tiempo, en este caso, se procederá a aplicar las denominadas soluciones transitorias, que consisten en resolver la incidencia de forma temporal hasta tanto se nos hace llegar la solución definitiva por parte del fabricante, momento en el cual y tras su implantación se da por resuelta la acción correctiva.

También existirá la posibilidad en la que en lugar de ser **INETUM** quien detecte la acción a corregir, ésta nos sea informada de forma directa por algún fabricante sin que a la fecha se nos haya presentado incidencia alguna.

Ante casos como el expuesto en el párrafo anterior, se verificarán todos los datos oportunos



con el fabricante, se analizará si procede o no realizar la corrección en cuestión, y en caso de aplicar, la misma se llevará a cabo por los profesionales que procedan de forma oportuna.

Tareas Adaptativas

Dentro de las tareas propias de gestionar el **ERP**, existen las que aplican sobre la evolución del servicio, las cuales se analizan día a día, verificando que todas las prestaciones se brindan de forma acorde según el volumen de información a tratar, los tiempos de respuesta esperados, así como demás parámetros propios de todo el software que pueden verse modificados en función de la propia necesidad del servicio.

Las tareas adaptativas surgen cuando la demanda del servicio crece y el sistema debe ser adaptado a esas nuevas necesidades, por lo tanto, los recursos afectados al proyecto deberán verificar entre otros los siguientes aspectos.

Revisar a diario el rendimiento de la base de datos y mantener su rendimiento a diario realizando las tareas que correspondan, generación de nuevos índices, o bien regenerar los mismos, mejorar los tiempos de acceso, las sentencias de SQL, y un largo etcétera que aplica sobre el gestor de base de datos.

También podemos citar adaptaciones a realizar sobre el sistema operativo, o bien sobre las herramientas de monitorización y control de la plataforma, así como otras como puede ser el gestor de backup, o el propio clúster, optimizando y adaptando su configuración para mantener y mejorar los tiempos de respuesta de todos y cada uno de los servicios que se requieren dentro del ERP.

Por último y no por ello menos importante, se encuentra el análisis, gestión y adaptación de otras herramientas de infraestructura utilizadas en el proyecto, tales como los servidores de aplicaciones, la base de datos y el servidor de documentación entre otros.

Estas herramientas como todas las enunciadas anteriormente son y serán analizadas de forma diaria y constante, con la finalidad de adaptar sus prestaciones y poder así mantener el rendimiento del sistema en su conjunto de forma óptima durante todas las jornadas de trabajo.

Para ello se analizarán logs, tiempos de acceso, la velocidad en el tratamiento de la mensajería, los tiempos de validación y servido de páginas, resultados que una vez obtenidos y analizados detalladamente, nos proporcionan toda la información necesaria como para optimizar configuraciones, instalaciones, instancias y un largo etcétera que aplican sobre el rendimiento final de las arquitecturas desplegadas en el proyecto.

Tareas Evolutivas

Puede resultar que producto de la evolución propia del servicio de portabilidad se deban de adecuar las prestaciones de los productos software instalados, se podría asegurar que



una evolución software debería de verse acompañada de una evolución previa del hardware, pero tanto para un caso como para el otro, se analizarán las nuevas necesidades y se propondrán las adecuaciones que correspondan.

Por citar algún ejemplo, podría presentarse una demanda elevada en la mensajería de portabilidad que no puede ser atendida correctamente por los servicios desplegados, ante una situación como esta, se propondrá la implantación de un nuevo servicio paralelo de mensajería con el fin de poder atender la mayor demanda.

Puede darse el caso también de que deba de generarse una nueva instancia en la base de datos como resultado de una evolución de la aplicación de portabilidad, conocidos los nuevos requerimientos los mismos se analizarán con el fin de adoptar la solución más eficiente y rápida para dar respuesta al nivel de servicio requerido.

Serían innumerables los casos que pueden tener que cubrirse dentro del presente apartado de tareas evolutivas que aplican sobre el software base, por lo expuesto, nuestro compromiso es evolucionar según así se requiera en todo momento y durante toda la vida del proyecto.

6.3.3 Actualización y Mantenimiento de Portaflow

Tareas Preventivas

Al igual que para todos los componentes anteriores que forman parte de la plataforma, de forma diaria se realizarán todas las tareas de prevención sobre las aplicaciones de negocio utilizadas en el proyecto, estas tareas de revisión y prevención, consisten en chequear **Portaflow** y todos sus módulos e interfaces, así como otros módulos que conforman las aplicaciones de portabilidad, revisiones desde todo punto de vista para que se pueda garantizar el nivel de servicio requerido en las bases del presente concurso.

Dentro de estas tareas se encuentra la verificación de que no se requiere instalar ninguna actualización (upgrade) o revisión (update o patch) sobre los mismos. Así como que no existe problema alguno con los parámetros y configuración utilizados por las aplicaciones desplegadas.

Tareas Correctivas

Es posible que, durante el uso de las aplicaciones de negocio desplegadas en el ente central, se presenten sobre éstas problemas denominados errores ocultos que, ante su detección, éstos se han de reportar de forma inmediata para obtener su pronta solución al equipo de soporte.

El equipo de trabajo de INETUM resolverá la incidencia dentro de los plazos establecidos por contrato con el fin de mantener el nivel de servicio requerido.

Estos fallos se resolverán desde nuestro centro de desarrollo ubicado en Madrid, momento en el cual y tras su implantación se da por resuelta la acción correctiva.



Tareas Adaptativas

Dentro de las tareas propias de gestionar las aplicaciones de negocio del ERP, existen las que aplican sobre la evolución del servicio, las cuales se analizan día a día, verificando que todas las prestaciones se brindan de forma acorde según el volumen de información a tratar, los tiempos de proceso en que se realizan las actividades, así como otros parámetros propios de nuestras aplicaciones que pueden verse modificados en función de la propia necesidad del servicio.

Las tareas adaptativas surgen cuando la demanda del servicio crece y las aplicaciones de negocio deben ser adaptadas a esas nuevas necesidades, es por ello que los recursos afectados al proyecto deberán verificar entre otros los siguientes aspectos.

Revisar a diario el rendimiento de las aplicaciones de negocio de forma individual y en conjunto con el fin de mantener su rendimiento y operatividad, realizando para ello las tareas que correspondan, tales como interactuar con los administradores del software base y el hardware para solicitar a éstos adaptaciones que promuevan una mejora no solo en las aplicaciones sino también en el conjunto de la plataforma.

Tareas Evolutivas

Puede resultar que producto de la evolución propia del servicio de portabilidad se deban de adecuar las prestaciones de las aplicaciones de negocio desplegadas, estas evoluciones pueden darse en principio por dos vías totalmente distintas.

La primera de ellas es que se promueva dentro del Comité de Técnico de Portabilidad una modificación sobre la especificación operativa y esta conlleve a generar una evolución sobre el sistema **Portaflow**, así como en la de los propios operadores.

La restante es que producto del día a día tanto INETUM como los operadores detecten la necesidad de mejorar / evolucionar ciertos aspectos de las aplicaciones de negocio de portabilidad desplegadas en el ERP.

Para ambos casos se recopilarán todos los requisitos necesarios para poder elaborar un plan de trabajo que consistirá en una planificación detallada de tareas, junto al debido sustento de cada una de ellas.

6.3.4 Procedimiento de actuación ante actualizaciones y mantenimientos

Ante situaciones como las descritas en los párrafos anteriores se llevará a cabo el siguiente procedimiento de actuación.

Análisis y Estudio de la Situación

Con independencia de la tipología de actualización y/o mantenimiento a llevar a cabo, el responsable del proyecto por parte de INETUM, analizará todos los aspectos que aplican sobre la tarea a realizar de forma conjunta con los diversos profesionales del proyecto que



puedan verse afectados por la intervención a realizar.

Para todo este tipo de actividades, se terminará diseñando un plan de acción que se basará en la premisa fundamental de realizar todas las intervenciones necesarias en el menor tiempo posible, con las máximas garantías de éxito.

Presentación del Plan de Acción

Ante situaciones como las descritas, el responsable máximo del proyecto por parte de **INETUM**, convocará a reunión al Comité de Portabilidad para presentar el Plan de Acción que corresponda en cada momento.

Se debatirá el contenido del citado documento, argumentando los porqué nos lleva a ejecutar las intervenciones propuestas, así como los riesgos de no acometerlas y las ventajas de llevarlas a cabo.

A continuación, se debatirá sobre la planificación de las tareas a realizar, argumentando cada una de las fechas y mencionando los tiempos de posible parada del servicio, así como las ventanas en las que se actuará para evitar la citada parada.

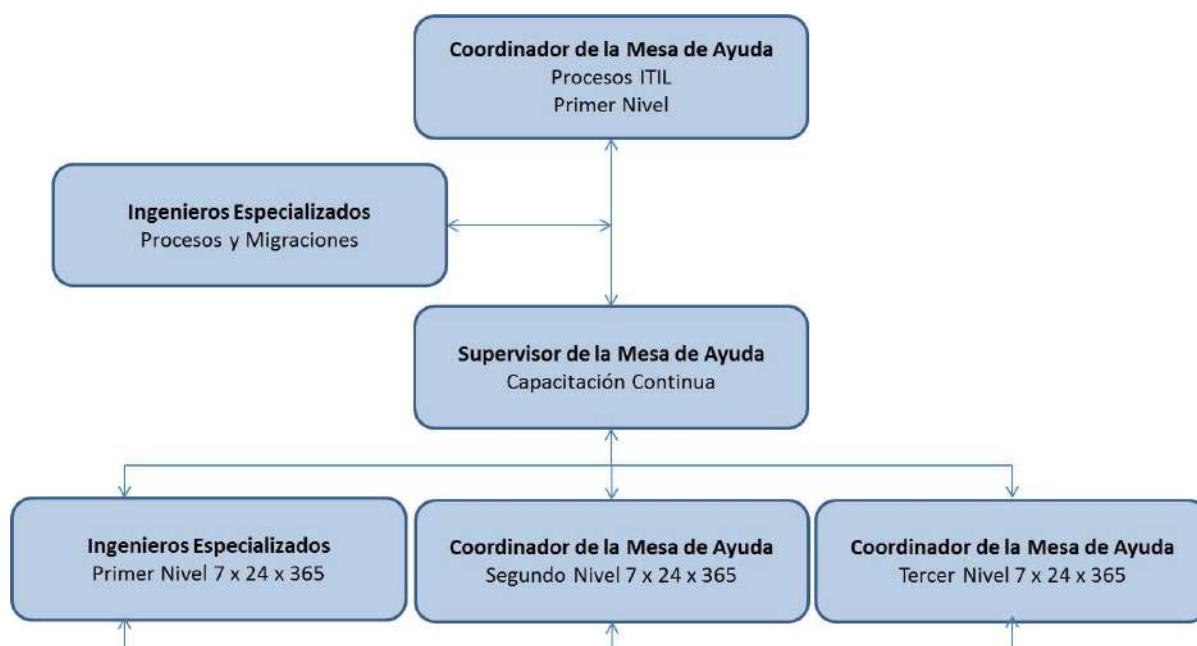
Se solicitará tras la exposición la aprobación del documento titulado "Plan de Acción" para que el mismo sea elevado para su aprobación final al Comité de Portabilidad.

Siempre se intentará llegar a un acuerdo total del Comité Técnico antes de elevar el documento para su aprobación final.

6.4 Soporte Técnico

INETUM incluye en su oferta la asistencia a través de una Mesa de ayuda en modalidad 24x7 para llevar a cabo la atención de incidencias ante fallos e imprevistos en los elementos de infraestructura, seguridad y aplicaciones software incluida **Portaflow**.

La administración de incidentes se llevará a cabo por medio de herramientas web o vía telefónica, que se notificarán oportunamente a las unidades participantes para recibir reportes, la evolución / seguimiento y cierre de las incidencias.



INETUM será el responsable de proporcionar el nivel de operación de la Infraestructura de Cómputo y del Soporte Técnico adecuado para regresar a su modo operativo el sistema en caso de que existiera algún problema con la operación del mismo, así como del mantenimiento de las aplicaciones, bases de datos, procesos de negocios, sistemas de alta disponibilidad y redundancia, servicios de seguridad y servicios de telecomunicaciones y acceso a Internet dentro del alcance.

Los Servicios de Soporte Técnico agruparán las tareas de apoyo y configuración de todos los elementos tecnológicos que forman las infraestructuras, será responsabilidad del Centro de Respuesta de INETUM el realizar y coordinar dichas tareas.

INETUM proveerá una Mesa de Ayuda como punto único de contacto para recibir y registrar reportes de incidencias, y recibiendo quien abra una incidencia un número de ticket único para que se pueda realizar el seguimiento correspondiente cumpliendo en todo momento con los SLAs exigidos en el pliego de condiciones.

La Mesa de Ayuda estará dedicada al servicio y utilizará el estándar mundial de ITIL (Information Technology Infrastructure Library) para dar el servicio, adaptar y medir la efectividad de los procesos de operación que son principalmente la administración de incidentes, problemas, cambios, continuidad, capacidad / rendimiento, soporte y asesoría aplicativa y niveles de servicio SLA, requeridos.

INETUM proveerá ingenieros de soporte técnico en un horario continuo las 24 horas del día los 7 días de la semana durante todos los días de año (7x24x365 tal y como define el Pliego de condiciones) para la recepción, registro, soporte, escalado (cuando proceda) y seguimiento de tickets hasta su solución.

La atención será accesible vía telefónica, email e interfaz Web GUI, y gestionada mediante



una aplicación de creación de tickets de problemas denominada **Mobydesk**, que es una herramienta propia de **INETUM** para la gestión de la Mesa de Ayuda y accesible desde Internet.

Los agentes de la Mesa de Ayuda tomarán la propiedad del incidente o solicitud reportados desde la identificación y/o notificación hasta la medición, cierre y reporte de desempeño.

INETUM ofrece los servicios de la Mesa de Ayuda bajo un esquema totalmente automatizado, facilitando múltiples canales de comunicación utilizando para ello una herramienta web con toda la funcionalidad que se requiere para un sistema de gestión de incidencias.

Los objetivos que cumplirá la **Mesa de Ayuda** son de manera enunciativa más no limitativa:

- Asegurar el cumplimiento con los Niveles de Servicio Comprometidos y llevar a cabo una atención profesional.
- Establecer un punto único de contacto para todas las solicitudes de servicio, requerimientos e incidencias.
- Asignar los requerimientos a través de la estandarización de servicios y procesos establecidos.
- Administrar el resultado del servicio conforme a los Acuerdos de Nivel de Servicio.
- Soportar procesos de mejores prácticas (ITIL) dentro y entre grupos funcionales.
- Identificación y administración Proactiva (preventiva) de fallas antes de que los usuarios del servicio se vean afectados.
- Establecimiento de métricas para un mejor control operacional y publicación de indicadores de resultados.
- Detección, notificación y escalamiento automático de incidencia.
- Comunicación directa a usuarios.
- Medición del desempeño y planeación de la capacidad.
- Llevar a cabo todas las acciones indicadas en el pliego ante un problema con la conexión de un operador o del ERPN.
- **Administración de incidentes.** Coordinación de actividades de terceros involucrados en el manejo de incidentes.

Administración de versiones y administración de cambios.

Con la responsabilidad de controlar las instalaciones de software y hardware, se gestionarán las peticiones de cambio evaluando la solicitud, el riesgo y definir si procede el cambio y la ventana de tiempo autorizada para la ejecución del mismo.

El desarrollo de aplicaciones es un proceso muy dinámico y cambiante el cual debe tener un control para que cumpla con las funciones para lo que está destinado.



Para un efectivo control de los aplicativos es necesario tener en cuenta un control de versiones o control de la configuración.

Este control debe administrar efectivamente las versiones de los cambios que se ejecuten en los sistemas.

El control de versiones provisto por **INETUM** se extiende a todos los elementos de software de bases de datos e interfaces, software operativo, aplicativo, de seguridad y de telecomunicaciones, de manera tal que se mantenga la integridad y la actualización de los controles de la configuración para los diversos ambientes y plataformas operativas.

El proceso de Manejo de Control de Cambios tiene como propósito introducir cambios en el ambiente de TI (Information Technology) rápidamente y sin interrupción a los servicios.

La gestión de cambios es responsable de cambios en la tecnología, sistemas, aplicaciones, hardware, herramientas de software, documentación, y procesos, así como cambios en los roles y responsabilidades de la organización.

Esta disciplina está a cargo de proporcionar un manejo eficiente de cualquier requerimiento de cambio (RfC – Request for Change –).

Una meta del proceso es asegurarse que todas las partes afectadas por un cambio dado estén conscientes del impacto de los cambios pendientes; ya que la mayoría de los sistemas / aplicaciones de negocios están altamente interrelacionadas, cualquier cambio hecho en una parte de un sistema puede tener un profundo impacto en otro sistema.

La administración de cambios de INETUM incluye identificar todos los sistemas afectados y los procesos antes de que el cambio sea implantado, con el fin de mitigar o eliminar el impacto adverso.

El proceso de Manejo de Control de Cambios recibe los RfC's, los registra dentro del sistema para habilitar el proceso, evalúa los mismos, aprueba o rechaza, y calendariza los RfC's aprobados para implantación.

Los RfC's son tramitados a los grupos responsables de procurar y/o desarrollar los componentes de software y hardware.

El proceso de Manejo de Control de Cambios monitorea la solicitud de cambio desde que se requiere un componente hasta que se implanta, ya sea un cambio requerido o una mejora propuesta para el ERPN.

También se asegura que todo el proceso sea correctamente documentado, este proceso trabaja muy cercanamente con el proceso de Manejo de Configuraciones, y se asegura que los cambios de TI se documenten apropiadamente en la base de datos de configuraciones (CMDB – Configuration Management Data Base), que es el repositorio utilizado para dar seguimiento al estatus de todos los componentes del ambiente de TI.

Un elemento de configuración (CI – Configuration Item –) es cualquier componente en el ambiente de TI, incluye hardware, software, básico, operativo, de seguridad, de



conectividad y aplicativo y su documentación relacionada.

El Administrador de Cambios y el responsable de implantar el cambio se encargan de proveer a la administración de configuraciones las entradas necesarias que está siendo implantado o removido del ambiente de TI.

Después de la implantación, la administración de cambios revisa y evalúa a todo el proceso de cambio ejecutado garantizando de este modo que toda tarea y el propio procedimiento se han cumplido de forma exitosa.

La mesa de ayuda ha de mantener por defecto todos los procedimientos, normas y controles redactados en el punto anterior, pero con el fin de hacer una descripción de cómo atenderá las incidencias que se reporten al ERPN, se describe a continuación una breve descripción del funcionamiento de la misma.

Cuando se desee abrir una incidencia, la misma podrá realizarse por medio del portal web facilitado oportunamente.

Ante la recepción de la incidencia se procederá por parte del nivel 1 de soporte a facilitar el número de incidencia (ticket) para poder hacer un seguimiento de la misma a través de éste.

Si el nivel 1 de soporte puede proporcionar la solución cerrará el ticket tras solventar la misma, caso contrario y según el tema que trate la incidencia, la misma comenzará a escalar al nivel 2 y 3 de soporte según sea la especialidad que se vea o pueda ver afectada.

Si la incidencia requiere de un análisis mayor, será la mesa de ayuda la que se ponga nuevamente en contacto con quien quedó registrado en la apertura de la misma para brindar la solución final al incidente, momento en el cual se procederá a cerrar el ticket.

Todos los tiempos que se consuman para la resolución de la incidencia se encontrarán adecuados a los SLA's solicitados en las bases, y por ende de obligado cumplimiento por parte de los recursos que INETUM afecte al proyecto.

6.5 Gestión de incidencias de la operación

6.5.1 Definición de incidente

Un incidente es cualquier evento que no es parte de las operaciones normales de un servicio y que causa, o pudiera causar, una interrupción o reducción en la calidad del servicio. Un incidente es definido por el **operador**, el **ERPN** o **SUTEL**.

6.5.2 Base de Datos Información de contactos

En caso de que exista un problema durante un incidente, se reportará y garantizará que se tomen las líneas de acción necesarias para resolverlo.



INETUM mantendrá una base de datos de contactos de los distintos operadores, SUTEL, el CTPN y del ERPN, las cuales estarán a disposición en **Mobydesk** y en el sistema de gestión de incidencias.

Esta base de datos podrá ser actualizada vía correo electrónico al ERPN, permitiendo así resguardar la veracidad de la información.

A modo de ejemplo los operadores deben entregar la siguiente información:

- Operador
- Nombre
- Cargo
- Correo electrónico
- Teléfono Fijo (si corresponde)
- Teléfono Móvil

La lista de contactos de SUTEL deberá contemplar:

- Nombre
- Cargo
- Correo electrónico
- Teléfono Fijo (si corresponde)
- Teléfono Móvil

Se creará una lista específica de contactos para diferentes procesos relevantes. Cada lista debe contener un mínimo los niveles de escalamiento para cada uno de los procesos. Será responsabilidad de cada Operador informar y actualizar la información de esta base de datos en caso de haber cambios.

6.5.3 Herramienta de gestión de incidentes

Como valor añadido, INETUM incluye en su propuesta una herramienta de Mesa de Ayuda que permite tanto la gestión de tickets con el ERPN como entre los propios operadores, denominada **Mobydesk**.

Fruto de la experiencia de **INETUM** como ERPN en otros países, se implementó esta solución a petición de los propios operadores de telefonía, como necesidad de poder gestionar incidencias entre ellos relativas a los procesos de portación, incluye también una posibilidad de escalado al regulador (**SUTEL**), en caso de controversia en operadores. Esta funcionalidad es opcional.

Las funcionalidades principales del sistema son las siguientes:

- Registro de una incidencia: el usuario registra una incidencia y recibe como resultado el número de ticket o número de incidencia para su seguimiento



- Gestionar una incidencia: la herramienta permite gestionar una incidencia, cambiarla de estado (aceptar, rechazar, etc.)
- Gestionar parámetros: se puede gestionar nuevos tipos de incidencia, notificaciones y SLAs.
- Gestión de usuarios: se permite dar de alta nuevos usuarios y asignarlos a perfiles, grupos y empresas.
- Notificaciones: la herramienta gestiona notificaciones a nivel de envío de e-mails.
- Reportes: se permiten obtener distintos reportes y estadísticas para el usuario administrador, además de los informes que se generarán mensualmente.

La herramienta permitirá gestionar dos grupos de trabajo, uno administrativo y uno técnico. Cada grupo podrá tener una tipificación de incidencias, por ejemplo:

- Problemas rechazo de portabilidad
- Incumplimiento de tiempos
- Genérica de Sistemas y/o comunicaciones
- Problemas con proceso de portabilidad
- Etc.

6.5.3.1 Perfiles de usuario

Existen varios perfiles de usuario, siendo posible que un usuario tenga más de un perfil asignado:

Usuarios finales

Los usuarios finales podrán:

- Abrir incidencias indicando el destinatario de la incidencia, el tipo, el nivel de criticidad y la descripción de la incidencia, podrá abrir la incidencia a otro operador o al ERP
- El regulador podrá tener usuarios finales con permisos para abrir incidencias a otros operadores y al ERP
- Anexar un fichero a la incidencia
- Consultar el estado de las incidencias abiertas por dicho usuario (grupo, operador destino, tipo de incidencia, descripción de la incidencia, fecha de apertura, estado y usuario de soporte que está tratando la incidencia)
- Consultar el histórico de las incidencias cerradas que fueron abiertas por el usuario (grupo, operador destino, tipo de incidencia, descripción de la incidencia, fecha de apertura, fecha de solución, descripción de la solución, usuario de soporte que solucionó la incidencia)



- Rechazar/Aceptar la solución de una incidencia: si la acepta se cierra automáticamente y pasa al histórico, si la rechaza deberá indicar el motivo por el que está rechazando la solución
- Estadísticas y generación de reportes

Usuario final supervisor

Tendrá los mismos permisos que el usuario final, pero con acceso a todas las incidencias creadas por los usuarios de su misma empresa y mismo grupo de trabajo.

Usuarios de soporte

Los usuarios de soporte podrán:

- Modificar el estado de una incidencia: cuando un usuario de soporte ponga estado "En proceso", automáticamente se le asignará a la incidencia dicho usuario, pero esto no significa que otro usuario de la misma empresa no pueda continuar con la solución de la incidencia. Se deberá generar una bitácora que registre las acciones de todos los usuarios de soporte sobre la incidencia
- Añadir una solución a la incidencia y modificar el estado a Solucionada
- Modificar el estado de una incidencia en estado ESCALADO A ERPN: cuando sea necesario hacer un escalado al ERPN en una incidencia entre operadores
- Consultar el histórico de cualquier incidencia abierta para el operador y grupo al que pertenece el usuario
- Estadísticas y generación de reportes

Usuarios de soporte SUTEL

Los usuarios de soporte de SUTEL podrán:

- Tratar incidencias en estado ESCALADO A SUTEL, el resto de las incidencias que sean creadas y no escaladas a SUTEL no serán visualizadas por este perfil
- Modificar el estado de una incidencia en estado ESCALADO A SUTEL: cuando un usuario de soporte de SUTEL ponga estado "En proceso", automáticamente se le asignará a la incidencia dicho usuario, pero esto no significa que otro usuario de la SUTEL no pueda continuar con la solución de la incidencia. Se deberá generar una bitácora que registre las acciones de todos los usuarios de soporte sobre la incidencia
- Modificar el estado de una incidencia en estado ESCALADO A ERPN: cuando sea necesario hacer un escalado al ABD en una incidencia entre operadores
- Añadir una solución a la incidencia y modificar el estado a Solucionada
- Consultar el histórico de cualquier incidencia abierta para el operador y grupo al que pertenece el usuario



- Estadísticas y generación de reportes

Usuarios de soporte ERP

Los usuarios de soporte de ERP podrán:

- Tratar incidencias en estado ESCALADO A ERP, el resto de las incidencias que sean creadas y no escaladas al ERP no serán visualizadas por este perfil
- Tratar incidencias abiertas directamente a la ERP
- Modificar el estado de una incidencia en estado ESCALADO A ERP
- Añadir una solución a la incidencia y modificar el estado a Solucionada
- Consultar el histórico de cualquier incidencia abierta o escalada al ERP
- Estadísticas y generación de reportes

Usuario administrador

El usuario administrador tiene como funcionalidad las siguientes opciones:

- Tendrá los mismos permisos que el usuario de soporte en cuanto a seguimiento y solución de incidencias
- Gestión de usuarios
- Estadísticas y generación de reportes

Usuario Super Administrador

El usuario super administrador tiene como funcionalidad las siguientes opciones:

- Seguimiento de todas las incidencias, del grupo que sea y del operador que sea
- Consulta del histórico de incidencias, del grupo que sea y del operador que sea
- Gestión de usuarios, empresas y parámetros de incidencias: notificaciones, SLAs, etc.
- Estadísticas y generación de reportes
- Consulta y descarga de productividad de usuarios y de SLAs

6.5.3.2 Notificaciones

La herramienta genera automáticamente las siguientes notificaciones por correo electrónico:

- **Apertura de incidencia** → cuando se abre una incidencia se envía un correo electrónico a la cuenta de correo que esté configurada en la entidad destino para el grupo correspondiente, describiendo los detalles de la incidencia
- **Aviso próxima superación del SLA** → cuando quede un tiempo X configurable para superar el SLA de atención de incidencias, se envía un correo electrónico a la cuenta



de correo que esté configurada en la entidad destino para el grupo correspondiente, informando de la situación

- **Superación del SLA** → cuando se supera el SLA y la incidencia no ha sido actualizada a otro estado, se envía un correo electrónico a la cuenta que esté configurada en la entidad destino para el grupo correspondiente, informando de la situación
- **Solución de la incidencia** → cuando el usuario de soporte soluciona la incidencia, se envía un correo electrónico al usuario final que abrió la misma, indicando el estado de solución y la propia solución
- **Rechazo de la solución** → cuando un usuario rechaza una solución se enviará un correo electrónico con los detalles de la incidencia y del rechazo a la cuenta que esté configurada para los usuarios del grupo y entidad que solucionó la incidencia

6.5.3.3 Reportes

Mensualmente la herramienta genera automáticamente por cada grupo de trabajo un reporte en PDF contiene tanto a nivel de tabla informativa como de forma gráfica:

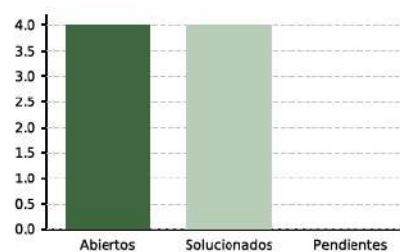
- Número de tickets abiertos en el mes, número de solucionados y número de tickets abiertos todavía, en total y en porcentaje
- Número de tickets abiertos en el mes, número de solucionados y número de tickets abiertos todavía abiertos (en total y en porcentaje), discriminados por tipificación
- Número de tickets abiertos en el mes, número de solucionados y número de tickets abiertos todavía (en total y en porcentaje), discriminados por empresa.
- Número de tickets abiertos en el mes agrupados por día
- Número de tickets abiertos por mes durante todo el año
- Número de tickets cerrados por mes durante todo el año



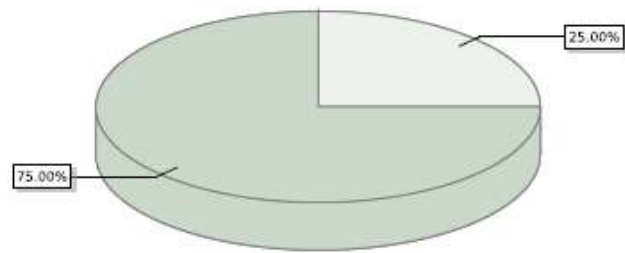
Reporte mensual de

Período del 01/02/2021 al 28/02/2021

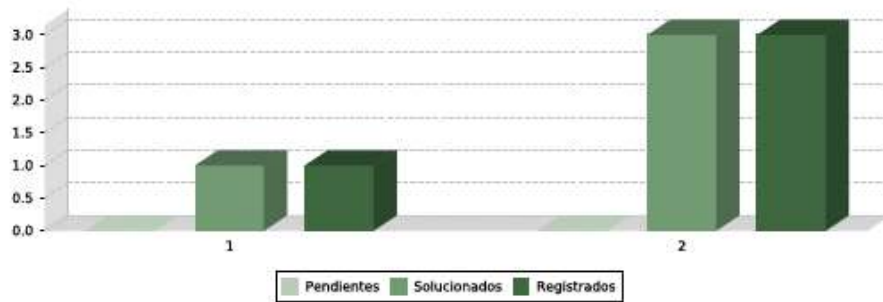
Número de tickets abiertos, solucionados y pendientes	
Número de tickets abiertos	4
Número de tickets solucionado	4
Número de tickets pendientes de	0
Porcentaje de tickets solucionados	100.00%
Porcentaje de tickets pendientes	0.00%



Número de tickets abiertos en el mes, solucionados y pendientes por tipo de incidencia				
N	Tipo Incidencia	Registrados	Solucionados	Pendientes
1	Incumplimiento de tiempos	1	1	0
2	Inconvenientes genéricos con la interfaz WEB y/o SOAP de Portaflow	3	3	0

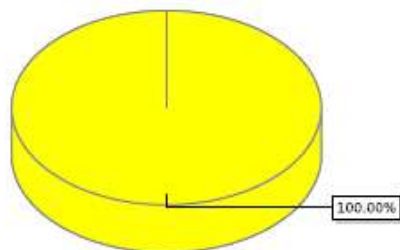


○ Incumplimiento de tiempos ○ Inconvenientes genéricos con la interfaz WEB y/o SOAP de Portaflow

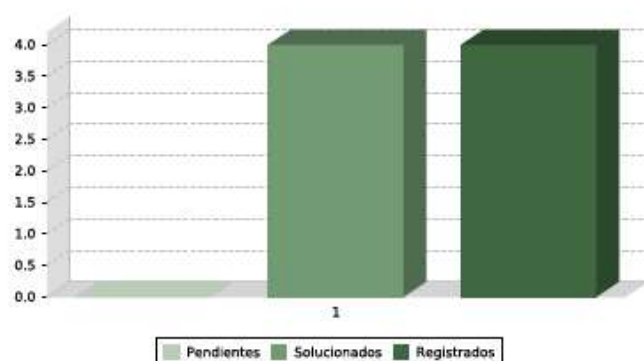


Número de tickets abiertos en el mes por empresa	
ERP	4

● ERP



Número de tickets abiertos en el mes, solucionados y pendientes por				
N	Empresa	Pendientes	Solucionados	Registrados
1	ERP	0	4	4



Número de tickets abiertos y solucionados por día		
Fecha	Registrados	Solucionados
01/02/2021	4	5



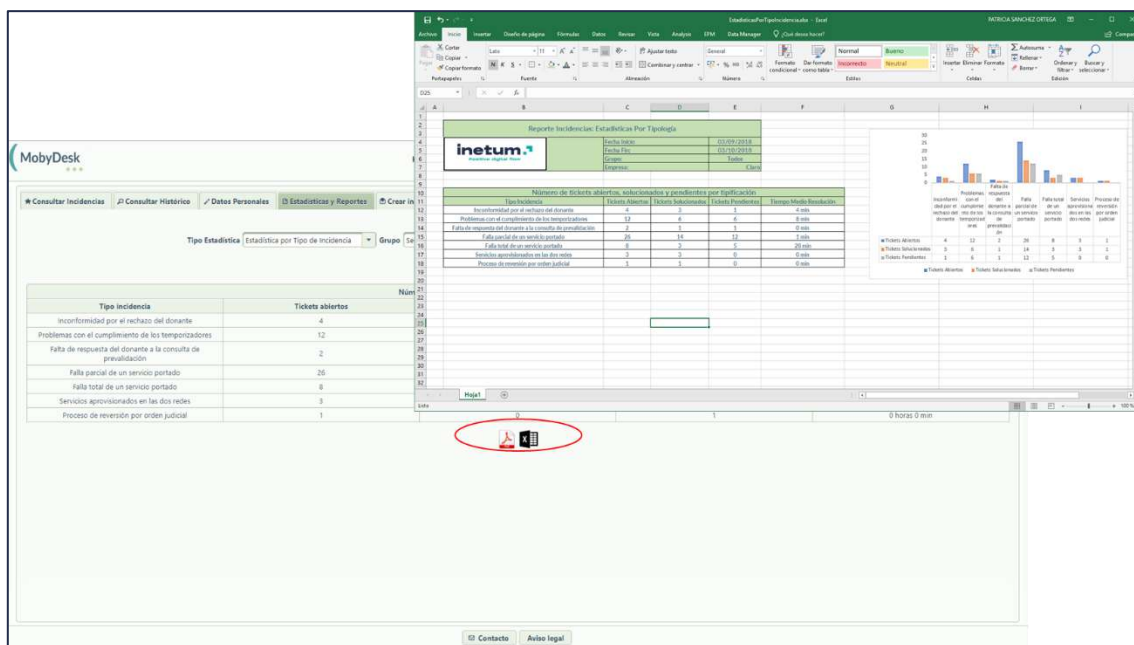
Número de tickets abiertos y solucionados por mes en el		
Fecha	Registrados	Solucionados
Marzo 20	8	8
Abril 20	3	3
Junio 20	6	6
Julio 20	4	4
Agosto 20	31	10
Septiembre 20	14	3
Octubre 20	28	7
Noviembre 20	12	5
Diciembre 20	44	0
Febrero 21	4	5

Existen además 3 tipos de reportes generados desde la aplicación a demanda:

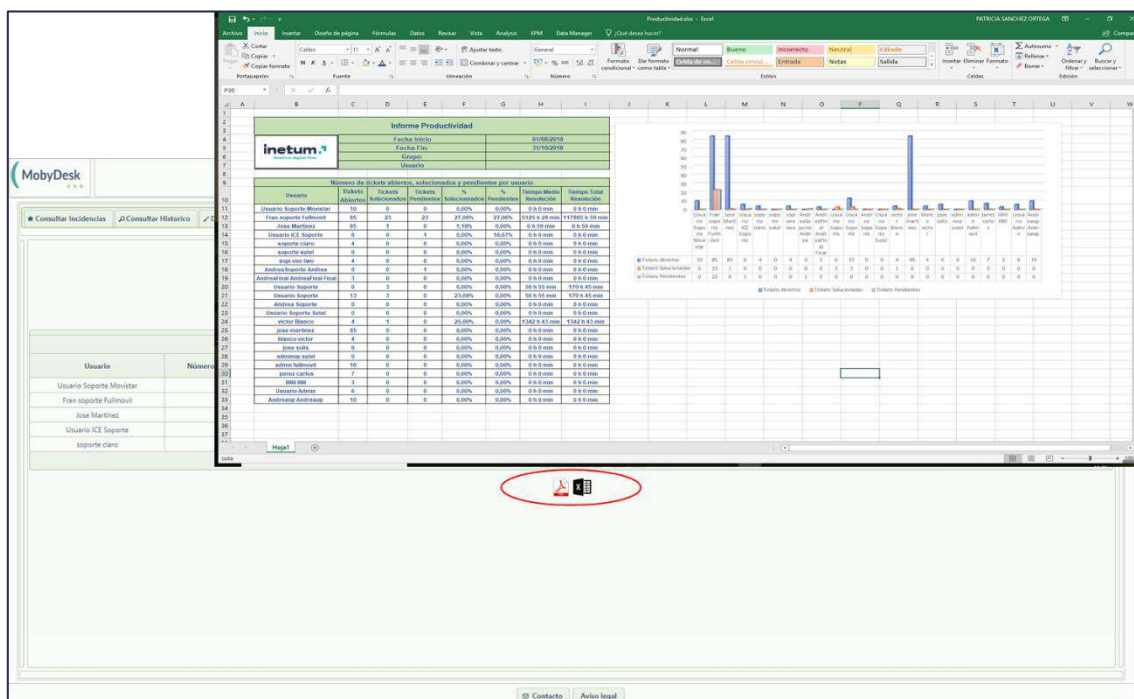
- **Reportes de incidencia por distintos criterios.** Desde el interfaz web se podrán realizar distintas consultas que podrán ser exportadas y descargadas en un fichero.
- **Reportes de productividad.** Estos reportes son descargados por el administrador para poder obtener datos de productividad de los diferentes usuarios de soporte

- **Reportes de cumplimiento de SLAs.** Estos reportes son descargados por el administrador para poder obtener datos de cumplimiento de los SLAs

A continuación, se muestran ejemplos de los informes que se pueden descargar:



Reporte incidencias por distintos criterios



Reporte productividad

Informe Productividad

Fecha Inicio: 01/08/2018
Fecha Fin: 31/10/2018
Grupo:
Usuario:

Resumen Cumplimiento SLAs

Atendidas en Tiempo	NO Atendidas en Tiempo	Cumplimiento Atención	Solucionadas en Tiempo	NO Solucionadas en Tiempo	Cumplimiento Solución
71	16	81.61%	36	3	92.31%

Tickets Abiertos por Empresa

Identificador Incidencia	Fecha Creación	Fecha Atención	Fecha Solución	Tiempo Atención	Tiempo Solución
70	16/08/2018 14:03:39	14/09/2018 14:32:56		17d 2h 38min 32sg	
93	29/08/2018 11:54:24	29/08/2018 13:39:55	27/09/2018 17:46:48	17sg	29d 4h 7min 10sg
95	29/08/2018 13:39:38	29/08/2018 14:40:48		15d 2h 42min 35sg	
96	30/08/2018 11:58:14	21/09/2018 12:47:45	01/10/2018 16:58:06	21d 2h 29min 41sg	31d 6h 40min 2sg
99	31/08/2018 10:18:04				

Lista

Atendidas en Tiempo	NO atendidas en Tiempo	Cumplimiento atención	Solucionadas en tiempo	NO solucionadas en tiempo	Porcentaje de Solución
71	16	81.61%	36	3	92.31%

Reporte cumplimiento SLAs

6.5.3.4 Acuerdos de Niveles de Servicio

Los acuerdos de niveles de servicio son configurables y se pueden definir a nivel de grupo de trabajo.

6.5.4 Definición del Proceso de Gestión de Incidentes

INETUM implementará un esquema de monitoreo 7x24x365, por medio del cual se identifican, diagnostican y atienden todos los incidentes tanto de forma preventiva como correctiva.

De este modo INETUM será responsable del diagnóstico proactivo, rápido, oportuno y eficiente de cualquier actividad sospechosa a fin de mitigar los riesgos de causar algún impacto a los servicios propuestos.

Los incidentes generados a partir del monitoreo automático al igual que todos los incidentes generados por las herramientas de la solución serán manejados por medio del proceso de control de cambios.

Cada incidente generará un registro en la Mesa de Ayuda, de forma tal que permita una solución puntual de acuerdo con los niveles de servicio comprometidos, la detección de patrones de incidentes, la base de datos de conocimiento sobre la naturaleza y acciones correctivas y la evaluación de vulnerabilidades.

INETUM se encargará de apoyar la ejecución de los procedimientos que conforman a las fases siguientes:

- Detección



- Análisis
- Respuesta
- Mejora Continua

Estos procedimientos garantizan el flujo correcto del proceso de incidentes, facilitando y verificando que los procesos avancen de manera óptima y sin contratiempos.

El servicio de Soporte de Inetum está dividido en 3 niveles para que la incidencia sea tratada en todo momento por técnicos especialistas:

- **Área de soporte nivel 1 y 2:** son las personas que están en la mesa de ayuda y que atienden las incidencias en primera instancia, ya sean notificadas mediante **Mobydesk** o mediante correo electrónico
- **Área de soporte nivel 3:** son desarrolladores e ingenieros que deben intervenir en caso de que la falla sea debida a un bug del software. En este nivel también se encuentra el equipo de soporte de la plataforma hardware, software base y comunicaciones con los operadores, el cual se encarga de monitorizar, dar soporte y mantenimiento y ejecutar cambios sobre todos los elementos contratados por Inetum para la implantación y ejecución de la ERP.

Como se podrá apreciar en este documento, no necesariamente un ticket ha de ser tratado por los 3 niveles de soporte, dado que en función de las características del caso a tratar el mismo puede llegar a ser resuelto por el 1º nivel de soporte sin necesidad de escalado alguno.

Tras la asignación de un número de ticket, el personal de nivel 1 y 2 realizará un análisis del caso indicado por el cliente, y procederá a verificar si el mismo carece de información como para comenzar a tratarlo y posteriormente solucionarlo.

Ante el caso de que sea necesaria la aportación de información adicional para continuar con el proceso de solución, el técnico (con independencia del nivel de soporte en que se encuentre), procederá a solicitar la misma al usuario que abrió el ticket.

Bajo el supuesto que el caso no pueda ser resuelto por estos niveles, se informará al cliente que el ticket ha escalado al último nivel de soporte (3º nivel), repitiéndose según sea el caso el proceder de comunicación entre soporte y el usuario de forma acorde a lo redactado con anterioridad.

Cualquier nivel de soporte una vez solventado el ticket puede proceder a su cierre de común acuerdo con el Cliente. Ante casos de no aportación de información y salvo que se indique lo contrario dentro del propio ticket, la falta de respuesta a un caso por parte de un Cliente por un plazo superior a 24 horas provocará el cierre automático del caso.

El procedimiento comienza siempre con la apertura de una incidencia por parte del cliente la cual se realizará según lo indicado en los canales de comunicación del apartado 2 del presente documento.



Ante dicho registro del caso y la asignación de un número de ticket, el analista de primer nivel de soporte analizará si el motivo del mismo es por una petición de servicio o por una incidencia que esté afectando la operación.

El usuario deberá indicar en el registro del ticket los siguientes datos:

- **Tipo de incidencia:** se deberá indicar el tipo o descripción corta del problema de acuerdo a la tipificación configurada en el sistema
- **Nivel de criticidad:** Se deberá indicar también el nivel de criticidad de la incidencia, este dato es aconsejable que sea totalmente objetivo, pues es susceptible de ser modificado por el equipo técnico de soporte si así lo considerase oportuno
- **Descripción de la incidencia:** El usuario deberá detallar en este campo el problema encontrado o bien la consulta que se quiera realizar. Si existe otra incidencia registrada con anterioridad por el mismo caso se debe indicar

6.5.4.1 Soporte inicial

Contando ya con la información necesaria para desarrollar esta tarea, existe la posibilidad de brindar un soporte inicial utilizando la información de errores conocidos y/o soluciones alternativas.

Si existe una solución o solución alternativa para lograr que el servicio vuelva a su funcionalidad rápidamente, se provee este soporte Inicial y se pasa al procedimiento de bloqueo de la incidencia de manera temporal para la verificación del correcto funcionamiento y en efecto ver si la solución aplica al caso. Una vez verificada su correcta aplicación, se procederá al cierre de la incidencia.

En caso de no contar con resultados positivos tras el soporte inicial brindado pasaremos al procedimiento de investigación y diagnóstico asignando a la incidencia el motivo por el cual aún no se ha brindado una solución a la misma.

- **Por Cliente:** aplica para las incidencias donde sea necesario la participación del cliente en pruebas o la resolución del mismo y no se logre establecer el contacto por parte de soporte.
- **Por Proveedor Externo:** aplica para las incidencias cuya solución / solución alternativa dependa de la participación de algún proveedor externo.
- **Desarrollo:** se está desarrollando la solución a aplicar para solucionar la incidencia.
- **Por Falta de Recursos:** aplica para las incidencias cuya solución / solución alternativa dependa de la recepción de un repuesto / parte.

6.5.4.2 Informar al cliente

El cliente será informado del estado de la incidencia y de su avance mediante correo



electrónico.

IMPORTANTE: Podrán existir incidencias denominadas “críticas”, que según casuística serán tratadas de manera personalizada y acordada con el cliente por vía telefónica.

6.5.4.3 Escalar la incidencia

Mecanismo por el cual se escala la incidencia al siguiente Nivel de Soporte si no se encontró solución o solución alternativa.

6.5.4.4 Evaluar incidencia

En esta etapa del ciclo de vida de la incidencia es donde se realiza toda la investigación y posterior diagnóstico para determinar posibles soluciones o bien escalar la misma a otros niveles de soporte según se vea la criticidad del caso.

Según sea el resultado del análisis el caso podrá escalar a otros niveles de soporte que serán los que se encargarán (según aplique) de hacer un análisis más detallado de la incidencia, aplicando su experiencia, buenas prácticas y consultas hacia quienes proceda en cada caso y siempre que resulte necesario (proveedores, operaciones, soporte, cliente y otros).

6.5.4.5 Solucionar e informar al primer nivel de soporte

En el momento en que se encuentra la solución a aplicar y con independencia del nivel de soporte en que se encuentre la misma, ésta, se documentará en todo lo que corresponda y se remitirá al primer nivel de soporte para que sea éste quien continúe con el caso.

6.5.4.6 Análisis y propuesta de solución o solución alternativa

Según la información recopilada, el análisis y el diagnóstico realizado, se proveerá la solución (al menos solución alternativa) para la incidencia.

6.5.4.7 Escalado de incidencias

En el caso en que la incidencia no se haya podido resolver en el nivel 1 y 2 de soporte, o de tratarse de una incidencia recurrente, se procederá a la generación de un registro del problema para que la causa raíz del mismo pueda ser analizada, identificada y eliminada definitivamente. Para ello se procederá a escalar la incidencia al máximo nivel de soporte, esto es, al nivel de soporte que brinda Inetum.

6.5.4.8 Ejecutar acciones para la solución

En esta fase se aplican las acciones de solución de la incidencia y se valida que la misma sea efectiva.

La solución aplicada será producto de información obtenida de la base de conocimientos o bien del avance de los análisis y consultas realizados por medio de los distintos niveles



de soporte que hayan participado en su resolución o de la activación del proceso de gestión de problemas.

La solución a aplicar podrá implicar la activación de un posible proceso de cambio del software.

Esta necesidad de activar el proceso de gestión de problemas surgirá dependiendo de las modificaciones que se deban de realizar para la aplicación de una solución o solución alternativa debido a posibles actualizaciones en el equipamiento informático, cambios de software y/o nueva documentación para la base de conocimientos, que deban de realizarse de forma añadida a la propia solución del caso.

En caso de que la solución de la incidencia no implique la activación del proceso de gestión de problemas, se ejecutarán directamente las acciones que correspondan para aplicar la solución / solución alternativa y deberá documentarse las tareas a realizar en el formulario de incidencias de forma detallada previo a su cierre.

Dependiendo de la problemática existe la posibilidad de que tras brindar la solución a la incidencia deban ejecutarse acciones de recuperación y/o regresión.

6.5.4.9 Ejecutar acciones para la recuperación

En esta fase se aplican las acciones de recuperación del servicio bajo impacto de la incidencia reportada y se valida que su solución sea efectiva.

Las mismas serán llevadas de forma acorde a lo que se requiera por todas las partes por ejemplo si fuera necesario realizar un backup de información previo a brindar una solución. En esta actividad se realizará la restauración de la información que había sido respaldada.

Al finalizar la tarea de aplicación de la solución y si se verifica la recuperación del servicio se completará la acción activando el procedimiento de cierre de incidencia.

6.5.4.10 Confirmación de la solución

Luego de implantar la solución o solución alternativa, o verificar que la incidencia ya había sido resuelta, el soporte de primer nivel se pondrá en contacto con el cliente para notificarle acerca de la resolución y confirmar su conformidad.

De acuerdo con la política definida, existirá un tiempo de respuesta y si no hay validación del cliente, se cierra la incidencia con el código respectivo.

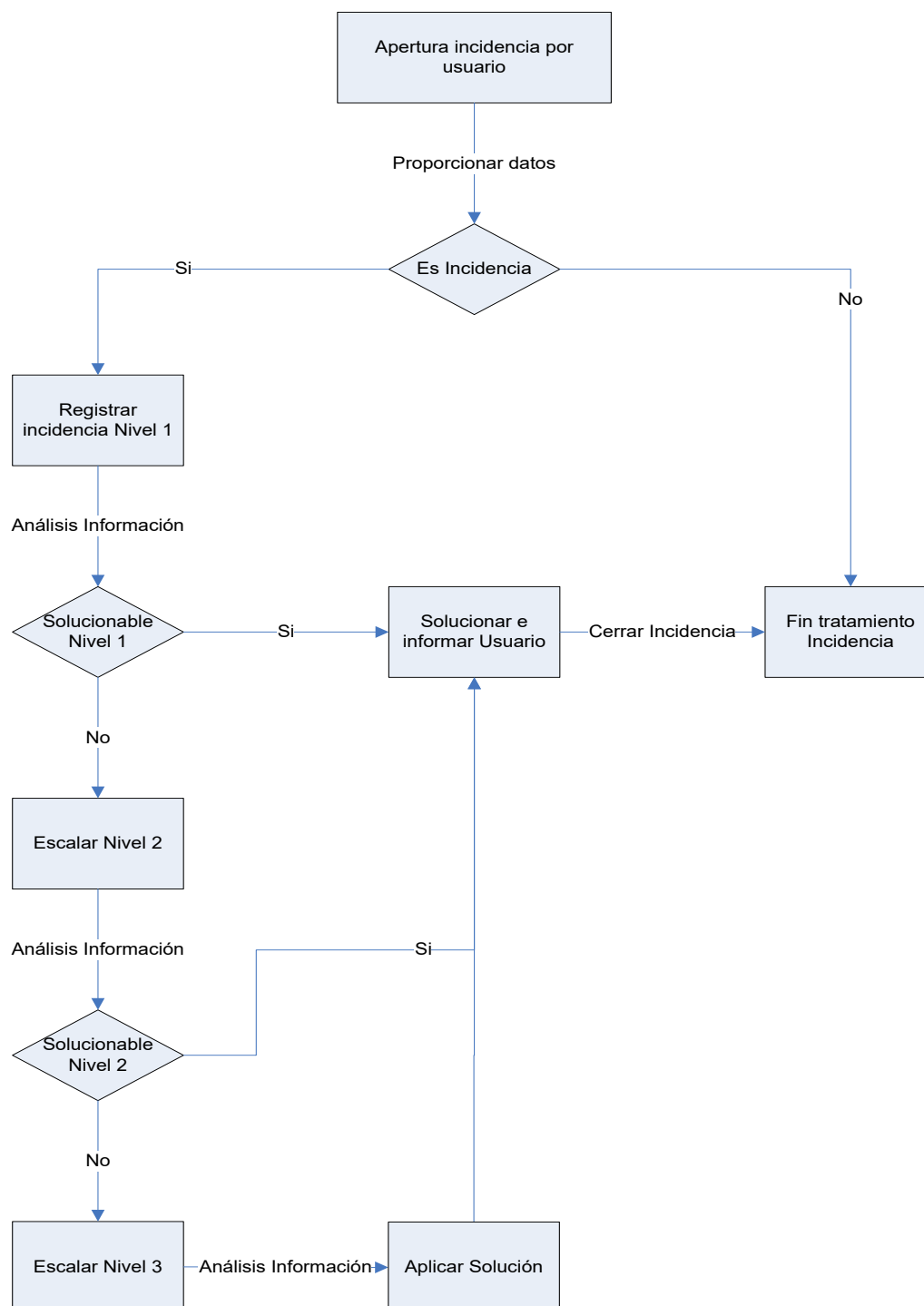
6.5.4.11 Cerrar la incidencia

En esta etapa llegamos al fin del ciclo de vida de una incidencia, aquí se procederá a realizar el cierre formal del mismo y a su cambio de estado mediante el código de cierre correspondiente.

6.5.4.12 Flujo de Actividad de los Niveles de Soporte



Se definen tres (3) niveles de soporte, y a grandes rangos se tendrá en cuenta el siguiente flujo de actividad:



Nivel 1 de soporte

El objetivo principal de este nivel de soporte es el de proveer al cliente que reporta una incidencia, soluciones rápidas y efectivas en aquellos casos que sea posible, o asegurar el escalado al área o persona de segundo nivel adecuadas para la resolución de la



incidencia.

Ante cualquier incidencia, el cliente podrá realizar la apertura de un ticket según el procedimiento acordado, dicha incidencia será atendida por el nivel 1 de soporte en un horario que dependerá del nivel de servicio contratado por el cliente.

El agente que atienda la incidencia comenzará a realizar el análisis del tema a solucionar. Las tareas a realizar en este primer nivel de soporte son:

- Verificar si la incidencia o solicitud está dentro del contrato del servicio y registrarla.
- Si detecta que la actividad solicitada por el cliente corresponde a un requerimiento de servicio se deberá seguir el procedimiento especificado para cada caso.
- Si existe otra incidencia registrada con anterioridad por el mismo caso se procede a informar al usuario y se relaciona con el existente ya registrado.
- Definir a qué categoría pertenece la incidencia, con el objetivo principal de asignar el grupo de resolución apropiado, y para fines estadísticos y reportes.
- Asignar la prioridad en función de la criticidad de la incidencia, definida en función de la urgencia y el impacto.
- Si existe una solución alternativa para lograr que el usuario vuelva a su operatividad rápidamente, proveer soporte inicial y pasar a la etapa de resolución y recuperación.
- Verificar si la incidencia tiene relación con otras o si existe un registro de problema asociado, para conocer el estado de resolución y poder relacionarlo.
- El cliente podrá ser informado, si está dentro del alcance del servicio, del estado de la incidencia o petición de servicio, mediante mail o web.
- Según el tipo de incidencia, se procede a la resolución, es decir, ejecutar la solución o la solución alternativa (workaround). Si la resolución debe ejecutarse en otro momento, se debe cambiar a un estado bloqueado.
- Si es necesario, ejecutar las acciones para recuperar el funcionamiento del servicio, según el nivel de servicio acordado con el cliente.
- Establecer contacto para notificar al cliente (usuario) acerca de la resolución y confirmar su conformidad. Si no hay validación del cliente, se cierra la incidencia con el código respectivo. Se efectuará una llamada telefónica con número de reintentos o un comunicado automático con tiempo de respuesta de cierre de Incidencia.
- Se procede al cierre formal de la Incidencia, y a su cambio de estado a cerrado.

Nivel 2 de soporte

Si el operador que recibió el ticket no fue capaz de resolver la incidencia en el primer nivel de soporte, escalará la misma al segundo nivel de soporte, el cual analizará la misma, y



determinará si resolverá la incidencia o se escalará al siguiente nivel de soporte.

Este segundo nivel es el que provee soluciones expertas a incidencias del área tecnológica a la que pertenece o posee la experiencia y conocimientos necesarios.

Ejecuta las actividades de clasificar, analizar, diagnosticar, resolver incidencias y escalar al siguiente nivel cuando se desconozca la causa raíz.

Las tareas a realizar en este segundo nivel de soporte son:

- Si se detecta que la actividad solicitada por el cliente corresponde a un requerimiento de servicio se deberá seguir el procedimiento especificado para cada caso.
- Definir a qué categoría pertenece la incidencia, con el objetivo principal de asignar el grupo de resolución apropiado, y para fines estadísticos y reportes
- Recibir la incidencia y hacer un análisis más detallado del mismo, y según la experiencia y consultas apropiadas, encontrar la manera más rápida de proveer una solución a la incidencia.
- Si la solución se encuentra en la base de conocimiento, proceder a entregar la solución, documentar e informar al soporte de primer nivel.
- Según la información recopilada, el análisis y el diagnóstico realizado se deberá proveer una solución (al menos solución alternativa) para la incidencia.
- Si la incidencia no está en la base de conocimiento y no existe el registro del problema, escalar la incidencia al siguiente nivel de soporte para su investigación.
- En caso de que la solución de la incidencia requiera solicitar un cambio en la infraestructura, el mismo deberá seguir el proceso de gestión de cambios que corresponda.
- Según el tipo de incidencia, se procede a la resolución, es decir, ejecutar la solución o la solución alternativa (workaround).
- Si la resolución debe ejecutarse en otro momento, se debe cambiar al estado bloqueado.
- Si es necesario, ejecutar las acciones para recuperar el funcionamiento del servicio, según el nivel de servicio acordado con el cliente.

Nivel 3 de soporte

El escalado al nivel 3 del soporte técnico, se realizará cuando ninguno de los niveles anteriores haya podido resolver la incidencia, y que probablemente se trate de un fallo mayor en el que deba de intervenir los profesionales del área de ingeniería y laboratorio, activando el proceso de gestión de problemas.



Este nivel también se corresponde con el proveedor encargado y responsable del correcto funcionamiento de toda la plataforma hardware (servidores, firewalls, sistema operativo, base de datos, unidades de almacenamiento, herramientas de backup y monitoreo).

En caso de resolución, se informará al cliente de la misma y se dará por concluida la incidencia con el acuerdo mutuo de ambas partes.

En caso de que la incidencia por la causa que fuese se alargue en el tiempo, por cuestiones propias de los procesos de portabilidad o bien por un fallo mayor, la incidencia pasará a estado bloqueado y se le informará a quien haya abierto la incidencia cuándo ha de ser llamado nuevamente para informarle sobre su caso en particular.

En caso de que la incidencia conlleve una modificación del producto, la incidencia pasará al área de ingeniería de Inetum para su análisis y solución, quedando la misma en estado bloqueado hasta que quede liberada por dicha área.

En cualquier caso, si la resolución de la incidencia se alargara en el tiempo, el cliente recibirá las notificaciones que procedan según sea el caso del departamento de soporte de Inetum.

6.5.5 Niveles de Severidad

Las siguientes clasificaciones de Niveles de Severidad pueden ser utilizadas en la Herramienta **Mobydesk**, y las mismas son configurables:

- Crítico
- Mayor
- Menor

Las características de los Niveles de Severidad son las establecidas en la siguiente tabla:

Severidad	Prioridad	Definición	Tiempo Atención Mesa de Ayuda (1)	Tiempo de Solución del Problema (2)
1	Crítico	Es cualquier defecto que impide que el ERPn complete un Proceso de Portación o parte del mismo.	30 minutos corridos	1 horas corridas
2	Medio	Es cualquier defecto que deteriore significativamente cualquier funcionalidad del ERPn y que no cumpla el criterio de severidad Crítica.	30 minutos corridos	6 horas corridas
3	Bajo	Cualquier otro defecto que no cumpla el criterio de severidad Crítico ni Grave.	60 minutos corridos	1 días hábiles

(1): Tiempo transcurrido entre la recepción del reclamo por la mesa de ayuda, y el contacto de un especialista del ERPn, con el reclamante.

(2): Tiempo transcurrido entre la recepción del reclamo por la mesa de ayuda, y la



verificación de la solución por parte del reclamante, la que debe ser realizada a través de la Mesa de Ayuda.

6.5.6 Acuerdo de Niveles de Servicio (SLA) de la mesa de ayuda

Los niveles de servicio asociados a la mesa de ayuda del ERPN serán medidos de acuerdo con lo especificado en las bases técnicas.

6.5.7 Protocolo de Emergencia ante caída prolongada del sistema de un Operador Donante

Si un Operador Donante lleva más de cuarenta y ocho (48) horas corridas (parametrizable) presentando Incidencia Crítica, la cual no permite ejecutar solicitudes de portabilidad como Donante, entonces el ERPN, previo acuerdo con el CTPN restringirá el permiso para que de esta forma este operador no pueda ejecutar solicitudes de portabilidad como Operador Receptor.

INETUM cuenta con un mecanismo denominado “Donante Universal”, el cual al activarse inhibe a un operador para realizar portabilidades como operador receptor y adicionalmente acepta de forma automática las portabilidades que se generen para dicho operador como donante, siempre y cuando hayan superado todas las validaciones que debe realizar el ABD.

Este procedimiento ha sido implementado por INETUM en aquellos países en los que se ha definido como requerimiento ante fallas prolongadas de un operador, pudiendo ser utilizado también ante impagos recurrentes de un operador al ABD.

7 Biometría

7.1 Introducción

De conformidad con el Código Nacional de Tecnologías Digitales del MICITT (2024), nuestro sistema de captura implementa las disposiciones de la normativa ISO/IEC 19794-5 y de las Estructuras de datos ISO/IEC 39794-5, en la medida en que son técnicamente aplicables al proceso de on-boarding digital.

El sistema de captura incorpora **mecanismos de control de calidad y retroalimentación en tiempo real**, que permiten verificar durante el propio proceso que la imagen obtenida cumple con los parámetros técnicos necesarios para su posterior uso en procesos de reconocimiento facial, minimizando rechazos y reprocesos.

Asimismo, la solución ha sido **evaluada conforme a metodologías de validación independientes reconocidas internacionalmente**, lo que constituye una evidencia objetiva de la robustez, calidad y conformidad del proceso de captura biométrica implementado.



En consecuencia, se garantiza que la solución propuesta **incorpora y aplica las mejores prácticas internacionales** en materia de captura de retratos para procesos de verificación de identidad digital, asegurando niveles adecuados de calidad, fiabilidad y cumplimiento normativo.

7.2 Proceso de validación biométrica

a solución propuesta incorpora un módulo avanzado de validación de documentos de identidad, diseñado para soportar los principales documentos oficiales utilizados en Costa Rica, incluyendo Cédula de Identidad Costarricense, Pasaporte, TIM, DIMEX y Cédula Jurídica.

Dicho módulo ha sido concebido para adaptarse a una amplia variedad de dispositivos, tales como computadoras de escritorio, portátiles, tabletas y teléfonos móviles con cámara integrada, garantizando una experiencia de uso homogénea y accesible, independientemente del dispositivo empleado por el usuario.

El sistema permite la captura y validación de las distintas vistas de cada documento (anverso y reverso, cuando aplique), asegurando la correcta obtención de la información necesaria para los procesos de verificación y validación de identidad. Asimismo, se contemplan mecanismos que facilitan la correcta alineación y calidad de la imagen capturada, contribuyendo a la fiabilidad del proceso.

A continuación, se presenta una tabla descriptiva en la que se detallan los distintos tipos de documentos soportados, sus correspondientes vistas y ejemplos ilustrativos, con el fin de facilitar la comprensión del alcance funcional de la solución en materia de validación documental.

Tipo documento	Descripción	Documento
Cédula costarricense	Documento nacional de identidad para ciudadanos costarricenses	
Pasaporte	Documento de viaje e identificación internacional emitido por el Estado costarricense.	



TIM (Tarjeta de Identidad de Menores)	Documento de identidad para costarricenses menores de 12 a 17 años.	
DIMEX (Documento de Identidad Migratorio para Extranjeros)	Documento de identificación para extranjeros residentes o con estatus migratorio en Costa Rica.	

La solución propuesta incorpora un mecanismo automatizado de verificación de identidad biométrica, mediante el cual se realiza la comparación entre la imagen facial extraída del documento de identidad y un selfie capturado en tiempo real por el usuario. Este enfoque permite ofrecer una solución segura, robusta y completamente automatizada, garantizando al mismo tiempo una experiencia de usuario fluida y sencilla.

Con el objetivo de validar la autenticidad del documento de identidad y verificar que la persona que realiza el proceso es efectivamente el titular del mismo, la solución permite ejecutar dicho procedimiento de manera ágil, usable y eficiente, manteniendo en todo momento altos estándares de seguridad, fiabilidad y precisión, en línea con los requisitos exigidos en entornos regulados.

El proceso de verificación se compone de **dos pasos automáticos claramente diferenciados**:

1. **Captura y validación del documento de identidad**, en la que se obtienen las imágenes necesarias del documento y se verifica su autenticidad y coherencia.
2. **Captura biométrica facial del usuario**, mediante la toma de un microvídeo o imagen en tiempo real, que se utiliza tanto para la comparación biométrica facial con la imagen del documento como para la ejecución de un **análisis de ataques de presentación (liveness detection)**.

La detección de vida se realiza mediante **técnicas avanzadas basadas en inteligencia artificial**, capaces de determinar si la imagen capturada corresponde a una persona real, sin necesidad de que el usuario realice acciones adicionales o movimientos específicos. Este enfoque de **prueba de vida pasiva** contribuye de forma significativa a mejorar la experiencia de usuario, reduciendo fricciones y tiempos de interacción, sin comprometer la seguridad del proceso.



A continuación, se presenta un **ejemplo ilustrativo del recorrido del usuario (customer journey)** durante el proceso de verificación de identidad, con el fin de facilitar la comprensión de las distintas etapas que lo componen y de la experiencia ofrecida por la solución.



- El usuario inicia el proceso en el que se le presentan las condiciones de uso y protección de datos. En este momento, tendrá que aceptar las condiciones y autorizar expresamente la realización del proceso (consentimiento).
- Se inicia el proceso de captura automática de documento de identidad. Se captura anverso y reverso en el caso de que el documento disponga de ambas caras.
- El usuario valida que las capturas son correctas y se toma un selfie con prueba de vida pasiva. La solución valida la identidad del usuario entre documento de identidad y selfie.
- Todas las validaciones y evidencias del proceso están disponibles en un portal de revisión para ser consultadas y revisadas en caso de que sea necesario.

A continuación, se detallan las **características de la solución** que cumplen con los requisitos solicitados por la Superintendencia de una forma más detallada:



Captura y validación del documento

Nuestro módulo de captura y validación de documentos de identidad está diseñado para proporcionar una solución integral y automatizada, capaz de operar tanto en plataformas móviles como en interfaces web, asegurando una experiencia de usuario fluida y segura. La captura se realiza a través de tecnología OCR.

Para la obtención de la información de los documentos de identidad, tanto en entornos nativos como web, la solución captura el anverso y el reverso del documento de identidad. Para el caso del pasaporte, el proceso queda reducido a una sola captura al disponer solo de una cara.

También es posible establecer un rango de documentos soportados y rechazar los procesos realizados con documentos diferentes.

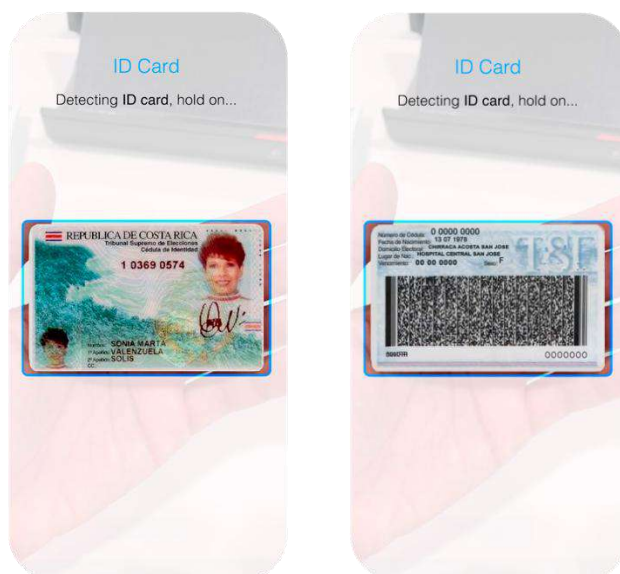
La herramienta es capaz de detectar automáticamente si el lado del documento mostrado es el correcto. Por ejemplo, si se solicita el anverso y el usuario presenta el reverso, el sistema lo detecta y solicita la captura adecuada.

Durante la captura, la solución controla la cámara del dispositivo y guía al usuario mediante instrucciones en pantalla, evitando que deba tomar fotografías manualmente.

En tiempo real la solución analiza diferentes “frames” dando feedback al usuario para guiarlo hasta que detecta de forma automática el documento esperado y realiza la captura.

Esto garantiza que la obtención de imágenes sea ágil, precisa y bajo las mejores condiciones posibles, ya que son los algoritmos los que deciden en tiempo real el momento óptimo para la captura.

La imagen resultante es optimizada en tiempo real mediante corrección de perspectiva y recorte automático, eliminando información innecesaria y mejorando la extracción de datos. La solución extrae la información, comprobando la vigencia del documento y detectando posibles manipulaciones, fotocopias, escaneos o capturas de pantalla según se detalla en el epígrafe



Además de la funcionalidad de captura automática, la solución permite habilitar un botón para que la captura se haga de forma manual mediante una foto para aquellos casos en que la captura automática no sea adecuada. Además, para casos de usos en los que sea requerido, la solución permite subida de documentos de identidad a través de una API para la extracción y validación de datos.

Validación biométrica facial con prueba de vida pasiva

Tras la verificación documental, el sistema realiza un proceso de matching facial comparando la imagen del documento con una captura facial obtenida durante el registro.





El sistema está entrenado para ofrecer las mayores tasas de seguridad siendo robusto ante aspectos como la diferencia de aspecto, el paso del tiempo o la deficiente conservación de la fotografía impresa. El resultado final se comunica al backoffice en forma de porcentaje de similitud o scoring.

Durante la captura del rostro, la aplicación guía al usuario para garantizar:

- Correcta posición dentro del marco de referencia.
- Iluminación adecuada.
- Resolución y nitidez óptimas.
- Ausencia de obstrucciones faciales.

La solución integra un módulo de detección de ataques de presentación (Presentation Attack Detection – PAD) para confirmar que la persona está viva y evitar fraudes (como deepfakes).

7.3 Prueba de vida

La tecnología propuesta de biometría facial incorpora mecanismos de detección de vida avanzada contra ataques de presentación. Nuestro sistema aprovecha el poder de la inteligencia artificial para enfrentar ataques de suplantación de identidad – Presentation Attack Detection (PAD) colaborativo o no colaborativo. Distingue y desvía inteligentemente los intentos de fraude de los instrumentos de ataque de presentación:

- Imágenes impresas.
- Máscaras de papel, silicona o látex.
- Capturas o imágenes en pantalla.
- Grabaciones de video.
- Caracterización o maquillaje.
- Deepfakes.
- Inyecciones de video.

El objetivo final de estas medidas es comprobar que no existe ningún intento de engaño o suplantación de identidad en la fase de captura biométrica, es decir, que ante la cámara se muestra una persona viva que no realiza actividades sospechosas.

Si bien ofrecemos mecanismos de detección de vida tanto activos como pasivos, recomendamos el método pasivo para conseguir una mejor experiencia de usuario.

A diferencia de los métodos activos que requieren acciones específicas del usuario, como mover la cabeza de un lado a otro, las medidas de vida pasiva funcionan perfectamente sin interacción del usuario, eliminando cualquier tipo de fricción en el proceso. Los usuarios simplemente posicionan sus rostros centrados en el óvalo.



Hay que indicar que en este proceso lo que se está captando es una pequeña secuencia de video (habitualmente 4-5 segundos) para su análisis mediante tecnologías de aprendizaje profundo. A la salida se obtiene un valor numérico como porcentaje de probabilidad en la prueba de vida.

La solución de Inetum cumple con los requisitos solicitados, poniendo a disposición un motor biométrico que ha sido **evaluado** dentro del programa Face Recognition Vendor Test 1:1 (FRVT 1:1) por parte del National Institute of Standards and Technology (**NIST**), obteniendo resultados acordes con el estado del arte actual de estas tecnologías.

Los siguientes resultados dentro de la categoría VISABORDER en la última evaluación FRVT1:1 (actualmente denominada FRTE1:1) enviada al NIST en octubre de 2024 (https://face.nist.gov/frte/reportcards/11/mobbl_005.html), nuestros algoritmos han obtenido en la configuración VISABORDER (que es aquella que evalúa nuestra solución para los procesos de onboarding digital en los que se compara la foto del documento de identidad con otro tipo de fotos similares a las que se pueden realizar en un selfie) los siguientes resultados:

- FNMR = 0.0045 (*)
- FMR = 0.000001

() Tasa de falsos negativos (FNMR) igual al 0,0045 en el punto de trabajo establecido: el que corresponde a una tasa de falsos positivos (FMR) de 0,000001.*

La solución cuenta también con otras evaluaciones NIST como FRTE 1:N y FATE Quality.

También, cumplimos con los estándares de la norma **ISO/IEC 30107-3**, lo que garantiza un alto nivel de seguridad en la detección de ataques de presentación. Como hemos detallado, el sistema es capaz de detectar y bloquear fotos impresas, imágenes en



pantalla, vídeos, máscaras de diversos materiales (látex, silicona), maquillaje profesional y deepfakes.

Además de estos estándares, la solución cuenta con la certificación LINCE (Certificación Nacional Esencial de Seguridad) del Centro Criptológico Nacional (CCN) de España, habiendo superado con éxito las evaluaciones de ataques de presentación y suplantación exigidas.

7.4 Fotografía

El sistema genera imágenes a color, centradas y correctamente enfocadas, con capacidad de exportación en formatos JPEG (**ISO/IEC 10918-1**), JPEG 2000 (**ISO/IEC 15444-1**) y PNG (**ISO/IEC 15948:2003**). Las imágenes capturadas presentan un color neutro, sin saturación, y cuentan con al menos **7 bits** de variación por canal RGB, lo que garantiza más de **128 valores** únicos por canal. Si bien la cámara utilizada corresponde al dispositivo del usuario, y por ende no se dispone de control directo sobre sus especificaciones de hardware, el sistema incorpora algoritmos avanzados de control de calidad que verifican automáticamente parámetros como el enfoque, la nitidez y la profundidad antes de aceptar la fotografía, asegurando así que los detalles faciales se representen con la máxima precisión posible dentro de las capacidades del dispositivo.

Adicionalmente, el software guía al usuario para que mire directamente a la cámara, adoptando una postura natural y evitando desviaciones o inclinaciones de la cabeza. Asimismo, la herramienta detecta si el rostro, la cabeza o la parte superior del cuello se encuentran demasiado cerca o alejados, proporcionando retroalimentación instantánea para que el usuario ajuste su posición, tanto en escala como en alineación horizontal respecto a la cámara. Como resultado, la imagen final incluye la cabeza completa, la parte superior del cuello y ambos lados del rostro, manteniendo una expresión neutra, con labios cerrados y sin inclinaciones.

El sistema garantiza que ambos ojos estén abiertos de forma natural, claramente visibles y sin obstrucciones causadas por el cabello u otros elementos. Igualmente, las imágenes presentan niveles óptimos de brillo y contraste que permiten distinguir claramente el rostro, el cabello y el fondo, asegurando una adecuada nitidez en todas las áreas faciales. La captura se realiza bajo condiciones de iluminación uniforme, evitando reflejos, sombras y el efecto de ojos rojos, sin emplear filtros de polarización que puedan alterar la textura de la piel.

Por otra parte, el sistema verifica que los ojos sean completamente visibles y que ni los marcos ni los cristales de las gafas generen obstrucciones o reflejos. Asimismo, se valida que no se utilicen lentes oscuros o con filtros, salvo en casos debidamente justificados por razones médicas. Del mismo modo, se comprueba que la persona no lleve la cabeza cubierta, excepto por motivos religiosos, en cuyo caso se garantiza que el rostro permanezca completamente visible, sin distorsiones ni sombras, desde la coronilla hasta la barbilla y de oreja a oreja, incluyendo la línea del cabello.



El sistema también valida la ausencia de elementos u ornamentaciones que puedan ocultar o distorsionar el rostro, permitiéndose únicamente aquellos accesorios que no interfieran en la visibilidad ni en la correcta captura de los rasgos faciales. En este sentido, la solución asegura que las imágenes cumplen con las especificaciones relativas a dimensiones y ubicación de la cabeza.

En cuanto a las características técnicas, las imágenes capturadas cumplen la resolución recomendada para **entornos web (72 ppp), con un peso aproximado de entre 200 y 300 KB y un tamaño máximo de 1200 píxeles** en el lado mayor. Este equilibrio permite garantizar tanto una calidad suficiente para su validación como una optimización adecuada para su transmisión y procesamiento eficiente en la plataforma.

Paralelamente, la solución guía al usuario en tiempo real para asegurar que la captura se realice bajo condiciones óptimas de iluminación y brillo. Detecta incidencias como iluminación insuficiente, destellos, reflejos o sobreexposición, proporcionando instrucciones inmediatas para su corrección. Este control garantiza una relación adecuada entre contraste y brillo, permitiendo distinguir con claridad los caracteres del fondo, lo cual resulta esencial para la legibilidad del documento y para el correcto funcionamiento de procesos posteriores como el reconocimiento óptico de caracteres (OCR).

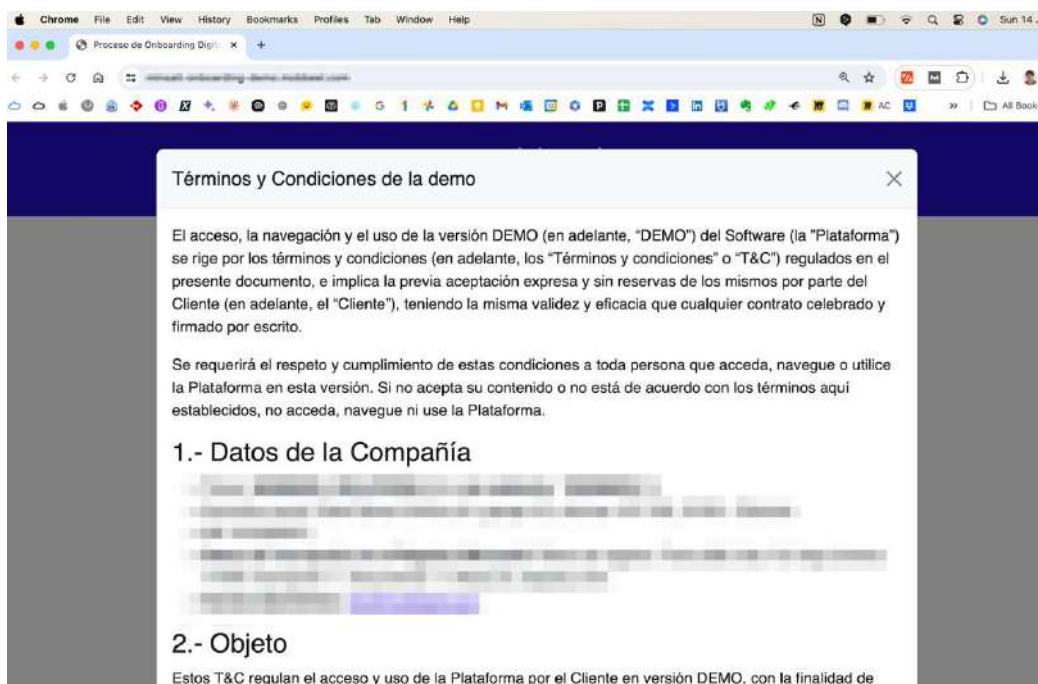
Adicionalmente, el sistema aplica técnicas automáticas de mejora de imagen destinadas a reducir o eliminar el ruido visual, optimizando la claridad del documento y facilitando un reconocimiento más preciso. La imagen obtenida tras la captura es además optimizada en tiempo real mediante recorte automático y corrección de perspectiva, lo que permite extraer la información de manera más precisa, ejecutar las validaciones correspondientes y obtener una imagen final de mayor calidad al eliminar elementos innecesarios.

Finalmente, durante el proceso de captura, la solución detecta automáticamente los bordes del documento, recorta el área de interés descartando el fondo y corrige posibles desviaciones de inclinación o rotación respecto a la cámara del dispositivo. De este modo, se garantiza que el documento quede perfectamente alineado y preparado para su procesamiento posterior.

7.5 Consentimiento

Como paso previo a la captura de datos para proceder a la validación biométrica, el sistema permite mostrar una pantalla en la que se le informará del propósito de los datos que se van a capturar, el detalle de los mismos, la base de legitimación, sus derechos de acceso, etc. para garantizar que se cumplen las obligaciones en materia de protección de datos. El usuario deberá confirmar explícitamente marcando una casilla el consentimiento del tratamiento de dichos datos, si no el proceso no podrá continuar. Esta acción explícita de consentimiento queda guardada en el sistema y las evidencias pueden ser recuperadas posteriormente en caso de una eventual reclamación.

A continuación, pueden verse pantallas de ejemplo de la solicitud de consentimiento y aceptación de la realización del proceso.



7.6 OCR

La solución utiliza tecnología OCR avanzada para extraer automáticamente los datos de las imágenes de los documentos de identidad. Esto permite que los caracteres de los documentos sean reconocidos y leídos por un dispositivo, evitando la entrada manual de información por parte del usuario. Esto permite que el sistema o servicio donde se integra la solución pueda recibir la información extraída para cualquier proceso requerido como puede ser sustituir ingresados manualmente por el usuario.

La herramienta es capaz de capturar y analizar toda la información visible del documento (VIZ), tanto del anverso como del reverso.

Además, lee y valida automáticamente la información contenida en la Zona de Lectura Mecánica (MRZ) para aquellos documentos que cuenten con MRZ, que incluye datos básicos como nombre, fecha de nacimiento, fecha de caducidad, país emisor y número de documento. La solución compara los datos de la VIZ con los de la MRZ para asegurar la coherencia y detectar cualquier discrepancia.

Adicionalmente, la solución reconoce y decodifica la información contenida en códigos bidimensionales como QR y PDF417, presentes en documentos oficiales. Estos códigos almacenan información cifrada o estructurada que puede incluir número único de identificación, firma digital de la autoridad emisora y otros campos relevantes.

7.7 Verificación de legitimidad

La herramienta captura y analiza toda la información visible del documento (VIZ), tanto del



anverso como del reverso, en caso de que ambos lados contengan datos. La zona de inspección visual es crucial, ya que contiene información detallada del titular del documento que debe ser verificada para asegurar la autenticidad y precisión del documento

La solución realiza las siguientes funciones enfocadas en la VIZ:

- **Captura completa de datos:** Se obtiene la información visible del documento, incluyendo texto, firma y otros elementos presentes en el anverso y reverso del documento. Esta captura exhaustiva garantiza que no se omite ningún dato relevante.
- **Verificación de coherencia de datos:** Se comparan los datos personales presentes en la VIZ con los datos básicos de la MRZ para asegurar su consistencia. Esto incluye la verificación de nombre, fecha de nacimiento, número de documento, nacionalidad, entre otros. Cualquier discrepancia entre la VIZ y la MRZ se identifica.
- **Análisis de elementos adicionales:** La VIZ puede incluir otros elementos críticos, como características de seguridad. La solución verifica que éstos cumplen con los estándares de seguridad del documento.
- **Detección de posibles anomalías:** La solución analiza todos los datos visibles en la VIZ para identificar cualquier inconsistencia que pueda indicar un posible fraude o alteración del documento.

La solución incorpora un análisis de medidas de seguridad avanzadas, es decir, mecanismos de verificación de la validez del documento capturado y medidas de control para garantizar la autenticidad del mismo. Además, analiza la vigencia del documento.

En cuanto a la vigencia, la herramienta es capaz de verificar que la **fecha de validez** del documento no ha expirado, o alertar en caso contrario.

La fecha de validez del documento se extrae y se compara con la fecha actual, de manera que si se detecta que se ha superado su periodo de validez se registra una evidencia en el backoffice del sistema.

A parte de determinar la vigencia, la tecnología permite detectar usos fraudulentos o manipulaciones en los procesos de enrolamiento digital mediante una serie de controles específicos. Estos controles se dividen en las siguientes categorías principales: controles de apariencia y controles basados en el contenido del documento.

Controles de apariencia

Mediante el uso de tecnologías de visión por computador se analiza el aspecto físico del documento para determinar si ha sufrido algún tipo de manipulación o se encuentra invalidado.

Para este análisis se tienen en cuenta los siguientes elementos:

- **Validación de fuentes tipográficas:** La fuente tipográfica de la MRZ coincide con la



oficial según el estándar ICAO 9303 (OCR-B).

- La zona donde se encuentra la imagen facial no está alterada (por ejemplo con otra imagen superpuesta).
- Validación de contorno: El contorno del documento corresponde a la forma esperada y no presenta cortes.
- Detección de fotocopia o escaneos: El documento no es una fotocopia en blanco y negro o un escaneo.
- Detección de capturas y ataques de pantalla: La imagen del documento no ha sido capturada a través de una pantalla.
- Validación de elementos distintivos: Se encuentran visibles todos los chips, emblemas, logotipos y distintivos oficiales.
- Análisis de códigos de barras y bidimensionales: Los códigos presentes en el documento deben ser legibles, sin alteraciones visuales ni degradaciones gráficas que indiquen manipulación (como pixelaciones, recortes o superposiciones). Además, se comprueba que correspondan al formato oficial esperado para el tipo de documento.

Controles basados en el contenido

Estas medidas se centran en la validación de los datos contenidos en el documento de identidad. La ICAO define en la serie de normas 9303 un estándar para los documentos oficiales de viaje, de manera que la inmensa mayoría de aquellos reconocidos internacionalmente como válidos se ajustan a una serie de patrones que hacen posible determinar si cumplen con la regulación.

Algunos de los aspectos analizados en este bloque son:

- Validación de dígitos de control y checksum de la cadena MRZ
- Validación entre ambas caras (correspondencia de datos entre anverso y reverso).
- Detección de especímenes y documentos de muestra.
- Validación de códigos de barras y bidimensionales: La solución verifica que el contenido decodificado de estos elementos coincide con la información visible y la MRZ, además de comprobar su integridad y estructura. En el caso de PDF417, se revisa que el bloque de datos no presente manipulación y que la firma digital embebida (cuando aplique) sea válida. Para los QR, se valida igualmente la integridad de los datos, su estructura y posibles firmas de seguridad emitidas por la autoridad correspondiente.
- Análisis de parámetros lógicos
- Detección de manipulaciones de archivos con software de edición fotográfica (para los procesos donde se permite el uso de imágenes adjuntas)



El sistema realiza una serie de controles específicos que son finalmente analizados en su conjunto para ofrecer un resultado global sobre la validez de la apariencia del anverso y reverso del documento. Todas estas medidas anteriores serán posibles dependiendo del tipo de documento y como este expone la información por lo que en algunas versiones o tipos de documentos puede darse el caso de que no sea posible como cuando no exista un código QR o PDF417 o que en caso de existir no permitan su lectura por terceros.



inetum.™



inetum.com