INTERNAL DOCUMENT

POLITICA DE SEGURIDAD ITALTEL ESPAÑA

Cliente: Italtel Country: España Data: 27.1.2025	Autor: Sergio Morón Aprobado por: Albert Soler

Índice

REVISION DEL DOCUMENTO

Versione	Data	Modifiche	Consegnata al cliente
27/06/2023	1.0	Pablo Rodríguez	Primera versión.
07/08/2023	2.0	Pablo Rodríguez	Versión inicial con los puntos desarrollados
06/09/2023	2.1	Pablo Rodríguez	Cambios en Objetivos, Marco Normativo, Roles
21/09/2023	2.2	Pablo Rodríguez	Cambios en los roles del comité de seguridad
26/09/2023	2.3	Pablo Rodriguez	Inclusión de nuevos roles y cambio de responsable
02/10/2023	2.4	Alejandro Garcia	Modificación comité seguridad
04/10/2023	2.5	Pablo Rodriguez	Adaptación nuevo formato de documento
23/11/2023	2.6	Javier Rubio	Firma Director General
27/01/2024	2.7	Sergio Morón	Adaptación al art 12 ENS

Aprobado por:

Albert Soler
Resp. de Seguridad

Alessandro Di Salvo
Director General

1 INTRODUCCIÓN

Italtel depende de los activos de información para alcanzar sus objetivos. Estos activos deben ser gestionados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad y/o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los activos de información deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, el uso previsto y el valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que todas las personas de Italtel, tanto propias como subcontratadas, (en adelante, las partes interesadas) deben aplicar las medidas de seguridad definidas, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las partes interesadas de Italtel deben cerciorarse de que la seguridad de la información es una parte integral de cada etapa del ciclo de vida de los activos de información, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, en el diseño, las compras y subcontrataciones, ...

Las partes interesadas de Italtel deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes de seguridad de la información.

2 ALCANCE

Esta política se aplica a todos los activos de información de Italtel y a partes interesadas, sin excepciones.
Esta política es punto de referencia para el desarrollo de las dimensiones de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información de Italtel.

3 MISIÓN

En Italtel S.A. queremos permitir que las personas, los activos de información y las redes se comuniquen para contribuir a construir un futuro mejor.
Trabajamos para hacer posible una ciudadanía digital plena y segura, y conseguir que la inclusión digital sea realidad en nuestra cultura.
Creemos que «nosotros» es más fuerte que la suma de las individualidades: colaboración, confianza mutua e involucración son nuestra fuerza.
Estamos convencidos de que nuestro valor reside en las personas y que la atención a su bienestar es un desafío para el futuro.
Pretendemos acelerar el desarrollo de infraestructuras inteligentes y de servicios digitales que mejoren la calidad de vida de las personas y la competitividad de los sistemas económicos.
Escuchamos a nuestros clientes, ponemos pasión en nuestro trabajo y desafiamos la complejidad buscando la excelencia.
Elegimos invertir en innovación y competencias, también en colaboración con nuestros partners.
Creemos en el valor de las empresas que saben cambiar y transformarse

4 MARCO NORMATIVO

En el caso de Italtel tiene especial relevancia el siguiente marco normativo:
Seguridad de la información:

- Esquema Nacional de Seguridad
- Ley que establece medidas para la protección de las infraestructuras críticas
- Reglamento de protección de las infraestructuras críticas
- Contenidos de Planes de Seguridad del Operador y de Planes de Protección Específicos
- Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales
- Reglamento de la Ley Orgánica de protección de datos de carácter personal
- Reglamento Europeo relativo a protección en el tratamiento de datos personales
- Ley Orgánica del Código Penal

Telecomunicaciones y usuarios:

- Ley de servicios de la sociedad de la información y de comercio electrónico
- Medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos
- Distintivo público de confianza en los servicios de la sociedad de la información
- Ley reguladora de determinados aspectos de los servicios electrónicos de confianza

- Ley General de Telecomunicaciones de 2014 (parcial)
- Ley General de Telecomunicaciones
- Ley de conservación de datos relativos a comunicaciones electrónicas y redes públicas
- Seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación

5 ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD

Objetivo: Establecer una estructura organizativa clara y un plan de implementación para asegurar la protección de la información.

5.1 Responsabilidad del responsable de seguridad:

Se nombra a un responsable de Seguridad de la Información (RSI), quien tendrá la responsabilidad general de implementar y mantener la política de seguridad y supervisar todas las actividades relacionadas.

5.2 Comité de Seguridad.

El Comité de Seguridad de la Información está formado por los responsables de datos de carácter personal, seguridad, sistemas, información y servicios.
El Comité de Seguridad de la Información tiene como función básica determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, velar por la seguridad de la información en Italtel y proponer la revisión y mantenimiento de la política y sistema de gestión de la seguridad de la información para cumplir con ese propósito.
También es responsable de proponer inversiones necesarias para asegurar el nivel de seguridad. Debe valorar los requisitos de seguridad de los servicios de Italtel, así como la consecuencia de un problema de seguridad en los mismos.
El secretario del comité de seguridad de la información será el responsable de Seguridad.
El Comité de Seguridad de la Información reporta al Comité de Dirección.

5.3 Roles: Funciones y responsabilidades

El responsable de seguridad es el encargado de satisfacer los requisitos de seguridad de la información y de los servicios. Debe asegurar la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Información

de la organización. También deberá promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

El responsable de sistema debe desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento. Debe definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo. Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad. En caso necesario se designará por parte del responsable de sistemas a uno o varios responsables de sistemas delegados para ciertas aplicaciones

El responsable de la información debe valorar el nivel de seguridad adecuado para la información que utiliza. Esta responsabilidad recae, por lo tanto, en el dueño de la información y debe valorar el nivel de seguridad adecuado para cada parte de la información que utilicen.

El responsable del servicio debe valorar el nivel de seguridad adecuado en el servicio que presta.

El responsable de protección de datos debe supervisar el cumplimiento de la normativa de protección de datos, colaborar con autoridades reguladoras, realizar evaluaciones de impacto de protección de datos, monitorizar la seguridad de los datos y mantener registros de todas las actividades relacionadas con la protección de datos

5.4 Procedimiento de designación

Los responsables serán nombrados por el Comité de Dirección a propuesta del Comité de Seguridad de la Información. Los nombramientos se revisarán anualmente o cuando el puesto quede vacante.

5.5 Planificación.

Se elaborará un plan de acción de seguridad a corto, medio y largo plazo, con plazos definidos, responsables y métricas de evaluación. Además, se establecerán procedimientos de comunicación claros para gestionar incidentes de seguridad y actualizaciones de la política.

6 ANÁLISIS Y GESTIÓN DE LOS RIESGOS

Objetivo: Evaluar y gestionar los riesgos de seguridad que puedan afectar los sistemas de información, con el fin de implementar medidas de mitigación adecuadas.

6.1 Identificación de activos.

Se realiza un inventario completo de todos los activos de información integrados en una CMDB (hardware, software, datos, etc.).

6.2 Evaluación de riesgos.

Se lleva a cabo un análisis de riesgos periódicamente, utilizando metodologías reconocidas como el análisis cualitativo y cuantitativo para identificar vulnerabilidades, amenazas y consecuencias. La probabilidad y el impacto de cada riesgo son evaluados y clasificados.

6.3 Tratamiento de riesgos.

Una vez evaluados los riesgos, se definen acciones correctivas y preventivas para reducir los riesgos a niveles aceptables. Esto puede incluir controles técnicos, físicos y organizacionales.

7 GESTIÓN DE PERSONAL

Objetivo: Asegurar que el personal esté capacitado y concienciado sobre la seguridad de la información y que se gestionen adecuadamente sus accesos y responsabilidades.

7.1 Selección de personal

Durante el proceso de selección, se incluirán evaluaciones sobre la fiabilidad del candidato en cuanto a seguridad (verificación de antecedentes, etc.).

7.2 Formación continua.

Se imparten formaciones periódicas sobre políticas de seguridad, buenas prácticas y concienciación ante amenazas como el phishing, malware, etc.

7.3 Gestión de acceso

Se mantiene un registro detallado de las personas que tienen acceso a los sistemas. Además, se proporcionarán permisos según los roles laborales, de acuerdo con el principio de "mínimo privilegio".

8 PROFESIONALIDAD

Objetivo: Asegurar que el personal con acceso a la información esté adecuadamente capacitado y sea competente para cumplir con las políticas de seguridad.

8.1 Certificación y capacitación

Los empleados en áreas críticas (como administración de sistemas, redes o seguridad) preferentemente deben obtener certificaciones en estándares de seguridad reconocidos y formación específica en los sistemas que operan.

8.2 Evaluación periódica.

Se realizarán evaluaciones periódicas del desempeño del personal técnico y su conocimiento en seguridad de la información, con el objetivo de detectar necesidades de formación adicionales.

9 AUTORIZACIÓN Y CONTROL DE LOS ACCESOS

Objetivo: Gestionar adecuadamente los accesos a los sistemas de información, asegurando que solo las personas autorizadas tengan acceso a los datos y recursos necesarios para sus funciones.

9.1 Control de acceso

Se implemente un sistema de control de acceso basado en roles (RBAC), donde se asignan permisos de acuerdo con las necesidades laborales específicas de cada usuario.

9.2 Autenticación fuerte.

Se adoptan métodos de autenticación robustos, como contraseñas complejas y autenticación multifactor (MFA).

9.3 Revisión de accesos.

Se realizarán auditorías periódicas para revisar y ajustar los privilegios de acceso de los empleados, especialmente cuando cambien de roles o salgan de la organización.

10 PROTECCIÓN DE LAS INSTALACIONES

Objetivo: Garantizar que las instalaciones físicas que albergan los sistemas y datos estén protegidas contra accesos no autorizados y amenazas físicas.

10.1 Control físico de acceso.

Implementamos controles de acceso como cerraduras electrónicas y tarjetas de acceso en áreas sensibles (servidores, centros de datos).

10.2 Vigilancia y protección.

Instalación de cámaras de seguridad y vigilancia las 24 horas del día, sistemas de alarma, y medidas contra incendios, inundaciones y otros desastres naturales.

10.3 Seguridad perimetral.

Control de las entradas y salidas de las instalaciones, incluyendo la validación de visitantes y la supervisión de las personas que acceden al área.

11 ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD

Objetivo: Asegurar que los productos de seguridad y los servicios contratados cumplan con los requisitos de la organización y la normativa de seguridad vigente.

11.1 Evaluación de proveedores.

Se establecerán criterios claros para la selección de proveedores de tecnología y servicios de seguridad, asegurando que estos cumplan con las normas de seguridad aplicables (por ejemplo, normas ISO 27001, ENS, etc.).

11.2 Auditorías de productos y servicios.

Todos los productos adquiridos (hardware, software, sistemas de seguridad) son auditados para verificar que sean seguros y compatibles con la infraestructura existente de la organización.

11.3 Contratos con proveedores.

Los contratos con proveedores de servicios externos incluyen cláusulas claras sobre la protección de la información y los controles de seguridad requeridos, así como auditorías periódicas para garantizar el cumplimiento.

12 MÍNIMO PRIVILEGIO

Objetivo: Garantizar que cada usuario tenga acceso solo a la información y sistemas necesarios para llevar a cabo sus funciones, minimizando riesgos derivados de accesos innecesarios.

12.1 Política de acceso basado en roles (RBAC).

Implementamos un sistema de acceso que limite el acceso a recursos en función de las responsabilidades laborales. Los usuarios no tendrán acceso a información fuera de su ámbito de trabajo.

12.2 Revisión regular de privilegios.

Se realizarán revisiones periódicas de los privilegios de acceso, sobre todo cuando haya cambios en el rol o cuando los usuarios dejen la organización.

13 INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

Objetivo: Asegurar que los sistemas operativos, aplicaciones y plataformas estén actualizados y no contengan vulnerabilidades explotables.

13.1 Gestión de parches.

Se implementará un procedimiento para asegurar que los sistemas reciban actualizaciones y parches de seguridad de manera oportuna.

13.2 Revisión de configuraciones.

Se realizarán auditorías regulares para asegurar que las configuraciones de seguridad estén alineadas con las mejores prácticas y no existan configuraciones inseguras.

14 PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

Objetivo: Asegurar que la información esté protegida tanto cuando está almacenada como cuando se transmite entre sistemas.

14.1 Cifrado de la información.

Todos los datos sensibles están cifrados.

14.2 Protección de comunicaciones.

Se emplearán siempre protocolos de comunicación seguros, utilizando métodos de cifrado robustos con el objetivo de garantizar la confidencialidad y la integridad de los datos, protegiendo así la información en tránsito.

15 PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS

Objetivo: Asegurar que los sistemas de información interconectados no representen un riesgo para la seguridad.

15.1 Firewalls y segmentación de redes.

Se han implementado firewalls y poseemos segmentación en las redes para limitar el acceso entre sistemas internos y externos.

15.2 Evaluación de interconexiones.

Antes de interconectar con sistemas externos (proveedores, clientes), se evaluarán los riesgos y se implementarán controles adecuados para proteger la organización.

16 REGISTRO DE LA ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO

Objetivo: Establecer mecanismos efectivos de registro y monitoreo de la actividad en los sistemas, con el fin de identificar comportamientos anómalos y detectar de manera temprana la presencia de código dañino, con el objetivo de prevenir, mitigar y responder a amenazas que puedan comprometer la seguridad, integridad y disponibilidad de los activos de la organización.

16.1 Monitoreo de actividad.

Se establecen sistemas de auditoría y monitoreo para registrar las actividades en los sistemas. Los registros se analizan periódicamente para identificar posibles incidentes de seguridad.

16.2 Antivirus y detección de malware.

Se implementan soluciones avanzadas de antivirus y sistemas de detección de malware, asegurando su actualización constante para prevenir, identificar y eliminar amenazas potenciales. Estas medidas garantizan la protección proactiva de los sistemas y la integridad de los activos digitales de la organización.

17 INCIDENTES DE SEGURIDAD

Objetivo: Gestionar eficientemente los incidentes de seguridad para minimizar su impacto y aprender de ellos.

17.1 Plan de respuesta a incidentes.

Se tiene una Normativa de respuesta a incidentes que incluye protocolos para identificar, contener, mitigar y analizar los incidentes.

17.2 Notificación y registro.

Todos los incidentes serán registrados y reportados, y se realizarán investigaciones para identificar las causas y mejorar las defensas.

18 CONTINUIDAD DE LA ACTIVIDAD

Objetivo: Garantizar la capacidad de la organización para mantener sus operaciones esenciales y minimizar interrupciones frente a situaciones de emergencia, asegurando así la continuidad del negocio y la resiliencia operativa.

18.1 Planes de contingencia.

Poseemos planes de recuperación ante desastres (DRP) y continuidad del negocio (BCP) para garantizar que los sistemas críticos puedan recuperarse rápidamente después de un incidente.

18.2 Pruebas periódicas.

Se realizan anualmente simulacros y pruebas para validar la eficacia de los planes de continuidad.

19 MEJORA CONTINUA DEL PROCESO DE SEGURIDAD

Objetivo: Garantizar que la política de seguridad se mantenga relevante y efectiva a lo largo del tiempo.

19.1 Revisión periódica.

Se establecen procedimientos de revisión continua de las políticas y procedimientos de seguridad, basados en auditorías internas, cambios tecnológicos y nuevas amenazas.

19.2 Lecciones aprendidas

Después de cada incidente o revisión, se documentarán las lecciones aprendidas y se ajustarán los procedimientos y controles según sea necesario.