POL-SI-01.DOC

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Propietario: CISO
Revisa: Dir. Delivery, Services and IT/IT Manager/ Responsable del SIG
Aprueba: CISO

Versión: 5
Fecha de Revisión: Abril 2024

INDICE

1. OBJETO

Esta Normativa de seguridad de la información, viene a desarrollar la Política de Seguridad de la información establecida por fibratel.

Esta normativa da cumplimiento al artículo 11 del Esquema Nacional de Seguridad (ENS), de requisitos mínimos de seguridad que establece la necesidad de disponer formalmente de una normativa de seguridad que articule la gestión continuada de la seguridad.

La normativa de seguridad se establece de acuerdo con los principios básicos establecidos en la política de seguridad de la información y se desarrolla aplicando los requisitos mínimos necesarios. Todos estos requisitos mínimos se establecen en proporción a los riesgos identificados en los sistemas de información, pudiendo algunos no requerirse en sistemas sin riesgos significativos.

2. ALCANCE

Esta Política afecta a todas las áreas de la organización que tengan un sistema de seguridad de la información establecido y a todos los lugares donde se desarrolle su actividad. Esta Normativa afecta tanto al personal interno de fibratel como al personal externo que trabaje en la empresa.

3. REFERENCIAS

- Norma UNE-ISO/IEC 20000-1.
- Norma UNE-EN-ISO 27001:2022
- Esquema Nacional de Seguridad (ENS2)
- TISAX VDA ISA6

4. CONTENIDO

En el Grupo fibratel (en adelante fibratel) consideramos la información como uno de los activos más importantes de nuestra organización, lo que hace que requiera una protección adecuada y específica. Entendemos que, como empresa líder en aportar soluciones tecnológicas a nuestros clientes, debemos también poner el foco de nuestra atención en prevenir la pérdida o el uso indebido de la información de partes interesadas que pueda llegar a suponer un riesgo para la organización y socavar la confianza de nuestros clientes.

Por este motivo la organización ha optado por aplicar un modelo de gestión, basado en el **Sistema de Gestión de Seguridad de la Información (SGSI)** sobre los estándares internacionales **UE-EN ISO/IEC 27001 y UNE-ISO/IEC 20000-1**, así como dar cumplimiento al **Esquema Nacional de Seguridad (ENS) en su nivel ALTO**, que permita, a través de un entorno de procesos de aseguramiento de la calidad, gestionar controles de seguridad en base a un trabajo constante de mejora continua basado en análisis de riesgos, evolución tecnológica, formación y concienciación de las personas y el cumplimiento y aseguramiento de las políticas definidas y transmitidas.

El objetivo del SGSI consiste en integrar la seguridad de la información como parte de la cultura y gestión de la organización con la finalidad de **garantizar la confidencialidad, disponibilidad, integridad, trazabilidad y autenticidad de la información**, mediante el establecimiento de directrices y políticas hacia las diferentes áreas y departamentos de la compañía dentro del marco legal.

Para poder lograr estos objetivos es necesario:

- **Cumplir con requisitos legales aplicables** y con cualesquiera otros requisitos que suscribimos además de los compromisos adquiridos con los clientes, así como la actualización continua de los mismos.
- **Identificar y analizar las amenazas potenciales**, así como el impacto en las operaciones de negocio que dichas amenazas, caso de materializarse, puedan causar.
- **Preservar los intereses de nuestras principales partes interesadas** (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.
- **Trabajar de forma conjunta con nuestros suministradores** y subcontratistas con el fin de mejorar la prestación de servicios de TI, la continuidad de los servicios y la seguridad de la información, que repercutan en una mayor eficiencia de nuestra actividad.
- Evaluar y garantizar la **competencia técnica del personal**, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros procesos, proporcionando la formación y la comunicación interna adecuada para que desarrollen buenas prácticas definidas en el sistema.
- Garantizar el **correcto estado de las instalaciones y el equipamiento** adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.
- Garantizar un **análisis** de manera continua de todos los **procesos relevantes**, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.
- **Mejorar continuamente** nuestro sistema de seguridad de la información
- Estructurar nuestro sistema de gestión de forma que sea fácil de comprender.

Con la implantación del SGSI, impulsado desde la Alta dirección, se facilita la gestión adecuada y eficaz de los riesgos existentes en los sistemas de información, permitiendo aumentar su seguridad. De este modo, al minimizarse los posibles riesgos de las TIC, se aumenta la confianza al ofrecer servicios con una alta seguridad y calidad en el uso de la tecnología.

ANEXO I: ESTRUCTURA DE LA SEGURIDAD DE LA INFORMACIÓN

A) ORGANIZACIÓN DE SEGURIDAD

La responsabilidad esencial de la Seguridad de la Información recae sobre la Dirección General a través del Comité de Dirección de la organización, ya que esta es responsable de organizar las funciones, responsabilidades, así como de facilitar los recursos adecuados para conseguir los objetivos del SGSI. Además, los directivos son también responsables de promover, y liderar con el ejemplo, las políticas y normas de seguridad establecidas.

Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento a través de la intranet.

Los roles o funciones de seguridad definidos por diferente reglamentos o normas se resumen y se asignan de la siguiente manera:

FUNCIÓN	DEBERES Y RESPONSABILIDADES	Asignado a
Responsable de la Seguridad	Determina las decisiones para satisfacer los requisitos de seguridad de la información de la empresa y de los servicios.	CISO
Responsable de la información	Tomar las decisiones relativas a la información tratada	Service Manager Directores o Responsables de Área
Responsable de los servicios	Garantizar los niveles de servicio, alineados con las necesidades de los clientes, y asegurando alcanzar los niveles de seguridad exigidos por los clientes.	Global Service Manager o IT Manager
Responsable de sistemas	Coordinar la implantación del sistema Mejorar el sistema de forma continua	Director TIC
Dirección	Proporcionar los recursos necesarios. Promover y liderar	Comité de Dirección
Representante de Dirección	Director responsable de Representación del Comité de Dirección	Diretor@ de Área que se designe
Comité de Seguridad	Coordinar la seguridad de la información en la entidad	Comité Operativo de Seguridad de la Información
Responsable de los Sistema Integrado de Gestión (SIG)	Responsable de la gestión integral de los Sistemas de Gestión	Responsable del SIG
Delegado de Protección de Datos (DPD)	Responsable de la gestión de los requisitos de Privacidad de Datos Personales	Legal Manager

Esta definición se completa en las fichas de competencias y en los documentos de los Sistemas Integrados de Gestión. Las funciones y responsabilidades se han realizado siguiendo los procedimientos internos.

El Comité Operativo del SIG 20/27, es el órgano con mayor responsabilidad dentro del sistema de Gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité. Los miembros del Comité Seguridad, será conformado por las personas designadas con los siguientes roles:

- Representante de Dirección
- Responsable de la información
- Responsable de los Servicios
- Responsable de la Seguridad (el propio comité)

- Responsable de Sistemas
- Responsable de los Sistemas Integrados de Gestión (SIG)
- Delegado de Protección de Datos (DPD)

Los miembros del **comité serán ratificados o sustituidos de forma anual**, por la propia designación de los roles, y comunicados al Comité de Dirección, quien tendrá la potestad de reasignar o cesar cualquiera de los roles. Sin embargo, el Comité Operativo del SIG 20/27 **siempre quedará subordinado al comité de Dirección.**

El **Comité Operativo de la Seguridad de la Información** (Comité Operativo del SIG20/27), es el brazo ejecutor en materia de seguridad de la información, y su función entre otras es asegurar que se ejecutan e implantan las estrategias definidas y las medidas necesarias, también es su responsabilidad la de escalar al Comité del SIG cualquier riesgo o necesidad detectada en materia de Seguridad de la Información.

El CISO, o bien el Representante de Dirección, elevarán cualquier conflicto a nivel de Comité Operativo será elevado por cualquiera de ellos al Comité de Dirección, siendo este último el **máximo responsable ante la resolución de conflictos o interdependencias.**

Está política se complementa con el resto de las políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión. Para más detalle se puede consultar el Procedimiento General de Comité de Gestión y Revisión por la Dirección.

B) ESTRUCTURA DOCUMENTAL

fibratel cuenta con una estructura documental definida, donde se establece una política de seguridad de la información; así como un conjunto de directrices por los cuales se regula Sistema de Gestión de Seguridad de la Información.

A continuación, se detalla el listado de los principales documentos relacionados con dicha estructura

- POL-SI-01.DOC Política de Seguridad de la Información
- PG-AR-01.DOC Metodología Análisis Riesgos
- PG-CI-01.DOC Clasificación e Intercambio de Información
- PG-CC-01.DOC Normativa de control de accesos
- PG-DP-01.DOC Protección de Datos Personales
- PG-EP-01.DOC Evaluación de Proveedores
- PG-FC-01.DOC Formación y Competencia
- PG-IP-01.DOC Seguridad Información para proveedores
- PG-RI-01.DOC Utilización de Recursos de la Información
- PG-RL-01.DOC Requisitos legales
- PG-CA-01.DOC Gestión de Cambios
- PG-SP-01.DOC Servicio posventa, gestión de incidencias y problemas

- PG-SM-01.DOC Seguimiento y medición
- PG-RC-01.DOC Reclamaciones de clientes
- PG-EM-01.DOC Evaluación y Mejora
- PG-RS-01.DOC Comité de Gestión y Revisión del Sistema

Estos documentos quedan regulados en su gestión bajo el Procedimiento General de Gestión de la Documentación (PG-GD-01).

C) GESTIÓN DE REQUISITOS LEGALES

Se dispone de una sistemática para identificar los requisitos legales de manera continua a través de servicios externos contratados y por el medio de una herramienta de gestión de cumplimiento legal. Se hace una evaluación semestral del cumplimiento legal y se registra en la herramienta. Dichos procedimientos lo regulan el Procedimiento de Requisitos Legales (PG-RL-01), y los resultados de las revisiones se registran como informes independientes de revisión en nuestra intranet.

D) GESTIÓN DE RIESGOS

Todos los sistemas de información sujetos a esta Normativa deberán realizar un análisis de riesgos, evaluando los activos según su criticidad, incluyendo sus vulnerabilidades, las amenazas y los riesgos a los que están expuestos. Este análisis se revisa regularmente, tal y como estable el procedimiento interno de Análisis de Riesgo:

- al menos una vez al año;
- cuando cambie la información manejada;
- cuando haya cambio relevante en los servicios prestados;
- cuando ocurra un incidente grave de seguridad;
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité operativo del SIG 20/27, establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados, así como dinamizará la operativa de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal. Los riesgos, los niveles de aceptación de los mismo y los recursos para afrontarlos deberán ser elevados al Comité de Dirección para su aprobación.

Para la realización del análisis de riesgos se tendrán en cuenta la metodología de análisis de riesgos reconocidas internacionalmente, que cuenta con su propio procedimiento.

E) GESTIÓN DEL PERSONAL

Todos los miembros de fibratel tienen la **obligación de conocer y cumplir la Política de Seguridad** de la Información.

Se establecerá un **programa de concienciación continua** para atender a todos los miembros de la fibratel, en particular a los de nueva incorporación. Todos los miembros de las sedes de fibratel atenderán a sesiones, o recibirán comunicados, de concienciación en materia de seguridad de la información a lo largo del año.

fibratel cuenta con un **plan de formación** en el que se pone especial interés en las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

RRHH incluirá funciones de seguridad de la información en las descripciones de los trabajos de los empleados, informará a todo el personal que contrate sus obligaciones con respecto al cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de los usuarios con respecto a esta Política.

De Igual manera, será responsabilidad de RRHH el establecer las sanciones que se aplicarán por incumplimiento de esta Política y en el tratamiento de incidentes de seguridad de la información.

F) PROFESIONALIDAD Y SEGURIDAD DE LOS RECURSOS HUMANOS

Los objetivos de controlar la seguridad del personal son:

- **Reducir los riesgos de error humano**, puesta en marcha de irregularidades, uso indebido de instalaciones y recursos, y manejo no autorizado de la información.
- **Explicar las responsabilidades de seguridad** en la etapa contratación del personal e incluirlas en los acuerdos a firmar y verificar su cumplimiento durante el desempeño de las tareas del empleado.
- Asegúrese de que los **usuarios estén concienciados, tanto de las amenazas y prioridades en materia de seguridad de la información** y estén capacitados para apoyar las Normativas de Seguridad de la Información de la organización en el curso de sus tareas normales.
- **Establecer compromisos de confidencialidad** con todo el personal y usuarios fuera de las instalaciones de procesamiento de información.
- **Implementar los procedimientos y mecanismos** adecuados para fomentar la comunicación de los **incidentes, riesgos y vulnerabilidades de seguridad** que se detecten, con el objetivo de reducir sus consecuencias y evitar que se repitan.

- Profesionalidad:

  - **Determinar la competencia necesaria del personal** para llevar a cabo el trabajo que afecta a la Seguridad de la Información
  - **Asegurar que las personas sean competentes sobre** la base de la educación, capacitación o experiencia adecuadas

- **Demostrar** mediante la información documentada que sea necesaria **la competencia del personal en materia de Seguridad de la Información**

G) AUTORIZACIÓN Y CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

El control del acceso a los sistemas de información tiene por objetivo:

- Evitar el acceso no autorizado a sistemas de información, bases de datos y servicios de información.
- Implementar la seguridad en el acceso de los usuarios a través de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de **fibratel** y otras redes públicas o privadas.
- Revisar los eventos críticos y las actividades llevadas a cabo por los usuarios en los sistemas.
- Concienciar sobre su responsabilidad por el uso de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y ordenadores personales para el trabajo remoto.

Se establece la normativa PG-CC-Normativa de control de accesos, donde se desarrolla toda la normativa interna.

H) PROTECCIÓN DE LAS INSTALACIONES

Los objetivos de esta normativa son:

- Prevenir el acceso no autorizado, daños e interferencias a la sede, instalaciones e información de fibratel.
- Proteger el equipo de procesamiento de información crítico de fibratel, colocándolo en áreas protegidas y protegido por un perímetro de seguridad definido, con las medidas de seguridad y controles de acceso adecuados. Asimismo, contemplar la protección de esta en su traslado y permanecer fuera de las áreas protegidas, por mantenimiento u otros motivos.
- Controlar los factores ambientales que podrían perjudicar el buen funcionamiento del equipo de cómputo que alberga la información de fibratel.
- Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus tareas habituales.
- Proporcionar protección proporcional a los riesgos identificados.

Esta normativa se aplica a todos los recursos físicos relacionados con los sistemas de información de fibratel: instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.

Las medidas de seguridad física y ambiental para la protección de los activos críticos serán definidas por los propietarios de los activos, tal y como se define en la metodología de análisis de riesgos, quienes a su vez serán responsable de asegurar y supervisar a la implantación y aplicación de las mismas. También verificará el cumplimiento de las disposiciones de seguridad física y medioambiental.

Todo el personal de fibratel es responsable del cumplimiento de la política de pantalla limpia y escritorio, para la protección de la información relacionada con el trabajo diario en las oficinas.

I) ADQUISICIÓN DE PRODUCTOS

Los diferentes departamentos establecen las necesidades de tecnología hacia el Departamento de IT. Quién evaluará la seguridad TIC, siguiendo los requisitos de validación que exige el CCN-CERT en materia de equipos homologados. Además, el Dpt. de IT realizará la gestión técnica del ciclo de vida del sistema, 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 serán validados por CISO**.

Las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC, y la compra gestionada por el Dpto. de Compras.

J) SEGURIDAD POR DEFECTO

fibratel considera estratégico que los procesos integren la seguridad de la información como parte de su ciclo de vida. Los sistemas de información y los servicios deben incluir la seguridad por defecto desde su creación hasta su retirada, incluyéndose la seguridad en las decisiones de desarrollo y/o adquisición y en todas las actividades en explotación estableciéndose la seguridad como un proceso integral y transversal.

K) INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

fibratel se compromete a garantizar la integridad de los sistemas mediante un **proceso de gestión de cambios** que permita el control de la actualización de los elementos físicos o lógicos mediante la autorización previa a su instalación en el sistema. Dicha evaluación será llevada a cabo principalmente por la dirección de sistemas que evaluará el impacto en la seguridad del sistema antes de realizar los cambios y controlará de forma documentada aquellos cambios que se evalúen como importantes o con implicaciones en la seguridad de los sistemas.

Mediante revisiones periódicas de seguridad se evaluará el estado de seguridad de los sistemas, con relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos.

L) PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

fibratel establece medidas de protección para la Seguridad de la Información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, dispositivos móviles, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

M) PREVENCIÓN DE SISTEMAS DE INFORMACIÓN INTERCONECTADOS

fibratel establece medidas de protección para la Seguridad de la Información para proteger el perímetro, en particular, si se conecta a redes públicas, especialmente si se utilizan en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público.

En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión electrónicas disponibles para el público.

N) REGISTROS DE ACTIVIDAD.

fibratel registrará las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

O) INCIDENTES DE SEGURIDAD

fibratel cuenta con procedimientos para gestionar los incidentes de seguridad y vulnerabilidades encontradas en los elementos del sistema de información. Estos procedimientos incluyen la detección, la clasificación, el análisis y la solución, así como la comunicación a las partes interesadas. Los objetivos principales de la Gestión de incidentes son los de:

- Garantizar que los servicios de IT vuelvan a tener un desempeño óptimo ante cualquier evento disruptivo.
- Reducir los posibles riesgos e impactos derivados del propio incidente.
- Velar por la integridad de los sistemas en el caso de un incidente de seguridad
- Comunicar el impacto de un incidente tan pronto como se detecte para activar la alarma; y poner en práctica un plan de comunicación empresarial adecuado.

La organización se compromete a informar, sensibilizar y capacitar al personal sobre los incidentes.

P) CONTINUIDAD DE LA ACTIVIDAD

fibratel con el objetivo de garantizar la continuidad de las actividades establece medidas para que los sistemas dispongan de copias de seguridad y establece mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Q) MEJORA CONTINUA DEL PROCESO DE SEGURIDAD

fibratel establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y metodología establecida en su Sistema Integrado de Gestión (SIG), basado en normas internacionales como ISO/IEC 27001:2013, ISO/IEC 20000:2011, Esquema Nacional de Seguridad (ENS), etc.

5. CONTROL DE MODIFICACIONES

Rev. / Edic.	Fecha	Apdo. modificado	Descripción de la modificación
0	Septiembre / 2012	___	Edición Inicial
1	Marzo / 2019	Todo el documento	Se actualiza el nuevo logotipo Se simplifica el documento, eliminando todos los apartados de la política, dejando solo una introducción seguida de las premisas de la política
2	Febrero / 2020	Todo el documento	Se adapta la ISO 27001 y a la misión y visión del Grupo fibratel. Se simplifica para mejor comprensión de todas las partes
3	Mayo/ 2020	Cabecera	Se modifica la codificación de los sistemas en la cabecera del documento
4	Abril 2022	Todo el documento	Adecuación al Esquema Nacional de Seguridad.
5	Marzo 2024	Actualización	Se hace revisión general. Se actualizan roles y gobierno.