FECHA:	01/10/2024	EDICIÓN:	1

Índice

EXPOCOM telecommunication	Política de Seguridad de la Información

FECHA:	01/10/2024	EDICIÓN:	1

1. Objetivos de la organización

La organización tiene como objetivo principal la venta, postventa y mantenimiento de dispositivos de telecomunicaciones y seguridad.

2. Marco regulatorio

Nº	Legislación
1	Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
2	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
3	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
4	Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
5	Real Decreto 1777/2004, de 30 de julio, por el que se aprueba el Reglamento del Impuesto sobre Sociedades
6	Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores
7	Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal
8	Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones
9	Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (Deroga ley 59/2003)
10	Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
11	Directiva (UE) 2022/2555 (NIS2) del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.

3. Responsabilidades y organización de la seguridad de la información

a. Comité STIC (Seguridad TIC)

Las actividades TIC se coordinan por medio del comité STIC. Este comité está compuesto de personal técnico de los diferentes departamentos para la toma de las decisiones.

El comité de Seguridad TIC estará formado por:

CARGO	NOMBRE
Dirección (*)	Eduard Oltra
Responsable de la Información (*)	Eduard Oltra
Responsable del Servicio (*)	Eduard Oltra
Responsable de la Seguridad (**)	Rafael Navarro
Responsable del Sistema (**)	Eduard Oltra

(*) Estas funciones pueden recaer en la misma persona.
(**) El Responsable de la Seguridad será distinto del Responsable del Sistema.

El Director preside el Comité STIC y es el principal responsable de:

- Usar el voto de calidad, para acordar las decisiones oportunas, cuando no se produce un acuerdo dentro del equipo.
- Implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información
- Asignar los recursos necesarios y aprobar el presupuesto
- Asignar y comunicar los roles, concretamente de los propietarios de los riesgos de seguridad de la información y los riesgos de calidad.

Otros de los roles de gran relevancia dentro del Sistema de Gestión de Seguridad de la Información son:

CARGO	NOMBRE	RESPONSABILIDADES
Administrador sistemas TIC	David Ruiz (PuntDoc)	Responsable de la implementación, configuración y mantenimiento de los servicios de seguridad relacionados con las TIC.
Operadores sistemas TIC	David Ruiz (PuntDoc)	Equipo de continuidad. Son los responsables de la operación diaria de los servicios de seguridad relacionados con las TIC.

b. Funciones y responsabilidades

Comité de STIC

- Establecer, revisar y aprobar el alcance del Sistema de Gestión de Seguridad de la Información, además de la política de seguridad de la información.
- Asegurar que las políticas de seguridad de la información, los procesos, procedimientos y leyes y regulaciones reflejan los requisitos del negocio y están alineados con los requerimientos de las partes interesadas, tanto internas como externas.
- Además de establecer, revisar y aprobar los objetivos del SGSI y comprobar si están eficazmente implementado y mantenido.
- Monitorizar los cambios importantes en la seguridad de la información.
- Revisar los incidentes de seguridad de la información y acordar las acciones necesarias, si procede.
- Aprobar las iniciativas más importantes para mantener la seguridad de la información y el nivel de calidad establecido.
- Realizar Revisiones por la Dirección a intervalos planificados.
- Asegurar que el personal está concienciado de la importancia de cumplir los requisitos de seguridad, los requisitos legales y regulatorios, las obligaciones contractuales, los requisitos de calidad, los niveles de calidad y los acuerdos de nivel de servicio.

Responsable de la Información

- Tiene la facultad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos
- Determina los niveles de seguridad de la información.

Responsable del Servicio

- Tiene la facultad de establecer los requisitos, en materia de seguridad, de los servicios prestados.
- Determina los niveles de seguridad del servicio.

FECHA:	01/10/2024	EDICIÓN:	1

Responsable de Seguridad

Responsable de la definición, coordinación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo a los objetivos.
Las funciones del Responsable de Seguridad de la Información son:

- Coordinar y controlar las medidas de seguridad de la información y de protección de datos.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
  - La estrategia de seguridad de la información definida por el Comité de Seguridad.
  - Las normas y procedimientos contenidos en la Política de Seguridad de la Información.
  - Supervisar los incidentes de seguridad.
  - Difundir entre el personal de la empresa las normas y procedimientos contenidos en el Sistema de Gestión de Seguridad de la Información, así como las funciones y obligaciones en materia de seguridad de la información.
  - Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables en materia de protección de datos personales y de seguridad de la información.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de la empresa.
- Aprobar la categorización del sistema.

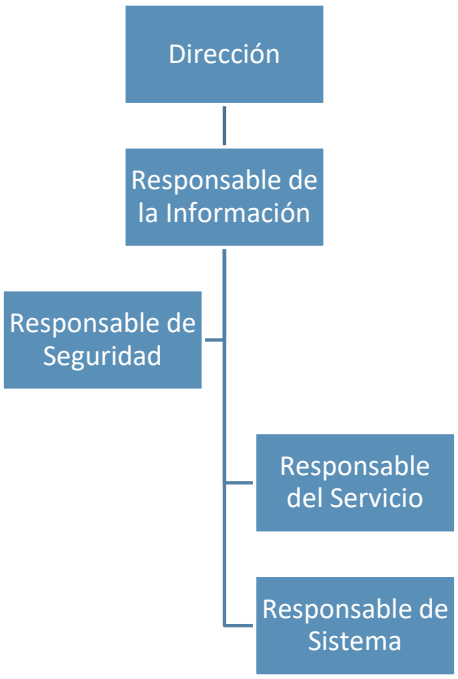
Responsable de Sistema

El responsable del sistema, por sí o a través de recursos propios o contratados, se encarga de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

El responsable del sistema adoptará las medidas correctoras necesarias derivadas de los informes de auditoría de la seguridad una vez hayan sido analizados por el Responsable de Seguridad y éste haya presentado sus conclusiones al Responsable del Sistema.

El Responsable del Sistema será distinto del Responsable de Seguridad, no existiendo ninguna clase de dependencia jerárquica entre ambos perfiles.

Dependencias de los roles



4. Designación y renovación de los roles de seguridad

Dirección es la máxima responsable de designar los diferentes roles de seguridad. Esta designación se realizará formalmente con la aprobación de la presente política. El original firmado por Dirección será archiva por el Responsable de Seguridad.
El organigrama establecido reflejará estas designaciones.

La designación se renovará en los casos siguientes:

- Baja a medio o largo plazo del personal designado.
- Personal causa baja indefinida de la empresa
- Falta de competencias
- Criterio de Dirección atendiendo a razones de gestión de RRHH y/o estratégicas.

5. Gestión del riesgo

Los activos sujetos a esta Política de Seguridad deberán ser sometidos a un análisis del riesgo, evaluando posibles amenazas y a que riesgos pueden estar expuestos. Este análisis se repetirá regularmente, al menos una vez al año o se reporten vulnerabilidades graves.

6. Recursos

Para la aplicación efectiva de la Política de Seguridad de la Información en la compañía, la Dirección dotará de los recursos necesarios para su buen desarrollo, tanto en las actividades de implantación como de operación y mejora de dicha política y de los controles de seguridad de la información que en cada momento se establezcan.

La protección de los activos de Información de la empresa y de sus clientes es vital para el correcto alineamiento con los objetivos de negocio. Con este fin, se ha establecido un Sistema de Gestión de Seguridad de la Información que implementa todos los procesos y controles necesarios para establecer la forma en que se protegen los activos de Información.

El Sistema de Gestión de Seguridad de la Información se actualiza y mejora continuamente para satisfacer las necesidades del negocio, de los clientes y de las partes interesadas, se establecen nuevos objetivos de forma periódica y se evalúan regularmente los procesos de negocio.

7. Datos de carácter personal

EXPOCOM trata datos de carácter personal. El documento RGPD EXPOCOM actualizado, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de EXPOCOM se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento.

8. Aprobación y revisión

El Sistema de Gestión de Seguridad de la Información se revisa anualmente o cuando se produce un cambio significativo en el negocio.
El Sistema de Gestión de Seguridad de la Información implementado, operado y mejorado, en base al Esquema Nacional de Seguridad (CCN) en la organización garantiza:

- Que establece y mantiene el contexto, determina las necesidades y expectativas de las partes interesadas
- Que los roles, responsabilidades y autoridades están asignados
- Que se establecen objetivos para el Sistema de Gestión de Seguridad de la Información, alineados con los objetivos estratégicos
- Que se establecen indicadores para medir el rendimiento de los controles y, se analizan y evalúan periódicamente

- Que se establece un criterio de riesgo para la identificación, el análisis, la evaluación y el tratamiento de riesgos
- Que todo el personal recibe formación y concienciación respecto a la seguridad de la información y las políticas de seguridad de la información (control de acceso físico y lógico, seguridad física, Ante código malicioso, copias de seguridad, clasificación de la información, tratamiento de la información, continuidad…) implementadas en la empresa
- Que el Sistema de Gestión se opera en base a la información documentada aprobada, políticas, procesos, procedimientos, …
- Que se verifica el cumplimiento a través de auditorías externas, seguimientos de los objetivos e indicadores y de las revisiones por la dirección.
- Que se corrigen las no conformidades y quejas, mediante la implementación de acciones correctivas, y la evaluación del resultado de las mismas.
- Que se realiza la mejora continua sobre el Sistema de Gestión de Seguridad de la Información.

Los principios de la Política de Seguridad de la Información son asumidos e impulsados por la Dirección, quien proporciona los medios necesarios y dota a los empleados de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento a través de una Política Estratégica de Seguridad de la Información.

00-2 Política Estratégica de la Seguridad de la Información

EXPOCOM, S.A., tiene implantado un Sistema de Gestión de la Seguridad de la Información cuyo alcance es:

Los sistemas de información que dan soporte al servicio de Post-venta y mantenimiento de productos de telecomunicaciones, con referencia a la Declaración de Aplicabilidad del Sistema y a la Categorización del Sistema vigentes.

Dimensión	Disponibilidad	Autenticidad	Confidencialidad	Integridad	Trazabilidad	CATEGORÍA
Nivel asignado	Medio	Medio	Medio	Medio	Medio	MEDIA

Como principios a tener en cuenta:

- La preservación de la **confidencialidad** de la información y evitando su divulgación y el acceso por personas no autorizadas.
- El mantenimiento de la **integridad** de la información procurando su exactitud y evitando su deterioro.
- Aseguramiento de la **disponibilidad** de la información en todos los soportes y siempre que sea necesaria.
- La **trazabilidad** de los registros.
- Y la **autenticidad** de los datos.

FECHA:	01/10/2024	EDICIÓN:	1

La seguridad de la información debe de ser flexible, eficaz y dar soporte al modelo de negocio de la compañía, por ello, la Dirección se compromete a desarrollar, implantar, mantener y mejorar continuamente su Sistema de Gestión de Seguridad de la Información con el objetivo de la mejora continua en la forma en que prestamos nuestros servicios y en la forma en que tratamos la información de nuestros clientes.

Por ello, establecemos las siguientes directrices:

- Establecimiento de objetivos con relación a la seguridad de la información.
- Cumplimiento de los requisitos legales y otros requisitos que podamos subscribir.
- Realizar actividades de formación y concienciación en materia de los procesos de seguridad de la información para todo el personal.
- Desarrollo del análisis, gestión y tratamiento del riesgo sobre los activos de información.
- Establecer todas las acciones requeridas para mitigar o eliminar los riesgos detectados.
- Establecer la responsabilidad de los empleados en relación el reporte de las incidencias de seguridad.
- Preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política.
- Cumplimiento por parte de todo el personal de las políticas y procedimientos del Sistema de Gestión de la Seguridad de la Información.

La Dirección asigna responsabilidades y autoridad al Responsable de Seguridad sobre el mantenimiento de esta política, prestando consejo y guía para su implementación y correcciones ante desviaciones en su cumplimiento, así como en la gestión de las políticas, procedimiento y actividades del SGSI.

La presente política de seguridad de la información se hallará siempre alineada con las políticas generales de la compañía.

9. Desarrollo de la política de seguridad de la información

8.1 Consideraciones generales:

Esta política de seguridad de la información complementa las políticas de seguridad de la información de la empresa en diferentes materias de seguridad en la intranet.

Esta política se desarrollará utilizando políticas de seguridad que aborden aspectos específicos. Estará a disposición de todos los miembros de la organización que necesiten conocerlo, en particular de quienes utilicen, operen o gestionen sistemas de información y comunicaciones.

La empresa procesa datos personales. El acceso a determinados documentos de seguridad sólo se concederá a personas autorizadas y responsables. Todos los sistemas de información de la empresa cumplirán con los niveles de seguridad exigidos por la normativa para la naturaleza y finalidad de los datos personales incluidos en el anterior documento de seguridad.

Las normas de seguridad estarán disponibles en la intranet.

10. Categoría de seguridad

La categoría de seguridad requerido es **MEDIO**, dentro del marco establecido en el artículo 40 y los criterios generales prescritos en el Anexo I del ENS. Algunos de los criterios que determinan dicho nivel es que el proceso está totalmente definido. El catálogo de procesos se mantiene actualizado y garantizan la consistencia de las actuaciones entre las diferentes partes de la organización.

Además de haber normativa establecida y procedimientos para poder reaccionar ante cualquier incidente de seguridad y se actualiza y mantiene de forma regular. Así mismo, existe una alta coordinación entre departamentos y los proyectos llevados a cabos.

El comité STIC contempla la posibilidad de modificar el nivel de seguridad requerido.

Los principios de la Política de Seguridad de la Información son asumidos e impulsados por la Dirección, quien proporciona los medios necesarios y dota a los empleados de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento a través de la presente Política de Seguridad de la Información.

11. Requisitos mínimos de seguridad

Esta política de seguridad se ha establecido de acuerdo con los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad:

- Estructura de Seguridad: Se establecerá un comité de seguridad que supervisará la implementación y el cumplimiento de la política de seguridad.
- Roles y Responsabilidades: Definir roles y responsabilidades claras para todos los empleados en relación con la seguridad de la información.
- Documentación: Mantener documentación actualizada sobre políticas, procedimientos y estándares de seguridad.

b) Análisis y gestión de los riesgos:

- Evaluación de Riesgos: Realizar evaluaciones periódicas de riesgos para identificar, evaluar y mitigar los riesgos asociados con los activos de información.
- Mitigación de Riesgos: Implementar controles adecuados para gestionar los riesgos identificados.
- Revisión Continua: Revisar y actualizar regularmente el análisis de riesgos y las medidas de mitigación.

c) Gestión de personal:

- Selección de Personal: Realizar verificaciones de antecedentes y evaluaciones de seguridad para todos los empleados.
- Capacitación: Proveer capacitación continua en seguridad de la información para asegurar que todo el personal esté al tanto de las políticas y procedimientos de seguridad.
- Conciencia de Seguridad: Fomentar una cultura de seguridad a través de programas de concienciación y formación.

d) Profesionalidad:

- Código de Conducta: Promover un comportamiento profesional y ético en todas las actividades relacionadas con la seguridad de la información.
- Desarrollo Profesional: Fomentar la mejora continua y la actualización de las habilidades y conocimientos del personal de seguridad.

e) Autorización y control de los accesos:

- Control de Acceso: Implementar un sistema de control de acceso basado en roles para asegurar que los usuarios solo tengan acceso a los datos y sistemas necesarios para sus funciones.
- Auditorías de Acceso: Realizar auditorías regulares de los permisos de acceso y revocar los accesos no necesarios.
- Autenticación: Utilizar mecanismos de autenticación fuertes y multifactoriales.

f) Protección de las instalaciones:

- Seguridad Física: Implementar medidas de seguridad física, como controles de acceso, cámaras de vigilancia y sistemas de alarma para proteger las instalaciones donde se manejan activos de información.
- Acceso Restringido: Limitar el acceso a áreas críticas solo a personal autorizado.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad:

- Criterios de Seguridad: Establecer criterios de seguridad para la adquisición de productos y servicios.
- Evaluación de Proveedores: Realizar evaluaciones de seguridad a proveedores y contratar solo aquellos que cumplan con los estándares de seguridad requeridos.

h) Mínimo privilegio:

- Principio de Mínimo Privilegio: Aplicar el principio de mínimo privilegio, asegurando que los usuarios y sistemas solo tengan los permisos mínimos necesarios para desempeñar sus funciones.
- Revisión de Privilegios: Revisar periódicamente los privilegios de acceso y ajustarlos según sea necesario.

i) Integridad y actualización del sistema:

- Integridad de Sistemas: Implementar procedimientos para garantizar la integridad de los sistemas y datos.
- Actualización de Software: Realizar actualizaciones regulares de software y parches de seguridad para proteger contra vulnerabilidades conocidas.

j) Protección de la información almacenada y en tránsito:

- Cifrado: Utilizar técnicas de cifrado para proteger la información tanto en almacenamiento como en tránsito.
- Controles de Acceso: Implementar mecanismos de autenticación y control de acceso para asegurar que solo los usuarios autorizados puedan acceder a la información.

k) Prevención ante otros sistemas de información interconectados:

- Control de Conexiones: Implementar controles de seguridad para gestionar y monitorizar las conexiones con otros sistemas de información.
- Evaluación de Riesgos: Evaluar y mitigar los riesgos asociados con la interconexión de sistemas.

l) Registro de la actividad y detección de código dañino:

- Registro de Actividades: Mantener registros detallados de todas las actividades del sistema y realizar auditorías regulares.
- Detección de Malware: Implementar herramientas de detección y prevención de código dañino (malware).

m) Incidentes de Seguridad:

- Gestión de Incidentes: Establecer procedimientos para la gestión de incidentes de seguridad, incluyendo la identificación, análisis, respuesta y reporte de incidentes.
- Simulacros de Incidentes: Realizar ejercicios y simulacros periódicos para asegurar la preparación ante incidentes.

n) Continuidad de la actividad:

- Planes de Continuidad: Desarrollar y mantener planes de continuidad del negocio y recuperación ante desastres.
- Pruebas Regulares: Realizar pruebas regulares de estos planes para asegurar su efectividad.

ñ) Mejora continua del proceso de seguridad:

- Ciclo de Mejora Continua: Implementar un ciclo de mejora continua (Planificar-Hacer-Verificar-Actuar) para evaluar y mejorar continuamente las políticas y procedimientos de seguridad.

- Revisiones Periódicas: Realizar revisiones periódicas de la Política de Seguridad de la Información para asegurar que se mantenga actualizada y relevante.

12. Aprobación de la política

Eduard Oltra
Dirección
EXPOCOM, S.A.

A fecha 01 de octubre de 2024.