Política de Seguridad de la Información

Grupo MASORANGE

Elaborado por:	Revisado por:	Aprobado por:
Ciberseguridad	Comisión de Auditoría y Riesgos	Consejo de Administración

Lista de Distribución
- Documento público

Control de versiones

Versión	Fecha de aprobación	Cambio respecto a la última versión
1.0	18/10/2024	*Versión inicial*

Referencia a otros documentos

Doc. Ref.	Documento
PSG-01	Política de Seguridad Global
PR-53-01	Política de Continuidad de Negocio
POL-05	Política de Control Interno
POL-06	Política de Control y Gestión de Riesgos
POL-07	Política de Privacidad

Índice

1. Resumen ejecutivo

El Consejo de Administración de MASORANGE, S.L., es el competente para determinar las políticas y la estrategia de la Sociedad y de las empresas que conforman su grupo de sociedades ("Grupo"). En ese sentido, decide implementar una Política de Seguridad de la Información conforme a las principales legislaciones aplicables y basada en las mejores prácticas, integrada en la actividad diaria y en la que deben participar todas las áreas de la compañía.

2. Propósito

La información, los servicios y los procesos y sistemas gestionados por el Grupo son activos fundamentales que constituyen un elemento estratégico y necesario para el desarrollo de sus actividades y, como tal, es necesaria su protección y salvaguarda.

La presente política se basa tanto en las recomendaciones del estándar internacional ISO/IEC 27001 y las buenas prácticas establecidas por la norma UNE-ISO/IEC 27002, como en el compromiso de cumplimiento de los principios básicos y requerimientos mínimos del Real Decreto que regula el Esquema Nacional de Seguridad (ENS). Está alineada con la legislación vigente en materia de protección de datos personales, seguridad de las redes y sistemas de información, sociedad de la información, comercio electrónico, ciberseguridad y telecomunicaciones. Todo ello con el fin de mantener la seguridad e integridad de la información, estableciendo en cada punto los controles y medidas adecuadas para preservar su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad

Todas las áreas, departamentos y equipos que forman parte del Grupo deben estar preparados para la:

- **Prevención**: se deben implantar las medidas y controles de seguridad identificados a través de una evaluación de amenazas y riesgos, estos controles deben estar claramente definidos y documentados. Para garantizar el cumplimento de la política los departamentos deben autorizar los sistemas antes de entrar en producción, evaluar regularmente la seguridad y solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.
- **Detección**: es imprescindible una monitorización continua de los sistemas para detectar posibles anomalías en los niveles de prestación de los servicios y actuar en consecuencia. Se establecerán mecanismos de detección, análisis y reporte hacia los responsables de manera regular y cuando se produzca una desviación significativa de los parámetros preestablecidos como normales.
- **Respuesta**: todas las áreas, departamentos y equipos del Grupo deben establecer mecanismos para responder eficazmente a los incidentes de seguridad, estableciendo puntos de contacto y protocolos para el intercambio de información relacionada con el incidente.
- **Recuperación**: para garantizar la disponibilidad de los servicios críticos se deben desarrollar planes de continuidad de los sistemas de información como parte del plan general de continuidad del negocio y actividades de recuperación.

Para el desarrollo de la presente política de seguridad de la información se han tomado en consideración los requisitos derivados de:

- El plan estratégico del Grupo.
- El contexto de la organización.
- Los principios generales recogidos en este mismo documento.
- El marco legal, normativo y regulatorio bajo el que opera el Grupo.
- El entorno actual y previsto de riesgos y amenazas de seguridad de la información.

Esta Política de Seguridad de la Información está alineada con la Política de Seguridad Global que define los principios, objetivos y principales responsabilidades de seguridad en el Grupo.

3. Principios

En el desarrollo de sus actividades el Grupo asume y se compromete con el cumplimiento de los siguientes principios básicos:

- Seguridad como proceso integral
- Gestión de la seguridad basada en los riesgos:
- Prevención, detección, respuesta y conservación
- Existencia de líneas de defensa
- Vigilancia continua
- Reevaluación periódica
- Diferenciación de responsabilidades

4. Misión y objetivos de la organización

El propósito de la organización es (re)conectar a las personas poniendo la tecnología al servicio de la mejor experiencia de cliente y, para ello, la Política de Seguridad de la Información establece los siguientes objetivos:

- Garantizar la protección de los activos en base a su criticidad para el negocio, incluyendo elementos técnicos, humanos, materiales y organizativos del Grupo en relación con la información.
- Establecer las pautas que se deben cumplir para la protección y gestión segura de la información de manera integrada y coordinada con los requerimientos propios del negocio, las leyes que en su caso apliquen y la normativa interna de la compañía, basada en estándares reconocidos internacionalmente.
- Implementar mecanismos de autorización y control de acceso a la información en base a los principios de mínimo privilegio y necesidad de conocer.
- Implementar medidas de protección de la información eficaces y eficientes mediante un enfoque basado en gestión de riesgos y en el análisis de coste/beneficio.

- Definir roles y responsabilidades en materia de seguridad de la información.
- Fomentar la cultura de la seguridad de la información en todos los niveles de la organización.
- Responder de manera rápida y eficaz ante posibles incidentes de seguridad, fomentando la resiliencia y mejorando la capacidad de continuidad de negocio.
- Asegurar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información a lo largo de todo su ciclo de vida.
- Adoptar una estrategia a largo plazo de cara a garantizar que la seguridad forma parte de un proceso de mejora continua.

5. Sistema de Gestión de Seguridad de la Información

El Grupo ha definido un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la mejora continua, con el fin de garantizar un enfoque sistemático y coherente de la seguridad de la información, controlar la aplicación de esta política, y dar cumplimiento a la legislación aplicable.

La presente Política establece los principios, requerimientos básicos y el marco de seguridad que sirven de base y rigen una serie de políticas temáticas, normativas y procedimientos técnicos que conforman el Marco Normativo de Seguridad de la Información (MNSI).

6. Alcance

La Política de Seguridad de la Información:

- Aplica a todas las entidades y actividades del Grupo, abarcando todas sus ubicaciones y emplazamientos.
- Es de obligado cumplimiento para todos los empleados, tanto en sus relaciones internas como con terceras entidades, para colaboradores y prestadores de servicios del Grupo, así como para cualquier otra persona que tenga acceso a los activos de información, ya sea de forma física o lógica.
- Incluye todos los sistemas y soportes de información del Grupo, así como la red de telecomunicaciones

7. Compromiso de la Dirección

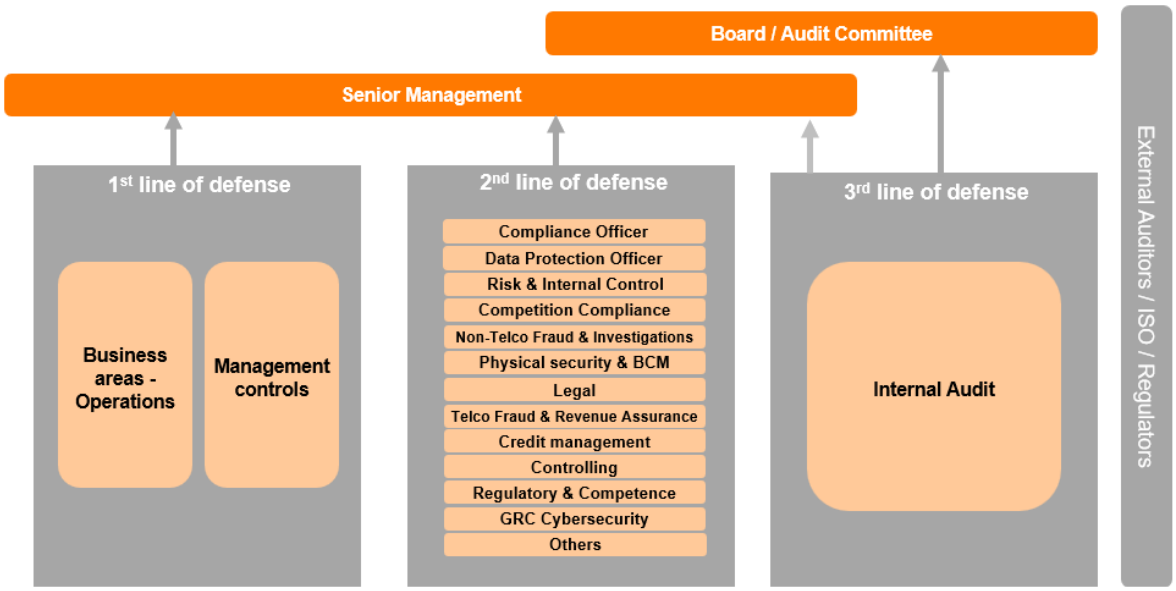
La Dirección del Grupo, consciente de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos de negocio, se compromete a:

- Cumplir y hacer cumplir los principios de la Política de Seguridad de la Información en las áreas corporativas.

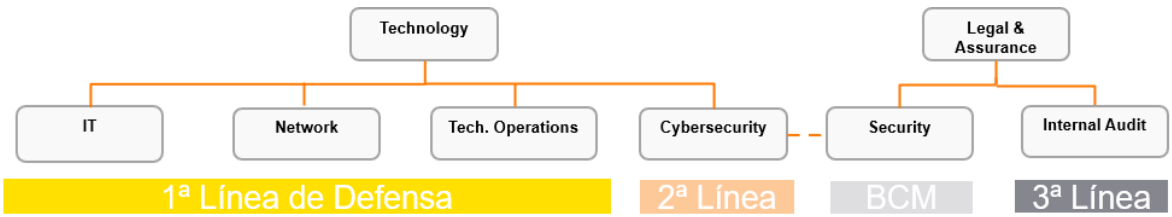
- Facilitar los recursos adecuados para asegurar el establecimiento de la Política, alcanzando así los objetivos de seguridad de la información definidos en ella y satisfaciendo los requisitos de seguridad recogidos en el MNSI.
- Promover la adecuada definición y asignación de roles y responsabilidades en el ámbito de seguridad de la información en el Grupo.
- Impulsar la divulgación y el conocimiento, así como exigir el cumplimiento de la política de seguridad de la información entre las partes interesadas del Grupo.
- Promover la mejora continua en el ámbito de la seguridad de la información en el Grupo, extendiéndola a los procesos corporativos.

8. Organización y responsabilidades

Tal y como se estipula en la Política de Control Interno del Grupo, MASORANGE sigue el modelo de aseguramiento de las 3 líneas de defensa (IIA: Institute of Internal Auditors):



De forma específica para seguridad de la información se sigue el siguiente esquema de líneas de defensa:



En la gestión de la Seguridad de la Información en MASORANGE, se definen los siguientes roles:

Consejo de Administración / Comisión de Auditoría y Riesgos

La determinación de la Política de Seguridad de la Información es responsabilidad del Consejo de Administración del Grupo como facultad indelegable.

Dirección

La dirección debe asumir y controlar los ciber-riesgos necesarios para implementar su estrategia y realizar sus actividades. La dirección es responsable de identificar, gestionar y controlar los ciber-riesgos para sí misma y para todos sus grupos de interés, ya sean internos o externos. Debe velar por la correcta aplicación en su ámbito de la Política de Seguridad de la Información establecida por MASORANGE y de una cultura corporativa centrada en la seguridad.

Función de Seguridad Global

Lidera y coordina las acciones de seguridad de MASORANGE. Desde un enfoque global y transversal, se asegura de la coherencia de las diferentes iniciativas y el control de los riesgos de seguridad en la compañía, relacionados con los dominios de Seguridad de la Información, Seguridad Física, Seguridad de las Personas y Seguridad Ambiental.

Función de Ciberseguridad

En MASORANGE la función de Ciberseguridad involucra en la gestión de ciber-riesgos a diferentes áreas de la organización, de forma coordinada y bajo supervisión de los órganos de gobierno de MASORANGE.

Sus principales funciones son las siguientes:

- Diseñar, mantener actualizado y supervisar un plan director de ciberseguridad para todo el Grupo.
- Definir y velar por el gobierno de la ciberseguridad en el Grupo, estableciendo los modelos de relación y responsabilidades entre líneas de defensa, áreas de negocio y servicios de ciberseguridad. Definir el MNSI, incluyendo las normativas, procedimientos, estándares y directrices asociadas.
- Identificar y evaluar los riesgos existentes en el Grupo en materia de ciberseguridad, así como los controles y medidas mitigadoras existentes, para determinar el riesgo residual, definir el Plan de Tratamiento de Riesgos y coordinar dicho plan.
- Implantar los estándares de referencia en el ámbito de la Seguridad de la información y del Sistema de Gestión de Seguridad de la Información (ISO, ENS, PCI-DSS, etc).
- Apoyar a los Business Owners en el desarrollo de sus funciones

Áreas de negocio (Business Owner)

Son los responsables del adecuado funcionamiento de los procesos corporativos, así como los propietarios de la información que se emplea. Por tanto, son los encargados de asegurar que se aplican las medidas adecuadas para garantizar la seguridad de la información en todo el ciclo de vida del proceso.

Órganos de gobierno

- **Comisión de Auditoría y Riesgos**: en su función asesora e informativa, brinda asistencia al Consejo de Administración con respecto a su supervisión del cumplimiento de las políticas y procedimientos de gestión de Seguridad de la Información en MASORANGE.
- **Comité de Seguridad Global:** es el órgano de máximo nivel para el gobierno de la seguridad corporativa. Está constituido por todos los interlocutores designados por cada una de las áreas de MASORANGE con impacto en la seguridad de la organización, y con la principal representación de la dirección de cada uno de los dominios de la seguridad (Seguridad de la Información, Seguridad Física, Seguridad de las Personas y Seguridad Ambiental).
- **Comité de Ciberseguridad**: es el órgano responsable de la toma de decisiones con impacto en materia de seguridad de la información, así como de monitorizar el cumplimiento de la legislación en este ámbito por parte del Grupo. Su función es coordinar las políticas y actuaciones de las distintas áreas involucradas en la gestión de la Seguridad de la Información, así como reuniones de carácter informativo y de seguimiento de la evolución de los principales ciber-riesgos, sus controles, planes de acción e indicadores, dotando de medios y capacidades para la consecución de dichos objetivos.

MASORANGE ha establecido y documentado, dentro del MNSI, las funciones y responsabilidades en materia de seguridad de la información definiendo en mayor detalle los diferentes roles de seguridad designados, sus funciones y el proceso de designación y renovación.

9. Legislación aplicable

El cumplimiento de la legislación que sea de aplicabilidad en materia de Seguridad de la Información se considera fundamental dentro del Grupo. Se identificará y mantendrá actualizada la relación de requisitos legales y normativos aplicados, analizando el ámbito de aplicación y lanzando las acciones necesarias para asegurar un debido cumplimiento.

Esta relación se puede encontrar en el documento de legislación aplicable incluido en el MNSI.

10. Datos de carácter personal

El Grupo considera prioritario el cumplimiento íntegro de los requerimientos establecidos en la legislación aplicable en materia de protección de datos, y en especial, en lo dispuesto en el Reglamento UE 2016/679, 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 (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), en consonancia con los valores y la cultura corporativa de la organización.

La citada normativa define como uno de los principios del tratamiento de datos personales la adopción de las medidas técnicas y organizativas apropiadas, a efectos de garantizar la

protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales. Siendo por tanto uno de los objetivos de la seguridad de la información garantizar la protección de los datos de carácter personal. El Grupo dispone de un Marco Normativo basado en materia de protección de datos que desarrolla el cumplimiento de dicho objetivo, así como un conjunto de tareas, procesos, reglas y responsabilidades, es decir, un sistema de gestión, para que sea llevado a cabo.

11. Resolución de conflictos

El Comité de Ciberseguridad, cuyos integrantes y responsabilidades se detallan en la documentación del MNSI, como máximo órgano de ciberseguridad, será el responsable de resolver cualquier conflicto de intereses y responsabilidades que puedan surgir en la interpretación de lo descrito en la política y en el resto de los documentos del SGSI y del MNSI.

12. Responsabilidades

Es responsabilidad de todo el personal del Grupo cumplir con la presente Política de Seguridad de la Información. Asimismo, deben asegurarse de tener acceso, conocer y aplicar las versiones vigentes de la presente norma.

Cualquier situación en la que el cumplimiento de la presente política no sea posible, se considerará una excepción, y se manejará como tal por el área de Ciberseguridad.

Los responsables de la elaboración de los documentos son los responsables de realizar la comunicación de la disponibilidad de dicha documentación en la organización y revisar su contenido como mínimo anualmente.

13. Revisión y supervisión

La presente Política se aprueba por el Consejo de Administración y entrará en vigor desde el día de su aprobación.

La aplicación de esta Política estará sujeta a las modificaciones que, según la legislación vigente en cada momento o la interpretación de la propia Sociedad y estime procedente incluir.

El Consejo de Administración evaluará periódicamente la eficacia de esta Política y adoptará las medidas adecuadas para solventar sus deficiencias, realizando las modificaciones oportunas.

14. Glosario de términos

A continuación, se describen los términos y acrónimos empleados en el documento, por orden alfabético:

- **ENS**. Esquema Nacional de Seguridad.
- **LOPDGDD**. Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.
- **MNSI**. Marco Normativo de Seguridad de la Información.
- **RD**. Real Decreto
- **RGPD**. Reglamento General de Protección de Datos.
- **SGSI**. Sistemas de Gestión de la Seguridad de la Información.
- **UE.** Unión Europea.