



Ref: DSEG.SG.POL.05.02
v.4.0

Fecha Efectiva
05/02/2024

Propietario
SEGURIDAD

Política

Política de Seguridad de la Información

una vez impreso, puede estar obsoleto, asegúrese de utilizar la versión en vigor

Elaborado por:

CISO
Orange Espagne S.A.U.

Revisado por

Comité de Seguridad
Orange Espagne S.A.U.

Aprobado por

CEO
Orange Espagne S.A.U.

Lista de Distribución

- Orange Espagne S.A.U
- Filiales consolidadas de Orange Espagne S.A.U
- Partes interesadas de Orange Espagne S.A.U

Política de Seguridad de la Información

tipología	Política	referencia	DSEG.SG.POL.05.02	revisión	4.0
nº revisión	fecha	modificaciones respecto de la revisión anterior			
1.0	20/11/2017	Versión inicial			
2.0	20/11/2017	Adaptación formato normalizado. Sin cambio de texto.			
3.0	30/09/2019	Adaptación formato normalizado. Adecuación al Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS).			
3.1	04/11/2019	Por hallazgo en la Auditoría de certificación de la conformidad respecto al ENS, extracción de la legislación aplicable a un documento externo, modificando el apartado actual. Adecuación del apartado relativo a datos de carácter personal por el equipo del DPO.			
4.0	05/02/2024	Adecuación a la nueva versión de la Política de Seguridad Global y actualización general del documento			

una vez impreso puede estar obsoleto, asegúrese de utilizar la versión en vigor

Índice

Prólogo	4
1 Propósito	5
2 Alcance	5
3 Aspectos generales	6
4 Compromiso de la Dirección	6
5 Objetivos.....	6
6 Roles y responsabilidades.....	7
7 Datos de carácter personal	8
8 Legislación aplicable.....	8
9 Terceras partes	9
10 Monitorización de la Seguridad de la Información.....	9
11 Cumplimiento	9
12 Consideraciones adicionales	10
12.1 Documentación relacionada.....	10
12.2 Glosario	10

Prólogo

En un mundo cada vez más conectado y dependiente de la tecnología, la seguridad de la información se ha convertido en un aspecto fundamental para garantizar la confianza y protección de nuestros clientes. En esta era digital, donde la información fluye constantemente a través de redes y sistemas de información, es crucial que Orange Espagne S.A.U. (en adelante **Orange**) establezca políticas y medidas de seguridad sólidas para garantizar su confidencialidad, disponibilidad, integridad, trazabilidad y autenticación.

La presente Política de Seguridad de la Información, ha sido diseñada para establecer un marco de referencia claro y coherente que guíe nuestras acciones en la protección de los activos de **Orange**, los cuales engloba desde la información clasificada hasta las personas, instalaciones, sistemas y tecnología sobre la que se soporta y procesa dicha información. A través de esta política, buscamos salvaguardar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de nuestros activos, así como prevenir y mitigar los riesgos asociados a posibles amenazas tanto internas como externas.

La implementación de esta política no solo es responsabilidad de la alta dirección, sino que involucra a todos los empleados de **Orange**. Cada uno de nosotros tiene un papel fundamental que desempeñar en la protección de la información, ya sea a través de la adopción de buenas prácticas de seguridad, la participación en programas de formación y concienciación de seguridad o la notificación de posibles incidentes de seguridad.

La seguridad de la información es un proceso continuo y en constante evolución. Por lo tanto, esta política se revisará y actualizará regularmente para adaptarse a los cambios tecnológicos, legales y organizativos que puedan surgir. Es fundamental que todos estemos comprometidos con su cumplimiento y mejora continua.

La presente **Política de Seguridad de la Información** entra en vigor a partir del día 05 de febrero de 2024, derogando, por tanto, la anteriormente vigente. Esta **Política de Seguridad de la Información** es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva **Política de Seguridad de la Información**.

Agradezco a todos los miembros de nuestra organización por su compromiso con la seguridad de la información y su contribución para hacer de nuestra empresa un entorno confiable y seguro. Juntos, podemos proteger y preservar la confianza de nuestros clientes y garantizar el éxito a largo plazo de nuestra organización.

Madrid, 5 de febrero de 2024
Ludovic Alain Pech
CEO de Orange Espagne S.A.U.

1 Propósito

La presente **Política de Seguridad de la Información** tiene por objeto el desarrollo de los criterios de la Política de Seguridad Global en materia de seguridad de la información, y constituye el marco de referencia para Orange y sus filiales en este ámbito, estableciendo las pautas básicas 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 empresa.

Las ideas expresadas en este documento constituyen la base en que se sustenta la adopción de normas, procedimientos operativos, o controles de seguridad homogéneos, que permitan alcanzar los objetivos de seguridad de información de Orange, siempre bajo el cumplimiento de la Política de Seguridad Global y de la legislación y normativa aplicable en materia de seguridad de la información.

Con el fin de garantizar un enfoque sistemático y coherente de la seguridad de la información, Orange ha establecido un marco de gestión de la seguridad de la información. Este marco está compuesto por un Sistema de Gestión de la Seguridad de la Información (en adelante, SGSI), más un Marco Normativo de Seguridad de la Información (en adelante, MNSI).

2 Alcance

Teniendo en cuenta el contexto de la organización, en el cual se determinan cuestiones internas y externas de la organización, así como las partes interesadas que son relevantes y sus requisitos para la seguridad de la información, se establecen los siguientes ámbitos de alcance para la Política de Seguridad de la Información:

Ámbito territorial: El presente documento se aplica en el ámbito de la actividad de Orange y sus filiales consolidadas, abarcando todas sus ubicaciones y emplazamientos.

Ámbito personal: El presente documento es de obligado cumplimiento para todos los empleados, colaboradores y prestadores de servicios de la compañía y sus filiales consolidadas, así como cualquier otra persona que tenga acceso a los activos de información, ya sea de forma física o lógica.

Ámbito material:

- El hardware, considerado como el continente o soporte informático de los sistemas de información.
- El software y la propia información tratada, considerados como el contenido de los sistemas de información.
- Las redes corporativas, intranets, los sistemas de comunicación, y toda la información de cualquier índole y naturaleza que circule por las mismas.

Política de Seguridad de la Información

tipología	Política	referencia	DSEG.SG.POL.05.02	revisión	4.0
-----------	----------	------------	-------------------	----------	-----

- Cualquier otro soporte o medio por el cual sea almacenada o transmitida la información.

En todo el documento, cualquier referencia a “Orange”, “Orange Espagne”, “la Empresa” o “la Compañía”, hará referencia al ámbito descrito.

3 Aspectos generales

Para el desarrollo de la presente Política de Seguridad de la Información se han tomado en consideración: los requisitos derivados de:

- El Plan Estratégico de Orange vigente.
- Los principios generales recogidos en la Política de Seguridad Global.
- El marco legal, normativo y regulatorio bajo el que opera Orange.
- El entorno actual y previsto de riesgos y amenazas de seguridad de la información.
- La vigencia, estructura y formato del presente documento se define según el Estándar de Gestión Documental, así como los procedimientos y responsables de su revisión periódica y mejora continua.

4 Compromiso de la Dirección

La Dirección de Orange, 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 presente Política, alcanzando así los objetivos de seguridad de la información definidos en ella y satisfaciendo los requisitos de seguridad aplicables que se encuentran recogidos en el MNSI.
- Promover la adecuada definición y asignación de roles y responsabilidades en el ámbito de seguridad de la información en Orange.
- Impulsar la divulgación y el conocimiento, así como exigir el cumplimiento de la Política de Seguridad de la Información entre las partes interesadas de Orange.
- Promover la mejora continua en el ámbito de la seguridad de la información en Orange, extendiéndola a los procesos corporativos.

5 Objetivos

La Política de Seguridad de la Información establece los siguientes objetivos:

Política de Seguridad de la Información

tipología	Política	referencia	DSEG.SG.POL.05.02	revisión	4.0
-----------	----------	------------	-------------------	----------	-----

- Garantizar la protección de los activos en base a su criticidad para el negocio, incluyendo elementos técnicos, humanos, materiales y organizativos de Orange 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 y;
- 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.

6 Roles y responsabilidades

Para poder alcanzar con éxito los objetivos de Seguridad de la Información, Orange establece una estructura de gestión **para coordinar de forma consistente y controlar de forma responsable** la implantación y operativa de la Seguridad de la Información.

Comité de Seguridad: es el principal rol para el gobierno y la toma de decisiones relacionadas con la Seguridad de la Información. Se encarga de ratificar la estrategia y objetivos de seguridad, hacer seguimiento de eventos e incidentes, monitorizar los indicadores de seguridad y dar seguimiento a los planes de acción.

El Comité de Seguridad se integra en el gobierno de la compañía y está patrocinado por el Secretario General de Orange y coordinado por el Chief Security Officer (CSO). En él están representados directivos de las unidades de negocio más relevantes de Orange y distintos responsables de áreas técnicas y de soporte con interlocución de seguridad. La dirección ejecutiva, así como cualquier otra parte necesaria en un momento dado, puede ser invitada ad hoc a participar en el Comité de Seguridad, a criterio del sponsor y del coordinador.

Chief Security Officer (CSO): como máximo responsable de la seguridad corporativa, vela por el correcto cumplimiento de las políticas y el MNSI, propone los objetivos de seguridad de la información y lidera la estrategia de seguridad.

Política de Seguridad de la Información

tipología	Política	referencia	DSEG.SG.POL.05.02	revisión	4.0
-----------	----------	------------	-------------------	----------	-----

Chief Information Security Officer (CISO): es responsable de definir, mantener, publicar y comunicar la Política de Seguridad de la Información y el MNSI. Asesora al CSO en materia de Seguridad de la información y es el responsable de la gestión de riesgos, así como de extender la formación y concienciación de seguridad de la información a nivel corporativo.

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.

El resto de roles y responsabilidades con impacto en seguridad de la información, incluidas las figuras de responsabilidad descritas en el Esquema Nacional de Seguridad, se encuentran recogidas en el MNSI.

7 Datos de carácter personal

Orange 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 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 (en adelante, 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 Orange.

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. Orange 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.

8 Legislación aplicable

El cumplimiento de la legislación que sea de aplicabilidad en materia de Seguridad de la Información se considera fundamental en Orange. Por lo tanto, se identificará y mantendrá actualizada la relación de requisitos legales y normativos que sean de aplicación, analizando el ámbito de aplicación y lanzando las acciones necesarias en cada caso con el fin de asegurar un debido cumplimiento.

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

9 Terceras partes

Cuando Orange preste servicios a terceras partes o maneje información de estas, se les hará partícipes de esta Política de Seguridad de la Información si así lo requieren. Además, se han definido procedimientos de actuación para la gestión de incidentes de seguridad.

En el caso específico de proveedores, estos también serán partícipes de esta Política y de la Normativa de Seguridad que atañe a los servicios subcontratados. Por lo tanto, estos terceros quedarán sujetos a las obligaciones establecidas en el MNSI.

10 Monitorización de la Seguridad de la Información

La información sobre el cumplimiento de seguridad de la información se reporta de manera periódica al Comité de Seguridad.

Cualquier indicador de seguridad puede ser factor desencadenante para que el CISO investigue el nivel de cumplimiento de un área, contratistas o sujeto específico, y actúe en consecuencia.

11 Cumplimiento

Tanto el cumplimiento de la Política de Seguridad de la Información como del resto del Marco Normativo de Seguridad de la Información es de obligatorio cumplimiento para todos los empleados, colaboradores y prestadores de servicios de la compañía dentro del alcance especificado.

Cualquier violación de lo indicado en la Política y en lo establecido en el MNSI puede dar lugar a reclamaciones contractuales y/o rescisión de contratos con contratistas o terceros, así como reclamaciones contractuales y/o medidas disciplinarias para los empleados de Orange.

Cualquier incumplimiento de la política debe ser notificado de cara a iniciar un proceso de derogación. El MNSI recoge el procedimiento a seguir para el tratamiento de derogaciones y excepciones.

Esta Política se revisará cada año, y se actualizará al menos cada cinco años o cada vez que resulte necesario por existir cambios de cierta relevancia que afecten tanto a la estructura de Orange como a la legislación aplicable.

Será misión del CISO realizar la revisión anual de esta Política de Seguridad de la Información. Además, la Política será aprobada por el CEO de Orange, y difundida para que la conozcan todas las partes afectadas.

12 Consideraciones adicionales

12.1 Documentación relacionada

A continuación, se indica el listado de documentación que complementan o amplían la información descrita en el documento:

- Política de Seguridad Global
- Marco Normativo de Seguridad de la Información de Orange
- Normativa de Orange basada en el Reglamento General de Protección de Datos (RGPD)
- Normativa de Orange basada en el Esquema Nacional de Seguridad (ENS)
- Normativa de Orange basada en la ISO 27001
- Legislación aplicable

12.2 Glosario

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

- **SGSI.** Sistemas de Gestión de la Seguridad de la Información.
- **MNSI.** Marco Normativo de Seguridad de la Información.
- **UE.** Unión Europea.
- **SOX.** Ley Sarbanes Oxley.
- **LOPDGDD.** Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.
- **RGPD.** Reglamento General de Protección de Datos.
- **ENS.** Esquema Nacional de Seguridad.
- **CSO.** *Chief Security Officer*- Responsable de Seguridad.
CISO. *Chief Information Security Officer.* Responsable de Seguridad de la Información.