

**SGSI –
POLÍTICA DE SEGURIDAD DE LA
INFORMACIÓN**

CONTROL DE VERSIONES

| REVISIÓN | | MODIFICACIONES |
|----------|-----------|-----------------|
| Nº | FECHA | |
| 1 | 1/12/2023 | Nueva redacción |
| | | |
| | | |
| | | |
| | | |
| | | |

ÍNDICE

| | |
|--|----------|
| 1. INTRODUCCIÓN | 4 |
| 2. OBJETIVO Y ALCANCE | 4 |
| 3. DIFUSIÓN | 4 |
| 4. POLÍTICA | 5 |
| ÁMBITO..... | 5 |
| OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN..... | 5 |
| CUMPLIMIENTO NORMATIVO | 6 |
| COMPROMISO DE LA DIRECCIÓN | 6 |
| MISIÓN | 6 |
| LEGISLACIÓN | 7 |
| ROLES Y RESPONSABILIDADES | 7 |
| TODO USUARIO AFECTADO POR LA PRESENTE POLÍTICA TENDRÁ LA OBLIGACIÓN DE:..... | 7 |
| COMITÉ DE SEGURIDAD DE LA INFORMACIÓN | 8 |
| CONTROL DE CUMPLIMIENTO | 8 |
| APROBACIÓN Y REVISIÓN | 8 |
| 5. REFERENCIAS | 9 |

1. INTRODUCCIÓN

Este documento expone la Política de Seguridad de la Información de DELETE, como el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, en el marco de las Norma ISO 27001 y Esquena Nacional de Seguridad (ENS).

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de la empresa. Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su conocimiento, procesado o tratamiento.

La Seguridad de la Información es la protección de este activo, con la finalidad de asegurar la calidad de la información y la continuidad del negocio, minimizar el riesgo y permitir maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información es un proceso que requiere medios técnicos y humanos y una adecuada gestión y definición de los procedimientos y en el que es fundamental la máxima colaboración e implicación de todo el personal de la empresa.

La dirección de la empresa, consciente del valor de la información, está profundamente comprometida con la política descrita en este documento.

2. OBJETIVO Y ALCANCE

El objetivo de la presente Política General de Seguridad de la Información es establecer un marco normativo en DELETE que permita identificar, desarrollar e implantar las medidas técnicas y organizativas necesarias para garantizar la seguridad y protección tanto de la información, privacidad de las personas incluidas, así como de los sistemas de información que dan soporte a la actividad de DELETE.

La presente Política de Seguridad de la Información se aplica en todo el ámbito de actuación de DELETE y, por ende, es de aplicación a todos los empleados, contratistas, clientes o cualquier otra tercera parte que tenga acceso a los sistemas o información de DELETE, independientemente del soporte automatizado o no en el que se encuentre.

3. DIFUSIÓN

El presente documento será publicado en un repositorio común de DELETE, de forma que sea accesible por todas personas que conforman la organización, y comunicado a todos los sujetos interesados, mencionados anteriormente, en especial al personal interno que maneje los activos de información de DELETE.

Así mismo, se realizará una publicación de este documento en el sitio web de DELETE <https://deletedoc.com/> para poder compartirlo con las partes interesadas externas de la organización.

4. POLÍTICA

Ámbito

DELETE protege los recursos involucrados en la gestión de la información relacionada con el normal desarrollo de sus funciones, dando cumplimiento a la legislación vigente, preservando la confidencialidad y privacidad de la información y asegurando la disponibilidad, acceso, integridad, calidad, trazabilidad, autenticidad y conservación. Estos objetivos se trasladan también a los sistemas de información utilizados para el desarrollo de su actividad.

Es voluntad de DELETE establecer condiciones de confianza en el uso de los medios electrónicos y la prestación continua de sus servicios, adoptando las medidas necesarias destinadas a proteger los sistemas de información de la organización de aquellas amenazas a los que se estén expuestos, con la finalidad de garantizar la seguridad de los sistemas de información, minimizar los riesgos y consolidar así las bases para prevenir, detectar, reaccionar y recuperarse de los posibles incidentes que puedan acaecer.

Objetivos de la Seguridad de la Información

Los objetivos que hay que lograr son:

- Garantizar, asegurar e implementar las medidas de seguridad adecuadas y necesarias sobre todos los recursos, procesos, funciones y servicios relacionados directa e indirectamente con usuarios internos y externos, y con clientes, proveedores, *partners* u otros terceros, con la finalidad de asegurar la disponibilidad, confidencialidad, integridad, autenticidad, trazabilidad de la información, y la conformidad con la legislación aplicable.
- Garantizar la continuidad, seguridad y calidad de los servicios ofrecidos.
- Implementar y mantener los procesos de mejora continua para favorecer la eficiencia y eficacia de las medidas de seguridad de la información.
- Reducir al máximo las posibilidades que produzcan incidentes de seguridad y minimizar el impacto de estos en caso de que se produjeran.
- Disponer de los medios por los que los diferentes usuarios de los servicios y procesos de DELETE hacen buen uso de la información, sistemas de la información y recursos utilizados en el desarrollo de sus funciones, obligaciones y responsabilidades, así como los que no comprometan la seguridad de la información de DELETE.
- Alinearse con las mejores prácticas y estándares de ámbito internacional en materia de seguridad de la información y/o ciberseguridad; principalmente, con la serie ISO 27000, ENS, CSF-NIST y COBIT.

De acuerdo con los objetivos citados, la presente Política General de Seguridad de la información busca la adopción de premisas de seguridad, garantizando:

- Disponibilidad: la información y sistemas de información pueden ser utilizados en los tiempos y forma requerida.
- Confidencialidad: los datos y sistemas de información solamente se accederán por las personas debidamente autorizadas.

- Integridad: exactitud de la información y de los sistemas de información contra la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
- Autenticidad: inequívoco al asegurar que una persona o entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- Trazabilidad: cualquier acción o transacción puede ser relacionada inequívocamente al sujeto que lo ha llevado a cabo.
- Legalidad: la información se trata de acuerdo con el marco normativo.
- Formación: de acuerdo con el principio de seguridad integral, garantizar un adecuado nivel de concienciación y capacitación en materia de seguridad de la información a todo el personal de la organización.
- Gestión de incidentes: el análisis y gestión de los riesgos como parte esencial del proceso de seguridad de la organización, manteniendo el entorno controlado y minimizando los riesgos, de acuerdo con las medidas de prevención, detección, reacción y recuperación, y estableciendo protocolos para el intercambio de información relacionada con los incidentes.

Cumplimiento Normativo

DELETE se compromete a dotar los recursos necesarios para dar cumplimiento a toda la legislación y regulación aplicable a su actividad en materia de seguridad de la información y establecer la responsabilidad de dicho cumplimiento sobre todos sus miembros. En este sentido, se velará por el cumplimiento de toda legislación, normativa o regulación aplicable.

Compromiso de la Dirección

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

- Promover en la organización las **funciones y responsabilidades** en el ámbito de seguridad de la información.
- Facilitar los **recursos** adecuados para alcanzar los objetivos de seguridad de la información.
- Impulsar la **divulgación y la concienciación** de la Política de Seguridad de la Información entre los empleados de DELETE.
- Exigir el **cumplimiento** de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- Considerar los **riesgos** de seguridad de la información en la toma de decisiones.

Misión

La misión del Servicio de Ciberseguridad de DELETE es la de supervisar y velar por la protección de la **Información y los Sistemas** de DELETE, de la información de los clientes internos y externos y los intereses de otras partes interesadas.

Esta protección se realizará ante cualquier amenaza o agresión interna y/o externa potencial, principalmente de tipología ciberataque, adoptando las medidas preventivas y reactivas correspondientes y según el presupuesto disponible. Se fomenta, así, una robusta cultura de la ciberseguridad y de desarrollo y aplicación de un marco normativo específico en esta materia.

Legislación

- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual
- Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual.
- Real Decreto 3/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad modificado por el Real Decreto 951/2015, de 23 de octubre.
- Artículo 11 del Real Decreto 3/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad modificado por el Real Decreto 951/2015, de 23 de octubre.
- Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad de 4 de mayo.
- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).

Roles y responsabilidades

Todo usuario afectado por la presente Política tendrá la obligación de:

- Cumplir en todo momento con la Política General de Seguridad de la Información, normas, procedimientos e instrucciones de Seguridad de la Información de la Organización.
- Tener un papel activo en la ciberseguridad de cualesquiera activos que sean objeto de protección dentro del ámbito de la presente Política.
- Mantener el secreto profesional y la confidencialidad respecto de la información de la Organización.
- Informar, de acuerdo con el correspondiente procedimiento, de situaciones sospechosas o anomalías, incidentes de seguridad, y no conformidades o incumplimientos de seguridad de los sistemas de información y/o activos de la organización.

La responsabilidad general de la Seguridad de la Información recae en la persona a la que se le asignen las funciones de Responsable del SGSI y la Dirección de DELETE.

La coordinación de la Seguridad de la Información se canalizará a través de un Comité de Seguridad de la Información, que se reunirá con carácter ordinario de forma trimestral. En caso de que se

considere oportuno, debido a circunstancias que así lo requieran, se podrán convocar reuniones extraordinarias.

En cuanto al incumplimiento de la Política General de Seguridad de la Información de DELETE y el resto de los documentos relacionados con la seguridad de la información, por parte de cualquiera al que le sean de aplicación y que ponga en riesgo la seguridad de la información en cualesquiera de sus dimensiones, la Dirección de DELETE se reserva el derecho de iniciar las acciones correspondientes según los códigos y normas internas de comportamiento y el marco legal vigente.

Comité de Seguridad de la Información

DELETE dispone de un Comité de Seguridad de la Información, encargado de alinear todas las actividades de la organización en materia de seguridad de la información, destacándose los aspectos de seguridad física y patrimonial (seguridad de las instalaciones), seguridad de la información, *Compliance* (seguridad y conformidad legal) y planes de contingencia.

Para el detalle en la operativa y estructura del comité, puede consultar el documento *SGSI-P2-A06-ORGANIZACION DE LA SEGURIDAD*.

Control de Cumplimiento

El grado de aplicación de esta política será medido periódicamente (como mínimo, anualmente) mediante autoevaluaciones coordinadas por el Comité de Seguridad de la Información y mediante auditorías internas o externas (como mínimo, bienales), y siempre que se produzcan cambios sustanciales en los sistemas de información de DELETE. La aprobación de la presente política se realiza en la Revisión por la Dirección, indicado en el SGSI.

Aprobación y Revisión

La Política General de Seguridad de la Información es aprobada formalmente por la Dirección de DELETE y el Responsable del SGSI. Este acto quedará reflejado en la correspondiente acta, y estará vigente hasta que sea reemplazada por una nueva versión. Así mismo, se revisará anualmente y siempre que se produzcan cambios significativos que lo requieran, con el fin de adaptarla a las nuevas circunstancias, técnicas y/u organizativas, evitando que quede obsoleta.

Para estos efectos, regularmente se revisará su idoneidad, oportunidad y precisión.

5. REFERENCIAS

Normativa

- ISO/IEC 27002:2013 “Information technology – Security techniques – Code of practice for information security management”.
- ISO/IEC 27001:2013 “Information technology – Security techniques – Information security management systems – Requirements”.
- Real Decreto 3/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad modificado por el Real Decreto 951/2015, de 23 de octubre.

SGSI

- SGSI-P1-PBUIA-Politica-Buen-Uso-Informacion-Activos.
- SGSI-P2-A08-GESTION DE ACTIVOS.
- SGSI-P2-A06-ORGANIZACION DE LA SEGURIDA.
- SGSI-P1-MSGSI-Manual-SGSI.
- SGSI-P2-A12-OPERACIONES.
- SGSI-P2-RD-REVISION POR DIRECCION.