Política de Segurdad de la Información

Marzo 2024

Headquarters (Spain)
Edificio Bluenet. Avda. Isaac Newton, 3
PCT Cartuja. 41092 Seville (Spain)
P: +34 955 036 800

Spain
Brazil
United States
United Kingdom
Argentina
Mexico
Chile

HOJA DE CONTROL DE DOCUMENTO

DOCUMENTO / ARCHIVO				
Título	Política de Seguridad de la Información	Nombre archivo	Política de Seguridad de la Información	
Código		Soporte lógico		
Fecha	Marzo 2024	Ubicación física		
Versión	3.1	Tipo	Público	
			Interno	x
			Confidencial	
			Reservado	

REGISTRO DE CAMBIOS		
Versión	Página	Motivo del cambio
0		Inicial
1		Se crea un nuevo punto que es
2		Actualización LOPD
3		Actualización de formato (2021)
3.1		Actualización de formato (2024)

DISTRIBUCIÓN DEL DOCUMENTO		
Preparado	Revisado	Aprobado
José Luis Sánchez	Manuel Alguacil	Manuel Losada

Índice

1 Introducción

1.1 Objetivos

Considerado el propósito básico de este documento establecer los fundamentos generales para la **protección de la información y los recursos asociados a las Tecnologías de la Información** utilizados, se pretende en concreto:

- Definir la política a seguir en relación con la seguridad de la información.
- Dar directrices para lograr los niveles adecuados de seguridad que permitan una buena gestión de los riesgos identificados.
- Proteger los activos de información conforme a su valor o importancia.
- Preservar la privacidad de clientes, empleados, proveedores y terceras partes.
- Garantizar el cumplimiento de los requerimientos en materia legal.
- Mejorar continuadamente el sistema de seguridad de la información.

1.2 Alcance

La empresa y terceras organizaciones relacionadas con ella que traten datos o información perteneciente o relativa a sus operaciones, son susceptibles de la aplicación de esta política. Abarca **la información de toda la organización, en cualquiera de sus formatos y en cualquier soporte** posible, recogiendo actividades y relaciones con clientes, empleados, proveedores y terceros implicados.

Por la naturaleza y objeto de actividad de nuestra empresa, se debe observar el **cumplimiento de normas de rango superior** (leyes, normas y disposiciones legales) que tendrán preferencia, cuando ello aplique, sobre las directrices de esta política de seguridad de la información:

1. Normativa española que regula esta actividad:
    a. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
    b. Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
    c. Ley 23/2003, de 3 de noviembre, General de Telecomunicaciones.
    d. Ley 34/2002, de 11 de julio, de Servicios de Sociedad de la Información y de Comercio Electrónico (LSSICC).
2. Normas españolas que provengan de organismos supranacionales de los que España sea miembro. Esta política cubre todas las actividades de la organización respecto al tratamiento de la información y los sistemas que le dan apoyo.
   El personal de la empresa, proveedores y terceros relacionados deben cumplir, como indica la presente política, con todo lo concerniente al tratamiento de la información perteneciente a la empresa (**creación, proceso, comunicación, distribución, almacenamiento y despliegue**). Esta política determina el nivel específico de control y el impacto potencial para la organización en:
    - su actividad;
    - las relaciones entre empleados;
    - su imagen pública.

1.3 Alcance certificado

Los Sistema de Información que dan soporte a las actividades vinculadas al diseño, desarrollo y mantenimiento de aplicaciones informáticas, y a la provisión de servicios de consultoría en seguridad informática.

2 Motivación

La **seguridad de la información ve crecer su importancia** debido a los siguientes aspectos:

- Se afronta la rápida expansión, utilización y dependencia de las Tecnologías de la Información, por lo que es necesario y razonable esperar que todos los empleados conozcan los métodos apropiados de gestión, tratamiento y salvaguarda de la información, así como de los recursos informáticos asociados a éstos.
- Las obligaciones derivadas del desarrollo legislativo asociado a la evolución de la sociedad de la información.
- La necesidad de proteger y evitar la difusión de información confidencial respecto a terceros, que implica la puesta en marcha de controles de seguridad razonables y eficaces.

3 Política general

La política considera la información como un activo que debe ser apropiadamente evaluado y protegido contra cualquier forma no autorizada de:

- Acceso
- Uso
- Revelación
- Modificación
- Destrucción
- Denegación

Los **controles de seguridad** de la información deben ser lo suficientemente efectivos para asegurar:

- La **confidencialidad**: La información no estará disponible o no será revelada a individuos o entidades no autorizados.
- La **integridad**: La información sólo será modificada por los usuarios autorizados para ello.
- La **disponibilidad**: La información y los recursos informáticos podrán ser accedidos por los usuarios autorizados cuando lo necesiten.

Los proyectos de Tecnologías de la Información deben proceder, en coordinación con la Dirección, y de acuerdo a la política de seguridad de clasificación e intercambio de la información, a la gestión de esta clasificación, siempre que esté bajo su control, y a la identificación de los niveles adecuados de protección.

El responsable tecnológico depositario de la información deberá asegurarse, y así reportarlo, de la **implementación de aquellos controles que hayan sido identificados y considerados necesarios** en relación al activo de información y su tratamiento.

Los propietarios de la información son responsables de la comunicación de cualquier cambio real en los niveles requeridos de protección y medidas de seguridad relacionadas con los activos, debiendo los sistemas de información garantizar, por tanto, la habilitación de las nuevas medidas de seguridad y de los recursos de los sistemas de información necesarios, ya sean técnicos o de procesos.

Estos controles de seguridad deben aplicarse teniendo en cuenta el valor de la información, y por tanto su nivel de clasificación, y los procesos asociados en cuanto a su tratamiento.

La información considerada confidencial requiere controles más estrictos en su tratamiento.

El responsable de seguridad tiene el deber de **asegurar la implementación, supervisión y mantenimiento de las políticas de seguridad** de la información, así como ofrecer asistencia en:

- El establecimiento de las políticas y procedimientos
- La implementación técnica y de procedimientos
- La auditoría y revisión

La seguridad de la información se ha organizado en áreas de seguridad específicas, integrando en cada una de ellas las políticas y otra documentación que forman el cuerpo normativo.

4 Cumplimiento

Los empleados han de conocer sus funciones y obligaciones en relación a las políticas de seguridad de la información, por lo que éstas les deben ser comunicadas en base al departamento en el que se encuentran o las funciones que desempeñan.

Todos los empleados de la organización deben conocer y actuar, por tanto, conforme a esta política y a sus desarrollos normativos.

En caso de actuaciones contrarias al contenido de esta política o de cualquiera de los desarrollos normativos en seguridad de la empresa, podrán ponerse en marcha **mecanismos correctivos o sancionadores.**

4.1 Excepciones a la política

Las excepciones a cualquier política deben limitarse a aquellos casos en los que sea estrictamente imprescindible con autorización expresa de la Dirección. Sólo se permitirán excepciones a la política de seguridad de la información si se demuestra que no exponen a la organización a niveles de riesgo inaceptables.

4.2 Comunicación de incidentes

Todos los casos, reales o sospechos, **de abuso o robo de activos de información**, así como amenazas potenciales (hackers, virus, fuego, etc.) o puntos débiles obvios que afecten a la seguridad, **deben ser reportados inmediatamente** mediante el procedimiento de comunicación de incidentes y, si se estima preciso, a la Dirección y/o al coordinador de la unidad pertinente.

5 Definiciones de la gestión de seguridad de la información

A continuación, se presentan una serie de definiciones que se utilizarán en esa política y el resto del cuerpo normativo.

5.1 Activos de información

Un **activo de información** es un conjunto de datos de información de negocio o soporte al negocio, creados o tratados por los sistemas de información y que se considera necesario proteger. Ejemplos: Información financiera, información de recursos humanos, …

Un **servicio de acceso** se compone de métodos, procesos o aplicaciones (sistemas) que crean, acceden o manipulan los activos de información.

Los **elementos de T.I.** son las dependencias tecnológicas, elementos tecnológicos tangibles, que gestionan, almacenan, albergan o manipulan los datos de los activos de información. Ejemplos: servidores, redes, PCs, edificios, …

El **modelo de dependencias** es la relación entre los servicios de la actividad y los elementos de los sistemas de información necesarios para que puedan operar.

5.2 Propietario de los activos de información

Cada activo o conjunto de activos de información debe tener asignado un responsable de la organización que sea representativo, que sea su propietario y tenga la responsabilidad de realizar y comunicar evaluaciones sobre su identificación, valoración, utilización y protección.

Los activos de información, además de en sistemas informáticos, pueden encontrarse en cualquier otro soporte, algunos ejemplos:

- Documentos en papel.
- Software.
- Archivos de datos informáticos.
- Archivos multimedia.

Las políticas de seguridad de la información tendrán aplicación sobre activos de información en cualquier soporte.

5.3 Clasificación de la información

Existe una política de clasificación y tratamiento de la información que forma parte de este marco normativo: *Política de clasificación e intercambio de información*.

6 Referencias

- Política General de Seguridad Integral
- Estructura normativa
- Política de clasificación e intercambio de información