

Objeto	Síntesis de la Política de Seguridad de la Información
Alcance	Todos los tratamientos de datos personales y otra información realizados por VALFONDO HOLDING, S.L. y sus sociedades participadas (en lo sucesivo denominada “VALFONDO”), así como las medidas de seguridad aplicables a dicha información.
Responsables	Dirección General, Responsable de Seguridad de la Información y Delegado de Protección de Datos.

Versiones

Versión	Fecha	Contenido de la modificación
0.0	10/12/2020	Redacción inicial
0.1	14/12/2020	Modificación documento inicial
0.2	24/03/2021	Aprobación
0.3	12/12/2023	Actualización (varios apartados)
0.4	24/06/2026	Actualización conforme al Sistema de Gestión de Seguridad de la Información (SGSI)

1 COMPROMISO CON LA SEGURIDAD DE LA INFORMACIÓN

En VALFONDO consideramos la seguridad de la información como un pilar estratégico para el desarrollo de nuestra actividad, la continuidad del negocio, y la protección de los intereses de clientes, empleados, proveedores y demás partes interesadas.

A través de la Política de Seguridad de la Información, VALFONDO establece los principios, responsabilidades y controles necesarios para gestionar los riesgos asociados a la información y a los datos personales, integrar la seguridad en sus procesos y promover una cultura organizativa basada en la responsabilidad compartida, la mejora continua y el cumplimiento de la normativa aplicable en materia de seguridad de la información y protección de datos personales, incluyendo el Reglamento General de Protección de Datos (RGPD).

2 PILARES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

- **Confidencialidad:** Asegurar que la información es accesible sólo para las personas autorizadas a tener acceso.

- **Integridad:** Garantizar que la información y los métodos de su procesamiento son exactos y completos.
- **Disponibilidad:** Asegurar que las personas autorizadas tienen acceso a la información y sus activos asociados, cuando lo requieran para el ejercicio de sus funciones.

3 OBJETIVOS

- Proteger los sistemas, aplicaciones, activos de información y datos personales frente a accesos no autorizados, alteraciones, pérdidas, destrucción o usos indebidos.
- Sensibilizar y formar al personal en relación con sus responsabilidades en materia de protección de la información, protección de datos personales y uso seguro de los sistemas, aplicaciones y recursos tecnológicos.
- Prevenir el uso indebido de los sistemas, aplicaciones, dispositivos y demás recursos tecnológicos, reduciendo los riesgos derivados de su utilización.
- Detectar, comunicar y gestionar de forma adecuada los incidentes de seguridad, mediante la aplicación de controles y procedimientos orientados a garantizar la seguridad en el tratamiento de la información propia, de terceros y de los datos personales.

4 PRINCIPALES MEDIDAS ADOPTADAS

- Control de accesos físicos y lógicos a los sistemas y dispositivos de la organización.
- Gestión segura de contraseñas con autenticación multifactor.
- Copias de seguridad periódicas y planes de recuperación ante desastres.
- Gestión y monitorización de incidentes de seguridad.
- Clasificación y tratamiento adecuado de la información confidencial.
- Restricción del uso de dispositivos de almacenamiento externo.
- Formación y concienciación continua a todo el personal sobre buenas prácticas en ciberseguridad.

Las medidas adoptadas se revisan de forma continua y se actualizan cuando resulta necesario, tomando en consideración los resultados de la evaluación de riesgos, la eficacia de los controles implantados, los resultados de las auditorías internas y externas, las incidencias y

eventos de seguridad registrados, así como las sugerencias y oportunidades de mejora identificadas, con el fin de asegurar la mejora continua del Sistema de Gestión de Seguridad de la Información.

5 GOBERNANZA Y CUMPLIMIENTO

La Política establece roles y responsabilidades claras en materia de seguridad de la información, incluyendo entre otros, a la Dirección General, al Responsable de Seguridad, al Delegado de Protección de Datos y Usuarios. Estos perfiles colaboran de forma coordinada para asegurar el cumplimiento normativo, la evaluación de riesgos y la respuesta ante posibles amenazas o vulnerabilidades.

En definitiva, la presente Política responde al compromiso de VALFONDO con el cumplimiento riguroso de la normativa vigente en materia de seguridad de la información y protección de datos personales, así como con la implementación de buenas prácticas que garanticen la continuidad operativa y la protección de los intereses de todas las partes implicadas.