# POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN

MUGE-DG-PLT-0048 - Rev. 7.4 Libre Difusión

| Elaborado por: | Revisado por: | Aprobado por: |
|---|---|---|
| Responsable de Seguridad | Gerencia de Calidad | Dirección General |
| Fecha: 01/07/2022 | Fecha: 01/07/2022 | Fecha: 01/07/2022 |

## HISTÓRICO DE REVISIONES

| DESCRIPCIÓN | FECHA | REVISIÓN |
|---|---|---|
| Elaboración del documento | 21/06/2010 | 1.0 |
| Revisión y actualización del documento | 30/09/2010 | 2.0 |
| Revisión y actualización del documento | 10/06/2011 | 3.0 |
| Revisión y actualización del documento<br>Adaptación del documento a los formatos de la Metodología OGMA | 24/02/2012 | 4.0 |
| Revisión y actualización del documento<br>Eliminar redundancia con instalación y uso de programas. Modificación párrafo porque el previo aviso lo constituye la difusión de este documento. | 25/09/2012 | 5.0 |
| Revisión y actualización del documento para incluir los requisitos de la norma ISO/IEC 27001:2014 y Ley Orgánica de protección de datos (LOPD) | 14/12/2015 | 6.0 |
| Se explicitan los Objetivos de la Política de Seguridad de la Información. | 31/03/2016 | 7.0 |
| Revisión de la Política de Seguridad – no hay cambios | 19/03/2018 | 7.1 |
| Revisión de la Política de Seguridad de la Información. Eliminación de la empresa Polar Consultores. | 22/01/2019 | 7.2 |
| Revisión del documento | 07/07/2021 | 7.3 |
| Revisión del documento | 13/04/2022 | 7.4 |
| Estandarización de formatos de todas las políticas corporativas de la Organización. | 01/07/2022 | 7.4 |

## ÍNDICE

# 1. Política Corporativa de Seguridad de la Información

## 1.1. Objetivos de la Política Corporativa de Seguridad de la Información

Se emite esta política con los siguientes objetivos:

1. Garantizar la Seguridad de la Información que se genera en la Organización durante el desarrollo de nuestra actividad, estableciendo los controles y medidas de protección necesarias para salvaguardarla de posibles amenazas.
2. Reducir los Riesgos derivados de la falta de disponibilidad, error humano, robo, pérdida o corrupción de la información.
3. Garantizar a nuestros clientes y proveedores el cumplimiento de los requisitos de Seguridad de la Información establecidos por todas las partes, y reforzar nuestra imagen y credibilidad.
4. Contar con un Sistema de Gestión eficaz que ayude a discernir qué hacer, cómo y cuándo ante incidencias relacionadas con la Seguridad de la Información.
5. Reforzar la organización interna de la información, definiendo responsabilidades y obligaciones, y proporcionando confianza y reglas claras al personal de la empresa.
6. Incorporar la Seguridad de la Información en nuestra Cultura como Organización, integrando en todas nuestras actividades criterios de desarrollo y de gestión de la información seguros.
7. Asegurar el cumplimiento normativo y legislativo en materia de Protección de Datos de Carácter Personal y otras regulaciones sobre gestión y seguridad de la información.
8. Formar, comunicar y capacitar de forma continua y fluida a todo el personal de la empresa en sus obligaciones en materia de seguridad de la información.
9. Monitorizar, supervisar y promover la mejora continua del Sistema de Gestión de la Seguridad de la Información, a través del compromiso absoluto de la Dirección y de todo el personal de la Organización, y estableciendo objetivos de mejora del Sistema.

## 1.2. Premisas de la Política Corporativa de Seguridad de la Información

Para el cumplimiento de los objetivos de esta política, la Organización establece las siguientes premisas y compromisos:

1. Organizativo: orientado a administrar la seguridad de la información dentro de nuestra organización y establecer un marco gerencial para controlar su implementación. Partiendo de la presente Política de Seguridad se desarrollará el resto del marco normativo de seguridad.

2. Operacional: constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

a) Planificación: mediante análisis de riesgos, controlando la arquitectura de seguridad y la adquisición de nuevos componentes entre otros aspectos.

b) Control de Acceso: orientado a controlar el acceso lógico a la información.

c) Explotación: medidas para la gestión de la seguridad en explotación, partiendo del inventario de activos y controlando la gestión de incidencias, cambios, gestión de la configuración y registros de actividad, entre otros.

d) Servicios externos: medidas de seguridad orientadas a garantizar que empresas y personas terceras que realicen servicios de cualquier clase contratados por la Organización o que de alguna manera se presten bajo el control y/o la dirección de la Organización, cumplan las políticas y normas de seguridad de la información establecidas por nuestra parte.

e) Continuidad del servicio: acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales.

f) Monitorización del sistema: orientado a garantizar la disponibilidad de las actividades diarias y proteger los procesos críticos de los efectos de fallos significativos o desastres.

3. Medidas de Protección: para la protección de activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

a) Protección de las instalaciones e infraestructuras: destinado a impedir accesos no autorizados, daños e interferencias en las instalaciones e infraestructuras de la Organización.

b) Gestión del personal: orientado a reducir los riesgos de error humano o uso inadecuado de las instalaciones y equipamientos. Cumplimiento de los controles y medidas de seguridad establecidos en las instrucciones de seguridad, pudiendo ser aplicable el proceso disciplinario definido en el Estatuto de los Trabajadores en su Capítulo IV, Faltas y sanciones de los trabajadores, en caso de violaciones intencionadas de la seguridad. Obligatoriedad de formación en temas de seguridad de la información en los términos establecidos en la instrucción de seguridad relativa a recursos humanos.

c) Protección de los equipos: medidas para la protección de los equipos informáticos.

d) Protección de las comunicaciones: dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información, elementos y sistemas de comunicación.

e) Protección de los soportes de información: para garantizar la información (registros) que contienen.

f) Protección de las aplicaciones informáticas: dirigido a garantizar la integración de la seguridad de la información en el método de gestión de proyectos de la Organización. De esta forma se asegura que los riesgos de seguridad de la información se identifican y se abordan como parte de un proyecto.

g) Protección de la información de datos de carácter personal: cumpliendo lo dispuesto en el Reglamento General de Protección de Datos (RGPD) y gestionando la información en base a su clasificación. Cumpliendo y dando conformidad a los requisitos legislativos y contractuales aplicables a la actividad de la empresa en materia de seguridad.

4. Para garantizar el cumplimiento de lo establecido por el SGSI, la Dirección delega la responsabilidad de supervisión, verificación y monitorización del sistema en el Responsable de Seguridad.

5. La Dirección se compromete a facilitar los medios necesarios y a adoptar las mejoras oportunas en toda la Organización, para fomentar la prevención de los riesgos y daños sobre los activos, mejorando así la eficiencia y eficacia del SGSI.

## 1.3. Alcance

En la Organización consideramos que la Seguridad de la Información es imprescindible para la competitividad de la empresa y, por tanto, para su supervivencia, por lo que hemos implantado un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO 27001:2014.

El objeto del presente documento es la concreción de la Política y las directrices de la Dirección sobre las normas y controles de seguridad que afectan tanto al personal de la Organización como a cualquier usuario del sistema en el desarrollo de sus funciones, así como las consecuencias en que puede incurrir en caso de incumplimiento en materia de seguridad de datos personales o seguridad de la información.

Esta Política se establece como marco en el que se deben desarrollar todas las actividades de la Organización cuyo alcance es “la información que soporta las actividades de comercialización, prestación de servicios, consultoría y desarrollo de software”, de manera que se garantice a los clientes y demás partes interesadas el compromiso adquirido.

# 2. Documentación

## 2.1. Normativa

1. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos (LOPD)

## 2.2. Documentación Aplicable/Referencia

| Nº | Código | Título |
|---|---|---|
| a) | UNE-EN ISO 9001 | Sistema de Gestión de la Calidad |
| b) | UNE-EN ISO 14001 | Sistema de Gestión Ambiental |
| c) | UNE-EN ISO 9000 | Sistemas de Gestión de la Calidad – Fundamentos y Vocabulario |
| d) | CMMI® (Capability Maturiy-Model Integration) para Desarrollo (CMMi-DEV) | |
| e) | CMMI® (Capability Maturiy-Model Integration) para Servicios (CMMi-SVC) en nivel 3 de madurez | |