CONSULTORES EN PROTECCIÓN DE DATOS, S.L.

(CONPRODAT)

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código	SG-06
Versión	0.2
Fecha de la versión:	17/01/2022
Aprobado por:	Miguel Miranda
Nivel de Confidencialidad	**Público**

I. INTRODUCCIÓN

Este documento expone la **Política de Seguridad de la Información de CONPRODAT** (en adelante, la empresa), como el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, en el marco de la Norma ISO 27001.

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 **CONPRODAT**, consciente del valor de la información, está profundamente comprometida con la política descrita en este documento.

II. DEFINICIONES

- **Sistema de Información**: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
- **Riesgo**: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
- **Gestión de riesgo**s: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
- **Sistema de Gestión de Seguridad de la Información (SGSI)**: sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

- **Disponibilidad**: Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten, especialmente la información crítica.
- **Integridad**: La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
- **Confidencialidad**: La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.

III. OBJETIVO Y PRINCIPIOS

El propósito de esta Política de la Seguridad de la Información es proteger los activos de información de la empresa, asegurando para ello la disponibilidad, integridad y confidencialidad de la información y de las instalaciones, sistemas y recursos que la procesan, gestionan, transmiten y almacenan, siempre de acuerdo con los requerimientos del negocio y la legislación vigente.

La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, comunicación, transporte, almacenamiento, difusión y hasta su eventual borrado o destrucción. Por ello, se establecen los siguientes principios mínimos:

- **Principio de confidencialidad**: los sistemas de información deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.
- **Principio de integridad y calidad**: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.
- **Principio de disponibilidad y continuidad**: se garantizará un nivel de disponibilidad en los sistemas de información y se dotarán los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.
- **Principio de gestión del riesgo**: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los sistemas de información.
- **Principio de proporcionalidad en coste**: la implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos, sin perjuicio de que se asegurará que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.

- **Principio de concienciación y formación**: se articularán iniciativas que permitan al personal conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De igual forma, se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.
- **Principio de prevención**: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.
- **Principio de detección y respuesta**: los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia respondiendo eficazmente a los incidentes de seguridad, a través de los mecanismos establecidos al efecto.
- **Principio de mejora continua**: se revisará el grado de cumplimiento de los objetivos de mejora de la seguridad planificados anualmente y el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos.
- **Principio de seguridad TIC en el ciclo de vida de los sistemas de información**: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

La Política de Seguridad de la Información es aprobada por la Dirección de **CONPRODAT** y su contenido y el de las normas y procedimientos que la desarrollan es de obligado cumplimiento.

- Todos los usuarios con acceso a la información tratada, gestionada o propiedad de la empresa tienen la obligación y el deber de custodiarla y protegerla.
- La Política y las Normas de Seguridad de la Información se adaptarán a la evolución de los sistemas y de la tecnología y a los cambios organizativos y se alinearán con la legislación vigente y con los estándares y mejores prácticas de la norma ISO/IEC 27001.
- Las medidas de seguridad y los controles físicos, administrativos y técnicos aplicables se detallarán en el Documento de Aplicabilidad y la empresa deberá establecer una planificación para su implantación y gestión.
- Las medidas de seguridad y los controles establecidos serán proporcionales a la criticidad de la información a proteger y a su clasificación.
- Los usuarios que incumplan la Política de Seguridad de la Información o las normas y procedimientos complementarios podrán ser sancionados de acuerdo con lo establecido en los contratos que amparen su relación con la empresa y con la legislación vigente y aplicable.

IV. REQUISITOS LEGALES

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 abril del 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD UE - 679/2016).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDyGDD).
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

Para conocer *in extenso* este punto, recomendamos consultar el **Documento SG-04 Lista de requisitos legales**.

V. ROLES Y RESPONSABILIDADES

La **dirección** de **CONPRODAT asigna, renueva y comunica** las responsabilidades y roles en lo referente a la seguridad de la información, determinando en cada caso los motivos. También se asegurará de que los usuarios conocen, asumen y ejercen las responsabilidades, autoridades y roles asignados, **resolviendo los conflictos** que se generen en relación a cada responsabilidad en Seguridad de la Información.

En este punto, y para conocer en detalle la asignación de roles y responsabilidades en **CONPRODAT** nos remitimos expresamente al Documento **SG-07 Matriz de responsabilidades**.

VI. REVISIÓN Y AUDITORÍAS

El responsable de seguridad revisará esta política anualmente o cuando haya cambios significativos que así lo aconsejen. Las revisiones comprobarán la efectividad de la política, valorando los efectos de los cambios tecnológicos y de negocio.

La dirección será responsable de aprobar las modificaciones necesarias en el texto cuando se produzca un cambio que afecte a las situaciones de riesgo establecidas en el presente documento.

El sistema de gestión de seguridad se auditará cada año, según un Programa de auditoría interna desarrollado por la Administradora de Sistemas y Auditora Interna.