# PO.SG.CLD

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

## Control de Documento

| | | | |
|---|---|---|---|
| **Título:** | **Política de Seguridad de la Información** | | |
| **Referencia:** | **PO.SG.CLD** | **Versión:** | **3** |
| **Fecha de Creación:** | **03/05/2022** | **Fecha de Revisión:** | 19/06/2024 |
| **Autor:** | **Ignacio Ludeña** | | 19/06/2024 |
| **Revisión:** | Domingo Hernández | | 19/06/2024 |
| **Aprobación:** | Domingo Hernández | | 19/06/2024 |

## Historia del Documento

| Versión | Fecha | Autor | Comentario |
|---|---|---|---|
| **Borrador inicial** | **03/05/2022** | BR | **Borrador inicial** |
| **Versión inicial** | **03/05/2022** | BR | **Versión inicial** |
| **Revisión** | 19/06/2024 | DH | Revisión proceso disciplinario |
| **Revisión** | | | |
| | | | |

**INDICE**

## 1. INTRODUCCIÓN

CALIDALIA, S.L, en adelante, la Organización, tiene una gran cantidad de información sensible en la que se basa su rendimiento, sostenibilidad, seguridad y capacidad para mantener el desarrollo de sus actividades resultados.

Este patrimonio de información cubre:

- Información sobre producción y gestión, necesaria para el funcionamiento de la actividad de la Organización.
- Patrimonio intelectual, compuesto por toda la información que se atesora en el conjunto con el conocimiento y el know-how de la Organización.
- Información sobre sus Socios o sus terceros con los que está en contacto, cuya alteración o divulgación podría dañar su imagen de marca, la de sus socios o de los terceros interesados, o incluso llevar a acciones legales,
- Información sobre su personal, como registros administrativos, cuya divulgación constituiría una violación de la privacidad.

El propósito de este documento es presentar la Política de Seguridad de los Sistemas de Información de CALIDALIA para proteger sus activos de información de la gama de amenazas (fraude, espionaje, accidentes, errores humanos, etc.), con el fin de establecer la confianza de nuestros Socios, cumplir con los marcos legales y reglamentarios aplicables a la Organización con los objetivos en materia de seguridad de la información.

Esta política es la piedra angular del programa global de seguridad de la información de la Organización, dirigido a la protección de los activos de información incluidos dentro del alcance del Sistema de Gestión de Seguridad de la Información (en adelante, SGSI).

Este documento proporciona el marco para la seguridad de la información y garantiza: disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de la información.

La alta dirección de la Organización se compromete a poner en marcha los medios y acciones necesarias para implementar esta política.

La política está accesible para cualquier empleado de la Organización a través de su intranet, tablón de anuncios, etc. Y, a través de la alta Dirección, para cualquier parte interesada que lo solicite.

## 2. ALCANCE

Esta política es un documento aplicable a todos los departamentos de la Organización y a todo su personal.

La estructuración de la Organización de roles / funciones de seguridad, se define a nivel corporativo y a nivel operativo, desarrollado en el modelo organizativo.

El perímetro funcional de esta política cubre todos los activos de información de la Organización, es decir, todos los medios para crear, adquirir, procesar, almacenar, distribuir o destruir Información, a saber:

- Información: Cualquier dato almacenado en formato electrónico o en papel perteneciente a la Organización, empleados, proveedores o de sus socios,
- Materiales: todos los elementos físicos que soportan procesos (portátil, servidor, impresora, soporte extraíble, lector, armario de almacenamiento, etc.),
- Software: Todos los programas o ejecutables que contribuyen a las operaciones de datos (sistema operativo, software de supervisión, suite ofimática, ejecutables, etc.),
- Red: todos los dispositivos de comunicación utilizados en la interconexión de diferentes ordenadores o elementos remotos de un sistema de información (Router, cortafuegos, línea de comunicaciones dedicadas, red telefónica, red IP, etc.),
- Personal: todos los involucrados en el sistema de información (personal de la Organización, subcontratistas, colaboradores, etc.),
- Ubicaciones: todos los emplazamientos de la Organización, si lo tuviera, y los requisitos físicos para el funcionamiento de estos sitios (edificio, oficinas, sala dedicada, líneas telefónicas, etc.),
- Estructura de la Organización: todos los elementos que forman parte de la Organización y su funcionamiento (modelo organizativo, procesos internos y de negocio, etc.).

Del mismo modo, el alcance definido dentro de su SGSI es el de sistema de la información que da soporte a los servicios de Central de Compras.

## 3. OBJETIVO

Esta política tiene como objetivo principal asegurar la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios, junto con la tecnología y los activos de información de la Organización.

Los objetivos genéricos que la Organización ha establecido son:

- Proporcionar la confianza a los Socios protegiendo su información durante todo su ciclo de vida.
- Facilitar la mejora continua de los procesos de seguridad, procedimientos, productos y servicios.
- Cumplir los requisitos legales de negocio y otros requisitos de Socios (explícitos e implícitos) relacionados con seguridad de la información.
- Garantizar la Continuidad del Negocio estableciendo proyectos de contingencia en los servicios críticos manteniendo en todo momento la seguridad.
- Garantizar que se provean los recursos necesarios para garantizar la seguridad, así como asignar funciones y responsabilidades a todo el personal de la Organización.
- Concienciar, formar y motivar al personal de la Organización sobre la importancia del desarrollo e implantación del Sistema de Gestión de la Seguridad de la Información para poder cumplir con los objetivos estratégicos de negocio y su implicación para su correcta consecución.

## 4. COMPROMISO DE LA DIRECCIÓN

Esta política expone los compromisos adquiridos por la alta dirección en materia de Seguridad de la Información. En concreto, LOGRAR UN ALTO NIVEL DE SEGURIDAD PARA NUESTROS SOCIOS, para ello:

- Garantizamos la seguridad de los activos de nuestros Socios: el patrimonio informacional que nos confían nuestros Socios debe ser protegido contra toda alteración, perdida, daño, divulgación o acceso no autorizado.
- Aseguramos un alto nivel de seguridad en los servicios que realizamos para nuestros Socios.
- Afianzamos la conformidad del SGSI con objeto de minimizar los riesgos para nuestros Socios.
- Fomentamos una cultura de seguridad de la información de toda la Organización.
- Gestionamos los incidentes de seguridad con objeto de limitar los impactos para la Organización y nuestros Socios.

## 5. MARCO LEGAL

El marco legal y regulatorio en el que desarrollamos nuestra actividad es:

- 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 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

## 6. PRINCIPIOS Y DIRECTRICES

La Organización depende, entre otros, de los sistemas TIC (Tecnologías de Información y Comunicación) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

## 6.1 Misión y Objetivos

En la Organización, desarrollamos, al menos, los siguientes objetivos:

- Utilización de recursos TIC corporativos, tales como el correo electrónico, el acceso a Internet, el equipamiento informático y de comunicaciones.
- Gestión de activos de información inventariados, categorizados y asociados a un responsable.
- Mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
- Seguridad física, de forma que los activos de información serán emplazados en áreas seguras, protegidos por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
- Seguridad en la gestión de comunicaciones y operaciones, de manera que la información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
- Control de acceso, limitando el acceso a los activos de información por parte de usuarios, procesos y sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.
- Adquisición, desarrollo y mantenimiento de los sistemas de información contemplando los aspectos de seguridad de la información en todas las fases del ciclo de vida de dichos sistemas.
- Gestión de los incidentes de seguridad implantando mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- Gestión de la continuidad implantando mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y manteniendo la continuidad de sus procesos de negocio.

## 6.2 Prevención

Para defenderse de las amenazas, los distintos departamentos de la Organización deben aplicar las medidas mínimas de seguridad, así como cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del servicio.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse ante incidentes.

Para garantizar el cumplimiento de esta política, los diferentes departamentos de la Organización deben:

- Autorizar los sistemas antes de entrar en operación.

- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Cuando existen requisitos especiales de seguridad en alguno de los servicios, la alta Dirección se lo comunicará al Departamento de Sistemas para su análisis e implementación.

### 6.3 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continuada para detectar anomalías en la prestación de sus servicios y actuar en consecuencia.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

### 6.4 Respuesta

La Organización y todos sus Departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente.

### 6.5 Recuperación

Para garantizar la disponibilidad de los servicios críticos, la Organización debe desarrollar un plan de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

## 7. ORGANIZACIÓN DE LA SEGURIDAD

La implantación de esta Política de Seguridad requiere que todos los miembros de la Organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado.

Como parte de esta Política, los principales roles quedan identificados y detallados del modo siguiente: Responsable de Seguridad y Responsable de Sistemas.

- La alta Dirección, será el encargado de aprobar la presente política y el responsable de la autorización de sus modificaciones, así como de toda la información documentada del SGSI de la entidad.
- El **Responsable de Seguridad** será quien tome las decisiones adecuadas para satisfacer los requisitos de seguridad de la información y de los servicios. Dispondrá de las siguientes funciones:
    - Supervisar el cumplimiento de la presente Política, sus normas y procedimientos derivados.

- Asesorar en materia de seguridad a los integrantes Comité de Seguridad que así lo requieran.
- Notificar la presente política a todo el personal de los cambios que en ella se produzcan.
- Coordinar las acciones de implantación, mantenimiento y mejora del SGSI de la Organización y de sus auditorias, junto con el Responsable de Sistemas.

– El **Responsable de Sistemas**, que se encargará de gestionar los requisitos técnicos y de seguridad de los sistemas de información.

– Todo el **personal de la Organización**, tanto interno como externo, será responsable de cumplir con la presente Política de Seguridad de la Información dentro de su área de trabajo, así como de aplicar toda la información documentada de los controles y medidas de seguridad del SGSI de la Organización en sus actividades laborales que afecta a su desempeño en seguridad de la información.

## 8. DIFUSIÓN, ACTUALIZACIÓN Y REVISIÓN DE LA POLÍTICA

Será misión de la alta Dirección, la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma.

La Política será aprobada por la alta Dirección de la Organización y será difundida para que la conozcan todas las partes afectadas.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la Organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

## 9. ESTRUCTURA DE LA DOCUMENTACIÓN

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de la documentación generada.

La documentación sobre la que se soporta esta política estará compuesta por un conjunto de normas, procedimientos, buenas prácticas y guías que ayudarán a los usuarios en el desarrollo de sus tareas.

## 10. DATOS DE CARÁCTER PERSONAL

El 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 y la legislación española en vigor, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, define las condiciones en las que el tratamiento de datos personales se puede hacer.
Otorga a las personas afectadas por el tratamiento el derecho a acceder y corregir los datos registrados en su cuenta.

La Organización solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos, y estos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativa necesarias para el cumplimiento de la normativa de Protección de

Datos. Estas medidas estarán recogidas en las políticas, normativas y procedimientos que emanan de la presente política de seguridad.

## 11. GESTÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, la Organización, establecerá una valoración de referencia para los diferentes tipos de información que manejan.

La gestión de riesgos quedará documentada en un Plan de análisis y gestión de riesgos.

## 12. PROCESO DISCIPLINARIO

En virtud de las disposiciones legales aplicables, todos los trabajadores y directivos de CALIDALIA deben desarrollar sus funciones profesionales atendiendo y respetando la Ley, así como las políticas y normativas internas que se hayan establecido en la Compañía para prevenir cualquier actuación antijurídica y/o delictiva en nuestra organización.

En este sentido, constituye un deber imperativo para todos los trabajadores y directivos de CALIDALIA actuar en todo momento guiados por los principios de ética, integridad, legalidad y transparencia en todos sus actos, y de acuerdo con lo dispuesto en el Código de Conducta de CALIDALIA, el cual se debe leer, comprender y tener siempre presente adaptándolo al desarrollo de las funciones laborales que cada uno tenga asignadas.

Asimismo, al objeto de prevenir o, en su caso, detectar cualquier conducta irregular que pudiera tener lugar en cualquiera de los niveles jerárquicos, se impone el deber de todos los trabajadores y directivos de CALIDALIA, de informar y denunciar a través de los procedimientos establecidos en el Canal de Denuncias implantado en nuestra organización, los posibles riesgos o incumplimientos de la Ley, del Código de Conducta, de cualquier otra normativa interna o protocolo de actuación implantado por CALIDALIA y/o de cualquier actuación que pudiera ser considerada antijurídica o delictiva.

Cualquier incumplimiento de las referidas normativas y políticas internas y/o de la Ley en el desarrollo de las funciones profesionales, se reputará como un incumplimiento laboral susceptible de ser sancionado, de conformidad con lo dispuesto en el artículo 54 del Estatuto de los Trabajadores, el cual dispone que “se considerarán incumplimientos contractuales: la indisciplina o desobediencia en el trabajo, la transgresión de la buena fe contractual, así como el abuso de confianza en el desempeño del trabajo”.

## 13. TERCERAS PARTE

Cuando la Organización utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política y de la Normativa de Seguridad que ataña a dichos servicios o información.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Si fuera necesario, se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

## 14. FORMACIÓN Y CONCIENCIACIÓN

Con carácter anual se realizará una acción de formación y concienciación en materia de seguridad. El objetivo de la acción formativa y de concienciación es doble:

- Mantener informado al personal más directamente relacionado con el manejo de información y los sistemas que la tratan sobre los procedimientos existentes de seguridad, riesgos, medidas de protección, planes de protección, etc.
- Concienciar al personal, en general, de la importancia de la seguridad y de los procedimientos básicos de manejo e intercambio de información.

## 15. TELETRABAJO

La presente política y sus procedimientos, normas y disposiciones asociadas serán de aplicación, y por lo tanto de obligado cumplimiento, para todo el personal de la Organización que se encuentre en la modalidad de teletrabajo.

## 17. INVESTIGACIÓN DE ANTECEDENTES

La comprobación de antecedentes de todos los candidatos al puesto se debe llevar a cabo de acuerdo con las leyes, normas y códigos éticos que sean de aplicación y debe ser proporcionales a las necesidades del negocio y la clasificación de la información a la que se accede y los riesgos percibidos.

## 18. RESPONSABILIDADES DE GESTIÓN

La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la Organización.

## 19. APROBACIÓN Y ENTRADA EN VIGOR

La presente Política de Seguridad de la Información será aprobada por la Alta Dirección mediante firma y será difundida a sus partes interesadas.

Así mismo, la alta Dirección dotará de los recursos necesarios para la aplicación efectiva de esta política, y para su buen desarrollo, tanto en las actividades de implantación como en su posterior mantenimiento y mejora de todo el SGSI de la Organización.