# POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SDG-SGSI-DOC-05-01-Política de Seguridad y Privacidad de la Información

CLASIFICACIÓN: USO INTERNO

# Control del documento

## A. Aprobación

| | |
|---|---|
| Fecha: | **26/03/2025** |
| Nombre: | Comité de Seguridad |
| Cargo: | |

## B. Control de cambios

Según control de versiones de la herramienta ofimática utilizada.

## C. Lista de distribución

| |
|---|
| Todo el personal de la empresa |
| |
| |

# Tabla de contenido

# 1. Introducción y aspectos generales

SDG CONSULTING, depende de los sistemas TIC (Tecnologías de la Información y las Telecomunicaciones) para alcanzar sus objetivos de negocio. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad de la información tratada o los servicios prestados y estando siempre protegidos contra las amenazas o los incidentes con potencial para incidir en la confidencialidad, integridad y disponibilidad de la información

Por tanto, para SDG CONSULTING, el objetivo de la Seguridad de la Información es garantizar la seguridad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier vulnerabilidad, amenaza o posible evento de seguridad y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible, con la aplicación de las medidas necesarias.

Por todo ello, SDG CONSULTING establece que la denominación de Sistema de Gestión de Seguridad de la Información comprenderá el cumplimiento de las normativas ISO 27001 y TISAX, adhiriéndose por lo tanto a las medidas mínimas de seguridad exigidas por dicha/s normativa/s, teniendo presente que la seguridad es una parte integral de cada etapa del sistema, desde su concepción y diseño hasta su retirada de servicio.

# 2. Alcance

Esta Política es aplicable a quienes tengan acceso a los recursos que hayan sido identificados como "activos de información" de la empresa, dentro del alcance formal definido en SDG-SGSI-DOC-04-1-Contexto, requisitos y alcance del SGSI. Dichos requisitos de protección afectan a toda la información en soporte electrónico o físico, y a los sistemas de información propiedad de SDG CONSULTING o gestionados por la empresa.

Todo el personal tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y su Normativa de Seguridad derivada, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue al personal afectado.

# 3. Referencias

| | |
|---|---|
| **Marco legal y Regulatorio** | • https://www.boe.es/eli/es/rd/2022/05/03/311/con<br>• 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 por el que se deroga la Directiva 95/ 46/ CE (Reglamento general de protección de datos) (boe.es)<br>• https://www.boe.es/eli/es/lo/2018/12/05/3<br>• ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements<br>• DOC-SGSI Legislación |
| **Norma y controles:** | • Norma UNE-EN ISO/IEC 27001:2023<br>o Control 5.1 Políticas para la seguridad de la información<br>o Apartado 9.2 Auditoría interna<br>• Norma ISO19011 "Directrices para la auditoría de los sistemas de gestión de la calidad y/o medioambiental" |

# 4. Glosario

| Concepto | Significado |
|---|---|
| Activo de información | Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. |
| Confidencialidad | Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. |
| Disponibilidad | Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. |
| Integridad | Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. |
| Amenaza | Cualquier evento o acción que, explotando una vulnerabilidad, pueda afectar a la confidencialidad, integridad o disponibilidad de la información causando un incidente de seguridad. |
| Incidente de Seguridad | Cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información. Esto puede incluir accesos no autorizados, pérdida de datos, ataques cibernéticos, y cualquier otra actividad que ponga en riesgo los activos de información. |

## 5. Actores y Responsabilidades

El documento SDG-SGSI-NS-05-01-Funciones y Responsabilidades de Seguridad de la Información establece todos los roles del SGSI y sus responsabilidades.

## 6. Decálogo de Principios básicos

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

1. Alcance estratégico: La dirección de SDG CONSULTING mostrará su compromiso y apoyo con la seguridad de la información, de forma que el SGSI esté coordinado e integrado con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.

2. Eficacia e Integridad de la Información: SDG CONSULTING se asegurará de que toda la información utilizada sea necesaria, suficiente, exacta y útil, y que se mantendrá disponible para el desarrollo de la actividad de la empresa, evitando redundancias y asegurando su relevancia.

3. Eficiencia en el procesamiento: Optimizar el uso de recursos humanos y materiales para el procesamiento de la información, garantizando que se realice de manera ágil y con el menor costo posible.

4. Responsabilidad determinada: Todos los roles que intervienen en el Sistema de Gestión de Seguridad de la Información (SGSI) se identificarán en la normativa donde se detallarán sus responsabilidades y requisitos mínimos. Se garantizará además que todas las partes interesadas son conscientes y responsables de tutelar la seguridad de los sistemas de información y de las acciones que se puedan emprender para reforzar la misma.

5. Privacidad de la Información Personal y de los datos confidenciales: Asegurar la seguridad en la recogida, uso, conservación, divulgación y eliminación de información personal y datos clasificados por SDG CONSULTING como confidenciales o secretos, cumpliendo con la normativa de protección de datos y la normativa de seguridad propia de la empresa.

6. Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos de SDG CONSULTING, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño hasta el fin de su ciclo de vida. Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

7. Cumplimiento legal y normativo: Asegurar que toda la información y los medios que la contienen, procesan y/o transportan cumplan con las regulaciones legales vigentes en cada ámbito, evitando sanciones y riesgos legales, pero además asegurando también el cumplimiento de las normas y certificaciones que SDG CONSULTING ha establecido aplicar.

8. Gestión de Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

9. Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información, y de los procesos y servicios afectados.

10. Mejora continua: Las medidas de seguridad se evaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

# 7. Objetivos de seguridad de la información

SDG CONSULTING establece como objetivos de la seguridad de la información los siguientes:

- Garantizar la calidad y protección de la información.

- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.

- Gestión de activos de información: Los activos de información de SDG CONSULTING se encontrarán inventariados y categorizados y estarán asociados a un responsable.

- Seguridad ligada a las personas: Se implantarán los 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 su uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.

- Seguridad física: Los activos de información serán, en la medida de lo posible, emplazados en áreas seguras, protegidas 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: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. 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: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

- Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

- Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

- Garantizar la prestación continuada de los procesos y servicios: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.

- Protección de datos: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad.

- Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

## 8. Datos personales

SDG CONSULTING sólo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y éstos 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 organizativas necesarias para el cumplimiento de la normativa de Protección de Datos.

## 9. Terceras partes

Cuando SDG CONSULTING preste servicios a otros organismos o maneje información de otros organismos, se les hará participe de esta Política de Seguridad de la Información. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.
Cuando SDG CONSULTING utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad 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. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.
Cuando algún aspecto de esta Política de Seguridad de la Información no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

## 10. Gestión de Riesgos

Todos los activos de información afectados por la presente Política de Seguridad de la Información están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos.
Este análisis se repetirá mínimo una vez al año, y siempre que cambien la información y/o los servicios manejados de manera significativa y/o cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.
El Responsable de la Seguridad será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información. Por su parte, el Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.
SDG CONSULTING dispone de una norma aprobada para el ciclo de gestión de riesgos, en el documento SDG-SGSI-DOC-06-01-Metodología aplicada de Análisis y Gestión de Riesgos

# 11. Gestión de Incidentes de Seguridad

## 9.1 Prevención

Para que la información no se vea perjudicada por incidentes de seguridad, SDG CONSULTING implementa las medidas de seguridad establecidas por TISAX y la ISO 27002, así como cualquier otro control adicional que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de todo el personal, están claramente definidos y documentados.
Para garantizar el cumplimiento de la política SDG CONSULTING:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo el análisis de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros, con el fin de obtener una evaluación independiente.

## 9.2 Detección

SDG CONSULTING establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia (vigilancia continua y reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales, se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

## 9.3 Respuesta

SDG CONSULTING establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Notificación de incidentes y comunicaciones:

## 9.4 Recuperación

Para garantizar la disponibilidad de los servicios, SDG CONSULTING dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

## 10. Mejora continua

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas. Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

1. Revisión de la Política de Seguridad de la Información.
2. Revisión de los procesos, servicios e información y su categorización.
3. Ejecución con periodicidad anual del análisis de riesgos.
4. Realización de auditorías internas o, cuando procedan, externas.
5. Revisión de las medidas de seguridad.
6. Revisión y actualización de las normas y procedimientos.

Anualmente, el Comité de seguridad revisará la política y, si procede, instará a la Alta Dirección a realizar modificaciones sobre la misma.

## 11. Auditoría Interna

La auditoría interna del SGSI tiene por objetivo verificar:

- Si se cumplen los requisitos de la norma internacional así como la legislación y otras normativas aplicables al SGSI.
- Si se cumplen los objetivos de seguridad identificados.
- Si se han implantado y mantienen los controles de forma efectiva.
- Si se están logrando los resultados esperados.

Para ello, todas las actividades de la auditoría interna (Preparar el plan de auditoría interna, Aprobación del plan de auditoría, Realización de las auditorías, Realización del informe de auditoría y Seguimiento y acciones derivadas) se realizarán siguiendo la Norma ISO 19011 - Auditoría de Sistemas de Gestión y la Norma ISO 27001- apartado 9.2 Auditoría interna.

## 12. Declaración de autoridad sobre la Política

El Comité de Seguridad de la Información tiene la autoridad para verificar el cumplimiento de la presente Política de Seguridad y Privacidad, la responsabilidad de hacer cumplir las directrices generales y actuaciones correspondientes contenidas en el mismo y la independencia para plantear acciones correctivas y preventivas necesarias para cumplir los objetivos del plan de tratamiento de riesgos y la mejora continua de la seguridad de la información.

Es responsabilidad de todas las personas y departamentos implicados en los procesos o servicios incluidos en el alcance el obligado cumplimiento de la presente Política de Seguridad y Privacidad. Para conseguir este propósito es necesaria la implicación y participación de todos los empleados de SDG CONSULTING.

También podrá requerir la participación de proveedores y terceros en la aplicación de las medidas de seguridad que se determinen como mínimos exigibles.

El Comité de Seguridad es responsable de la Política de Seguridad y Privacidad, y deberá realizar la revisión periódica en respuesta a los cambios en la normativa, legislación y/o requisitos contractuales, a los cambios de estrategia de negocio, o del entorno de la organización, ya sea a nivel técnico, organizativo, o en lo concerniente a las amenazas actuales y previstas para la seguridad de la información, así como por el conocimiento adquirido gracias al estudio de los eventos e incidentes que puedan haber ocurrido y al análisis de los resultados de las auditorías internas y externas realizadas. En todo caso, dicha revisión se realizará como mínimo una vez al año.

En caso de que se detecte un uso indebido que atente contra la seguridad de la empresa, contra la normativa vigente -especialmente en materia de protección de datos-, o bien que contravenga la presente Política de Seguridad, la empresa podrá tomar las medidas correctoras o sanciones disciplinarias oportunas en función de la gravedad de la infracción, así como proceder a registrar el contenido de los equipos afectados si fuere necesario, siempre respetando el contenido del artículo 18 del Estatuto de los Trabajadores.