# PO.SG.SCL-1

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

| CONTROL DE MODIFICACIONES | | | |
|---|---|---|---|
| **Edición** | **Fecha** | **Aptdo.** | **Descripción de la Modificación** |
| 1 | 1/02/2018 | | Edición Inicial |
| 2 | 4/05/2018 | | Se ha incluido la política de mesas y pantallas limpias |
| 3 | 1/10/2021 | | Clasificación del documento |
| 4 | 1/11/2021 | | Sustituye en su totalidad a la revisión anterior |
| 5 | 15/12/21 | | Modificación de la clasificación del documento |
| 6 | 01/07/23 | | Cambio denominación social de la empresa |

| **Aprobado por:** |
|---|
| Managing Director |
|  <br>Manuel Castillo |

## 1. INTRODUCCIÓN

SCALIAN CONSULTING SPAIN, S.L., en adelante SCALIAN SPAIN, tiene una gran cantidad de información sensible en la que se basa su rendimiento, sostenibilidad, seguridad y capacidad para mantener y desarrollar sus actividades y resultados.

Este patrimonio de información cubre:

- Información sobre preventa, producción y gestión, necesaria para el funcionamiento de las distintas entidades del grupo,
- Patrimonio intelectual, compuesto por toda la información que se atesora en el conjunto con el conocimiento y el know-how del grupo,
- Información sobre sus clientes o los terceros con los que está en contacto, cuya alteración o divulgación podría dañar su imagen de marca, la de sus clientes 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 SCALIAN SPAIN para proteger los activos de la información de la amplia gama de amenazas (fraude, espionaje, accidentes, errores humanos, etc.), con el fin de establecer la confianza de nuestros clientes, cumplir con los marcos legales y reglamentarios y con los objetivos de SCALIAN SPAIN en seguridad de la información.

Esta política es la piedra angular del programa global de seguridad de la información de SCALIAN SPAIN, 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. Garantiza: disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de la información.

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

La política está accesible para cualquier empleado de SCALIAN SPAIN a través de la intranet y a través de la Dirección de Seguridad para cualquier parte interesada que lo solicite.

## 2. ALCANCE

Esta política es un documento aplicable a todas las Áreas y a todo el personal de SCALIAN SPAIN, y para todos sus Centros de trabajo.

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 SCALIAN SPAIN, es decir, todos los medios para crear, adquirir, procesar, almacenar, distribuir o destruir Información:

- Información: Cualquier dato almacenado en formato electrónico o en papel perteneciente a SCALIAN SPAIN, empleados, proveedores o de sus clientes,
- 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 SCALIAN SPAIN, subcontratistas, colaboradores, etc.),
- Ubicaciones: todos los emplazamientos de SCALIAN SPAIN 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.).

## 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 SCALIAN SPAIN.

Los objetivos genéricos que SCALIAN SPAIN ha establecido son:

- Proporcionar la confianza a los clientes 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 clientes (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 SCALIAN SPAIN.
- Concienciar, formar y motivar al personal de SCALIAN SPAIN 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 CLIENTES, para ello:

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

## 5. MARCO LEGAL

El marco legal y regulatorio en el que desarrollamos nuestras actividades 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 3/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad modificado por el Real Decreto 951/2015, de 23 de octubre
- 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.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

## 6. PRINCIPIOS Y DIRECTRICES

SCALIAN SPAIN depende 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 SCALIAN SPAIN somos una Comunidad de expertos con talento con la misión de ayudar a nuestros clientes a transformar los silos de información, la complejidad de los datos y los procesos de digitalización en verdaderas oportunidades de negocio que les ayuden a tomar mejores decisiones, ser más eficientes y desarrollar mejores productos y servicios.

EN SCALIAN SPAIN 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, las distintas Áreas y Departamento de SCALIAN SPAIN deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema.

Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en las ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

Para garantizar el cumplimiento de la política, los departamentos 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.

### 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 los servicios y actuar en consecuencia según lo establecido en el art. 8 y art. 9 del ENS.

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

SCALIAN SPAIN y todas sus Áreas y 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, las Áreas y Departamentos de SCALIAN SPAIN deben desarrollar planes 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 en SCALIAN SPAIN 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, Responsable de la Información, Responsable del Servicio y Responsable de Sistemas.

- El **Comité de Seguridad** será el órgano encargado de aprobar la política y será el responsable de la autorización de sus modificaciones, así como de toda la información documentada del SGSI/ENS 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, de sus normas y procedimientos derivados.
    - Asesorar en materia de seguridad a los integrantes Comité de Seguridad que así lo requieran.
- El **Responsable de la Información**, será el encargado de notificar la presente política a todo el personal de SCALIAN SPAIN y de los cambios que en ella se produzcan, así como de coordinar las acciones de implantación, mantenimiento y mejora del SGSI/ENS 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 de seguridad de los sistemas de información
- El **Responsable del Servicio**, se encargará de gestionar los requisitos de seguridad de las actividades de su área para la prestación de los servicios.
- Todo el **personal de SCALIAN SPAIN**, 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/ENS de SCALIAN SPAIN en sus actividades laborales que afecta a su desempeño en seguridad de la información.

## 8. NOMBRAMIENTOS Y RESOLUCIÓN DE CONFLICTOS

La coordinación se lleva a cabo en el seno del Comité de Dirección de SCALIAN SPAIN, que podrá delegar en el Comité de Seguridad.

Los nombramientos los establece la alta Dirección de SCALIAN SPAIN y se revisan cada 2 años o cuando un puesto queda vacante.

Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité de Seguridad y prevalecerá en todo caso el criterio de la Dirección ejecutiva.

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

Será misión del Comité de Seguridad 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 SCALIAN SPAIN 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.

## 10. 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, guías y procedimientos que ayudarán a los usuarios en el desarrollo de sus tareas.

## 11. 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.

SCALIAN SPAIN ha designado un rol, Data Protection Officer, cuya misión es garantizar el cumplimiento de dichas disposiciones.

Antes de realizar cualquier tratamiento, es obligatorio que el responsable/encargado del tratamiento consulte con el DPO.

SCALIAN SPAIN 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.

## 12. 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, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información que manejados y los diferentes servicios prestados.

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.

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

## 13. INCUMPLIMIENTOS

SCALIAN SPAIN podrá tomar las medidas adecuadas contra toda aquella persona que contravenga la presente Política de Seguridad y que derive en una amenaza para el negocio y/o mantenimiento de la actividad o en una violación de las normativas legales y/o acuerdos contractuales a los que SCALIAN SPAIN estuviese obligado.

El nivel y grado de las medidas dependerá de la naturaleza, intencionalidad y alcance de lo contravenido.

Tanto en el caso de relaciones laborales como de otra naturaleza, SCALIAN SPAIN se reserva el derecho de emprender acciones legales, independientemente de la rescisión de la relación contractual, en función del daño causado a la empresa.

## 14. TERCERAS PARTE

Cuando SCALIAN SPAIN 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.

Cuando algún aspecto de la Política 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.

## 15. 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.

## 16. 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 SCALIAN SPAIN que se encuentre en la modalidad de Teletrabajo

## 17. 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 las partes interesadas de SCALIAN SPAIN.

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/ENS de SCALIAN SPAIN.