

Política de Gestión de la Seguridad de la Información

1. Introducción	2
2. Propósito	2
3. Alcance	2
4. Marco Normativo y de Referencia.....	3
5. Principios de Seguridad de la Información	3
6. Organización de Seguridad.....	4
7. Comité de Seguridad	5
8. Gestión Basada en Riesgos.....	5
9. Protección de Infraestructuras y Servicios Críticos	6
10. Gestión de Terceros y Cadena de Suministro.....	6
11. Cultura Organizativa, Formación y Concienciación.....	6
12. Mejora Continua y Supervisión.....	7
13. Registro de cambios	7
14. Aprobación y vigencia.....	7

1. Introducción

Grupo Solarig, una empresa multinacional especializada en el desarrollo, financiación, construcción y operación de proyectos renovables y soluciones energéticas sostenibles reconoce que, la información y los sistemas que la soportan constituyen activos estratégicos esenciales para la sostenibilidad del negocio, la continuidad operativa y la confianza de nuestras partes interesadas. Por eso establece la presente Política Corporativa de Seguridad de la Información como marco estratégico y de gobernanza que rige la protección de la información y de los servicios críticos del Grupo en todas las jurisdicciones en las que opera.

La Alta Dirección de Solarig asume la responsabilidad última del establecimiento, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información y se compromete a:

- Integrar la seguridad de la información en la estrategia corporativa y en la gestión global de riesgos.
- Proveer los recursos humanos, técnicos y financieros necesarios.
- Designar responsabilidades claras en materia de ciberseguridad y resiliencia digital.
- Supervisar periódicamente el desempeño del Sistema de Gestión de Seguridad de la Información.
- Impulsar una cultura organizativa basada en la seguridad y la gestión responsable de la información.

2. Propósito

Esta Política define los principios y directrices que rigen la gestión y protección de la información en todas las sociedades, líneas de negocio, filiales y países donde opera la organización.

Su objetivo es garantizar que la información sea protegida de manera adecuada durante todo su ciclo de vida, asegurando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

3. Alcance

Esta Política constituye el marco de referencia del Sistema de Gestión de la Seguridad de la Información y es de obligado cumplimiento para todas las sociedades, filiales, unidades de negocio, proyectos y centros operativos bajo el control del Grupo Solarig, independientemente del país en el que desarrollen su actividad.

El alcance comprende toda la información gestionada por la organización, cualquiera que sea su formato o soporte —digital, físico o verbal—, así como los sistemas de información, infraestructuras tecnológicas, redes, plataformas en la nube, aplicaciones corporativas y entornos industriales o tecnológicos asociados a la operación de activos energéticos, incluidos los sistemas de control industrial y operación remota cuando resulten aplicables.

La Política es vinculante para empleados, directivos, miembros de órganos de gobierno, contratistas, proveedores, colaboradores y cualquier tercero que tenga acceso a información o sistemas de la organización.

4. Marco Normativo y de Referencia

El Sistema de Gestión de la Seguridad de la Información de Solarig se establece y mantiene conforme a:

- ISO/IEC 2700 Seguridad de la información, ciberseguridad y protección de la privacidad
- 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 (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Real Decreto 311/2022, de 3 de Mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS2)
- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Regulaciones sectoriales energéticas aplicables en los países de operación.
- Compromisos contractuales y estándares internacionales reconocidos.

5. Principios de Seguridad de la Información

Solarig se compromete a garantizar los principios fundamentales de la seguridad de la información:

- **Confidencialidad:** La información solo será accesible a personas, entidades o sistemas debidamente autorizados, bajo el principio de mínimo privilegio y necesidad de acceso. Se implementarán acuerdos de confidencialidad (NDA) con empleados y

terceros, controles de acceso a sistemas y documentación sensible, y políticas de clasificación de la información.

- **Integridad:** La información será protegida frente a alteraciones no autorizadas, pérdidas accidentales o manipulaciones indebidas, asegurando su exactitud y fiabilidad.
- **Disponibilidad:** La información y los servicios críticos estarán disponibles en el momento requerido, mediante medidas de resiliencia, continuidad de negocio y recuperación ante incidentes.
- **Autenticidad y Trazabilidad:** Se garantizará la identificación fiable de usuarios y sistemas, así como el registro y trazabilidad de las actividades relevantes, especialmente en servicios esenciales y críticos. Se establecerán mecanismos de monitorización de accesos y transferencias de información, así como análisis de incidentes de seguridad.

6. Organización de Seguridad

La responsabilidad esencial recae sobre la Dirección General de la organización, ya que esta es responsable de organizar las funciones y responsabilidades y de facilitar los recursos adecuados para conseguir los objetivos del ENS. Los directivos son también responsables de dar buen ejemplo siguiendo las normas de seguridad establecidas.

Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándose y poniéndolos en público conocimiento a través de la presente Política Integrada de Sistemas de Gestión.

Los roles o funciones de seguridad definidos son:

Función	Deberes y responsabilidades
Responsable de la información (RINFO)	Tomar las decisiones relativas a la información tratada
Responsable de los servicios (RSER)	- Coordinar la implantación del sistema - Mejorar el sistema de forma continua
Responsable de la seguridad (RSEG o CISO)	- Determinar la idoneidad de las medidas técnicas - Proporcionar la mejor tecnología para el servicio
Responsable del sistema (RSIS)	- Coordinar la implantación del sistema - Mejorar el sistema de forma continua
Dirección	- Proporcionar los recursos necesarios para el sistema - Liderar el sistema
Administrador de Seguridad (AS)	Implantación, gestión y mantenimiento de las medidas de seguridad.

Esta definición de deberes y responsabilidades se completa en los perfiles de puesto y en los documentos del sistema Registro de responsables, roles y responsabilidades.

Resolución de conflictos:

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 General.

7. Comité de Seguridad

El procedimiento para su designación y renovación será la ratificación en el comité de seguridad.

El comité para la gestión y coordinación de la seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité

Estos miembros son designados por el comité, único órgano que puede nombrarlos, renovarlos y cesarlos.

El comité de seguridad es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento de nuestra empresa.

La organización de la Seguridad de la información se desarrolla en el documento complementario a esta Política de Organización de la Seguridad

Esta política se complementa con el resto de las políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión.

8. Gestión Basada en Riesgos

La seguridad de la información en Solarig se gestiona bajo un enfoque sistemático basado en riesgos, integrando la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar a los activos de información y a los servicios esenciales del negocio. Se identifican y evalúan amenazas internas y externas, riesgos tecnológicos (incluyendo daños informáticos, ciberataques y accesos no autorizados a sistemas), riesgos asociados a terceros (proveedores, contratistas y socios), riesgos derivados del contexto geopolítico y regulatorio en cada país de operación, así como riesgos relativos al descubrimiento y revelación de secretos empresariales e información confidencial. Se evalúan igualmente los impactos operativos, financieros, legales y reputacionales de cada riesgo identificado.

La organización adopta medidas de prevención, detección, respuesta y recuperación proporcionales al nivel de riesgo identificado, incluyendo controles de ciberseguridad, control de accesos, monitorización de sistemas, auditorías IT y canales de denuncia interna. Se refuerza la resiliencia digital y la continuidad de las operaciones, en coherencia con los principios exigidos por ISO 27001, ENS y NIS2.

9. Protección de Infraestructuras y Servicios Críticos

En atención a la naturaleza estratégica del sector energético, la organización implementa medidas específicas para proteger tanto los entornos tecnológicos corporativos (IT) como los sistemas industriales u operacionales (OT) que soportan la generación, monitorización y operación de activos energéticos.

Se establecen controles de seguridad lógica y física, mecanismos de segmentación de redes, gestión de accesos, supervisión continua y planes de continuidad de negocio y recuperación ante desastres, orientados a minimizar el impacto de incidentes de seguridad. Ante incidentes de seguridad se implementarán medidas de investigación interna, medidas disciplinarias cuando proceda, revisión y refuerzo de controles, y actualización de políticas y procedimientos. Los incidentes que puedan afectar de manera significativa a la prestación de servicios esenciales serán gestionados conforme a los procedimientos establecidos y notificados, cuando proceda, a las autoridades competentes en los plazos legalmente establecidos.

10. Gestión de Terceros y Cadena de Suministro

La organización reconoce que la seguridad de la información debe extenderse a su cadena de suministro y a las relaciones con terceros. Por ello, integra criterios de ciberseguridad, protección de la información y debida diligencia en los procesos de selección, contratación, homologación y evaluación periódica de proveedores, contratistas y socios estratégicos.

Los contratos incorporarán cláusulas específicas relativas a confidencialidad, protección de la información, continuidad del servicio, gestión de incidentes, cumplimiento normativo y compliance. Se establecerán mecanismos de auditoría de terceros y, en caso de incumplimiento grave, se aplicarán medidas que podrán incluir la rescisión de la relación contractual, garantizando un nivel adecuado de seguridad en las relaciones con terceros.

11. Cultura Organizativa, Formación y Concienciación

Grupo Solarig promueve una cultura corporativa basada en la responsabilidad individual y colectiva respecto a la protección de la información y la prevención de conductas ilícitas. Para ello, se desarrollan programas periódicos de formación y concienciación adaptados a los distintos niveles de responsabilidad y exposición al riesgo, con especial énfasis en la protección de información confidencial, uso adecuado de sistemas y el deber de comunicar conductas irregulares a través del canal ético.

La seguridad de la información es considerada una obligación profesional inherente a cada función dentro de la organización. Por eso se promueven programas continuos de formación y sensibilización para:

- Fomentar una cultura de ciberseguridad.
- Reducir riesgos derivados del factor humano, incluyendo la prevención de revelación no autorizada de información confidencial.
- Garantizar el conocimiento de responsabilidades individuales.

- Promover el uso responsable del canal ético como herramienta fundamental para la detección y comunicación de conductas irregulares o incidentes de seguridad de la información.

12. Mejora Continua y Supervisión

El Sistema de Gestión de Seguridad de la Información es objeto de seguimiento continuo mediante auditorías internas, auditorías IT, revisiones por la Dirección, evaluación periódica de riesgos, revisión de permisos de acceso, y análisis de incidentes de seguridad de la información.

La organización se compromete a mejorar de forma continua la eficacia del sistema, adaptándolo a la evolución tecnológica, a las nuevas amenazas y a los cambios regulatorios o estratégicos que puedan afectar a su actividad.

La gestión de nuestro sistema se encomienda al Responsable de Sistemas Informáticos y el sistema estará disponible en nuestro sistema de información en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento en vigor de gestión de los accesos.

La documentación referida a la seguridad del sistema se encuentra estructurada en carpetas dentro del servidor de ficheros de la compañía, dividido en subcarpetas nombradas por puntos de norma y marcos de operación, las cuales recogen los distintos procedimientos, registros y evidencias, con acceso restringido para el personal de la compañía, no pudiendo acceder personal externo no autorizado.

La Política se integra en el Sistema Integrado de Gestión del Grupo, alineado con los estándares internacionales ISO 9001, ISO 14001, ISO 45001, ISO 27001 e ISO 37001, reforzando el compromiso corporativo con la excelencia operativa, la sostenibilidad, la ética y la resiliencia empresarial.

13. Registro de cambios

Edición	Fecha	Punto y motive de la modificación
00	01/03/2022	Primera edición
01	19/03/2026	Revisión política - certificaciones

14. Aprobación y vigencia

La presente **Política de Gestión de la seguridad de la información** entrará en vigor en la fecha de su aprobación por el **Comité de Asuntos Corporativos de Solarig Global Services, S.A.**

Se comunica formalmente a los grupos de interés relevantes y se pone a disposición de todas las partes internas y externas a las que resulta de aplicación.

La Política permanecerá vigente hasta que su derogación sea aprobada por la Comisión de Auditoría Sostenibilidad y Mejora Continua o sea reemplazada por una nueva versión.

Fecha de aprobación: 19 de marzo de 2026