POL Política de seguridad de la información

Historial de versiones

Versión	Fecha	Autor	Aprobado por
1	14/07/2026	Fernando Gómez López	Jorge Vázquez González

Índice

- Propósito
- Ámbito de aplicación
- Referencias normativas
- Términos y definiciones
- Roles y responsabilidades
- Comité de Seguridad de la Información: funciones y responsabilidades
- Roles de seguridad: funciones y responsabilidades
- Procedimientos de designación
- Resolución de conflictos
- Objetivos de seguridad de la información
- Principios fundamentales de seguridad de la información
- Tratamiento de datos personales en la organización
- Gestión de riesgos
- Desarrollo de la política de seguridad de la información
- Obligaciones del personal
- Terceros, prestadores de servicios y proveedores de soluciones
- Gestión de incidentes de seguridad
- Protección de activos fuera de las instalaciones
- Archivo y actualización
- Documentos de referencia

Propósito

La Dirección General de Redegal expresa en esta política su compromiso con la protección de la información que la organización trata para sí misma y para sus clientes. La política es el documento marco del Sistema de Gestión Integrado (SGI), que Redegal mantiene conforme a ISO/IEC 27001:2022 y al Real Decreto 311/2022. Establece la misión de seguridad, los objetivos estratégicos y los principios que orientan todas las políticas y procedimientos del SGI.

La organización se compromete a preservar la confidencialidad, la integridad, la disponibilidad, la autenticidad y la trazabilidad de la información y de los servicios que presta. De este modo sostiene la confianza de sus clientes, en particular grandes empresas de distribución, de bienes de consumo y del sector bancario, y apoya el crecimiento del negocio.

Ámbito de aplicación

La política se aplica a la prestación de servicios de marketing y comunicación online, que incluye el desarrollo de páginas web, la gestión de campañas en redes sociales, los servicios de paid media, el diseño e implementación de estrategias de comunicación y el desarrollo de software. Comprende los procesos, los sistemas de información, los activos y los datos que sostienen estos servicios en las sedes de Av. de Santiago, 9, Bajo, 32001 Ourense y de Av. Linares Rivas 56, Bajo, 15005 A Coruña, así como los equipos y la información utilizados fuera de ellas. Afecta a todo el personal, a los colaboradores y a los terceros con acceso a la información o a los sistemas de Redegal. Queda excluida la oficina y filial de México, ya que por ahora solo se certifican las sedes de España.

Referencias normativas

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- Real Decreto 311/2022
- Guías CCN-STIC
- Reglamento (UE) 2016/679
- Ley Orgánica 3/2018
- Real Decreto Legislativo 2/2015

Términos y definiciones

- Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información.

- Confidencialidad: propiedad de la información por la que no se pone a disposición ni se revela a personas, entidades o procesos no autorizados.
- Integridad: propiedad de exactitud y completitud.
- Disponibilidad: propiedad de ser accesible y utilizable a petición de una entidad autorizada.
- Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o en que garantiza la fuente de la que proceden los datos.
- Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
- Riesgo: efecto de la incertidumbre sobre los objetivos.
- Evento de seguridad de la información: ocurrencia que indica una posible brecha de seguridad de la información o un fallo de los controles.
- Incidente de seguridad de la información: uno o varios eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de la organización o comprometer sus operaciones.
- Alta dirección: persona o grupo de personas que dirige y controla una organización al más alto nivel.
- Parte interesada: persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.
- Política: intenciones y dirección de una organización, expresadas formalmente por su alta dirección.

Roles y responsabilidades

- Dirección General: aprueba esta política, asigna los recursos necesarios para el SGI, designa el Comité y los roles de seguridad y adopta la decisión final cuando el Comité no alcanza el consenso.
- Comité de Seguridad de la Información: revisa y propone la política y la normativa asociada, coordina la seguridad y resuelve los conflictos de responsabilidad entre los responsables.
- Responsable de la Información: determina los requisitos de seguridad de la información y aprueba formalmente sus niveles de seguridad, actuando como propietario del riesgo.
- Responsable del Servicio: determina los requisitos y los niveles de seguridad de los servicios prestados y define los servicios críticos.
- Responsable de Seguridad: decide las medidas de seguridad aplicables, supervisa su implantación, aprueba la Declaración de Aplicabilidad y actúa como punto de contacto con las autoridades ante incidentes.
- Responsable del Sistema: desarrolla la implantación técnica de la seguridad en los sistemas de información y supervisa su operación diaria.

- Administrador del Sistema: aplica y mantiene las medidas de seguridad de los sistemas y comunica las anomalías al Responsable del Sistema y al Responsable de Seguridad.
- Responsable del Sistema de Gestión: mantiene la documentación del SGI, coordina su revisión y difusión e informa a la Dirección General sobre su desempeño.
- People&Culture Manager: coordina con el Responsable del Sistema de Gestión la comunicación de esta política al personal y conserva los registros de formación en seguridad.
- Personal: conoce y cumple esta política y comunica de inmediato los eventos de seguridad que observe o sospeche.

Comité de Seguridad de la Información: funciones y responsabilidades

Redegal adopta un modelo de gobierno de la seguridad basado en la diferenciación de responsabilidades, en el que un órgano colegiado coordina la seguridad y unos roles específicos responden de la información, los servicios y los sistemas. La Dirección General constituye el Comité de Seguridad de la Información, que rinde cuentas ante ella y le eleva los riesgos, las necesidades de recursos y las decisiones relevantes.

La composición del Comité refleja los roles de seguridad del modelo:

Miembro	Aportación al Comité
Responsable de la Información	Requisitos y niveles de seguridad de la información
Responsable del Servicio	Requisitos y niveles de seguridad de los servicios
Responsable de Seguridad	Medidas de seguridad, riesgos, incidentes y auditorías
Responsable del Sistema	Implantación técnica y operación de los sistemas
Administrador del Sistema	Estado operativo de las medidas de seguridad

El Comité puede invitar a otros miembros del personal o a colaboradores externos cuando los temas tratados lo requieran.

El Comité se reúne al menos una vez al año y, además, tras un incidente de seguridad grave, ante cambios significativos en los sistemas de información o a petición de cualquiera de sus miembros. Puede reunirse de forma presencial o telemática y deja constancia de cada reunión en un acta. El Comité tiene, entre otras, estas funciones:

- revisar y proponer la política de seguridad de la información para su aprobación por la Dirección General y supervisar el cumplimiento del ENS y de ISO/IEC 27001:2022;
- aprobar las medidas de seguridad, la gestión de riesgos y los planes de tratamiento y de mejora;
- revisar los incidentes de seguridad relevantes y supervisar las auditorías internas y externas;
- aprobar los cambios relevantes que afecten a la seguridad y revisar periódicamente el SGI;
- coordinar al Responsable de la Información, al Responsable del Servicio, al Responsable de Seguridad y al Responsable del Sistema.

Roles de seguridad: funciones y responsabilidades

Cada rol de seguridad tiene asignadas funciones propias, que el MOD Manual de funciones describe en detalle. La organización reconoce al Responsable de la Información como responsable de cada información tratada por el sistema; en Redegal, esta persona ejerce también como Responsable del Servicio.

El Responsable de Seguridad mantiene su independencia respecto del Responsable del Sistema, de modo que quien supervisa la seguridad no es quien opera los sistemas. El Administrador del Sistema actúa bajo las directrices del Responsable del Sistema. Todos los demás puestos incorporan en su descripción deberes de seguridad, como proteger la información, aplicar el mínimo privilegio y comunicar los incidentes.

El organigrama de Redegal no recoge actualmente la figura de Delegado de Protección de Datos. Si la normativa aplicable lo exigiera, la organización lo incorporará a este modelo de roles.

Procedimientos de designación

La Dirección General designa formalmente al Comité de Seguridad de la Información mediante un acta de constitución. Los roles de seguridad se asignan mediante actas de nombramiento, que el People & Culture Director formaliza y que la persona designada firma para aceptar sus funciones.

Los nombramientos permanecen vigentes hasta que la Dirección General los modifique expresamente. Cualquier cambio en la composición del Comité o en la titularidad de un rol se documenta en una nueva acta. En caso de vacante o de ausencia que comprometa el ejercicio de un rol, la Dirección General designa un sustituto por el mismo procedimiento. Son incompatibles las funciones de Responsable de Seguridad y de Responsable del Sistema.

Resolución de conflictos

El Comité de Seguridad de la Información resuelve los conflictos entre los distintos responsables y adopta sus decisiones por consenso. Cuando el consenso no es posible, la

Dirección General toma la decisión final. Los roles que exige la normativa de protección de datos se coordinan con este modelo a través del propio Comité.

Objetivos de seguridad de la información

Redegal presta servicios digitales a empresas que le confían sus datos, sus cuentas publicitarias y sus plataformas de comercio electrónico. Por ello, la organización persigue estos objetivos estratégicos:

- proteger la información de los clientes y de la propia organización frente a accesos, divulgaciones o modificaciones no autorizados;
- garantizar la disponibilidad y la continuidad de los servicios prestados con los niveles que requiere cada cliente;
- cumplir los requisitos legales, reglamentarios y contractuales aplicables a la seguridad de la información, así como los requisitos del ENS y de ISO/IEC 27001:2022;
- integrar la seguridad en el desarrollo del software y de los productos propios;
- consolidar una cultura de seguridad en todo el personal y en los terceros que colaboran con la organización;
- mejorar de forma continua la eficacia del SGI.

Esta política proporciona el marco para fijar los objetivos operativos. El Comité de Seguridad de la Información los establece de forma coherente con estos objetivos estratégicos, los hace medibles mediante indicadores y revisa su grado de cumplimiento en la revisión por la dirección.

Principios fundamentales de seguridad de la información

Las decisiones de seguridad de Redegal se rigen por los principios básicos del Real Decreto 311/2022, que la organización integra con los requisitos de ISO/IEC 27001:2022:

- Seguridad como proceso integral: la seguridad abarca los elementos técnicos, humanos, materiales y organizativos, y la organización evita cualquier actuación puntual o tratamiento coyuntural.
- Gestión de la seguridad basada en los riesgos: las medidas son proporcionales a los riesgos y se justifican por ellos.
- Prevención, detección, respuesta y conservación: la organización previene los incidentes, los detecta a tiempo, responde con rapidez y conserva la información y los servicios.
- Líneas de defensa: la estrategia de protección se articula en varias capas, de modo que el fallo de una medida no compromete el conjunto.
- Vigilancia continua y reevaluación periódica: la organización vigila la actividad de los sistemas para detectar anomalías y reevalúa las medidas de forma periódica.

- Diferenciación de responsabilidades: la responsabilidad de la seguridad se separa de la de explotación de los sistemas.
- Seguridad por defecto y desde el diseño: los sistemas ofrecen solo la funcionalidad necesaria para el servicio y la seguridad se considera desde su concepción.

A estos principios se suma el de responsabilidad compartida: la seguridad compromete a todos los niveles de la organización, desde la Dirección General hasta cada persona que usa la información, y se coordina con las demás iniciativas estratégicas de Redegal.

Tratamiento de datos personales en la organización

Redegal trata datos personales de su personal, de sus clientes, de sus proveedores y de los usuarios de las plataformas que gestiona. La organización se compromete a tratarlos conforme al Reglamento (UE) 2016/679 y a la Ley Orgánica 3/2018, y recoge las actividades de tratamiento en el MOD Registro de tratamientos del responsable.

La organización evalúa los riesgos de cada tratamiento y realiza una evaluación de impacto cuando un tratamiento puede entrañar un alto riesgo para los derechos de las personas. Además, aplica la privacidad desde el diseño y por defecto, según desarrollan la POL Política de protección de PII y la POL Política de privacidad por diseño y por defecto. El tratamiento de estos riesgos se coordina con el del ENS, en especial en el control de los proveedores y en la respuesta a las violaciones de datos personales.

Gestión de riesgos

Redegal adopta un enfoque basado en el riesgo para todos los sistemas sujetos a esta política. La organización analiza sus riesgos al menos una vez al año y, además, cuando cambian la información tratada o los servicios prestados, tras un incidente grave o cuando se detectan vulnerabilidades graves. El PRO Procedimiento de gestión de riesgos define la metodología, las escalas de valoración y el umbral de aceptabilidad.

Los riesgos que superan el umbral de aceptabilidad se tratan con medidas proporcionadas. El Responsable de la Información y el Responsable del Servicio aceptan el riesgo residual dentro de los criterios establecidos, y el Responsable de Seguridad coordina el análisis, el tratamiento y la Declaración de Aplicabilidad.

La organización determina el nivel de seguridad requerido para cada información y cada servicio según los criterios del Anexo I del Real Decreto 311/2022. Las responsabilidades sobre estos niveles se reparten así:

- el Responsable de la Información asigna a cada información su nivel de seguridad en cada dimensión, lo documenta y lo aprueba formalmente, y es el único facultado para modificarlo;
- el Responsable del Servicio asigna y aprueba los niveles de seguridad de los servicios;
- el Responsable de Seguridad determina, a partir de esas valoraciones, la categoría del sistema.

La POL Política de clasificación y etiquetado de la información desarrolla estos criterios y los niveles de clasificación Público, Limitado y Confidencial.

Desarrollo de la política de seguridad de la información

Esta política se desarrolla mediante una normativa de seguridad estructurada en niveles, en la que cada documento detalla el anterior sin contradecirlo:

Nivel	Contenido
Política de seguridad de la información	Misión, objetivos, principios y organización de la seguridad
Políticas específicas	Normas de obligado cumplimiento por materia, como el uso aceptable, la clasificación o la seguridad operativa
Procedimientos	Cómo se realizan las tareas habituales, quién hace qué y cómo se identifican y notifican los comportamientos anómalos
Instrucciones, guías y registros	Pautas operativas, materiales formativos y evidencias de la aplicación del SGI

La Dirección General aprueba esta política, y los demás niveles se aprueban conforme a las reglas del PRO Procedimiento de gestión de información documentada. Este procedimiento regula la elaboración, la aprobación, el control de versiones y el acceso a estos documentos, y el MOD Lista de documentación recoge todos los documentos del SGI. La organización pone la normativa a disposición del personal en el repositorio documental corporativo, con un acceso acorde a su nivel de clasificación y a la necesidad de conocer de cada puesto. Presta especial atención a quienes usan, operan o administran los sistemas de información.

El tratamiento de la información según su nivel de seguridad incluye el control de accesos, el archivo, la copia, el etiquetado de los soportes y la transmisión telemática. Lo desarrollan la POL Política de clasificación y etiquetado de la información, el PRO Procedimiento de gestión y control de accesos lógicos y el PRO Procedimiento de cifrado y gestión de claves criptográficas. El marco jurídico completo en el que la organización desarrolla sus actividades se mantiene actualizado en el MOD Lista de normas.

Obligaciones del personal

Todo el personal de Redegal tiene el deber de conocer y cumplir esta política y la normativa que la desarrolla. Al incorporarse, cada persona firma las normas internas de seguridad y confidencialidad, y su deber de secreto se mantiene incluso después de terminar la relación laboral. La organización se compromete a dar a conocer la política a través de sus canales de comunicación interna y a facilitar formación y concienciación continuas en seguridad, con atención especial a las nuevas incorporaciones.

La organización establece normas de uso aceptable de la información y de los recursos asociados, que la POL Política de seguridad operativa desarrolla. El personal se compromete, entre otras cosas, a:

- usar los equipos, servicios e instalaciones solo como herramientas de trabajo y únicamente mediante dispositivos, aplicaciones y canales autorizados por Redegal;
- mantener los puestos de trabajo despejados, sin más material que el necesario en cada momento, y guardar en un lugar cerrado los documentos y soportes de información una vez utilizados;
- no dejar desatendida una sesión abierta, ya que los equipos se bloquean automáticamente tras un periodo de inactividad y exigen una nueva autenticación para reanudar el trabajo;
- utilizar accesos nominales, no compartir credenciales y compartir la información solo con destinatarios autorizados;
- comunicar de inmediato cualquier evento de seguridad observado o sospechado.

El incumplimiento de esta política o de su normativa constituye una falta laboral, que la organización gestiona conforme al convenio colectivo aplicable y al Real Decreto Legislativo 2/2015. Según su gravedad, puede llegar al despido disciplinario y generar responsabilidades civiles y penales. El Código Ético recoge los derechos y deberes del personal en esta materia.

Terceros, prestadores de servicios y proveedores de soluciones

Redegal se apoya en proveedores críticos, como plataformas de marketing, de comercio electrónico y de servicios en la nube, y en un proveedor de centro de proceso de datos. La organización se compromete a hacer partícipes de esta política a los terceros que acceden a su información y a exigirles un nivel de seguridad equivalente al propio. Para ello formaliza acuerdos de confidencialidad y requisitos de seguridad en los contratos, según desarrolla el PRO Procedimiento de gestión de compras y terceros.

Cuando un proveedor no puede cumplir un requisito de esta política, el Responsable de Seguridad analiza los riesgos y propone su tratamiento, y el Responsable de la Información y el Responsable del Servicio deciden sobre la aceptación del riesgo residual antes de la contratación. Del mismo modo, antes de adquirir, desarrollar o desplegar sistemas de inteligencia artificial, el Responsable de Seguridad analiza sus riesgos y supervisa su implantación.

Cuando Redegal presta servicios a sus clientes o trata información de terceros, coordina con ellos los canales de comunicación y de respuesta ante incidentes. En estos casos, el Responsable de Seguridad actúa como punto de contacto.

Gestión de incidentes de seguridad

Redegal dispone de un mecanismo para que el personal comunique con prontitud, a través de los canales establecidos, cualquier evento de seguridad observado o

sospechado, como un acceso indebido, una pérdida de información o un intento de phishing. La organización registra cada incidente en el MOD Registro de incidentes de seguridad de la información para analizarlo y extraer lecciones aprendidas.

El PRO Procedimiento de gestión de incidentes de seguridad de la información desarrolla la detección, la clasificación, la contención, la recuperación y el análisis posterior de los incidentes, y se integra con la gestión de las violaciones de datos personales. El Responsable de Seguridad califica la gravedad de los incidentes. Cuando procede, los notifica sin dilación indebida a los organismos competentes, como el CCN-CERT o el CSIRT de referencia y la Agencia Española de Protección de Datos. Si es necesario, informa también a las fuerzas y cuerpos de seguridad.

Protección de activos fuera de las instalaciones

La organización protege sus activos de información también cuando se utilizan fuera de sus sedes, por ejemplo en el teletrabajo, en los desplazamientos o en las instalaciones de clientes. Cada equipo se entrega a su usuario mediante el MOD Formulario de asignación de bienes, con el que la persona asume su custodia.

Fuera de las instalaciones, el personal se compromete a:

- custodiar los equipos con especial diligencia y mantener la información y los equipos de la empresa protegidos en todo momento;
- guardar bajo llave, o protegida de forma adecuada, la información que conserve temporalmente en su domicilio;
- acceder a los sistemas corporativos solo mediante los medios de comunicación aprobados por la empresa;
- comunicar de inmediato cualquier pérdida, robo o daño de un equipo, que la organización trata como un evento de seguridad;
- devolver los equipos al finalizar la relación laboral o cuando se realice una nueva asignación, mediante el MOD Formulario de devolución de bienes.

La POL Política de seguridad operativa desarrolla las reglas del trabajo remoto y de la protección de los dispositivos móviles.

Archivo y actualización

El Responsable del Sistema de Gestión archiva esta política en el repositorio documental del SGI y conserva sus versiones anteriores. El Comité de Seguridad de la Información la revisa al menos una vez al año y cuando se producen cambios significativos en la organización, en los servicios, en la tecnología o en las amenazas, y propone las modificaciones a la Dirección General, que las aprueba. Cada nueva versión se comunica al personal por los mismos canales utilizados para su difusión y se pone a disposición de las partes interesadas, incluida su publicación en el sitio web corporativo.

Documentos de referencia

- MOD Manual de funciones
- MOD Registro de tratamientos del responsable
- POL Política de protección de PII
- POL Política de privacidad por diseño y por defecto
- PRO Procedimiento de gestión de riesgos
- POL Política de clasificación y etiquetado de la información
- PRO Procedimiento de gestión de información documentada
- MOD Lista de documentación
- PRO Procedimiento de gestión y control de accesos lógicos
- PRO Procedimiento de cifrado y gestión de claves criptográficas
- MOD Lista de normas
- POL Política de seguridad operativa
- Código Ético
- PRO Procedimiento de gestión de compras y terceros
- MOD Registro de incidentes de seguridad de la información
- PRO Procedimiento de gestión de incidentes de seguridad de la información
- MOD Formulario de asignación de bienes
- MOD Formulario de devolución de bienes