



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

IMPORTANTE: Este documento ha sido realizado para uso exclusivo de trabajadores de PROSELEC SEGURIDAD S.A. Queda terminantemente prohibido su uso y distribución sin un consentimiento expreso por escrito por parte de Proselec Seguridad.

Copyright © 2025 por Proselec Seguridad. Todos los derechos reservados.



INDICE

1.	OBJETIVO Y DESARROLLO	6
1.1.	DECLARACIÓN DE PRINCIPIOS	6
1.2.	ALCANCE	6
1.3.	COMPROMISO DE PRESIDENCIA	7
1.4.	OBJETIVOS ESTRATÉGICOS	7
1.5.	CUMPLIMIENTO NORMATIVO Y MARCO LEGAL	8
1.6.	PRINCIPIO FUNDAMENTALES	8
2.	OBJETIVO Y DESARROLLO	9
2.1.	ENFOQUE ORGANIZATIVO	9
2.2.	PRESIDENCIA	9
2.3.	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	9
2.4.	RESPONSABLE	10
2.5.	PROPIETARIO DE LA INFORMACIÓN	11
2.6.	RESPONSABLE DEL SISTEMA	11
2.7.	USUARIO Y PERSONAL	11
2.8.	RELACIÓN CON PROVEEDORES	11
2.9.	PRINCIPIOS DE FUNCIÓN DIFERENCIADA	12
2.10.	DOCUMENTACIÓN DE SOPORTE	12
3.	GESTIÓN DE RIESGOS	13
3.1.	ENFOQUE GENERAL	13
3.2.	POLÍTICA DE GESTIÓN DE RIESGOS	13
3.3.	ALCANCE Y FECUENCIA DEL ANÁLISIS	13
3.4.	METODOLOGÍA	14
3.5.	HERRAMIENTAS Y DOCUMENTACIÓN	14
3.6.	CRITERIOS DE IMPACTO Y PROBABILIDAD	15
3.7.	PLAN DE TRATAMIENTO DE RIESGOS	15
3.8.	REVISIÓN Y MEJORA	16
4.	OBJETIVO Y DESARROLLO	16
4.1.	PRINCIPIOS GENERALES	16
4.2.	ALCANCE DE CLASIFICACIÓN	16
4.3.	CRITERIOS DE CLASIFICACIÓN	17



4.4.	PROCEDIMIENTO DE LA CLASIFICACIÓN	18
4.5.	RESPONSABILIDADES	18
4.6.	APLICACIÓN DE MEDIDAS DE PROTECCIÓN	19
4.7.	ETIQUETADO DE LA INFORMACIÓN	19
4.8.	REVISIÓN Y ACTUALIZACIÓN	19
5.	GESTIÓN DE ACTIVOS	20
5.1.	INTRODUCCIÓN	20
5.2.	TIPOS DE ACTIVOS	20
5.3.	INVENTARIO DE ACTIVOS	21
5.4.	PROPIEDAD Y CUSTODIA	21
5.5.	CICLO DE VIDA DEL ACTIVO	22
5.6.	CONTROL DE SOPORTES FÍSICOS Y DIGITALES	22
5.7.	GESTIÓN DE ACTIVOS EN MOVILIDAD	23
5.8.	AUDITORIA Y REVISIÓN DE ACTIVOS	23
6.	CONTROLES DE ACCESOS Y AUTENTICACIÓN	23
6.1.	INTRODUCCIÓN	23
6.2.	PRINCIPIOS RECTORES	23
6.3.	GESTIÓN DE IDENTIDADES	23
6.4.	AUTENTICACIÓN Y CONTROL DE CREDENCIALES	24
6.5.	CONTROL DE ACCESOS A LA RED	24
6.6.	ACCESO REMOTO Y DISPOSITIVOS MÓVILES	25
6.7.	REVISIÓN Y AUDITORIA DE ACCESOS	25
7.	PROTECCIÓN DE INFRAESTRUCTURAS Y SISTEMAS	25
7.1.	INTRODUCCIÓN	25
7.2.	SEGURIDAD FÍSICA	26
7.3.	SEGURIDAD LÓGICA	26
7.4.	PROTECCIÓN CONTRA MALWARE	26
7.5.	SEGURIDAD DE REDES Y COMUNICACIONES	27
7.6.	COPIAS DE SEGURIDAD	27
8.	GESTIÓN DE INCIDENTES DE SEGURIDAD	27
8.1.	INTRODUCCIÓN	27
8.2.	DEFINICIÓN DE INCIDENTE	27



**POLÍTICA DE SEGURIDAD DE LA
INFORMACIÓN**

Edición: 01
FECHA: 23/04/2025
Página 5 de 33
Conf.: Uso Interno

8.3.	CICLO DE GESTIÓN DE INCIDENTES	28
8.4.	ROLES Y RESPONSABILIDADES	28
8.5.	REGISTRO DE TRAZABILIDAD	28
9.	CONTINUIDAD DEL SERVICIO	29
9.1.	OBJETIVOS	29
9.2.	ENFOQUE DE GESTIÓN	29
9.3.	COPIAS DE SEGURIDAD Y REDUNDANCIA	29
9.4.	PRUEBAS DE CONTINUIDAD	29
10.	FORMACIÓN Y CONCIENCIACIÓN	29
10.1.	PRINCIPIOS	30
10.2.	PLAN DE FORMACIÓN	30
10.3.	CONCIENCIACIÓN CONTINUA	30
10.4.	EVALUACIÓN DE EFICACIA	31
11.	SUPERVISIÓN, AUDITORIA Y MEJORA CONTINUA	31
11.1.	SUPERVISIÓN Y MONITOREO	31
11.2.	AUDITORIA INTERNA Y EXTERNA	31
11.3.	REVISIÓN POR LA DIRECCIÓN	32
11.4.	MEJORA CONTINUA	32
12.	CUMPLIMIENTO LEGAL Y NORMATIVO	32
12.1.	COMPROMISO LEGAL	32
12.2.	PROTECCIÓN DE DATOS PERSONALES	32
12.3.	AUDITORIAS DE CUMPLIMIENTO	33
13.	FIRMA Y VALIDACIÓN	33
14.	APROBADA Y VALIDADA POR PRESIDENCIA	33

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Edición: 01 FECHA: 23/04/2025 Página 6 de 33 Conf.: Uso Interno
---	--	--

1. OBJETIVO Y DESARROLLO

1.1. DECLARACIÓN DE PRINCIPIOS

La presente **Política de Seguridad de la Información** constituye el documento de más alto nivel en materia de protección de la información en **PROSELEC SEGURIDAD S.A.**, siendo de aplicación transversal a todas las unidades organizativas, procesos, sistemas, infraestructuras, proveedores y personas que, de forma directa o indirecta, participen en la gestión, tratamiento o soporte de activos de información.

Esta política tiene por objeto **establecer el marco estratégico, organizativo y normativo** para la protección de la información,

–según el **Real Decreto 311/2022** y la **Guía CCN-STIC 805**, asegurando así:

- La **confidencialidad** de la información tratada, evitando el acceso no autorizado.
- La **integridad**, asegurando la exactitud, completitud y validez de los datos y sistemas.
- La **disponibilidad**, garantizando el acceso oportuno a los recursos cuando se requieran.
- La **autenticidad**, asegurando la veracidad del origen de la información.
- La **trazabilidad**, permitiendo registrar, verificar y auditar las acciones realizadas sobre la información y los sistemas que la soportan.

Este documento también responde a la exigencia de definir una **política única, alineada e integradora** que combine en un marco coherente los principios, obligaciones y controles derivados tanto del marco nacional

1.2. ALCANCE

Esta política es de aplicación a todos los sistemas de información de PROSELEC que dan soporte a la provisión de servicios internos y externos, independientemente de su naturaleza (tecnológica, física, organizativa) y del modelo de prestación (interno, externalizado, mixto), incluyendo:

- Sistemas TIC utilizados por el personal interno, proveedores o terceros autorizados.
- Servicios alojados en **entornos locales, híbridos o en la nube**.
- Plataformas web, dispositivos móviles, redes internas y puntos de acceso.
- Servicios críticos sujetos a requisitos de continuidad operativa.
- Flujos de información internos y externos, en cualquier formato (digital o físico).

Asimismo, la política se extiende a todos los **empleados** que, en el ejercicio de sus funciones, accedan, gestionen o procesen información de PROSELEC o de sus clientes, socios o entidades colaboradoras.



1.3. COMPROMISO DE PRESIDENCIA

Presidencia de PROSELEC SEGURIDAD, consciente de los riesgos asociados al entorno digital y regulatorio, **asume un compromiso explícito y permanente** con la seguridad de la información como elemento estratégico para:

- Proteger los intereses legítimos de la organización, sus clientes, accionistas y partes interesadas.
- Cumplir rigurosamente con la legislación vigente.
- Generar confianza y transparencia en sus operaciones.
- Asegurar la **resiliencia operativa** y reputacional frente a amenazas y ciberataques.

Dicho compromiso se materializa en la **asignación de recursos técnicos, organizativos y humanos**, en la validación periódica de esta política, y en la participación activa de la Dirección en el Comité de Seguridad, responsable de la supervisión y evolución del CSI.

1.4. OBJETIVOS ESTRATÉGICOS

Los objetivos de la política de seguridad son:

- **Establecer un marco de referencia para la gobernanza de la seguridad**, que permita integrar controles de forma sistemática, medible y auditable.
- **Reducir los riesgos tecnológicos y de seguridad**, aplicando una gestión proactiva y basada en escenarios.
- **Fortalecer la cultura organizativa de seguridad**, sensibilizando a todo el personal y fomentando comportamientos seguros.
- **Garantizar la continuidad operativa**, mediante medidas preventivas, reactivas y planes de contingencia probados.
- **Alinear la seguridad con los objetivos de negocio**, asegurando que el sistema de seguridad sea un habilitador de la estrategia empresarial.
- **Impulsar la mejora continua** mediante auditorías, revisiones y evolución de capacidades técnicas y organizativas.

1.5. CUMPLIMIENTO NORMATIVO Y MARCO LEGAL

La presente política asegura el cumplimiento con:

- **Real Decreto 311/2022.**
- **Guía CCN-STIC-805**, en lo relativo a requisitos y estructura de la política de seguridad.
- **Reglamento (UE) 2016/679** (GDPR), y su transposición en la **Ley Orgánica 3/2018**, de Protección de Datos y Garantía de los Derechos Digitales.
- **Ley 34/2002** de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE).
- Requisitos contractuales con clientes y proveedores.
- Otras disposiciones normativas sectoriales que le sean aplicables.

1.6. PRINCIPIO FUNDAMENTALES

PROSELEC adopta los siguientes **principios rectores** en su enfoque de seguridad de la información:

Principio	Definición
Seguridad Integral	Enfoque multidisciplinar que abarca tecnología, procesos, personas e instalaciones.
Gestión basada en el riesgo	Priorizar recursos según el impacto y la probabilidad del riesgo.
Prevención, detección y respuesta	Modelo de defensa en profundidad.
Proporcionalidad	Los controles deben ser adecuados al nivel de riesgo y al impacto potencial.
Responsabilidad	Cada actor debe conocer y asumir sus funciones en materia de seguridad.
Mejora continua	Revisión, evolución y adaptación constante a amenazas y cambios tecnológicos.
Legalidad	Cumplimiento estricto de las normas legales y contractuales aplicables.
Coordinación	Integración de la seguridad en todos los niveles organizativos.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Edición: 01 FECHA: 23/04/2025 Página 9 de 33 Conf.: Uso Interno
---	--	--

2. OBJETIVO Y DESARROLLO

2.1. ENFOQUE ORGANIZATIVO

La organización de la seguridad de la información en PROSELEC SEGURIDAD S.A. se fundamenta en un modelo estructurado, jerarquizado y basado en funciones diferenciadas, que permite una **gestión eficiente, coordinada y trazable** de la seguridad de los sistemas de información.

Este modelo define con claridad las **autoridades responsables, funciones, niveles de decisión y mecanismos de control**.

La **estructura de gobierno de la seguridad** se basa en los siguientes niveles:

- Presidencia
- Comité de Seguridad de la Información
- Responsable del Sistema de Gestión de Seguridad de la Información
- Responsables de Seguridad de las Unidades/Áreas
- Propietarios de la Información
- Usuarios y personal operativo
- Terceros y proveedores

2.2. PRESIDENCIA

Presidencia de PROSELEC SEGURIDAD tiene la **máxima responsabilidad en materia de seguridad de la información**, garantizando que los objetivos de seguridad estén alineados con los objetivos estratégicos de la organización y que se disponga de los recursos necesarios (humanos, técnicos y financieros) para su implementación efectiva.

Entre sus funciones específicas se incluyen:

- Aprobar la política de seguridad y sus revisiones periódicas.
- Impulsar la cultura de seguridad en todos los niveles de la organización.
- Designar a los miembros del Comité de Seguridad.
- Evaluar el desempeño del CSI y liderar su mejora continua

2.3. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN



El **Comité de Seguridad de la Información** es el órgano colegiado de carácter permanente que **coordina, supervisa y toma decisiones estratégicas** en relación con la seguridad de la información.

Composición

El Comité está compuesto por:

- Presidencia.
- Responsable del Seguridad de la información
- Responsable del Sistema.
- Responsable del Servicio

Funciones del Comité:

- Definir la estrategia y el marco de gobierno de la seguridad.
- Aprobar los planes de seguridad, análisis de riesgos y medidas técnicas.
- Evaluar los informes de incidentes, auditorías y revisiones internas.
- Supervisar la eficacia de la formación y concienciación en seguridad.
- Establecer mecanismos de control y priorización de inversiones en seguridad.

Reuniones y funcionamiento:

El Comité se reúne como mínimo de forma anual, o con carácter extraordinario ante eventos relevantes (incidentes críticos, cambios normativos, auditorías externas). Se levantan actas de cada sesión, que son custodiadas conforme a lo dispuesto en la política de documentación.

2.4. RESPONSABLE

El **Responsable del Sistema Seguridad de la Información (RCSI)** tiene la **responsabilidad operativa y técnica** de liderar el diseño, implantación, seguimiento y mejora continua del CSI.

Funciones principales:

- Desarrollar, mantener y promover el CSI
- Elaborar y revisar políticas, normas y procedimientos de seguridad.
- Supervisar el cumplimiento de controles técnicos y organizativos.
- Gestionar los análisis de riesgos y coordinar su tratamiento.
- Informar periódicamente a la Dirección y al Comité sobre el estado de la seguridad.
- Coordinar la respuesta ante incidentes de seguridad.
- Colaborar en la selección, evaluación y monitorización de proveedores críticos.
- Asegurar la formación del personal en materias de seguridad.

El RCSI dispone de **autoridad suficiente**, acceso directo a la Dirección y autonomía para la toma de decisiones en el ámbito de sus funciones.



2.5. PROPIETARIO DE LA INFORMACIÓN

Son los responsables funcionales de los activos de información bajo su control. Su rol incluye:

- Clasificar la información conforme a su sensibilidad y criticidad.
- Establecer los requisitos de acceso y uso de la información.
- Aprobar o denegar solicitudes de acceso.
- Validar el ciclo de vida de los activos (creación, uso, archivo, eliminación).
- Participar en la identificación de riesgos relacionados con su información.
-

2.6. RESPONSABLE DEL SISTEMA

En las unidades organizativas críticas o con procesos sensibles, se designa responsable del sistema.

- Actúan como enlace entre su unidad y el CSI.
- Velan por la correcta aplicación de las políticas en su área.
- Informan de incidentes, debilidades o desviaciones.
- Apoyan las auditorías internas y externas.

2.7. USUARIO Y PERSONAL

Todos los usuarios de los sistemas de información de PROSELEC, tienen la obligación de:

- Conocer y cumplir la presente política y normativa de seguridad.
- Participar en las actividades de formación y concienciación.
- Reportar cualquier debilidad o incidente de seguridad detectado.
- Hacer uso de los sistemas y activos de forma ética, profesional y conforme a las directrices establecidas.

El incumplimiento de estas obligaciones podrá dar lugar a medidas disciplinarias o contractuales, según lo previsto en los procedimientos internos y la normativa aplicable.

2.8. RELACIÓN CON PROVEEDORES

a política de seguridad también se extiende a todos los **proveedores** que tengan acceso a información, instalaciones o sistemas de PROSELEC.



Para garantizar un nivel adecuado de protección:

- Se definen cláusulas de seguridad en los contratos.
- Se exige la firma de acuerdos de confidencialidad y tratamiento seguro.
- Se realizan evaluaciones de seguridad durante el proceso de homologación.
- Se aplican controles de acceso y segmentación lógica en entornos compartidos.
- Se supervisa el cumplimiento de las obligaciones contractuales en seguridad.

2.9. PRINCIPIOS DE FUNCIÓN DIFERENCIADA

PROSELEC SEGURIDAD establece una **separación clara entre las funciones de explotación y las de seguridad**, con el fin de evitar conflictos de interés y garantizar la independencia en la evaluación de controles.

Esto implica que:

- El personal que administra sistemas no puede auditar su propia actividad.
- Las decisiones sobre seguridad no dependen exclusivamente de quienes operan los sistemas.
- Las funciones de control están jerárquicamente diferenciadas de las operativas.

2.10. DOCUMENTACIÓN DE SOPORTE

Las funciones, dependencias y mecanismos de actuación descritos en esta sección se desarrollan y formalizan en los siguientes documentos:

- Manual del Sistema de Gestión de Seguridad de la Información.
- Procedimiento de Gobierno y Coordinación de la Seguridad.
- Actas del Comité de Seguridad.
- Organigrama funcional de seguridad.
- Fichas de roles y responsabilidades

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Edición: 01 FECHA: 23/04/2025 Página 13 de 33 Conf.: Uso Interno
---	--	---

3. GESTIÓN DE RIESGOS

3.1. ENFOQUE GENERAL

la gestión de riesgos en PROSELEC SEGURIDAD constituye el pilar central sobre el que se construye el modelo de protección de activos y continuidad operativa. Su propósito es:

- **Identificar proactivamente amenazas** internas y externas que puedan afectar a los sistemas de información y servicios esenciales.
- **Evaluar la probabilidad e impacto** de materialización de dichos riesgos.
- **Determinar y aplicar medidas** de seguridad proporcionales, eficaces y sostenibles.
- **Priorizar actuaciones y recursos** en función del nivel de exposición y criticidad.

Este enfoque está plenamente alineado con:

- El ciclo de mejora continua PDCA.
- La Guía CCN-STIC 830.

3.2. POLÍTICA DE GESTIÓN DE RIESGOS

La política de gestión de riesgos establece que:

- Todos los **activos, procesos, servicios y sistemas de información** sujetos a esta Política de Seguridad deberán ser evaluados conforme al procedimiento de análisis y gestión de riesgos establecido.
- Se aplicará una **metodología uniforme y documentada**, orientada a la valoración del impacto sobre la **confidencialidad, integridad y disponibilidad, Trazabilidad y adaptabilidad (CIDTA)**.
- La gestión de riesgos será **continua, trazable y basada en evidencia**, incluyendo revisiones periódicas y eventos desencadenantes.

3.3. ALCANCE Y FECUENCIA DEL ANÁLISIS

El análisis de riesgos deberá realizarse para todos los **sistemas de información clasificados** dentro del alcance del CSI y, de forma obligatoria, en los siguientes casos:

- En el diseño o implantación de un nuevo sistema o servicio.
- Al producirse cambios significativos en la arquitectura, tecnología o ubicación.
- Tras un incidente de seguridad que haya afectado a la información o activos críticos.
- Cuando se detecten nuevas amenazas, vulnerabilidades o cambios normativos relevantes.
- De forma **periódica, al menos una vez al año**, o según el calendario definido por el Comité de Seguridad.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Edición: 01 FECHA: 23/04/2025 Página 14 de 33 Conf.: Uso Interno
---	--	---

3.4. METODOLOGÍA

PROSELEC aplica una **metodología propia documentada** de análisis y tratamiento de riesgos, basada en los siguientes pasos:

1. **Identificación de activos:** Se identifican los activos primarios (información, servicios) y secundarios (personas, TIC, ubicaciones).
2. **Valoración de activos:** Se evalúa el valor del activo en función de su impacto en la organización y su entorno (económico, reputacional, legal, operacional).
3. **Identificación de amenazas y vulnerabilidades:** Se documentan las amenazas relevantes, tanto externas como internas, así como las vulnerabilidades técnicas u organizativas existentes.
4. **Valoración del riesgo:** Se calcula el nivel de riesgo combinando probabilidad e impacto, siguiendo una matriz normalizada (BAJO-MEDIO-ALTO).
5. **Aceptación o tratamiento:** Los riesgos identificados pueden ser aceptados, mitigados, transferidos o evitados.
6. **Selección de controles:** Se definen los controles más eficaces y proporcionales al riesgo

3.5. HERRAMIENTAS Y DOCUMENTACIÓN

El proceso de análisis y gestión de riesgos queda formalizado en:

- **Procedimiento ANÁLISIS DE RIESGOS PROSELEC 2025.xlsx:** recoge los criterios, escalado, categorías y valoración.
- **Mapa de activos y propietarios.**
- **Matrices de impacto por nivel CDITA**
- **Informes de evaluación de riesgo residual y riesgo aceptado.**
- **Plan de tratamiento de riesgos.**
- **Registro de decisiones del Comité de Seguridad.**

3.6. CRITERIOS DE IMPACTO Y PROBABILIDAD

Para la valoración del impacto, se tienen en cuenta:

Impacto	Confidencialidad	Integridad	Disponibilidad
Bajo	Pérdida menor sin impacto significativo.	Cambios triviales reversibles.	Pequeñas interrupciones tolerables.
Medio	Divulgación moderada con implicaciones legales o reputacionales.	Alteración que afecta operaciones críticas.	Interrupción relevante que afecta SLA.
Alto	Acceso no autorizado a información clasificada o sensible.	Manipulación grave de datos.	Caída de servicio crítico con pérdidas notables.

Estos criterios se combinan con factores de probabilidad (frecuencia, historial, amenazas activas) para obtener el nivel de riesgo.

3.7. PLAN DE TRATAMIENTO DE RIESGOS

Una vez identificados y evaluados los riesgos, se elabora un **plan de tratamiento** que:

- Define acciones concretas para mitigar los riesgos.
- Establece responsables y plazos para su implementación.
- Describe los controles aplicables (organizativos, técnicos, físicos).
- Asigna prioridades de ejecución según la gravedad del riesgo.
- Determina el nivel de riesgo residual tras la aplicación de controles.

El tratamiento de riesgos debe estar **alineado con la estrategia de negocio**, considerando la relación coste-beneficio de cada control.



3.8. REVISIÓN Y MEJORA

El Comité de Seguridad revisará de forma periódica los resultados del análisis de riesgos y del plan de tratamiento, para:

- Validar que los riesgos están controlados dentro de niveles aceptables.
- Actualizar la estrategia ante nuevas amenazas, cambios tecnológicos o incidentes.
- Proponer mejoras en políticas, procedimientos o controles existentes.
- Reasignar recursos o redefinir prioridades de seguridad.

Este proceso será registrado y auditado, contribuyendo a la mejora continua del CSI.

4. OBJETIVO Y DESARROLLO

4.1. PRINCIPIOS GENERALES

La **clasificación de la información** es un proceso esencial para la **gestión del ciclo de vida de los activos** y la aplicación proporcional de medidas de seguridad. Esta clasificación permite identificar:

- **El valor estratégico, legal, operativo y reputacional** de la información.
- **El nivel de protección necesario (CDITA)**.
- Las **responsabilidades asociadas** a cada tipo de información.

4.2. ALCANCE DE CLASIFICACIÓN

La clasificación aplica a **toda la información tratada por PROSELEC SEGURIDAD S.A.**, con independencia de su formato (electrónico, físico, verbal), soporte (digital, papel), origen (interno o externo), o ubicación (local, nube)

También se clasifican:

- Los **activos de información** (bases de datos, informes, documentos, registros, etc.).
- Los **medios de tratamiento** (aplicaciones, sistemas, redes).
- Las **personas que acc**

4.3. CRITERIOS DE CLASIFICACIÓN

Nivel de clasificación	Confidencialidad	Integridad	Disponibilidad
Pública	Puede ser divulgada sin restricciones.	Su alteración no afecta a operaciones ni decisiones.	Su no disponibilidad no causa perjuicio.
Interna	Acceso restringido a empleados y colaboradores.	Alteraciones afectan decisiones operativas limitadas.	Su no disponibilidad puede causar interrupciones menores.
Restringida	Acceso solo a personal autorizado expresamente.	Su modificación tiene efectos legales, contractuales o reputacionales.	Su pérdida puede afectar servicios relevantes.
Confidencial	Su revelación pone en riesgo a la organización.	Alteraciones provocan daños operativos y regulatorios.	Su indisponibilidad compromete la actividad crítica.

4.4. PROCEDIMIENTO DE LA CLASIFICACIÓN

El proceso de clasificación se compone de las siguientes fases:

1. **Identificación del activo de información.**
2. **Asignación del propietario del activo** (rol funcional).
3. **Evaluación del impacto CDITA** en caso de pérdida o alteración.
4. **Asignación del nivel de clasificación aplicable** (conforme a los criterios definidos).
5. **Documentación de la clasificación** en el inventario de activos.
6. **Aplicación de medidas de protección asociadas.**
7. **Revisión periódica** o tras cambios significativos en el activo.

Este procedimiento se formaliza en los documentos:

- **Clasificación activos PROSELEC.xlsx** (registro y niveles aplicados).
- **Política de Uso Aceptable de Activos.**

4.5. RESPONSABILIDADES

Rol	Responsabilidad principal
Propietario del activo	Determina y revisa la clasificación; autoriza accesos.
Comité de Seguridad	Supervisa la coherencia del modelo de clasificación.
Responsable del CSI	Evalúa la aplicación técnica de medidas de protección.
Usuarios	Conocen y respetan el nivel de protección asignado.

4.6. APLICACIÓN DE MEDIDAS DE PROTECCIÓN

Cada nivel de clasificación conlleva un conjunto proporcional de medidas de seguridad, tanto técnicas como organizativas, que deben asegurar la protección efectiva durante todo el ciclo de vida de la información.

Ejemplos de medidas por nivel:

Nivel	Medidas obligatorias
Pública	Sin restricciones. Control de versiones y fuentes autorizadas.
Interna	Control de acceso lógico y físico. Control de copia y difusión.
Restringida	Cifrado en tránsito y reposo. Registros de acceso. Protección documental.
Confidencial	DLP, cifrado fuerte, acceso controlado.

4.7. ETIQUETADO DE LA INFORMACIÓN

Toda información clasificada deberá estar **etiquetada claramente** según su nivel. El etiquetado puede ser:

- **Visual:** mediante marcas o leyendas en cabeceras/pies (ej. "Confidencial")
- **Digital:** metadatos incrustados en documentos electrónicos.
- **Físico:** etiquetas en carpetas, archivadores o soportes removibles.

4.8. REVISIÓN Y ACTUALIZACIÓN

La clasificación de activos deberá revisarse:

- Anualmente, como parte del ciclo del CSI.
- Siempre que cambie el uso, la criticidad o el propietario del activo.
- Cuando se detecten desviaciones en el etiquetado, acceso o protección.

Estas revisiones se documentan en el Registro de Activos y son supervisadas por el Comité de Seguridad.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Edición: 01 FECHA: 23/04/2025 Página 20 de 33 Conf.: Uso Interno
---	--	---

5. GESTIÓN DE ACTIVOS

5.1. INTRODUCCIÓN

La **gestión de activos** es un componente fundamental para la protección efectiva de la información y los sistemas que la soportan. Un activo mal identificado, mal documentado o protegido es un riesgo potencial para la seguridad, la disponibilidad del servicio y la conformidad regulatoria.

Este apartado establece los criterios para:

- Identificar, inventariar y mantener los activos asociados al sistema de información.
- Asignar responsabilidades claras sobre su uso y protección.
- Controlar su ciclo de vida desde su adquisición hasta su retirada o destrucción segura.

Esta gestión está alineada con:

5.2. TIPOS DE ACTIVOS

Se consideran activos a todos aquellos elementos que intervienen en la generación, tratamiento, almacenamiento, transmisión o protección de la información. Se clasifican en:

- **Activos de información:** datos, registros, informes, correos, bases de datos.
- **Activos tecnológicos:** servidores, ordenadores, redes, dispositivos móviles, software.
- **Activos físicos:** edificios, salas técnicas, archivos, documentos impresos.
- **Activos humanos:** empleados, proveedores, consultores con acceso autorizado.
- **Activos lógicos:** identidades digitales, claves criptográficas, tokens de acceso.

Cada activo será vinculado a un **activo primario** (servicio o proceso de negocio) y a un propietario funcional.

5.3. INVENTARIO DE ACTIVOS

PROSELEC SEGURIDAD mantiene un **inventario actualizado y documentado** de todos los activos relevantes para la seguridad de la información.

Requisitos del inventario:

- Identificación única de cada activo.
- Tipo y descripción del activo.
- Ubicación y soporte (físico o lógico).
- Clasificación de seguridad asignada (ver bloque anterior).
- Propietario del activo.
- Relación con procesos críticos y servicios esenciales.
- Dependencias y relaciones con otros activos.
- Estado (activo, en uso, retirado, en cuarentena, eliminado).

El inventario está almacenado en formato digital, accesible exclusivamente para los roles autorizados y vinculado con la base de clasificación y riesgo.

5.4. PROPIEDAD Y CUSTODIA

Todo activo debe tener asignado un **propietario** y, en su caso, uno o más **custodios técnicos**.

Rol	Función
Propietario	Usuario con responsabilidad funcional; decide el uso, clasificación y control del activo.
Custodio	Área o persona encargada de su administración técnica y operativa.

El propietario del activo es responsable de:

- Definir y revisar el nivel de clasificación.
- Establecer los requisitos de protección y acceso.
- Autorizar transferencias, modificaciones o destrucciones.
- Asegurar que los activos bajo su control sean revisados periódicamente.



5.5. CICLO DE VIDA DEL ACTIVO

Los activos deben ser gestionados de forma segura durante todo su ciclo de vida, desde su incorporación hasta su retirada definitiva.

Etapas del ciclo:

1. **Adquisición:** Revisión de requisitos de seguridad antes de incorporar activos (hardware, software, servicios).
2. **Registro e Inventariado:** Asignación de propietario, clasificación y ubicación.
3. **Uso y mantenimiento:** Aplicación de medidas de protección, gestión de acceso, actualizaciones, supervisión.
4. **Transferencia:** Protección durante el traslado físico o lógico; control de cifrado, logs y consentimiento.
5. **Retiro/Eliminación:** Eliminación física o lógica segura, conforme a procedimientos establecidos (borrado seguro, destrucción física, trazabilidad documental).

5.6. CONTROL DE SOPORTES FÍSICOS Y DIGITALES

Los **soportes de información** (papel, discos, USB, backups, etc.) deben ser controlados rigurosamente durante su uso, almacenamiento y eliminación.

Medidas aplicables incluyen:

- Etiquetado conforme a la clasificación.
- Cifrado de soportes removibles si contienen información Restringida o superior.
- Almacenamiento en ubicaciones seguras.
- Registro de préstamos, traslados y eliminaciones.
- Destrucción segura mediante trituradoras, software de borrado o servicios certificados.



5.7. GESTIÓN DE ACTIVOS EN MOVILIDAD

Dado que parte de los activos puede ser utilizada en movilidad (teletrabajo, dispositivos BYOD, acceso remoto), PROSELEC aplica controles específicos para:

- Autenticación fuerte..
- Gestión centralizada de dispositivos.
- Segmentación de red para equipos externos.
- Revocación remota de credenciales en caso de pérdida o robo.

5.8. AUDITORIA Y REVISIÓN DE ACTIVOS

Se realizará una **verificación del inventario de activos** de forma:

- Anual, como parte del ciclo del CSI.
- Ante cambios tecnológicos, reorganizaciones o incidentes.
- Tras la retirada o alta de activos críticos.

Esta verificación será auditada, documentada y reportada al Comité de Seguridad.

6. CONTROLES DE ACCESOS Y AUTENTICACIÓN

6.1. INTRODUCCIÓN

El control de accesos constituye uno de los mecanismos más críticos en la seguridad de los sistemas de información. Un acceso indebido, no autorizado o mal gestionado puede comprometer la **CDITA** de los activos, además de generar incumplimientos normativos, pérdida de reputación y riesgos operativos graves.

Por ello, PROSELEC SEGURIDAD establece una política estricta de **control de accesos físicos**.

6.2. PRINCIPIOS RECTORES

- **Necesidad de saber (Need-to-Know):** El acceso a la información se otorga únicamente a quienes lo necesitan para desempeñar sus funciones.
- **Privilegios mínimos (Least Privilege):** Se otorgan los permisos mínimos indispensables.
- **Segregación de funciones:** Separación de roles críticos para evitar conflictos de interés.
- **Identidad individual y no compartida:** Toda persona tendrá un identificador único.
- **Responsabilidad y trazabilidad:** Toda acción será atribuible a un usuario identificado.

6.3. GESTIÓN DE IDENTIDADES



Alta de usuarios:

- Requiere validación formal por el propietario del activo.
- Se gestiona mediante procedimientos documentados por el área TIC.
- Cada identidad será única, intransferible y asignada a un perfil funcional.

Modificación y baja:

- Cambios de rol, funciones o unidad implican revisión de permisos.
- Las cuentas deben ser desactivadas **de forma inmediata** en caso de baja, cese o desvinculación del usuario.

Control de cuentas privilegiadas:

- El acceso administrativo, root, o de alto privilegio estará **restringido y monitorizado**.
- Se establecerán controles adicionales: doble factor, registro de sesiones, control de comandos ejecutados.

6.4. AUTENTICACIÓN Y CONTROL DE CREDENCIALES

La autenticación debe garantizar que solo usuarios legítimos puedan acceder a sistemas y datos. Se aplicarán las siguientes medidas:

- Contraseñas: longitud mínima, complejidad, caducidad periódica.
- Autenticación multifactor (MFA) para accesos remotos, aplicaciones críticas o cuentas privilegiadas.
- No reutilización de credenciales personales/profesionales.
- Prohibición expresa del uso de cuentas compartidas, excepto bajo procedimientos excepcionales y auditables.
-

6.5. CONTROL DE ACCESOS A LA RED

Se definen diferentes **zonas de seguridad** en la red corporativa, y se aplican medidas de segmentación, filtrado y monitorización:

- Uso de firewalls de nueva generación y listas de control de acceso.
- Supervisión de conexiones entrantes y salientes.
- Desactivación de puertos o servicios innecesarios.
- Detección y bloqueo de conexiones no autorizadas o anómalas.

6.6. ACCESO REMOTO Y DISPOSITIVOS MÓVILES

- Solo se autoriza el acceso remoto a sistemas de información tras una evaluación de riesgos y mediante M365.
- Se aplican políticas de **gestión de dispositivos móviles (MDM)** para proteger la información en portátiles, tablets y smartphones.
- Los dispositivos personales deberán cumplir requisitos de seguridad y ser autorizados explícitamente.

6.7. REVISIÓN Y AUDITORIA DE ACCESOS

PROSELEC lleva a cabo revisiones periódicas de los accesos, que incluyen:

- **Revisión trimestral de permisos** asignados en sistemas críticos.
- Auditorías anuales del cumplimiento de las políticas de acceso.
- Supervisión continua de sesiones activas, intentos fallidos, actividades fuera de horario, etc.
- Conservación de logs durante los plazos legales y conforme a los niveles de categoría del sistema (Básica, Media, Alta).
- Trazabilidad completa en acciones sensibles: acceso a información clasificada, cambio de configuración, extracción de datos.

7. PROTECCIÓN DE INFRAESTRUCTURAS Y SISTEMAS

7.1. INTRODUCCIÓN

La protección efectiva de las **infraestructuras físicas y lógicas** es esencial para garantizar la **resiliencia, disponibilidad y seguridad** de los sistemas de información. PROSELEC SEGURIDAD implementa medidas organizativas y técnicas para asegurar que:

- Las instalaciones estén protegidas frente a accesos no autorizados, sabotajes o siniestros.
- Los sistemas TIC estén configurados, operados y mantenidos conforme a buenas prácticas de seguridad.
- Las actualizaciones, cambios e integraciones no introduzcan vulnerabilidades.
- Las amenazas físicas y ambientales sean evaluadas y mitigadas.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Edición: 01 FECHA: 23/04/2025 Página 26 de 33 Conf.: Uso Interno
---	--	---

7.2. SEGURIDAD FÍSICA

Se adoptan controles para evitar el acceso no autorizado a instalaciones y equipos, así como para proteger los sistemas frente a riesgos ambientales (fuego, agua, calor, interferencias).

Medidas principales:

- Control de acceso físico con registro de visitas y zonas restringidas.
- Videovigilancia, alarmas y sensores en áreas críticas (servidores, racks).
- SAI (sistemas de alimentación ininterrumpida), extintores, sistemas antiincendios.
- Control de temperatura y humedad.

Estas medidas se documentan en el **Plan de Seguridad Física**

7.3. SEGURIDAD LÓGICA

Configuración segura:

- Todos los sistemas se implantan con **parámetros de seguridad por defecto**.
- Se eliminan funcionalidades innecesarias y se desactivan servicios no requeridos.
- Se aplican políticas de endurecimiento (hardening) en sistemas operativos, redes y software.

Actualización y mantenimiento:

- Todos los sistemas están sujetos a un **ciclo regular de actualizaciones** de seguridad (sistema operativo, firmware, software).
- Se aplican **parches críticos** en un plazo razonable según criticidad.
- Se documentan los cambios mediante un sistema de gestión del cambio.
- Las actualizaciones son validadas antes de su despliegue en entornos de producción.

7.4. PROTECCIÓN CONTRA MALWARE

- Se utilizan **soluciones antimalware** actualizadas y supervisadas.
- Se aplican restricciones sobre ejecución de scripts, macros y software no autorizado.
- Se implementan soluciones **EDR** (Endpoint Detection and Response) en equipos críticos.
- Se realizan campañas de concienciación sobre phishing, ingeniería social y malware.



7.5. SEGURIDAD DE REDES Y COMUNICACIONES

- Segmentación de red con control de tráfico entre zonas.
- Firewalls perimetrales y de host.
- Detección de intrusos (IDS) y mecanismos de prevención (IPS).
- Cifrado en todas las comunicaciones sensibles
- Supervisión de logs de red, alertas y comportamiento anómalo.

7.6. COPIAS DE SEGURIDAD

- Se ejecutan copias de seguridad automáticas y periódicas, conforme al plan de continuidad.
- Las copias se almacenan en ubicación física y lógica separada.
- Se validan periódicamente mediante restauraciones parciales o completas.
- Están protegidas por cifrado, autenticación y control de acceso.

8. GESTIÓN DE INCIDENTES DE SEGURIDAD

8.1. INTRODUCCIÓN

La capacidad de **detectar, responder y aprender** de los incidentes de seguridad es esencial para cualquier CSI maduro. Un incidente mal gestionado puede desencadenar:

- Pérdidas económicas.
- Daños reputacionales.
- Vulneración de datos personales.
- Incumplimiento legal.

PROSELEC SEGURIDAD establece un **procedimiento formal de gestión de incidentes**.

8.2. DEFINICIÓN DE INCIDENTE

Un incidente de seguridad es cualquier evento que:

- Compromete o pone en riesgo la **confidencialidad, integridad o disponibilidad** de la información o los servicios.
- Vulnera las políticas de seguridad establecidas.
- Puede tener consecuencias legales, contractuales o reputacionales.

Ejemplos: accesos no autorizados, malware, fuga de información, caída de servicios, fallos en backup, uso indebido de privilegios, etc.

8.3. CICLO DE GESTIÓN DE INCIDENTES

1. **Detección:** Identificación del incidente por usuarios, sistemas automáticos, alertas o terceros.
2. **Notificación:** Comunicación inmediata al Responsable del CSI a través del canal oficial.
3. **Registro:** Documentación estructurada del incidente (fecha, origen, tipo, activo afectado, impacto).
4. **Análisis y clasificación:** Valoración de la gravedad, tipo de amenaza y alcance.
5. **Respuesta:** Contención, erradicación, recuperación.
6. **Comunicación:** Información a partes interesadas (internas o externas), incluyendo la AEPD si aplica.
7. **Lecciones aprendidas:** Análisis post-incidente, revisión de controles, refuerzo de medidas.
8. **Documentación y cierre:** Informe final, cierre del ticket y evaluación de eficacia.

8.4. ROLES Y RESPONSABILIDADES

Rol	Función
Usuarios	Detectar y reportar inmediatamente cualquier anomalía.
Responsable del CSI	Coordinar la gestión del incidente y las acciones correctivas.
Comité de Seguridad	Evaluar incidentes críticos, decidir medidas estructurales.
Propietario del activo	Colaborar en el análisis, impacto y tratamiento del incidente.
Soporte técnico / TIC	Ejecutar medidas técnicas de contención y recuperación.

8.5. REGISTRO DE TRAZABILIDAD

Todos los incidentes se registran en un **registro centralizado y auditado**, que incluye:

- Cronología detallada.
- Medidas aplicadas.
- Impacto estimado y real.
- Lecciones aprendidas.
- Cambios estructurales derivados del incidente.

Los registros se conservan como evidencia y para su revisión periódica por el Comité de Seguridad.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Edición: 01 FECHA: 23/04/2025 Página 29 de 33 Conf.: Uso Interno
---	--	---

9. CONTINUIDAD DEL SERVICIO

9.1. OBJETIVOS

La continuidad del servicio busca **garantizar la operación ininterrumpida de los procesos críticos**, incluso ante eventos disruptivos, incidentes de seguridad, desastres naturales, fallos tecnológicos o errores humanos.

Este enfoque está basado en el principio de **resiliencia operativa**, que implica anticipación, respuesta y recuperación eficaces ante cualquier situación que afecte los sistemas de información.

9.2. ENFOQUE DE GESTIÓN

PROSELEC SEGURIDAD mantiene un **Plan de Continuidad de Negocio** Identificación de procesos y sistemas críticos.

- Análisis de impacto en el negocio (BIA).
- Estrategias de contingencia.
- Procedimientos de activación, escalado y comunicación.
- Equipos responsables y recursos alternativos.

9.3. COPIAS DE SEGURIDAD Y REDUNDANCIA

- Copias de seguridad cifradas, automáticas.
- Verificaciones periódicas mediante restauraciones de prueba.
- Infraestructura de respaldo en local y/o en la nube.

9.4. PRUEBAS DE CONTINUIDAD

- Se realizan **simulacros anuales** para validar la eficacia de los planes.
- Las lecciones aprendidas se documentan y aplican a la mejora de los procedimientos.
- Toda modificación en la infraestructura crítica conlleva una **revisión del plan de continuidad**.

10. FORMACIÓN Y CONCIENCIACIÓN



10.1. PRINCIPIOS

El **factor humano** es clave en la ciberseguridad. PROSELEC promueve una cultura organizativa basada en la **concienciación, la formación continua y la corresponsabilidad**.

10.2. PLAN DE FORMACIÓN

Incluye:

- Formación inicial al incorporarse.
- Formación específica por perfil de riesgo (administradores, desarrolladores, soporte).
- Formación sobre cumplimiento legal
- Formación sobre gestión de incidentes, phishing, ingeniería social y uso seguro de tecnologías.

10.3. CONCIENCIACIÓN CONTINUA

- Boletines informativos mensuales.
- Cartelería y recordatorios en espacios comunes.
- Campañas internas (mes de la ciberseguridad, simulacros de phishing).
- Test de autoevaluación para empleados.



10.4. EVALUACIÓN DE EFICACIA

- Indicadores de formación (cobertura, nivel de retención, satisfacción).
- Revisiones anuales del plan.
- Inclusión de resultados en revisiones por la dirección.

11. SUPERVISIÓN, AUDITORIA Y MEJORA CONTINUA

11.1. SUPERVISIÓN Y MONITOREO

- Supervisión en tiempo real de logs, accesos, tráfico, integridad y disponibilidad.
- Herramientas SIEM e IDS/IPS en sistemas críticos.
- Detección de anomalías y comportamientos no esperados.
-

11.2. AUDITORIA INTERNA Y EXTERNA

- Auditorías internas del CSI según el plan anual.
- Auditoría externa bianual ENS (para sistemas categoría MEDIA/ALTA).
- Resultados documentados y comunicados al Comité de Seguridad.

11.3. REVISIÓN POR LA DIRECCIÓN

- Se realiza una **revisión anual** del CSI, que evalúa:
 - No conformidades.
 - Progreso de objetivos.
 - Riesgos nuevos o modificados.
 - Incidentes ocurridos.
 - Recomendaciones de auditoría.
 - Propuestas de mejora.

11.4. MEJORA CONTINUA

- El CSI sigue el ciclo **PDCA (Plan-Do-Check-Act)**.
- Se establecen KPIs y métricas.
- Toda desviación relevante genera acciones correctivas.

12. CUMPLIMIENTO LEGAL Y NORMATIVO

12.1. COMPROMISO LEGAL

PROSELEC SEGURIDAD garantiza el cumplimiento de:

- **Ley Orgánica 3/2018 y Reglamento (UE) 2016/679 (GDPR)**.
- **LSSI-CE (Ley 34/2002)**.
- **Contratos suscritos con clientes, proveedores y socios**.
- **Propiedad intelectual y licencias** de software utilizado.
- **Obligaciones sectoriales** específicas que puedan aplicar.

12.2. PROTECCIÓN DEDATOS PERSONALES

- Existencia de **registro de tratamientos**.
- Evaluaciones de impacto (EIPD) cuando aplique.
- Delegado de Protección de Datos (DPO) designado.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Edición: 01 FECHA: 23/04/2025 Página 33 de 33 Conf.: Uso Interno
---	--	---

12.3. AUDITORIAS DE CUMPLIMIENTO

- Evaluación periódica del cumplimiento de normativas por parte del Comité de Seguridad.
- Registro y seguimiento de no conformidades legales o contractuales.

13. FIRMA Y VALIDACIÓN

La presente Política de Seguridad de la Información ha sido aprobada por Presidencia de PROSELEC SEGURIDAD S.A. y es de obligado cumplimiento para todo el personal, así como para colaboradores y terceros con acceso a sistemas o información bajo control de la organización.

Será revisada anualmente y siempre que existan cambios significativos en el entorno tecnológico, normativo o estructura

14. APROBADA Y VALIDADA POR PRESIDENCIA

23/04/2025

