PROSELEC

POLÍTICA DE SGSI

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.

Versión actual

Versión:	01
Fecha de la versión:	23/04/2025
Creado por:	Responsable SGSI
Aprobado por:	Presidencia
Objetivo:	Adaptación a ISO/IEC 27001:2022

Alcance de modificaciones

Edición	Fecha	Alcance de Modificaciones	Revisado	Aprobado
01	23/04/2025	Edición inicial	Resp. SGSI	Presidencia

INDICE

1. OBJETIVO Y DESARROLLO 4

1.1. ORGANIZACIÓN DE SEGURIDAD 6
1.2. GESTIÓN DE RIESGOS 8
1.3. GESTION DEL PERSONAL 9
1.4. PROFESIONALIDAD Y SEGURIDAD DE LOS RECURSOS HUMANOS 9
1.5. AUTORIZACIÓN Y CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN 11
1.6. PROTECCIÓN DE LAS INSTALACIONES 11
1.7. ADQUISICIÓN DE PRODUCTOS 13
1.8. SEGURIDAD POR DEFECTO 13
1.9. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA 14
1.10. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO 15
1.11. PREVENCIÓN DE SISTEMAS DE INFORMACIÓN INTERCONECTADOS 15
1.12. REGISTROS DE ACTIVIDAD. 15
1.13. CONTINUIDAD DE LA ACTIVIDAD 17
1.14. MEJORA CONTINUA DEL PROCESO DE SEGURIDAD 17
1.15. INFORMACION DOCUMENTADA Y CALIFICACION DE LA INFORMACION 17

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

1. OBJETIVO Y DESARROLLO

PROSELEC SEGURIDAD SA, como empresa dedicada a Sistemas de Información que soportan los servicios de diseño, integración, comercialización, instalación y servicio posventa de productos de seguridad (hardware y software), asume su compromiso con la seguridad de la información, comprometiéndose a la adecuada gestión de la misma, con el fin de ofrecer a todos sus grupos de interés las mayores garantías en torno a la seguridad de la información utilizada.

PROSELEC SEGURIDAD SA también considera de forma activa el contexto organizativo en el que opera, incluyendo los factores internos y externos que afectan a su capacidad para lograr los objetivos de seguridad de la información. Asimismo, se tienen en cuenta los requisitos pertinentes de las partes interesadas, tanto internas como externas, que puedan influir en la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI).

Por todo lo anteriormente expuesto, la Dirección establece los siguientes objetivos de seguridad de la información:

- Proporcionar un marco para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficaz.
- Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones
- Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

Para poder lograr estos objetivos es necesario:

- Mejorar continuamente nuestro sistema de seguridad de la información, conforme a los principios de mejora continua establecidos en la norma ISO/IEC 27001:2022

- Cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que suscribimos además de los compromisos adquiridos con los clientes, así como la actualización continua de los mismos. 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 311/2022, de 3 de mayo, de desarrollo del Esquema Nacional de Seguridad modificado por el Real Decreto 951/2015, de 23 de octubre.
    - Norma UNE-EN ISO/IEC 27001 para la seguridad de la información.
    - Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- Identificar las amenazas potenciales, así como el impacto en las operaciones de negocio que dichas amenazas, caso de materializarse, puedan causar.
- Preservar los intereses de sus principales partes interesadas (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.
- Trabajar de forma conjunta con nuestros suministradores y subcontratistas con el fin de mejorar la prestación de servicios de TI, la continuidad de los servicios y la seguridad de la información, que repercutan en una mayor eficiencia de nuestra actividad.
- Evaluar y garantizar la **competencia técnica del personal**, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros procesos, proporcionando la formación y la comunicación interna adecuada para que desarrollen buenas prácticas definidas en el sistema.
- Garantizar el **correcto estado de las instalaciones y el equipamiento** adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.
- Garantizar un **análisis** de manera continua de todos los **procesos relevantes**, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.
- Estructurar nuestro sistema de gestión de forma que sea fácil de comprender.

-

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

Nuestro sistema de gestión tiene la siguiente estructura:

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.

1.1. 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 establecidos en el Sistema de Gestión de Seguridad de la Información (SGSI), conforme a la norma ISO/IEC 27001:2022 y al Esquema Nacional de Seguridad (ENS). La alta dirección también debe demostrar liderazgo y compromiso con el sistema, promoviendo su integración en todos los procesos y asegurando el cumplimiento de los principios de seguridad.

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

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

Los roles o funciones de seguridad definidos son:

Función	Deberes y responsabilidades
Responsables del Sistema de Gestión de Seguridad de la Información (SGSI)	- Tomar las decisiones relativas a la información tratada - Coordinar la implantación del sistema - Mejorar el sistema de forma continua - Determinar la idoneidad de las medidas técnicas - Proporcionar la mejor tecnología para el servicio - Mejorar el sistema de forma continua - Coordinar la implantación del sistema
Dirección	- Proporcionar los recursos necesarios para el sistema - Liderar el sistema

Esta definición se completa en los perfiles de puesto y en los documentos del sistema.

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. Los miembros del comité de seguridad de la información son:

- Responsables del Sistema de Gestión de Seguridad de la Información
- Dirección Empresa (socios-administradores)

Funciones y responsabilidades del comité de seguridad.

Las funciones y responsabilidades del comité de seguridad se definen en REGISTROS\Acta comité de seguridad \ **AR220118_SGSI Acta de constitución SGSI** y **AR240916_SGSI Acta Reunión Transición a ISO-IEC 27001-2022**

Periodo de renovación del comité de seguridad.

Los miembros del comité de seguridad serán ratificados o sustituidos de forma anual, en la reunión del propio comité.

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

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:

Política de Seguridad de las Operaciones y comunicaciones ISO-IEC 27001-2022.pdf

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

1.2. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas, vulnerabilidades y los riesgos a los que están expuestos. Este análisis permitirá conocer el nivel de riesgo inherente y residual, y garantizará la aplicación de controles proporcionales y adecuados al contexto y criticidad de los activos implicados.Este análisis será revisado de forma periódica y, en todo caso, en los siguientes escenarios:

- 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 incorporen nuevos activos o tecnologías relevantes;
- ando cambien los requisitos legales, contractuales o regulatorios;
- cuando se reporten vulnerabilidades graves.

Con el objetivo de mantener la coherencia y trazabilidad, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los distintos servicios prestados, incluyendo criterios de impacto sobre la confidencialidad, integridad y disponibilidad (CID), conforme a lo exigido por la ISO/IEC 27001:2022 y el Esquema Nacional de Seguridad.

El Comité de Seguridad será responsable de promover y garantizar la disponibilidad de los recursos necesarios para atender a las necesidades de seguridad identificadas en los distintos análisis, impulsando aquellas inversiones de carácter horizontal que refuercen el nivel general de protección de los sistemas.

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

Para la realización del análisis de riesgos se aplicará la metodología establecida y documentada en el procedimiento **ANÁLISIS DE RIESGOS PROSELEC 2025.xlsx**, el cual contempla los criterios, escalado y valoración necesarios para una adecuada evaluación y tratamiento del riesgo, conforme a la cláusula 6.1 .

1.3. GESTION DEL PERSONAL

Todos los miembros de PROSELEC tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de PROSELEC asistirán a una sesión de concienciación en materia de seguridad al menos una vez al año. Además, se establecerá un programa de concienciación continua para garantizar que todos los empleados, colaboradores y partes relevantes reciban la información necesaria para desempeñar sus funciones de forma segura, con especial atención al personal de nueva incorporación o aquellos que cambien de rol.

Las personas con responsabilidad en el uso, operación o administración de sistemas recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El programa de formación y concienciación se alinea con los requisitos del control **A.6.3 (Concienciación, educación y formación en seguridad de la información)**, y tiene como objetivo reducir el riesgo derivado del factor humano mediante la sensibilización continua y la capacitación técnica adecuada.

El Comité de Seguridad, junto con el área de Recursos Humanos, será responsable de supervisar y evaluar la eficacia del programa formativo, asegurando su actualización frente a cambios normativos, tecnológicos o de amenazas emergentes.

1.4. PROFESIONALIDAD Y SEGURIDAD DE LOS RECURSOS HUMANOS

Los objetivos principales relacionados con la seguridad de los recursos humanos son:

- Reducir los riesgos de error humano, uso indebido de instalaciones y recursos, y manejo no autorizado de la información.
- Establecer responsabilidades de seguridad desde la etapa de reclutamiento, incluyendo su formalización en acuerdos laborales.
- Garantizar que el personal esté informado sobre las amenazas a la seguridad de la información y capacitado para cumplir con esta política durante sus actividades laborales.

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

- Formalizar compromisos de confidencialidad con todo el personal y usuarios externos.
- Promover mecanismos eficaces para la notificación de debilidades e incidentes de seguridad.

Profesionalidad:

- Determinar la competencia necesaria del personal en materia de seguridad de la información.
- Asegurar dicha competencia en base a formación, experiencia o cualificación adecuada.
- Conservar evidencia documentada que acredite la competencia del personal.

Esta política aplica a todos los trabajadores y personal externo que desempeñe funciones para PROSELEC.

Responsabilidades:

- **Recursos Humanos (RRHH):**
  - Incluir funciones de seguridad en las descripciones de los puestos.
  - Informar a los empleados sobre sus obligaciones en relación con la seguridad de la información.
  - Gestionar los compromisos de confidencialidad.
  - Coordinar las acciones formativas y de concienciación en colaboración con el Comité de Seguridad.
- **Equipo responsable de la gestión de seguridad de la información**
  - Supervisar, documentar y analizar los incidentes de seguridad reportados.
  - Comunicar dichos incidentes a los propietarios de la información y al Comité de Seguridad.
  - Colaborar en la redacción de compromisos de confidencialidad y asesorar sobre sanciones por incumplimiento de la política.
  - Establecer canales y procedimientos para la gestión de incidentes.
  - Supervisar la evolución de los incidentes y evaluar la eficacia de las acciones tomadas.
  - Impulsar medidas organizativas y técnicas para prevenir y resolver incidentes.

- **Compromiso del personal:**

Todo el personal de PROSELEC es responsable de comunicar de forma inmediata cualquier debilidad o incidente de seguridad que detecte en el curso de sus actividades.
Este apartado está alineado con los controles:

- **A.6.1 – Selección y contratación**
- **A.6.2 – Condiciones contractuales**

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

1.5. AUTORIZACIÓN Y CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

El control del acceso a los sistemas de información tiene por objetivo:

- Evitar el acceso no autorizado a sistemas de información, bases de datos y servicios de información.
- Implementar la seguridad en el acceso de los usuarios a través de técnicas de autenticación robusta y autorización basada en roles y necesidades de negocio.
- Controlar la seguridad en la conexión entre la red de PROSELEC y otras redes públicas o privadas, aplicando medidas como VPN, firewalls, y segregación de red.
- Revisar y registrar los eventos críticos y las actividades llevadas a cabo por los usuarios en los sistemas, conforme al principio de responsabilidad y trazabilidad.
- Concienciar a los usuarios sobre su responsabilidad en el uso seguro de credenciales (contraseñas, tokens, certificados) y del equipo asignado.
- Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles, dispositivos móviles y equipos personales para el trabajo remoto o en movilidad, conforme a las políticas de BYOD y teletrabajo establecidas.

Este punto está alineado con los controles del dominio **A.5 (Controles organizativos)** y **A.8 (Controles tecnológicos)**:

- **A.5.16** Gestión de identidades
- **A.5.17** Información de autenticación
- **A.5.18** Derechos de acceso
- **A.5.19** Revisión de derechos de acceso
- **A.8.4** Servicios de acceso remoto
- **A.8.5** Autenticación segura

El cumplimiento de estas medidas forma parte del compromiso de PROSELEC con la protección de los activos de información y la mitigación de riesgos derivados del acceso no controlado a los sistemas.

1.6. PROTECCIÓN DE LAS INSTALACIONES

Los objetivos de esta política son:

- Prevenir el acceso no autorizado, daños e interferencias a la sede, instalaciones e información de PROSELEC.
- Proteger el equipo de procesamiento de información crítico, ubicándolo en áreas protegidas, con un perímetro de seguridad definido y controles físicos y lógicos adecuados. También se garantizará su protección durante traslados o mientras se encuentren fuera de dichas áreas por mantenimiento u otras razones justificadas.
- Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento de los sistemas y equipos que gestionan la información de PROSELEC.

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

- Aplicar medidas de protección adecuadas al contexto operativo de las oficinas, garantizando la confidencialidad y seguridad de la información manejada por el personal.
- Asegurar que las medidas implementadas sean proporcionales a los riesgos identificados en el análisis de riesgos.

Esta política se aplica a todos los recursos físicos relacionados con los sistemas de información de PROSELEC, incluyendo:

- Instalaciones
- Equipos
- Cableado estructurado
- Expedientes físicos
- Medios de almacenamiento, entre otros.

El Responsable del Sistema de Gestión de Seguridad de la Información (RSGSI) [CISO], en colaboración con los propietarios de la información, definirá las medidas físicas y ambientales necesarias para la protección de los activos críticos, basándose en los resultados del análisis de riesgos, conforme a los controles del dominio **A.7 (Controles físicos)**
Asimismo, el CISO supervisará la implementación y cumplimiento de las disposiciones relacionadas con la seguridad física y ambiental.
Los responsables de cada departamento definirán los niveles de acceso físico del personal a las zonas restringidas bajo su responsabilidad. Los propietarios de información autorizarán formalmente el trabajo fuera de sitio con información sensible cuando se considere oportuno, garantizando que se implementen las medidas necesarias para mantener el nivel de seguridad exigido.
Todo el personal de PROSELEC es responsable de cumplir con la política de escritorio limpio y pantalla bloqueada, contribuyendo así a la protección de la información en el entorno habitual de trabajo.

Este punto se alinea con los siguientes controles:

- **A.7.1 a A.7.14**, incluyendo la protección del perímetro, control de accesos físicos, escritorio limpio, ubicación del equipamiento, mantenimiento, eliminación segura, entre otros.

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

1.7. ADQUISICIÓN DE PRODUCTOS

Los diferentes departamentos deben garantizar que la seguridad de las tecnologías de la información y comunicaciones (TIC) esté integrada en cada etapa del ciclo de vida de los sistemas, desde su concepción hasta su retirada de servicio, incluyendo las fases de desarrollo, adquisición, implantación, operación, mantenimiento y desmantelamiento.
Los requisitos de seguridad de la información deberán ser identificados desde la fase de planificación e incluidos en:

- La definición de necesidades y análisis de viabilidad.
- Las solicitudes de oferta y condiciones contractuales.
- Los pliegos de licitación y evaluación de proveedores.
- Los planes de mantenimiento y gestión del cambio.

  Asimismo, deberá garantizarse que se contemplen las necesidades asociadas a:
- Evaluación de riesgos vinculados a los sistemas o servicios a adquirir.
- Compatibilidad con la arquitectura de seguridad existente.
- Financiación de medidas de seguridad durante todo el ciclo de vida.
- Formación técnica asociada a nuevas tecnologías implementadas.

  En lo relativo a la adquisición y mantenimiento de sistemas de información, se prestará especial atención a:
- La validación de controles de seguridad en software adquirido o desarrollado internamente.
- La documentación técnica y de seguridad asociada.
- Las actualizaciones, parches y gestión del cambio de forma controlada.

La seguridad deberá mantenerse activa durante la operación del sistema y garantizarse en procesos como la retirada, eliminación o reutilización de equipos y software.
Estas directrices están alineadas con los controles:

- **A.5.10 - Adquisición, desarrollo y mantenimiento de sistemas**
- **A.8.9 - Instalación de software**
- **A.8.11 - Separación de entornos de desarrollo, prueba y producción**
- **A.5.14 - Gestión de la seguridad de los cambios**

La política de desarrollo, adquisición y mantenimiento de sistemas de información se encuentra documentada en: **Política Adquisición, Desarrollo y Mantenimiento de Sistemas**.

1.8. SEGURIDAD POR DEFECTO

PROSELEC considera estratégico para la entidad que los procesos y sistemas integren la seguridad de la información desde su concepción, aplicando el principio de "seguridad por defecto" y "seguridad desde el diseño". Esto implica que la seguridad se incorpora como una característica básica e indispensable en cada etapa del ciclo de vida de los sistemas de

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

información, desde su diseño, desarrollo o adquisición, hasta su operación y retirada de servicio.

La seguridad por defecto implica que:

- Los sistemas y servicios deben estar configurados con los niveles mínimos de exposición y con controles de protección activos desde su implantación.
- Las configuraciones inseguras o no justificadas deben ser deshabilitadas por defecto.
- Se aplican controles técnicos y organizativos apropiados sin necesidad de intervención del usuario final.
- Las decisiones de desarrollo y adquisición deben priorizar soluciones que incorporen buenas prácticas de seguridad y cumplimiento por diseño.
- El mantenimiento operativo debe garantizar que las actualizaciones no afecten negativamente al nivel de seguridad establecido.

Este enfoque se alinea con los principios del control **A.5.**

1.9. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

PROSELEC se compromete a garantizar la integridad del sistema mediante un proceso formal de gestión de cambios que asegure el control previo y posterior de las modificaciones en los componentes físicos y lógicos del sistema de información.

Antes de la implantación de cualquier cambio, este será evaluado por el área de sistemas TIC para valorar su impacto en la seguridad. Aquellos cambios clasificados como significativos o con implicaciones en la seguridad serán autorizados, documentados y gestionados conforme al procedimiento establecido.

Asimismo, se realizarán revisiones periódicas de seguridad para verificar el estado de los sistemas respecto a:

- Especificaciones del fabricante
- Vulnerabilidades conocidas
- Disponibilidad y aplicación de actualizaciones

Estas acciones permiten actuar con agilidad ante posibles riesgos, reforzando la protección y continuidad del entorno tecnológico de PROSELEC.

Este apartado está alineado con los controles:

- **A.5.14 – Gestión de la seguridad de los cambios**
- **A.8.8 – Protección contra código malicioso**
- **A.8.9 – Instalación de software**
- **A.8.10 – Limitación de instalación de software**

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

1.10. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

PROSELEC implementa medidas técnicas y organizativas para garantizar la protección de la información tanto en reposo como durante su transmisión, especialmente cuando esta circula o se almacena en entornos considerados inseguros.

Se consideran entornos inseguros aquellos en los que la información puede estar expuesta a riesgos elevados, tales como equipos portátiles, dispositivos móviles (incluyendo tablets y smartphones), medios de almacenamiento removibles y comunicaciones a través de redes públicas o con cifrados obsoletos o débiles.

Para mitigar estos riesgos, se adoptan mecanismos como el cifrado robusto, controles de acceso, segmentación de redes y procedimientos seguros de transferencia y almacenamiento. Estas medidas forman parte de la estrategia integral de protección de activos de información, y se revisan periódicamente para adaptarse a las amenazas emergentes.

Este apartado está alineado con los controles:

- A.5.10 – Políticas para el uso de criptografía
- A.8.23 – Protección de la información en tránsito
- A.8.24 – Protección de la información almacenada
- A.8.28 – Uso seguro de servicios en la nube
- A.5.17 – Supervisión, revisión y mejora de los controles de seguridad de la información

1.11. PREVENCIÓN DE SISTEMAS DE INFORMACIÓN INTERCONECTADOS

PROSELEC establece medidas de protección para asegurar la integridad, confidencialidad y disponibilidad de los sistemas de información en escenarios de interconexión, especialmente cuando se conectan a redes públicas o de terceros, como es el caso de servicios de comunicaciones electrónicas accesibles al público.

Se realiza un análisis detallado de riesgos antes de permitir cualquier tipo de interconexión, considerando las vulnerabilidades asociadas al perímetro y los posibles vectores de ataque. Los puntos de unión entre redes son gestionados bajo estrictos controles de seguridad, incluyendo segmentación de red, sistemas de detección y prevención de intrusos (IDS/IPS), firewalls de nueva generación y mecanismos de autenticación robusta.

Estas medidas se complementan con procedimientos de monitoreo continuo, revisión periódica de configuraciones y actualización de controles de acuerdo con la evolución del panorama de amenazas.

Este apartado está alineado con los controles:

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

- A.5.15 – Principios de ingeniería de seguridad
- A.7.4 – Separación de entornos de desarrollo, prueba y producción
- A.8.20 – Seguridad de los servicios de red
- A.8.21 – Seguridad de servicios en red prestados externamente
- A.8.22 – Interconexiones de sistemas de información

1.12. REGISTROS DE ACTIVIDAD.

PROSELEC mantendrá registros detallados de las actividades de los usuarios y de los sistemas, asegurando la disponibilidad de información suficiente para monitorear, analizar, investigar y documentar acciones indebidas o no autorizadas. Estos registros permitirán, en todo momento, identificar a la persona responsable de una acción concreta, garantizando trazabilidad y responsabilidad.
Asimismo, se establece un sistema integral para la gestión de incidentes de seguridad de la información, con el objetivo de:

- Detectar y responder de forma oportuna a código malicioso y otras amenazas.
- Disponer de procedimientos formalizados para el reporte, análisis, tratamiento, resolución y documentación de incidentes y vulnerabilidades detectadas en el sistema de información.
- Clasificar los incidentes según su criticidad e impacto potencial.
- Registrar todas las actuaciones realizadas como base para la mejora continua del sistema.
- Asegurar la continuidad operativa y el restablecimiento óptimo de los servicios IT.
- Minimizar los impactos técnicos, operativos y reputacionales derivados de incidentes de seguridad.
- Comunicar, de forma estructurada, el impacto de los incidentes a las partes interesadas relevantes y activar protocolos de respuesta rápida.
- Fomentar una cultura organizacional resiliente y eficiente frente a incidentes de ciberseguridad.

Este apartado está alineado con los controles:

- A.5.1 – Políticas de seguridad de la información
- A.5.28 – Gestión de incidentes de seguridad de la información
- A.5.29 – Evaluación posterior a los incidentes de seguridad de la información
- A.8.12 – Registro de actividades
- A.8.16 – Monitoreo de sistemas
- A.8.15 – Control de acceso a programas fuente
- A.8.7 – Protección contra código malicioso

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

1.13. CONTINUIDAD DE LA ACTIVIDAD

PROSELEC con el objetivo de garantizar la continuidad de las actividades establece medidas para que los sistemas dispongan de copias de seguridad y establece mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

1.14. MEJORA CONTINUA DEL PROCESO DE SEGURIDAD

PROSELEC establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y metodología establecida en normas internacionales como ISO 27001.

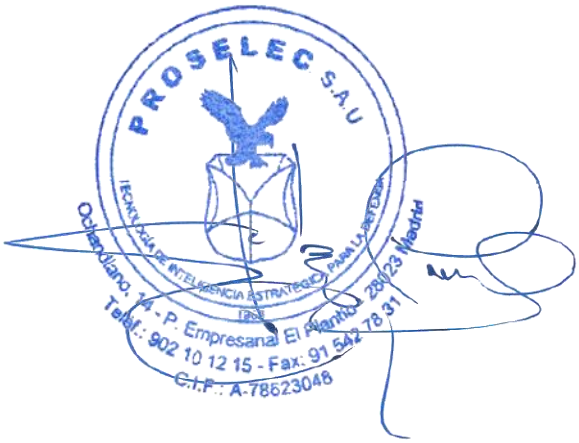
1.15. INFORMACION DOCUMENTADA y CALIFICACION DE LA INFORMACION

PROSELEC establece criterios y procedimientos formales para la gestión de la información documentada, asegurando su adecuada creación, revisión, aprobación, control de versiones, acceso, distribución, almacenamiento y conservación, conforme a su valor, criticidad y nivel de sensibilidad.
La estructuración y control de la documentación relacionada con la seguridad del sistema de información se encuentra definida en el procedimiento: **PROCEDIMIENTO DE ELEBORACIÓN DE LA DOCUMENTACIÓN.pdf**
Adicionalmente, PROSELEC aplica una política de clasificación de la información, detallada en el documento: **Clasificación activos PROSELEC.xlsx**, donde se establecen los niveles de confidencialidad y las medidas de protección asociadas para cada tipo de activo de información. Esta clasificación permite aplicar controles proporcionales según la sensibilidad y el impacto potencial de su divulgación, modificación o pérdida.
Estas prácticas aseguran el cumplimiento normativo, la protección de los activos de información y una gestión eficiente del conocimiento organizacional.
Este apartado está alineado con los controles:

- A.5.2 – Información documentada de seguridad de la información
- A.5.3 – Clasificación de la información
- A.5.4 – Gestión de activos
- A.8.1 – Gestión del ciclo de vida de la información

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI

En Madrid, a 23 de abril de 2025



Presidencia

El presente Documento es propiedad exclusiva de PROSELEC SEGURIDAD, quedando prohibida su reproducción sin el consentimiento del Responsable de SGSI