Política de Seguridad de la Información de ASOCIACIÓN PUNTO OMEGA

ÍNDICE

1. IDENTIFICACIÓN DEL DOCUMENTO

Título del documento:	Política de Seguridad de la Información
Código del documento:	PSI-APO-001
Versión:	1.0
Fecha de aprobación:	30 de abril de 2026
Fecha de vigencia:	Hasta nueva versión
Próxima revisión:	30 de abril de 2027
Responsable de la Política:	David Barriopedro Ayuso.
Responsable de la Seguridad:	Andrés Carmona Durán
Aprobado por:	Asamblea de la Asociación Punto Omega
Distribución:	Todo el personal, voluntarios y colaboradores
Clasificación:	PÚBLICO

2. MISIÓN DE LA ORGANIZACIÓN

La Asociación Punto Omega tiene como misión la intervención social y sanitaria con colectivos vulnerables y reconoce que la información es un activo fundamental para el cumplimiento de su **misión**, la prestación de servicios a las personas que atiende y la protección de los derechos de las personas que confían en ella.

Esta Política de Seguridad de la Información (PSI) establece el marco general de actuación para proteger frente a daños accidentales o deliberados que puedan afectar a la confidencialidad, integridad autenticidad, trazabilidad y disponibilidad de la información tratado o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor

de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados, tanto para los productos que desarrolla y sus servicios asociados, cómo en lo que se refiere al software base adquirido de terceros.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS (Artículo 8. Prevención, detección, respuesta y conservación).

3. ALCANCE

Esta Política es de aplicación a:

- **Personas**: Todos los miembros de la Junta Directiva, personal por cuenta propia o ajena, voluntariado, alumnado en prácticas, colaboradores y cualquier persona que acceda a los sistemas o información de la Asociación Punto Omega.
- **Activos de Información**: Todos los datos, información y sistemas de información propiedad de la Asociación o bajo su custodia, independientemente de su formato (electrónico, papel, audiovisual, etc.).
- **Ubicaciones**: Todas las sedes, oficinas, locales y espacios donde se desarrollen actividades de la Asociación, incluyendo el acceso remoto y los dispositivos móviles utilizados para el desarrollo de la actividad.

- **Procesos**: Todas las actividades y procesos de la Asociación que involucren la creación, recepción, tratamiento, almacenamiento o transmisión de información.

4. OBJETIVOS

- Proporcionar un marco que nos permita una gestión eficaz de la información.
- Establecer las condiciones que permitan la recuperación rápida y eficiente de los servicios frente a desastres o contingencias que puedan ocurrir y pongan en riesgo la continuidad de los servicios.
- 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 con independencia del soporte que se trate.

5. MARCO NORMATIVO

Uno de los objetivos debe ser el de cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que suscribimos además de los compromisos adquiridos con los grupos de interés, así como la actualización continua de los mismos. Para ello, 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.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la

Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)

6. DESARROLLO

Para poder lograr nuestros objetivos es necesario:

- Realizar un registro de las actividades de tratamiento de la información.
- Identificar las amenazas potenciales, así como el impacto en las distintas actuaciones de los servicios que dichas amenazas, caso de materializarse, puedan causar.
- Preservar los intereses de los grupos de interés (personas usuarias, voluntarias, trabajadoras, …).
- Trabajar de forma conjunta con nuestros proveedores con el fin de mejorar los servicios de Tecnología de la Información, la continuidad de los servicios prestados y la seguridad de la información, que repercutan en una mayor eficiencia de nuestra actividad.
- Evaluar y garantizar las competencias técnicas del personal en el uso de las herramientas y promover la participación activa en la mejora de los procesos de tratamiento de la información, proporcionando la formación y herramientas adecuadas para el desarrollo de las buenas prácticas definidas en el sistema.
- Garantizar los equipamientos tecnológicos adecuados al uso de los tratamientos que se requieren para la prestación correcta de los servicios así como el correcto estado de las instalaciones.
- Garantizar un análisis de manera contínua de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.

- Estructurar el sistema de gestión de la información de forma comprensible para todas las personas que forman parte de la organización, dando acceso a cada miembro de la misma en función de los perfiles y requisitos de acceso definidos.

7. ORGANIZACIÓN DE SEGURIDAD

En última instancia, la responsabilidad recae sobre la Junta Directiva y por delegación en la Dirección General de la Asociación, en tanto en cuanto es responsable de organizar las funciones y responsabilidades así como facilitar los recursos adecuados para conseguir adecuar la organización a los requerimientos del ENS. También los miembros de la Junta Directiva y las direcciones de los programas tienen la responsabilidad de servir de ejemplo en el cumplimiento de los requerimientos de seguridad establecidos.

Las diferencias de criterio que puedan surgir se tratarán en el seno del comité de seguridad.

8. COMITÉ DE SEGURIDAD

El comité de seguridad es el órgano de mayor responsabilidad dentro del sistema de gestión de seguridad de la información. Todas las decisiones importantes relacionadas con el sistema se acuerdan por este comité, que estará formado por:

1. Responsable de la información.
2. Responsable de la seguridad.
3. Responsable del sistema.
4. Dirección General.

El comité de seguridad responderá ante la Junta Directiva de la Asociación Punto Omega, si bien será autónomo en la toma de decisiones.

La organización de la seguridad de la información se desarrolla en un documento complementario a esta Política de Seguridad de la Información y se complementará con el

resto de políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión de la información.

9. REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Se mantendrá actualizado un inventario de las actividades de tratamiento realizadas por la organización donde se relacionarán todos los tratamientos autorizados en cada uno de los servicios prestados por la organización y por los propios servicios centrales de la Asociación, así como los mecanismos adoptados para su gestión.

10. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se revisará regularmente:

- Al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

El análisis de riesgos establecerá una valoración del sistema en función de la información a tratar y el servicio que compromete.

Para la realización del análisis de riesgos se tendrá en cuenta la metodología de análisis de riesgos Magerit 3.0.

11. GESTIÓN DE PERSONAL

Todo el equipo humano de Punto Omega tiene 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 todos los afectados.

Todo el personal de la entidad participará en las sesiones de formación que se programen para la concienciación en materia de seguridad y de uso seguro de herramientas TIC.

Se facilitará a las personas trabajadoras, en especial en el momento de su incorporación, información relativa a las medidas de seguridad a adoptar en el tratamiento de la información que su servicio requiere. Las direcciones de los programas serán responsables de facilitar dicha información a las nuevas incorporaciones a la plantilla.

12. PROFESIONALIDAD Y SEGURIDAD DE LOS RECURSOS HUMANOS

Esta Política se aplica a todo el personal de la Asociación Punto Omega y al personal externo que realice tareas dentro de las instalaciones de los servicios de Punto Omega.

Recursos Humanos informará en el momento de la contratación de las obligaciones con respecto al cumplimiento de la Política de Seguridad de la Información, gestionará los compromisos de confidencialidad correspondientes y coordinará las tareas de capacitación de los usuarios con respecto a esta política.

El Responsable de la Seguridad de la Información, es responsable de monitorizar, documentar y analizar los incidentes de seguridad reportados, así como comunicar al Comité de Seguridad de la Información (CSI) y a los propietarios de la información.

El Comité de Seguridad de la Información (CSI) será responsable de establecer los medios y canales necesarios para que el responsable de Seguridad maneje informes de incidentes y anomalías del sistema. El Comité también estará al tanto, supervisará la investigación, supervisará la evolución de la información y promoverá la resolución de incidentes de seguridad de la información.

El responsable de la Seguridad y el Delegado de Protección de datos participarán en la preparación del Compromiso de Confidencialidad que firmarán las nuevas contrataciones (tanto cuenta propia como ajena).

Todo el equipo humano de Punto Omega es responsable de informar acerca de las debilidades, vulnerabilidades e incidentes de seguridad de la información que se detecten de forma inmediata y por los canales de comunicación establecidos.

La formación de los recursos humanos estará orientada a evaluar la adecuación de los conocimientos para el uso de las herramientas TIC y la información que tengan asignadas a fin de:

- Reducir riesgos de error humano, uso indebido de equipos y recursos y manejo no adecuado de información.
- Verificar el conocimiento y el cumplimiento de las medidas de seguridad durante el desempeño de las tareas.
- Asegurar que el personal esté al tanto de las amenazas y preocupaciones de seguridad de la información y esté capacitado para apoyar la Política de Seguridad de la Información.
- Conocer los cauces para reportar incidencias y vulnerabilidades detectadas a fin de minimizar sus efectos y prevenir reincidencias.

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

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

- Evitar accesos no autorizados a sistemas de información y bases de datos.
- Implantar la seguridad en el acceso de los usuarios a través de técnicas de autenticación y autorización.
- Controlar la seguridad de las redes de Punto Omega.
- Revisar los eventos críticos y las actividades llevadas a cabo por los usuarios en los sistemas.

- Concienciar acerca de la responsabilidad en la gestión de las contraseñas en las aplicaciones y los equipos.
- Garantizar la seguridad de la información cuando se utilicen ordenadores portátiles y de sobremesa para el trabajo.

14. PROTECCIÓN DE LAS INSTALACIONES.

Los objetivos de esta política en materia de protección de las instalaciones son:

- Prevenir el acceso no autorizado, daños, robos e interferencias a las instalaciones de Punto Omega.
- Controlar los accesos por personal no autorizado a los equipos de trabajo de Punto Omega.
- Establecer las medidas de control establecidas para la protección de la información manejada por el personal de los distintos programas en función del inventario de las actividades de tratamiento.
- Proporcionar protección proporcional a los riesgos identificados.

Esta política se aplica a todos los recursos físicos relacionados con los sistemas de información: instalaciones, equipos, cableado, expedientes, medios de almacenamiento, …

Hay que resaltar que todos los sistemas de tratamiento de información en soporte digital se encuentran ubicados externamente en un hosting seguro, por lo que son únicamente los portátiles y periféricos los que se deben proteger localmente, además de los ficheros físicos que contienen información a proteger.

El responsable de seguridad, junto con el Responsable de la Información definirá las medidas de seguridad física y ambiental para la protección de los activos críticos, sobre la base de un análisis de riesgos y supervisará su aplicación. También verificará el cumplimiento de las disposiciones de seguridad física y medioambiental.

El responsable de seguridad junto a las direcciones de los programas definirán los niveles de acceso físico a las áreas restringidas bajo su responsabilidad, estableciendo los registros de acceso oportunos.

El responsable de seguridad autorizará formalmente el trabajo fuera de las instalaciones de Punto Omega cuando sea necesario y se considere apropiado.

Todo el equipo humano de Punto Omega es responsable del cumplimiento de la política de pantalla limpia y escritorio limpio, para la protección de la información relacionada con el trabajo diario

15. ADQUISICIÓN DE PRODUCTOS.

La seguridad de la información será una parte integral en todo el proceso de adquisición de equipos o software, así como en los desarrollos que se puedan acometer.

16. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO.

Establecer medidas de protección para la Seguridad de la información almacenada o en tránsito, bien porque se realice a través de redes que puedan comprometer la seguridad o con un cifrado débil o bien porque se trate de información en soporte físico y deba protegerse de accesos no autorizados o transportarse en soportes autorizados por personas claramente identificadas.

Clasificación y etiquetado de la información: cada persona deberá conocer el nivel de confidencialidad de la información que maneja.

Control de accesos: bajo el principio de mínimo privilegio y asegurando la fortaleza de las contraseñas utilizadas.

Protección adecuada de los equipos y dispositivos que tengan acceso a los sistemas.

Seguridad en las comunicaciones.

Notificación inmediata de las incidencias.

Formación y concienciación del equipo humano.

17. REGISTROS DE ACTIVIDAD.

Los sistemas dispondrán de un log con el suficiente nivel de detalle que permita registrar todas las actividades de los usuarios a fin de monitorizar, analizar, investigar y documentar cualquier actuación indebida o no autorizada, permitiendo asegurar la trazabilidad de las actuaciones.

En los soportes físicos se deberá asegurar la misma información.

Para ello se dispondrá de un procedimiento que permitirá detectar y gestionar los incidentes de seguridad y las debilidades detectadas, resolverlas y comunicar a las partes afectadas e interesadas la situación identificada y las medidas adoptadas.

Estos registros deberán ser utilizados en mejora continua del sistema y reducir los riesgos e impactos que puedan causar los incidentes.

18. CONTINUIDAD DE LA ACTIVIDAD

Con el objetivo de garantizar la continuidad de los servicios y la integridad de la información, se acordará con los proveedores un sistema copias de seguridad y de restablecimiento de los servicios en caso de incidentes graves.

19. MEJORA CONTÍNUA DEL PROCESO DE SEGURIDAD

Punto Omega establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y metodología establecida en el Esquema Nacional de Seguridad (ENS).

20. DOCUMENTOS RELACIONADOS

1. Registro de Actividades de Tratamiento (RGPD).
2. Análisis de riesgos.
3. Procedimiento de Gestión de Incidentes de Seguridad.
4. Política de Uso Aceptable de los Recursos Informáticos.
5. Procedimiento de Copias de Seguridad (Backup).
6. Documentación del **proceso de autorización**.