POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Índice

1. Aprobación y entrada en vigor

La presente Política de Seguridad de la Información ha sido aprobada por las Direcciones de las entidades incluidas en el alcance del Sistema de Gestión de Seguridad de la Información (SGSI), conforme al Esquema Nacional de Seguridad (ENS) y a la norma ISO/IEC 27001:2022

- **Fundació Catalana de l'Esplai / Fundesplai.**
- **7 i Tria, S.L.**
- **Fundación Esplai Ciudadanía Comprometida.**

Esta Política estará vigente desde la fecha de aprobación y permanecerá en vigor hasta que sea sustituida por una nueva versión.

2. Introducción

Las entidades incluidas dependen de los sistemas de información para desarrollar sus actividades, prestar sus servicios y cumplir sus objetivos. Estos sistemas deben administrarse con diligencia, aplicando medidas adecuadas y proporcionales al riesgo para protegerlos frente a daños accidentales o deliberados que puedan afectar a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada y de los servicios prestados.

El objetivo último de la seguridad de la información es garantizar que las entidades puedan desarrollar sus funciones y prestar sus servicios con calidad, continuidad y confianza, actuando preventivamente, supervisando la actividad y reaccionando con celeridad ante incidentes.

Los sistemas TIC (Tecnologías de la Información y la Comunicación) deben estar protegidos frente a amenazas cambiantes con potencial impacto sobre la información, los servicios, las personas usuarias, las entidades colaboradoras, los proveedores y el funcionamiento interno. Para ello, se aplicará una estrategia de seguridad basada en el Esquema Nacional de Seguridad, en la norma ISO/IEC 27001:2022, en la gestión de riesgos, en la vigilancia continua, en la respuesta ante incidentes y en la mejora continua.

La seguridad deberá estar integrada en todas las fases del ciclo de vida de los sistemas: concepción, adquisición, desarrollo, implantación, explotación, mantenimiento y retirada. Los requisitos de seguridad y las necesidades asociadas deberán tenerse en cuenta en la planificación, contratación, adquisición de servicios TIC, desarrollo de aplicaciones, gestión de proveedores y prestación de servicios.

3. Alcance

Esta Política se aplica a los sistemas de información incluidos en el alcance ENS y en el alcance del SGSI de las siguientes entidades:

- Fundació Catalana de l'Esplai / Fundesplai.
- 7 i Tria, S.L.
- Fundación Esplai Ciudadanía Comprometida.

Las entidades incluidas desarrollan actividades educativas, sociales, ambientales, de ocio educativo, servicios escolares, formación, inclusión digital, acompañamiento a entidades, proyectos europeos, soporte al Tercer Sector y gestión de servicios dirigidos a personas, familias, centros educativos, entidades sociales, administraciones y comunidad en general.

La certificación se plantea de forma individual para cada entidad. No obstante, existe un modelo tecnológico y de seguridad con elementos comunes y centralizados, especialmente en lo relativo a infraestructura, plataformas corporativas, gestión técnica, soporte, control de accesos, copias de seguridad, seguridad técnica, proveedores y evidencias.

La Política se aplicará a todo el personal, personas colaboradoras, terceros, proveedores y prestadores de servicios que accedan a información, activos o sistemas incluidos dentro del alcance ENS y/o del SGSI de cualquiera de las entidades indicadas.

4. Misión

Para alcanzar sus objetivos, les entidades asumen su compromiso con la seguridad de la información, comprometiéndose a la adecuada gestión de esta, con el fin de ofrecer a todos sus clientes las mayores garantías en torno a la seguridad de la información utilizada. Los sistemas serán administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

En este sentido, la misión y objetivos de seguridad que esta Política pretende garantizar son:

- Asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.
- Garantizar la continuidad de los servicios incluidos en el alcance ENS y/o del SGSI.
- Implantar medidas de seguridad en función del riesgo, de la categorización del sistema y de los requisitos aplicables del ENS y/o del SGSI.
- Aplicar el principio de mínimo privilegio y reforzar el deber de confidencialidad.
- Formar y concienciar al personal en seguridad de la información.
- Proteger los activos físicos y lógicos mediante controles proporcionales al riesgo.
- Establecer controles de seguridad en las comunicaciones, accesos remotos, redes y servicios cloud.
- Integrar la seguridad en la adquisición, desarrollo, mantenimiento y retirada de sistemas.
- Gestionar incidentes para su detección, contención, mitigación, resolución y prevención de recurrencias.
- Proteger los datos personales conforme al RGPD (Reglamento General de Protección de Datos), la LOPDGDD (Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales" y los riesgos asociados a los tratamientos.
- Supervisar de forma continuada el estado de la seguridad e impulsar la mejora continua.

Los objetivos de seguridad de la información se establecerán, revisarán y actualizarán periódicamente, de forma coherente con esta Política, con los riesgos identificados, con los requisitos ENS y con los requisitos del SGSI conforme a ISO/IEC 27001:2022.

5. Principios rectores de la política

La seguridad de la información se regirá por los siguientes principios:

- **Alcance estratégico:** la seguridad debe estar alineada con la misión, objetivos y actividades de las entidades incluidas.
- **Seguridad integral:** la protección debe contemplar personas, procesos, información, instalaciones, tecnología y proveedores.

- **Gestión basada en riesgos:** las medidas de seguridad se adoptarán en función de un análisis de riesgos previo y serán proporcionales a los riesgos identificados.
- **Prevención, detección, respuesta y recuperación:** se impulsarán medidas para prevenir incidentes, detectarlos a tiempo, responder adecuadamente y recuperar la operativa afectada.
- **Defensa en profundidad:** se establecerán controles en distintas capas organizativas, físicas, lógicas y operativas.
- **Vigilancia y mejora continuas:** el estado de la seguridad se revisará periódicamente para detectar desviaciones y mejorar los controles implantados.
- **Diferenciación de responsabilidades:** las funciones y responsabilidades en materia de seguridad estarán definidas de forma clara y separada, siempre que sea posible.
- **Coordinación entre entidades:** los elementos comunes del modelo tecnológico y de seguridad deberán gestionarse de forma coordinada entre las entidades incluidas.

6. Marco normativo

La presente Política se fundamenta, entre otras, en las siguientes normas y referencias:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Reglamento General de Protección de Datos —RGPD, Reglamento (UE) 2016/679.
- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales —LOPDGDD—.
- Ley 9/2017, de Contratos del Sector Público, cuando aplique.
- Ley 34/2002, de servicios de la sociedad de la información y comercio electrónico —LSSI-CE—.
- Guías CCN-STIC relacionadas con el ENS.
- Norma ISO/IEC 27001:2022, Sistemas de Gestión de la Seguridad de la Información.
- Normativa sectorial, contractual o administrativa aplicable a los servicios prestados.

La identificación, revisión y seguimiento de los cambios normativos y requisitos legales aplicables se realiza de acuerdo con el procedimiento de **Determinación de las obligaciones legales**. Para los requisitos ambientales, de seguridad industrial y de pública concurrencia, se aplica adicionalmente el procedimiento de **Determinación de las obligaciones legales, ambientales, de seguridad industrial y de pública concurrencia.**

Cuando un cambio normativo pueda afectar al sistema de información o al cumplimiento del ENS, se comunica a las personas responsables correspondientes para valorar su impacto y adoptar las medidas necesarias.

7. Organización de la seguridad

La organización de la seguridad se articula mediante los roles ENS definidos en el Real Decreto 311/2022, diferenciando las responsabilidades sobre la información, los servicios, la seguridad y la operación técnica del sistema.
Los roles principales son los siguientes:

- **Responsable de la Información:** determina los requisitos de seguridad de la información tratada, especialmente en relación con su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Participa en la valoración de la

información, la categorización del sistema y la aceptación del riesgo residual que afecte a la información bajo su responsabilidad.

- **Responsable del Servicio:** determina los requisitos de seguridad de los servicios prestados y valora el impacto que tendría una interrupción, degradación o alteración del servicio. Participa en la definición de prioridades de continuidad, recuperación y tratamiento de riesgos.
- **Responsable de Seguridad:** coordina, impulsa y supervisa la seguridad de la información, velando por la implantación y seguimiento de las medidas ENS. Supervisa el cumplimiento de la Política de Seguridad, la Declaración de Aplicabilidad, el análisis y tratamiento de riesgos, la gestión de incidentes, las auditorías y las acciones de mejora.
- **Responsable del Sistema:** se encarga de la explotación, administración y control técnico del sistema de información. Garantiza que las decisiones de seguridad se implantan correctamente en la infraestructura, aplicaciones, comunicaciones, accesos, configuraciones, actualizaciones, copias de seguridad y procedimientos técnicos.

Asimismo, se constituye un **Comité de Seguridad de la Información** como órgano de gobierno, coordinación y seguimiento de la seguridad. Sus funciones principales son supervisar la aplicación de esta Política, revisar riesgos, incidentes, auditorías y planes de acción, resolver conflictos entre roles cuando sea necesario e impulsar la mejora continua de la seguridad.

La designación concreta de personas responsables, la composición del Comité de Seguridad y el funcionamiento detallado del modelo de gobierno se establecen en los documentos:

- **Designación de Roles, Órganos y Responsabilidades ENS.**
- **Acta de Constitución del Comité de Seguridad de la Información.**

Dado que existe un modelo tecnológico y de seguridad con elementos comunes y centralizados, determinados roles, órganos, procedimientos, controles y evidencias pueden ser compartidos entre las entidades, sin perjuicio de que cada entidad mantenga sus responsabilidades sobre la información tratada y los servicios prestados en su ámbito.

El Comité de Seguridad será responsable de supervisar la aplicación de esta Política, revisar riesgos, incidentes, auditorías y planes de acción, resolver conflictos entre roles cuando sea necesario e impulsar la mejora continua de la seguridad.

8. Tratamiento de datos personales

Las entidades incluidas en el alcance de la presente Política tratan datos personales de acuerdo con sus respectivos registros de actividades de tratamiento, con la normativa aplicable en materia de protección de datos y con la documentación interna vigente en cada entidad en materia de protección de datos.

Los riesgos asociados a los tratamientos deberán valorarse periódicamente y coordinarse con el análisis de riesgos ENS, especialmente cuando afecten a la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información.

Cuando se identifiquen tratamientos de alto riesgo, se realizará, cuando corresponda, una Evaluación de Impacto relativa a la Protección de Datos —EIPD—. La implantación de

medidas de seguridad se coordinará con los procedimientos de gestión de riesgos, proveedores, control de accesos, continuidad y respuesta ante incidentes.

El delegado de Protección de Datos asesorará y supervisará los aspectos relativos al cumplimiento de la normativa de protección de datos, incluyendo la gestión de brechas de seguridad que afecten a datos personales.

9. Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán contar con un análisis de riesgos adecuado a la naturaleza de la información tratada, los servicios prestados, los activos afectados, la categoría ENS aplicable y los requisitos del sistema de gestión de seguridad de la información conforme a ISO/IEC 27001:2022.

El análisis de riesgos deberá revisarse:

- Al menos una vez al año.
- Cuando cambien los servicios prestados o la información tratada.
- Cuando se incorporen nuevos sistemas, aplicaciones, proveedores o servicios relevantes.
- Ante incidentes de seguridad significativos.
- Ante vulnerabilidades críticas o cambios relevantes en el entorno tecnológico.
- Cuando se modifiquen tratamientos de datos personales o evaluaciones de impacto.

El Comité de Seguridad realizará seguimiento de los riesgos y planes de tratamiento, priorizando las acciones necesarias para reducir los riesgos no aceptables.

Las decisiones relevantes se reflejarán en la Declaración de Aplicabilidad, en el Plan de Tratamiento de Riesgos, en el análisis de riesgos del SGSI y en las evidencias correspondientes.

10. Sistema de Gestión de Seguridad de la Información

Las entidades incluidas establecen, implantan, mantienen y mejoran de forma continua un Sistema de Gestión de Seguridad de la Información —SGSI— conforme a los requisitos de la norma ISO/IEC 27001:2022 y de manera integrada con el Esquema Nacional de Seguridad.

El SGSI tiene como finalidad asegurar que la seguridad de la información se gestiona de forma sistemática, documentada y basada en riesgos, incluyendo la identificación de activos, el análisis y tratamiento de riesgos, la selección de controles, la definición de objetivos de seguridad, la gestión de incidentes, la evaluación del desempeño, la auditoría interna, la revisión por la Dirección y la mejora continua.

La aplicación de los controles de seguridad se documentará mediante la Declaración de Aplicabilidad, teniendo en cuenta tanto los requisitos del ENS como los controles aplicables del SGSI conforme a ISO/IEC 27001:2022.

La Dirección se compromete a proporcionar los recursos necesarios, promover el cumplimiento de esta Política, apoyar la consecución de los objetivos de seguridad de la información y revisar periódicamente la eficacia del SGSI.

11. Desarrollo de la Política de Seguridad

Esta Política se desarrolla y complementa mediante el Sistema de Gestión de Seguridad de la Información —SGSI—, así como mediante normas, procedimientos, instrucciones y registros específicos, que incluyen, entre otros:

- Normativa de Seguridad.
- Control de accesos.
- Copias de seguridad y recuperación.
- Gestión de incidentes.
- Gestión de proveedores.
- Gestión de cambios.
- Normas de uso
- Inventario de activos
- Declaración de Aplicabilidad.
- Análisis de riesgos
- Alcance del SGSI.
- Metodología de análisis y tratamiento de riesgos.
- Objetivos de seguridad de la información.
- Declaración de Aplicabilidad ENS / ISO 27001:2022.
- Seguimiento, medición, auditoría interna y revisión por la dirección.

La documentación asociada estará disponible para el personal que necesite conocerla, en función de sus responsabilidades, y deberá mantenerse actualizada en el repositorio documental definido.

12. Obligaciones del personal

Todo el personal deberá conocer y cumplir esta Política, la **Normativa del uso de los recursos TIC** y las normas de seguridad asociadas que resulten aplicables.

Las entidades incluidas garantizarán la difusión de la Política y de la normativa interna de uso TIC, y promoverán acciones de formación y concienciación en seguridad de la información.

El personal deberá:

- Utilizar los sistemas de información conforme a las normas internas de uso TIC y a las instrucciones de seguridad aplicables.
- Proteger sus credenciales y no compartir usuarios o contraseñas.
- Respetar el principio de mínimo privilegio.
- Mantener la confidencialidad de la información a la que tenga acceso.
- Comunicar incidentes, sospechas de incidentes o usos indebidos de los sistemas.
- Cumplir las instrucciones relativas a protección de datos, seguridad, uso de dispositivos, acceso remoto y tratamiento de información.
- Participar en las acciones de formación o concienciación que se establezcan.

Las personas que administren operen o gestionen sistemas TIC deberán recibir formación adecuada a sus responsabilidades y actuar conforme a los procedimientos técnicos y de seguridad aplicables.

13. Terceros, proveedores y prestadores de servicios

Cuando las entidades incluidas utilicen servicios de terceros o permitan el acceso de proveedores a información, activos o sistemas incluidos en el alcance ENS y/o del SGSI, deberán establecerse los requisitos de seguridad aplicables en función del riesgo, la criticidad del servicio y la información tratada.

Los terceros y proveedores deberán cumplir las obligaciones legales, contractuales y de seguridad que les resulten aplicables, incluyendo, cuando proceda, los requisitos del ENS, la normativa de protección de datos y las condiciones específicas establecidas por la organización.

En servicios cloud, hosting, soporte técnico, aplicaciones externas, plataformas SaaS (Software como Servicio) o servicios críticos, se atenderá a los requisitos de seguridad aplicables, a las guías CCN-STIC correspondientes y a las evidencias de seguridad disponibles del proveedor.

Cuando un proveedor trate datos personales por cuenta de alguna de las entidades, deberá formalizarse el correspondiente contrato o acuerdo de encargado del tratamiento, cuando aplique.

Si algún requisito de seguridad no pudiera ser satisfecho, el Responsable de Seguridad, con la participación de los responsables afectados, valorará el riesgo y propondrá las medidas de tratamiento oportunas. La continuidad del servicio o contratación deberá ser aceptada por los responsables correspondientes cuando exista riesgo residual relevante.

Para el uso de sistemas o servicios basados en inteligencia artificial, deberá valorarse previamente el impacto en seguridad, protección de datos, confidencialidad, integridad de la información, cumplimiento normativo y dependencia tecnológica.

Se procederá para la selección, evaluación y homologación de proveedores, incluidos los proveedores críticos, según lo establecido en el procedimiento de **Selección, evaluación y homologación de proveedores**.

14. Gestión de incidentes de seguridad

Las entidades incluidas dispondrán de procedimientos para la gestión de eventos e incidentes que puedan afectar a la información, los sistemas o los servicios incluidos en el alcance ENS y/o del SGSI. Concretamente, se actuará según lo establecido en el procedimiento **Notificaciones de las brechas de seguridad**.

La gestión de incidentes deberá permitir:

- Detectar y registrar eventos e incidentes.
- Clasificar su gravedad e impacto.
- Contener y mitigar los efectos.
- Coordinar la respuesta técnica, funcional, jurídica y de protección de datos cuando corresponda.
- Comunicar los incidentes a los responsables afectados.
- Notificar a autoridades competentes cuando sea exigible.
- Analizar causas y definir acciones correctoras.
- Evitar recurrencias.
- Mantener evidencias de la gestión realizada.

Cuando el incidente afecte a datos personales, se coordinará la respuesta con el delegado de Protección de Datos y se valorará la necesidad de notificación a la autoridad de control y, en su caso, a las personas afectadas.

Los incidentes relevantes serán comunicados al Comité de Seguridad de la Información.

15. Revisión de la Política de seguridad de la información

La presente Política será revisada:

- Al menos una vez al año.
- Cuando se produzcan cambios relevantes en la organización, servicios, sistemas, proveedores o alcance ENS y/o del SGSI.
- Cuando se produzcan incidentes de seguridad significativos.
- Como consecuencia de auditorías, revisiones o cambios normativos.
- Cuando el Comité de Seguridad lo considere necesario.

La revisión será coordinada por el responsable de Seguridad y elevada al Comité de Seguridad para su validación y aprobación por las Direcciones correspondientes.

16. Aprobación

La presente Política de Seguridad de la Información es aprobada por las Direcciones de las entidades incluidas, que se comprometen a promover su cumplimiento, proporcionar los recursos necesarios y apoyar la mejora continua de la seguridad de la información.

El Prat de Llobregat, a 4 de junio de 2026

Cristina Rodríguez Portillo
Directora General de Fundesplai y
Presidenta del Consejo de Administración
de 7iTria

Víctor Hugo Martínez Buixeda
Director General Fundación Esplai
Ciudadanía Comprometida