La Sapiència
Fundació Social

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código:	SAP STIC-POL-1
Versión:	1.0
Fecha de la versión:	12/01/2026
Creado por:	Responsable de Seguridad de la Información
Aprobado por:	Comité de Seguridad de la Información
Nivel de confidencialidad:	Uso oficial

Firmado por ***2995** JOAN JOSEP SEGUI (R: ****5087*) el día 28/05/2026 con un certificado emitido por AC Representación

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
12/01/2026	1.0	FUNDACIÓ SOCIAL LA SAPIÈNCIA	Primera versión publicada

Tabla de contenido

1. Aprobación y Entrada en Vigor

Texto aprobado el día 04 de febrero de 2026 por el Comité de Seguridad.

Esta Política se Seguridad de la Información está vigente desde la fecha de aprobación (o publicación para las entidades que sea obligatoria su publicación oficial) y hasta que sea reemplazada por una nueva Política.

2. Introducción

La Fundació Social La Sapiència, en adelante la Organización, depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos, ejercer sus competencias y prestar los servicios que tiene atribuidos. Estos sistemas deben ser 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.

El objetivo de la seguridad de la información es garantizar la confidencialidad, integridad, autenticidad y trazabilidad 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 la valoración de su coste deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

3. Misión de La Fundació Social La Sapiècia

La Organización es una entidad privada de carácter permanente cuya finalidad es atender y promover la inclusión social de personas en situación de vulnerabilidad o exclusión. La entidad centra su actuación en la prestación de servicios sociales de calidad, orientados a la mejora de la autonomía personal, la integración comunitaria y la inserción laboral.

En el marco de su misión, la Fundació desarrolla los siguientes servicios y programas:

- **Centro de acogida “Casa de Família”:** prestación de alojamiento temporal, acompañamiento social y apoyo educativo a personas y familias en situación de emergencia habitacional.

- **Casal de Ruberts y Casal de Binissalem:** espacios de intervención comunitaria y promoción social en los que se realizan actividades formativas, de refuerzo escolar, integración y ocio saludable.

- **Programas de inserción laboral y talleres ocupacionales:** acciones de capacitación profesional, formación en competencias laborales y mediación con empresas para facilitar el acceso al mercado de trabajo.

- **Servicios de atención básica y apoyo individualizado:** cobertura de necesidades esenciales (alimentación, higiene, ropa) y seguimiento social personalizado orientado a la inclusión.

- **Itinerarios de inserción socio-laboral:** programas estructurados que incluyen diagnóstico inicial, orientación, formación específica y acompañamiento en la búsqueda activa de empleo.

- **Colaboración institucional:** coordinación con administraciones públicas, servicios sociales y entidades del tercer sector para optimizar recursos y ampliar el alcance de la atención.

La Fundació Social La Sapiència se configura como un agente de referencia en la atención, promoción e inclusión social de personas en situación de vulnerabilidad, asegurando una gestión profesional y orientada a resultados sociales sostenibles.

4. Alcance

Esta Política se aplicará a los sistemas de información de la organización que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo y que se encuentran dentro del ámbito de aplicación del Esquema Nacional de Seguridad (ENS).

5. Principios Rectores de la Política

- Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente
- Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- Gestión de la seguridad basada en el riesgo: la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas. y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.
- Prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, danto una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.

- Existencia de líneas de defensa, la estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.
- Vigilancia continua y reevaluación periódica: la entidad implementa medios la detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos, Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.
- Seguridad por defecto y desde el diseño: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.
- Diferenciación de responsabilidades, en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.

6. Marco Normativo

Las principales normas que afectan a esta Política son:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- SAP STIC-REG-1 Registro Normativo

7. Modelo de Gobernanza

Para garantizar el cumplimiento del Esquema Nacional de Seguridad y establecer la Organización de la seguridad de la información adaptada a las necesidades y particularidad de esta organización, se propone una designación de roles por bloques de responsabilidad: Gobierno, Supervisión y Operación.

De acuerdo con esta estructura, se han asignado las siguientes responsabilidades y funciones de seguridad:

Bloque de Gobierno:

- Responsable de Gobierno, cuyas funciones ejercita la DIRECCIÓN de la organización, que integra los siguientes roles y funciones ENS:
    - Comité de Seguridad de la Información.
    - Responsable de la Información.
    - Responsable del Servicio.

Bloque Ejecutivo/Supervisión:

- Responsable de Supervisión, cuyas funciones ejercita la Secretaría de la organización y que integra el siguiente rol ENS:
    - Responsable de la Seguridad.
- Responsable de Protección de Datos, Secretario. apoyando al Responsable de Supervisión, con funciones de asesoramiento y supervisión en materia de protección de datos.

Bloque de Operación:

- Responsable de Operación, cuyas competencias ejercita un empleado que ocupa el puesto Administrativo, y que integra el siguiente rol ENS:
    - Responsable del Sistema.
    - Administradores del Sistema.

7.1. Responsabilidades Asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad ENS:

- Funciones del Responsable de la Información y de los Servicios.
- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto del Esquema Nacional de Seguridad.
- Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.
- Funciones del Responsable de Seguridad
- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar a la Dirección la aprobación de cambios y otros requisitos del sistema.
- Funciones del Responsable del Sistema
- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Prestar al Responsable de Seguridad de la Información asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.

- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

7.2. Funciones del Comité de Seguridad de la Información

- Las funciones propias de un Comité de Seguridad de la Información son las siguientes:
- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:

    - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
    - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
    - Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
    - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
    - Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
    - Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.
    - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
    - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
    - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
    - Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

7.3. Procedimientos de Designación

La designación de los Responsables identificados en esta Política ha sido realizada por el Director y comunicada a las partes afectadas La designación de los responsables en nuestro modelo de Gobernanza se ha comunicado efectivamente a través de comunicados internos.

Los roles de seguridad serán revisados cada dos años, en el caso de que exista una vacante la misma deberá ser cubierta en el plazo de un mes, siguiendo el mismo procedimiento.

La Organización debe disponer de un mecanismo que permita la sustitución de los responsables designados en caso de ausencias de larga duración o aquellas de menor duración pero que puedan provocar ineficiencias en las funciones de cada uno de ellos que afecten al sistema.

7.4. Resolución de Conflictos

Si hubiera conflicto entre los Responsables, será resuelto por el Comité de Seguridad de la Información.

8. Datos de Carácter Personal

La Organización trata datos de carácter personal, según se describe en el Registro de Actividades del Tratamiento. La misma deberá evaluar los riesgos relacionados con los datos personales tratados proponiendo un plan de actuación para la corrección de aquellos riesgos que superen el umbral autorizado

El análisis de riesgos será reevaluado de forma periódica, contando con el asesoramiento y supervisión que realice el Responsable de Protección de Datos, y, en todo caso, cuando se detecte un tratamiento de alto riesgo, debiendo realizar, en su caso, una evaluación de impacto. La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de los procedimientos o normas de seguridad con las derivadas de las obligaciones en materia de protección de datos, especialmente en el control de los prestadores de servicios o la respuesta a incidentes y/o brechas de datos personales.

9. 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 repetirá:

- regularmente, al menos una vez al año.
- cuando se produzcan cambios en la información manejada.
- cuando se produzcan cambios en los servicios prestados.
- cuando ocurra un incidente grave de seguridad.
- cuando se reporten vulnerabilidades graves.
- cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes

servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Se tendrán en cuenta los riesgos en protección de datos, contando con la opinión del Responsable de Protección de Datos, además se coordinarán los planes del tratamiento del riesgo.

10. Desarrollo de la Política de Seguridad de la Información

El cumplimiento de los objetivos marcados en esta Política de Seguridad se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad asociados al cumplimiento del Esquema Nacional de Seguridad. Para su organización se ha definido una Norma para la Gestión de la Documentación, que establece las directrices para la organización, gestión y acceso.

La revisión anual de la presente Política corresponde al Responsable de Gobierno, proponiendo en caso de que sea necesario mejoras de la misma, para su aprobación por parte del mismo órgano que la aprobó inicialmente.

11. Obligaciones del Personal

Todos los miembros de la Organización tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normas, procedimientos o guías que la desarrollen, siendo responsabilidad de la Organización a través del Comité de Seguridad y del área de personal de disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de la Organización atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC 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.

12. Terceras Partes / Proveedores de Soluciones

Cuando el preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. La organización definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que la organización lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando la organización utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que atañe a dichos

servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias.

Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogida en la Disposición adicional segunda (Desarrollo del Esquema Nacional de Seguridad) del Real Decreto Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en consideración a la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Dicho informe deberá ser aprobado por los responsables de información y los servicios, con carácter previo al inicio de la relación con la tercera parte.

13. Gestión de Incidentes

La Organización dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios.

Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.

14. Aprobación de la Política y Entrada en Vigor/Efectividad

Las modificaciones de la presente Política que supongan cambios o adaptaciones ante ineficiencias las realizará el Comité de Seguridad de la Información, que deberá revisarla anualmente.

En caso de que los cambios supongan una modificación sustancial o de los principios o responsabilidades designadas, el Comité de Seguridad propondrá los cambios que deberán ser aprobados, en su caso, por la persona u órgano con las debidas competencias.

La sustitución de la Política será instada por el Comité de Seguridad de la Información y ratificada por la persona u órgano con las debidas competencias, de lo que se informará adecuadamente a los interesados por los mismos canales usados para su difusión.

15. Anexo I. Herramientas para Implementar la Política

Dado que la Política de Seguridad está escrita a un nivel muy amplio, se requiere complementarla con documentos más precisos que ayuden a llevar a cabo lo propuesto. Para ello se utilizan otros instrumentos que reciben diferentes nombres, siendo comunes los siguientes:

- normas de seguridad (security standards) que en el ámbito de la administración pública se podrán equiparar a instrucciones de servicio.
- guías de seguridad (security guides).
- procedimientos de seguridad (security procedures).

Las normas uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

Las guías tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.

Los procedimientos (operativos) de seguridad afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

Las organizaciones no siempre separan nítidamente estos diferentes tipos de herramientas, sino que a veces se generan manuales y reglamentos de seguridad que tienen un poco de todos los elementos anteriormente mencionados, buscando siempre una mayor efectividad en la concienciación y formación de los usuarios del sistema.

Si bien los manuales y reglamentos de carácter mixto pueden servir como herramientas importantes, a menudo es útil distinguir claramente entre lo que es política (abstracta) y su aplicación concreta. De esta forma se es más flexible y se consigue una cierta uniformidad de resultados incluso cuando cambia la tecnología o los mecanismos empleados.