POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Fundación para el Fomento de la Investigación Sanitaria y Biomédica de la Comunitat Valenciana (Fisabio)

CONTROL DE VERSIONES

Versión	Fecha	Resumen de cambios	Elaborado	Revisado
1.00	21/05/2026	Edición inicial	Comité Técnico de Seguridad de la Información	Comité de Seguridad de la Información

.

1. INTRODUCCIÓN

La Fundación para el Fomento de la Investigación Sanitaria y Biomédica de la Comunitat Valenciana (en adelante, Fisabio) depende de los sistemas de información y de las tecnologías de la información y las comunicaciones (TIC) para la prestación de sus servicios. Estos sistemas deben gestionarse con la diligencia debida, adoptando las medidas necesarias para protegerlos frente a amenazas internas o externas, accidentales o deliberadas, que puedan afectar a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada y de los servicios prestados.

Para hacer frente a estas amenazas, se requiere una estrategia capaz de adaptarse a las condiciones del entorno y asegurar la disponibilidad de los servicios. Esto implica aplicar las medidas mínimas de seguridad exigidas por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), así como realizar un seguimiento continuo de los niveles de prestación de los servicios, monitorizar y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los ciber incidentes.

Bajo esta premisa, Fisabio concibe la seguridad de la información como un proceso integral y continuo, presente en todas las fases del ciclo de vida de los sistemas, desde su concepción y adquisición hasta su explotación y retirada. Para ello, se establece la presente Política de Seguridad de la Información (PSI) como marco de referencia para la gestión de la seguridad, conforme a los requisitos del ENS y la normativa vigente en materia de administración electrónica y protección de datos.

En consecuencia, Fisabio orienta su seguridad de la información a garantizar la calidad de la información y la continuidad de los servicios. Para ello, actúa de forma preventiva, supervisa la actividad diaria para detectar anomalías y asegura una respuesta ágil ante cualquier incidente que permita restaurar los servicios a la mayor brevedad, según lo establecido en el artículo 8 del ENS y mediante las medidas detalladas a continuación.

1.1. Prevención

Para salvaguardar la integridad de su información y servicios frente a incidentes de seguridad, Fisabio implementa las medidas exigidas por el ENS y controles adicionales basados en un análisis continuo de amenazas y riesgos. La entidad garantiza la transparencia mediante roles y responsabilidades de seguridad claramente documentados para todo el personal.

Para asegurar la eficacia de esta Política, Fisabio se compromete a:

- Autorizar formalmente todos los sistemas antes de su puesta en marcha.
- Evaluar de forma continua la seguridad, supervisando los cambios que se puedan producir en las configuraciones.
- Someterse a auditorías externas periódicas para obtener una valoración independiente y objetiva de nuestros procesos.

1.2. Detección

Fisabio establece controles operativos en sus sistemas de información con el fin de detectar anomalías en la prestación de los servicios bajo principios de vigilancia continua y reevaluación periódica previstas en el artículo 10 del ENS. Adicionalmente, en cumplimiento del artículo 9, relativo a la existencia de líneas de defensa, cualquier desviación significativa de los parámetros de normalidad activará protocolos de detección, análisis y reporte regular ante los responsables designados.

1.3. Respuesta

Fisabio establecerá las siguientes medidas de respuesta ante incidentes:

- Mecanismos de actuación rápida para mitigar el impacto de cualquier brecha de seguridad.
- Un punto de contacto único para coordinar las comunicaciones sobre incidentes con otros departamentos u organismos.
- Protocolos de intercambio de información que aseguren una comunicación bidireccional fluida con el Equipo de Respuesta de Incidentes de Seguridad (CERT) de referencia.

1.4. Recuperación

Con el fin de asegurar la continuidad operativa, Fisabio dispone de los mecanismos y la infraestructura necesarios para garantizar la restauración de sus servicios esenciales ante cualquier interrupción.

2. MISIÓN

Fisabio es una fundación del sector público instrumental de la Generalitat Valenciana, de carácter científico y sin ánimo de lucro, cuyo fin primordial es promover, favorecer, difundir, desarrollar y ejecutar la investigación científico-técnica y la innovación en el ámbito sanitario y biomédico de la Comunitat Valenciana.

Para cumplir con su misión, Fisabio coordina y gestiona actividades de investigación, innovación y transferencia del conocimiento. Su labor abarca desde la investigación biomédica y en salud pública hasta la gestión de proyectos y ensayos clínicos, la colaboración con los departamentos de salud del sistema sanitario valenciano y la participación en redes de investigación.

El desarrollo de estas actividades requiere el tratamiento de información científica, técnica, administrativa y de carácter personal, así como la prestación de servicios soportados por sistemas de información, lo que hace imprescindible garantizar un nivel adecuado de seguridad de la información y de continuidad de los servicios.

3. PRINCIPIOS FUNDAMENTALES

La presente PSI define los principios fundamentales que rigen la gestión de la seguridad de la información. Estos criterios resultan de aplicación a la totalidad de los sistemas y actividades de la Fundación, siempre en alineación con el ENS. Se establecen los siguientes:

3.1. Compromiso estratégico

La seguridad de la información es una responsabilidad de toda la entidad y cuenta con el compromiso y apoyo de la alta dirección de Fisabio, de forma que se integra como un elemento estratégico dentro de los objetivos institucionales y la cultura organizativa. De este modo, Fisabio considera la seguridad como un componente esencial para todas sus iniciativas y procesos.

3.2. Responsabilidad y roles

Para garantizar un gobierno eficaz y coherente conforme al ENS y la normativa vigente, se identifican y asignan responsabilidades específicas en materia de seguridad de la información. Se distinguen los roles de Responsable de la Información, que determina los requisitos de seguridad de la información tratada; Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados; Responsable del Sistema, que tiene responsabilidad sobre el/los sistema(s) de información que soportan los servicios y la información que estos manejan, y Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad y supervisa el cumplimiento de las medidas implantadas.
Sin perjuicio de estos roles, la seguridad de la información es una responsabilidad de todo el personal vinculado a Fisabio. Todo usuario tiene el deber de conocer sus obligaciones y notificar de manera inmediata cualquier vulnerabilidad, debilidad, anomalía o sospecha de incidente a través del canal establecido.

3.3. Seguridad integral y continua

La seguridad se entiende como un proceso integral que abarca aspectos técnicos, humanos, organizativos y materiales, y que se aplica desde el diseño y la adquisición de los sistemas hasta su explotación y retirada. La seguridad forma parte inherente de todas las fases del ciclo de vida de la información y de los sistemas. En esta línea, el diseño e implantación de tecnologías emergentes, incluyendo herramientas de Inteligencia Artificial, deberá incorporar medidas de seguridad y privacidad desde su planteamiento. En consecuencia, el tratamiento de información de Fisabio se realizará únicamente mediante herramientas autorizadas por la organización.

3.4. Gestión basada en riesgos

La identificación y tratamiento de riesgos son pilares fundamentales para garantizar un entorno controlado. Las medidas de seguridad se seleccionan bajo un principio de proporcionalidad entre el coste y la eficacia, en el que se tendrá en cuenta la naturaleza de la información, la criticidad de los servicios y las amenazas detectadas. En este análisis, se considerarán de forma prioritaria los riesgos derivados del tratamiento de datos de carácter personal.

3.5. Proporcionalidad

Las medidas de seguridad adoptadas deberán ser proporcionales a los riesgos, al valor y criticidad de la información y a los servicios afectados a fin de evitar tanto una sobreprotección que dificulte la operativa como una subprotección que pueda exponer a la Fundación a incidentes.

3.6. Principio de mínimo privilegio

Los sistemas se configuran para otorgar únicamente los permisos estrictamente necesarios para el desempeño de las funciones autorizadas. Esta configuración minimiza la vulnerabilidad ante posibles incidentes y refuerza la capacidad de respuesta de la organización.

3.7. Concienciación y formación

Tanto el personal propio como el externo de Fisabio contará con formación e información continua sobre sus responsabilidades de seguridad. Esta medida perseguirá consolidar una cultura preventiva que ayude a minimizar los riesgos asociados al factor humano.

3.8. Vigilancia y mejora continua

Fisabio mantendrá una monitorización permanente de sus sistemas y servicios para la detección temprana de anomalías que puedan derivar en un incidente de seguridad. Este control se refuerza con auditorías periódicas y una actualización regular de la política de seguridad para adecuarse a los cambios tecnológicos, cumplir con la normativa vigente y responder con agilidad a nuevas amenazas.

3.9. Seguridad por defecto

Los sistemas deberán diseñarse y configurarse para garantizar un nivel adecuado de seguridad desde su puesta en marcha para evitar la necesidad de intervenciones adicionales inmediatas.

4. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Fisabio determina los siguientes objetivos de seguridad de la información:

4.1. Garantizar la confidencialidad y la disponibilidad de la información

Proteger la información frente a accesos no autorizados o pérdidas. El sistema deberá garantizar la preservación y disponibilidad inmediata para los usuarios legítimos.

4.2. Gestión y control de activos de información

Mantener un inventario actualizado y categorizado de los activos de información. En función de su nivel de criticidad, se asignará la responsabilidad de su gestión y su protección.

4.3. Seguridad ligada a las personas

Promover la formación y responsabilidad de todo el equipo, tanto interno como externo, con el fin de establecer una conciencia compartida que ayude a evitar riesgos por un uso inadecuado de los sistemas.

4.4. Seguridad física y ambiental

Asegurar que las áreas e instalaciones críticas dispongan de controles de acceso físico adecuados como medida de prevención a entradas no autorizadas protegiendo así los sistemas y los activos de información frente a posibles daños ambientales o físicos.

4.5. Gestión segura de las comunicaciones y las operaciones

Establecer pautas que garanticen la seguridad en la gestión y la actualización de los sistemas TIC para proteger el envío de información en función de su nivel de confidencialidad.

4.6. Control de acceso

Implementar controles de acceso y autenticación que limiten el uso de los sistemas únicamente a usuarios y dispositivos autorizados. Asimismo, se mantendrán registros que permitan rastrear y auditar todas las actividades realizadas.

4.7. Seguridad en el ciclo de vida de los sistemas

Garantizar que la seguridad sea una prioridad en todas las etapas de un sistema para que los equipos sean seguros por defecto desde su puesta en marcha hasta su baja.

4.8. Gestión de incidentes de seguridad

Disponer de canales claros para detectar, analizar y resolver con agilidad cualquier incidente que pueda afectar a nuestros servicios o a la información gestionada.

4.9. Continuidad de los servicios

Garantizar que los sistemas esenciales sigan funcionando ante cualquier imprevisto. Para ello, se contará con planes de recuperación que permiten restablecer el servicio con la agilidad posible.

4.10. Protección de datos personales

Aplicar todas las medidas técnicas y organizativas necesarias para proteger la privacidad de las personas conforme a la normativa vigente y realizar un análisis de los riesgos de cada tratamiento.

4.11. Cumplimiento normativo

Asegurar que toda la actividad respeta el marco legal vigente en el que se incluye el cumplimiento del ENS, la normativa de procedimiento administrativo y el RGPD.

5. ALCANCE

Esta Política se aplica a todos los sistemas y servicios que soportan actividades de investigación, gestión administrativa, soporte, gestión económica, protección de datos, así como las plataformas corporativas de Fisabio vinculados al ejercicio de sus competencias, tanto para el acceso a la información como para el desarrollo de sus actividades de investigación e innovación.

Su cumplimiento, enmarcado en el ámbito de aplicación del ENS, es obligatorio tanto para el personal de la Fundación como para los terceros que mantengan relación contractual o de colaboración, con acceso a la información o que utilicen sus sistemas de información.

Es responsabilidad de todas las personas comprendidas en el ámbito de aplicación de esta PSI conocerla y cumplirla, así como su normativa de seguridad derivada. Para garantizarlo, el Comité Técnico de Seguridad dispondrá de los medios necesarios para que toda la información de seguridad llegue de forma efectiva al personal afectado.

6. MARCO NORMATIVO

El marco normativo aplicable al desarrollo de las actividades y competencias de Fisabio está constituido por normas jurídicas estatales y europeas orientadas a la administración electrónica, la seguridad de la información, la gestión de servicios y la protección de datos de naturaleza personal.

Dichas normas se encuentran recogidas en el registro interno denominado “Doc. externa”, el cual se mantiene actualizado de forma periódica para mantener la adecuación constante a la normativa aplicable.

En particular, este marco normativo se fundamenta en las siguientes disposiciones:

- Normativa de Procedimiento Administrativo Común y Régimen Jurídico del Sector Público.
- El Esquema Nacional de Seguridad (ENS)
- El Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- La Ley de Investigación Biomédica.

Asimismo, serán de aplicación las Instrucciones Técnicas de Seguridad, las guías y recomendaciones del Centro Criptológico Nacional (CCN), así como la normativa propia de la Generalitat Valenciana y de Fisabio en materia de seguridad de la información.

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.1. Criterios utilizados

Para dar cumplimiento al RD 311/2022 que regula el ENS, la Fundación establece en este apartado su marco organizativo y la estructura de responsabilidades. Este modelo adopta las directrices de la guía CCN-STIC 801 y se fundamenta en la diferenciación de competencias y la rendición de cuentas. Como consecuencia, se han definido y designado los roles de Responsable de la Información, Responsable del Servicio, Responsable de la Seguridad, Responsable del Sistema, así como los órganos: Comité de Seguridad de la Información y Comité Técnico de Seguridad de la Información.

7.2. Roles y Responsabilidades asociadas al Esquema Nacional de Seguridad

7.2.1. Responsable de la Información (RI)

Perfil: Directora Gerente

Responsabilidades:

- Aprobar los requisitos y niveles de seguridad aplicables a la información dentro del marco del Anexo I del RD ENS a propuesta del Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
- Demostrar compromiso con respecto al sistema de gestión de seguridad de la información.
- Fomentar una cultura corporativa de seguridad de la información.
- Asegurar que están disponibles los recursos y el presupuesto necesarios para el correcto funcionamiento del sistema de gestión de seguridad de la información.
- Determinar las medidas, sean disciplinarias o de cualquier otro tipo, que pudieran aplicarse a los responsables de violaciones de seguridad.
- Aceptar los niveles de riesgo residual sobre la información tras el proceso de gestión de riesgos.

7.2.2. Responsable del Servicio (Rse)

Perfil: Directora Gerente

Responsabilidades:

- Dictaminar respecto a los derechos de acceso y la prestación de los servicios.
- Tiene la potestad de suspender la prestación de un servicio si se detecta deficiencias graves de seguridad en coordinación con el Responsable de Seguridad.
- Aceptar los niveles de riesgo residual que afecten a la continuidad y prestación de los servicios.
- Comunicar al Responsable de Seguridad cualquier variación o incorporación de nueva información relevante a su cargo.
- Definir los requisitos de disponibilidad y continuidad del servicio para que el Responsable de Seguridad proponga las medidas técnicas adecuadas.

7.2.3. Responsable de la Seguridad (RS)

Perfil: Responsable de estrategia de ciberseguridad. No depende jerárquicamente del Responsable del Sistema ni se trata de la misma persona.

Responsabilidades:

- Realizar el análisis de riesgos y elaborar la Declaración de Aplicabilidad.
- Elaborar los requisitos y niveles de seguridad aplicables a la información dentro del marco del Anexo I del RD ENS.
- Determinar la categoría del sistema (básica, media, alta) en colaboración con el Responsable del Sistema y proponerla al Comité.
- Mantener y verificar el nivel adecuado de seguridad de la información y de los servicios prestados.
- Comprobar que las medidas de seguridad de la información han sido adecuadamente implementadas por el Responsable del Sistema mediante procesos de verificación y monitorización continua.
- Proponer al Comité la Política de Seguridad y la normativa de seguridad para su aprobación.
- Gestionar las auditorías internas y externas en colaboración con la persona responsable del área de Calidad.
- Calificar la peligrosidad de los ciberincidentes (Guía CCN-STIC 817), actuar como punto de contacto con las autoridades competentes y gestionar la notificación de ciberincidentes al CCN-CERT cuando corresponda.
- Promover la formación y concienciación del personal en materia de ciberseguridad en colaboración con la persona responsable del área de Recursos Humanos.

- Supervisar que la configuración de seguridad del sistema se mantenga actualizada frente a nuevas amenazas detectadas.

7.2.4. Responsable del Sistema (RSi)

Perfil: Ingeniero de software, jefe de informática o técnico de sistemas (nivel operativo).

Responsabilidades:

- Desarrollar, operar y mantener el sistema de información durante su ciclo de vida (instalación, configuración, mantenimiento).
- Elaborar los procedimientos operativos necesarios (especialmente de respaldo, recuperación y gestión de parches).
- Implementar las medidas de seguridad y asegurar su correcta configuración técnica según las directrices del RS.
- Asegurar que los controles de seguridad técnicos (antivirus, *backups*) se cumplen estrictamente.
- Gestionar las autorizaciones y privilegios concedidos a los usuarios del sistema y sus privilegios, monitorizando su actividad.
- Prestar al RS asesoramiento para la determinación de la categoría del sistema.
- Aprobar los cambios en la configuración del hardware y software asegurando que no comprometen la seguridad.
- Paralizar o suspende el acceso o el servicio ante deficiencias graves de seguridad técnica, informando de inmediato al Responsable de Seguridad.
- Colaborar en la investigación y resolución técnica de incidentes de seguridad.
- Informar al RS de cualquier anomalía o vulnerabilidad que comprometa la seguridad del sistema.
- Mantener el inventario de activos actualizado para garantizar que todos los sistemas están bajo el alcance de la seguridad.

7.3. Comité de Seguridad de la información (COMSEGINF)

Composición:

- Presidencia: Responsable de la Información y Responsable del Servicio. (Directora Gerente).
- Secretaría: Responsable de Seguridad
- Vocales:
  - Miembros permanentes:
    - Responsable del Sistema
    - Responsable del Departamento Jurídico-RRHH-Formación
    - Responsable del Departamento de Calidad

- Miembros no permanentes: El Comité de Seguridad podrá solicitar la presencia en sus reuniones tanto de otros miembros de Fisabio como de especialistas externos que, por su experiencia o vinculación con los asuntos tratados, considere necesaria o aconsejable. Su participación será con carácter asesor y las aportaciones que realicen durante la sesión se hará constar en acta cuando así se considere relevante.

  Sin perjuicio de lo anterior, el/la responsable interno en materia de protección de datos participará en las reuniones el Comité de Seguridad de la Información, con carácter no permanente, cuando se aborden cuestiones relacionadas con el tratamiento de datos de carácter personal o cualquier otro asunto que requiera su intervención conforme a la normativa vigente. En todo caso, sus observaciones se reflejarán expresamente en acta, preservando su carácter independiente.

Responsabilidades:

- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad para asegurar consistencia y evitar duplicidades.
- Atender las inquietudes que, en materia de seguridad, se planteen desde los diferentes departamentos de la entidad.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Mediar y resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables (información, servicio, seguridad, sistema) o áreas de gestión. En caso de falta de acuerdo persistente, la Presidencia ejercerá su voto de calidad para la resolución del conflicto.
- Revisar y aprobar la Política de Seguridad de la Información, así como el mapa normativo y los procedimientos de seguridad para la implantación del ENS.
- Realizar el seguimiento de los principales riesgos residuales asumidos por la Fundación y recomendar actuaciones.
- Proponer planes de mejora y priorización de actuaciones.
- El Comité de Seguridad de la Información ejercerá las funciones de gobierno mencionadas contando para su ejecución y asesoramiento especializado con el Comité Técnico de Seguridad, el cual se encargará del despliegue operativo y la gestión técnica de las medidas de seguridad.

Periodicidad de las reuniones y adopción de acuerdos:

Durante el desarrollo del proyecto de adecuación al ENS, para evaluar el desarrollo de este y posibilitar su adecuado seguimiento, el Comité de Seguridad de la Información se reuniría, al menos, una vez al trimestre.

Una vez alcanzada la correspondiente certificación de conformidad con el ENS, el Comité de Seguridad de la Información se reunirá, al menos, dos veces al año con carácter semestral.

Sin perjuicio de lo anterior, el Comité se reunirá con carácter extraordinario cuando existan incidentes de seguridad de impacto alto o muy alto o cambios significativos en los sistemas o la organización que lo justifiquen, así como a petición del Comité Técnico de Seguridad de la Información (COMTECSI), a iniciativa (motu proprio) de cualquiera de sus miembros permanentes o por acuerdo mayoritario del Comité.

Las reuniones se convocarán formalmente por su Presidencia, a través del Secretario.

El Secretario será el encargado de preparar los temas a tratar en las reuniones del Comité, recabando la información de los diferentes responsables. Así mismo elaborará y remitirá el acta de las sesiones a los asistentes conservando las mismas de acuerdo con los criterios de conservación documental de la entidad.

Las decisiones se adoptarán preferentemente por consenso de los miembros permanentes. En caso de no alcanzarse, las decisiones se tomarán por mayoría simple de los asistentes con derecho a voto contando la Presidencia con voto de calidad en caso de empate.

7.4. Comité Técnico de Seguridad de la información (COMTECSI)

Dentro de la estructura de gobernanza de la ciberseguridad se constituye el Comité Técnico de Seguridad de la Información, cuyas competencias estarán relacionadas con las siguientes áreas de trabajo: adecuación al ENS, normativa y gestión de riesgos, análisis y mejora continua, seguridad de las interconexiones y conectividad y otras funciones conexas o concordantes. Para su composición se propone:

<u>Composición:</u>

- Presidencia: Responsable de Seguridad.
- Secretaría: Responsable del proyecto de adecuación, implementación y certificación en el ENS
- Vocales:
  - Miembros permanentes:
    - Responsable del Sistema.
    - Técnico/a Jurídico/a especializado/a en Protección de Datos.
    - Responsable del Departamento de Calidad o gestor/a o técnico/a en quien delegue
    - Responsable del Departamento Jurídico-RRHH-Formación o técnico/a en quien delegue.

- Miembros no permanentes: El Comité Técnico de Seguridad de la Información podrá solicitar la presencia en sus reuniones tanto de otros miembros de Fisabio como de especialistas externos que, por su experiencia o vinculación con los asuntos tratados, considere necesaria o aconsejable. Su participación será con carácter asesor y las aportaciones que realicen durante la sesión se hará constar en acta cuando así se considere relevante.

Responsabilidades:

- Gestión y operativa de la seguridad del Proyecto de Adecuación, Implantación y Gestión de la Conformidad en el ENS, análisis y gestión de riesgos, explotación, normativa y mantenimiento.
- Redacción y presentación de propuestas al Comité de Seguridad de la Información. Elaborará los aspectos relacionados con la ciberseguridad y los debatirá, en primera instancia, para ser trasladados al Comité.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
  - Elaborar y revisar regularmente la Política de Seguridad de la Información para su revisión y posterior aprobación.
  - Elaborar la normativa de Seguridad de la Información para su aprobación por el Comité de Seguridad de la Información.
  - Validar técnicamente 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 protección de datos.
  - 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.
  - Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto a ellos.
  - Promover la realización de las auditorías periódicas ENS y RGPD que permitan verificar el cumplimiento de las obligaciones de Fisabio en materia de seguridad de la información y protección de datos.

Periodicidad de las reuniones y adopción de acuerdos:

El Presidente del COMTECSI convocará las reuniones de trabajo de sus miembros a través del Secretario/a, por iniciativa propia o por alguno de sus miembros permanentes. Además, recabará los acuerdos alcanzados, de los que dará cuenta al Comité de Seguridad de la Información (COMSEGINF), para su aprobación definitiva.

El COMTECSI podrá desarrollar sus funciones en pleno o en grupos de trabajo para el análisis y realización de propuestas específicas. Las propuestas planteadas en el Comité Técnico serán sometidas a análisis y debate técnico, siendo la decisión final de aprobación competencia del Comité de Seguridad de la información.

Se reunirá, al menos, una vez al mes y, en todo caso, siempre antes de las celebraciones del Comité de Seguridad de la información.
Las decisiones se adoptarán por mayoría de sus miembros, contando la Presidencia (Responsable de Seguridad) con voto de calidad en caso de empate.

7.5. Responsabilidades de perfiles transversales

7.5.1. Referente interno en materia de Protección de Datos y Técnico/a Jurídico/a especializado/a en Protección de Datos.

Dada la estructura de la Fundación, las funciones propias del ámbito del Delegado/a de Protección de Datos y del Técnico/a Jurídico/a especializado/a en Protección de Datos son asumidas por la persona que ostenta la responsabilidad del proyecto de adecuación al ENS, la cual actúa como referente interno y punto de contacto en materia de protección de datos, en coordinación con el Delegado de Protección de Datos de la Generalitat Valenciana que ostenta formalmente la función a efectos del artículo 37 del RGPD.
Este perfil actúa como rol transversal y permanente en la coordinación, la supervisión de normativa y el asesoramiento jurídico, quedando excluidas las funciones ejecutivas tanto de los medios técnicos para el tratamiento de los datos personales como de las medidas de seguridad de los sistemas de información.

De conformidad con el art. 38 del RGPD, se considera que no existe conflicto de intereses, dado que la implantación de los sistemas de información, así como la adopción de medidas de seguridad, corresponden exclusivamente al Responsable del Sistema, limitándose el rol del Responsable del Proyecto a la planificación, al seguimiento y a la coordinación de los hitos de cumplimiento establecidos por el ENS, así como a la coordinación del equipo de trabajo, sin capacidad decisoria sobre los medios y fines del tratamiento de datos personales. No obstante, para garantizar la máxima transparencia e independencia, esta persona no realizará auditorías internas sobre los procesos cuya implantación haya coordinado en el marco del proyecto de adecuación al ENS, delegando esta función en el Departamento de Calidad o en un tercero independiente.

Responsabilidades:

- Supervisar el cumplimiento del RGPD, la LOPDGDD y de las políticas internas de protección de datos de la Fundación, asegurando su alineación con el ENS.
- Informar y asesorar a la organización, y a los usuarios que se ocupen del tratamiento, en materia de protección de datos personales, incluyendo el asesoramiento y la supervisión de las

evaluaciones de impacto (DPIA) relativas a la protección de datos personales, validando que los controles del ENS cubren los riesgos identificados para los derechos de los interesados.
- Evaluar el impacto jurídico de los incidentes de seguridad que afectan a datos personales y asesorar al Responsable de Seguridad en su correcta calificación.
- Supervisar el proceso de gestión y notificación de brechas de seguridad ante la Agencia Española de Protección de Datos (AEPD), dentro de los plazos legalmente establecidos.
- Cooperar con la AEPD y actuar como punto de contacto, en coordinación con el Delegado de Protección de Datos de la Generalitat Valenciana.
- Participar con voz, pero sin voto, en el Comité de Seguridad de la Información (COMSEGINF).

7.5.2. Responsable del proyecto de certificación en el ENS

Responsabilidades:
- Coordinar todas las actividades y recursos asignados al plan de trabajo para la adecuación y certificación del ENS
- Realizar el seguimiento de los hitos y plazos establecidos.
- Redactar la propuesta de Política de Seguridad para su validación por el COMTECSI y posterior aprobación por el COMSEGINF.
- Servir de enlace operativo en el desarrollo del proyecto de adecuación entre los distintos departamentos.

7.5.3. Responsable del Departamento Jurídico-RRHH-Formación

Responsabilidades:
- Revisar y asegurar la inclusión de las cláusulas obligatorias de seguridad y tratamiento de datos en los contratos y acuerdos con proveedores y terceros.
- Asesorar al Comité de Seguridad sobre cualquier cambio en la legislación de seguridad que pueda afectar a la Fundación.
- Asesorar en la gestión de aquellos incidentes de seguridad que puedan derivar en responsabilidades legales o reclamaciones de terceros.
- Garantizar que todo el personal reciba la formación adecuada sobre la política de seguridad.
- Colaborar con el RSi y el RS para asegurar que los procedimientos de alta, baja y modificación de personal incluyan la gestión segura de los accesos y la firma de compromisos de confidencialidad.
- Colaborar con la Dirección Gerencia en la aplicación del régimen disciplinario por incumplimientos graves de las políticas de seguridad

7.5.4. Responsable del Departamento de Calidad

Responsabilidades:

- Planificar y ejecutar las auditorías internas periódicas del sistema de gestión de seguridad para verificar el cumplimiento del ENS y comprobar que se encuentre alineado y sea coherente con las políticas y objetivos de calidad de la Fundación.
- Monitorizar la implementación y efectividad de las acciones correctoras y preventivas derivadas del Plan de Tratamiento de Riesgos.
- Informar al Comité de Seguridad sobre el grado de cumplimiento de las políticas y el nivel de riesgo residual garantizando la objetividad en las revisiones donde el DPD/Responsable del proyecto pudiera tener un conflicto de intereses.

8. CENTRO DE OPERACIONES DE CIBERSEGURIDAD (COCS)

El Centro de Operaciones de Ciberseguridad (COCS) será el formado por la suma de las atribuciones que estén bajo la responsabilidad de:

- Área de Informática de Fisabio
- Oficina de Seguridad de la Información de la Conselleria de Sanitat de la Generalitat de la Comunitat Valenciana (en adelante OSI)
- Centro de Seguridad TIC de la Comunitat Valenciana (CSIRT-CV) adscrito a la Dirección General de Tecnologías de la Información y las Comunicaciones dentro de la Conselleria de Hacienda y Modelo Económico de la Generalitat de la Comunitat Valenciana.

Serán funciones del Área de Informática de Fisabio:

- Vigilar y monitorizar la seguridad de los sistemas y de los dispositivos de defensa, ya sea mediante interfaces previstas.
- Análisis y correlación de eventos de seguridad y registros de actividad de los sistemas.
- Podrá constituir un Equipo de Respuesta a Incidentes de Seguridad: Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Análisis forense digital y de seguridad.

Serán funciones de la Oficina de Seguridad de la Información de la Conselleria de Sanitat de la GVA:

- Prestar asistencia técnica, legal y administrativa al responsable de la seguridad de la información para el ejercicio de sus funciones. El director de esta oficina será el responsable de la seguridad de la información

- Facilitar la coordinación entre los servicios de seguridad prestados por proveedores de dentro y fuera de la Conselleria de Sanidad, complementándolos en la medida de lo posible

Serán funciones del CSIRT-CV:

- Vigilar y monitorizar la seguridad de los sistemas y de los dispositivos de defensa, ya sea mediante interfaces previstas o instalando las correspondientes sondas.
- Análisis y correlación de eventos de seguridad y registros de actividad de los sistemas.
- Servicio de Alerta Temprana (SAT) de alertas de seguridad en las redes corporativas y en las conexiones a Internet de los sistemas.
- Apoyo en el Análisis Forense Digital y de Seguridad.
- Servicio de cibervigilancia que posibilite la prospectiva sobre la ciberamenaza.

El Área de Informática de Fisabio deberá, por un lado, coordinarse con la OSI en la definición y aplicación de las medidas de seguridad en los sistemas e infraestructuras que estén bajo su responsabilidad; por otro, colaborar con el CSIRT-CV en las tareas de operativa diaria.

9. COMPROMISO CON LA PROTECCIÓN DE DATOS PERSONALES

La Fundación Fisabio se compromete a garantizar la protección de los datos personales que trata en sus actividades de investigación, innovación y gestión. Este compromiso se fundamenta en el cumplimiento estricto del RGPD, la LOPDGDD y la normativa vigente.

Los datos se recaban exclusivamente para fines legítimos y específicos bajo un enfoque de transparencia y lealtad. De este modo, la información que se trata es la mínima necesaria, manteniéndola exacta y limitando su conservación al tiempo requerido para alcanzar sus objetivos.

Para salvaguardar esta información, Fisabio aplica medidas técnicas y organizativas que garantizan la confidencialidad, la integridad y la disponibilidad de los datos. Estos controles están diseñados para evitar cualquier acceso no autorizado, pérdida o daño accidental de manera que se proteja el derecho fundamental a la intimidad y a la privacidad conforme a los principios de la Constitución Española y el marco legal nacional e internacional vigente.
Finalmente, la gestión de la información personal se realiza con la máxima diligencia y responsabilidad proactiva. La Fundación promueve activamente una cultura de protección de datos entre todo su personal y sus colaboradores a través de mecanismos de transparencia, control y rendición de cuentas en cada uno de los tratamientos realizados.

10. OBLIGACIONES DEL PERSONAL

Todo el personal deberá aceptar la Normativa de Uso de Medios Electrónicos, Privacidad y Confidencialidad a través de los canales de comunicación interna habilitados. Quedará constancia de su recepción y compromiso en los sistemas de registro de la Fundación.

Para garantizar este compromiso, la Fundación desarrolla unos Planes de Formación continua organizados según el tipo de actividad y el nivel de interacción con los sistemas de información. Este, incluye planes formativos periódicos y un plan de acogida específico para nuevas incorporaciones a fin de asegurar que todo el equipo conozca sus deberes y las buenas prácticas desde su primer día en la organización. Las personas con responsabilidades en la administración y gestión de los sistemas de información recibirán formación especializada y obligatoria. Esta capacitación se actualiza ante cualquier cambio en sus responsabilidades que afecte a la seguridad. De este modo, las competencias técnicas se mantienen alineadas con los riesgos y exigencias de cada puesto.
Por último, el personal actuará con responsabilidad y diligencia debida en el uso de los sistemas. En este sentido, será responsabilidad de cada profesional conocer las normas de uso y colaborar en la detección de riesgos. Ante el conocimiento de cualquier fallo de seguridad o posible incidente deberá informar inmediatamente a través del canal destinado a tal fin.

11. GESTIÓN DE RIESGOS

Todos los sistemas y servicios gestionados por Fisabio se someten a un proceso continuo de análisis y gestión de riesgos. El objetivo de este procedimiento es identificar amenazas y vulnerabilidades para establecer las medidas necesarias que mitiguen cualquier riesgo inaceptable. Este análisis se realiza de forma periódica, como mínimo una vez al año, y se actualiza de manera inmediata ante cambios significativos en los servicios, la detección de vulnerabilidades graves o tras la ocurrencia de incidentes de seguridad relevantes.

La coordinación y supervisión de este proceso recae en el Responsable de Seguridad, quien identifica las debilidades existentes y traslada dicha información al Comité de Seguridad de la Información para la toma de decisiones y la asignación de recursos. El proceso comprende fases esenciales que van desde la categorización de los activos según su criticidad hasta la evaluación de los riesgos asociados a los mismos. Sobre esta base, se seleccionan medidas de seguridad proporcionadas que equilibran el valor de la información con el coste de su implantación.

Este proceso se realiza según lo dispuesto en los Anexos I y II del Real Decreto 311/2022, de 3 de mayo, y conforme a las instrucciones y guías del CCN. De este modo, la gestión de riesgos forma parte de la estrategia de la Fundación.

12. GESTIÓN DE INCIDENTES

Fisabio dispone de un sistema estructurado para gestionar cualquier amenaza a la seguridad de la información, organizado en las siguientes fases:

12.1. Prevención de incidentes de seguridad y brechas de datos personales

Para evitar que la información o los servicios se vean afectados por incidentes de seguridad o brechas de datos personales, se aplican las medidas del ENS junto con las

derivadas del análisis de riesgos. Estos controles minimizan la probabilidad de incidentes y refuerzan la protección de la información ante posibles amenazas.

12.2. Monitorización y detección de incidentes

Se mantiene una vigilancia constante de los servicios para identificar de forma temprana cualquier anomalía. Para ello, se dispone de mecanismos que permiten la detección, el análisis y la notificación oportuna de los eventos a los responsables correspondientes.

12.3. Respuesta ante incidentes de seguridad o brechas de datos personales

La entidad cuenta con un procedimiento unificado de gestión de incidentes, a través del documento Gestión de Ciberincidentes, que integra la respuesta ante amenazas técnicas y el protocolo específico para brecha de datos personales, el cual incluye la designación de puntos de contacto y la coordinación con organismos como el CCN-CERT del Centro Criptológico Nacional, el CSIRT-CV, la OSI y la Agencia Española de Protección de Datos (AEPD).

De acuerdo con el art.33 del ENS (Real Decreto 311/2022), la entidad notificará al CCN-CERT aquellos incidentes que presenten un impacto alto o muy alto.

En el supuesto de que el incidente constituya una brecha de seguridad de datos personales, el proceso incorpora la notificación al Delegado de Protección de Datos para evaluar los riesgos, ejecutar las acciones necesarias y gestionar, si procede, la comunicación oficial ante la AEPD como autoridad competente.

12.4. Recuperación y planes de continuidad

Para asegurar la restauración rápida de los servicios críticos, se mantienen actualizados los planes de continuidad y recuperación ante desastres. De este modo, los sistemas de información pueden volver a operar con el menor impacto posible tras un incidente.

13. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Para cumplir con los objetivos de esta Política, la misma se completa con un conjunto de normas, procedimientos técnicos, informes y registros de seguridad.

La estructura normativa se organiza en tres niveles jerárquicos para facilitar su aplicación:

- Nivel 1: Política de Seguridad de la Información, normativa de uso de medios electrónicos y directrices generales.
- Nivel 2: Normas específicas de seguridad que desarrollan la política general.
- Nivel 3: Procedimientos e instrucciones técnicas que detallan las acciones concretas en los procesos de seguridad.

El Comité de Seguridad de la Información revisa esta Política anualmente para evaluar su vigencia. Cualquier modificación requiere la aprobación de la Gerencia y Junta de Gobierno. Asimismo, este texto se integra con los principios y garantías establecidos en la normativa vigente de protección de datos personales.

Es responsabilidad de todas las personas sujetas al ámbito de esta Política conocer y cumplir tanto la normativa interna como los procedimientos de seguridad. El Comité de Seguridad facilita los medios necesarios para la consulta de la documentación, que está disponible en formato digital a través de la intranet corporativa.

14. RELACIÓN CON TERCERAS PARTES

Cuando Fisabio preste servicios a otros organismos o gestione información de terceros, garantizará que estos conozcan y participen en esta Política de Seguridad. Para ello, se establecerán canales de comunicación y coordinación entre los Comités de Seguridad respectivos, así como procedimientos conjuntos para la gestión de incidentes.

Del mismo modo, los proveedores externos o entidades que reciban información de la Fundación deberán cumplir con los requisitos de seguridad establecidos en esta Política y su normativa interna. Estas terceras partes podrán emplear sus propios procedimientos operativos siempre que aseguren los estándares exigidos. Asimismo, se requerirá que su personal cuente con una formación y concienciación en seguridad equivalente a la de Fisabio.

En cumplimiento del ENS, los proveedores y operadores privados deberán disponer de la correspondiente Declaración o Certificación de Conformidad, según la categoría del sistema o servicio. Si una tercera parte no pudiera satisfacer alguna obligación de esta Política, el Responsable de Seguridad emitirá un informe detallado que identifique los riesgos y proponga medidas de mitigación. Dicho informe deberá ser aprobado por los responsables de la información y los servicios antes de iniciar la relación contractual o el intercambio de datos.

15. MEJORA CONTINUA

La gestión de la seguridad en Fisabio es un proceso dinámico que requiere una revisión y actualización constante. Los cambios organizativos, la evolución de las amenazas, los avances tecnológicos y las actualizaciones legislativas exigen un compromiso permanente con la mejora de los sistemas. Para ello, la Fundación desarrolla un proceso de mejora continua que incluye las siguientes acciones:

- Revisión de la Política de Seguridad de la Información: Se revisa anualmente para asegurar su vigencia y adecuación a las necesidades actuales.
- Actualización de activos: Los servicios e información gestionados se recategorizan periódicamente para que reflejen el contexto y los riesgos presentes.
- Análisis de riesgos: Se realiza, como mínimo una vez al año, un análisis que permite identificar nuevas amenazas y vulnerabilidades.
- Auditorias: Se ejecutan auditorías internas y, cuando proceda, externas, para verificar el cumplimiento y la eficacia de las medidas aplicadas.
- Evolución de medidas de seguridad: Se evalúan y actualizan constantemente según el entorno y los resultados de las revisiones.
- Gestión documental. Las normas, los procedimientos y el resto de documentación vinculada se mantienen en un proceso de revisión y actualización permanente.

Del mismo modo, se vigilan los activos y sistemas de forma constante para detectar cualquier comportamiento anómalo. Esta supervisión permite reaccionar con rapidez y reducir el impacto de posibles incidentes.

Por otra parte, cualquier cambio en el inventario, ya sea físico o técnico, deberá contar con autorización previa que garantice un control exhaustivo de las modificaciones realizadas. Este compromiso garantiza que la seguridad sea siempre efectiva y esté alineada con los objetivos de la Fundación.

16. APROBACIÓN Y ENTRADA EN VIGOR

La presente Política de Seguridad de la Información ha sido aprobada por la Junta de Gobierno de Fisabio el día 21 de mayo de 2026 y entrará en vigor y será efectiva en la fecha de su aprobación, hasta que sea reemplazada por una nueva versión debidamente aprobada.