IIS La Fe
Instituto de
Investigación Sanitaria

IT-POL-001_V1.0

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Fundación para la Investigación del Hospital Universitario y Politécnico La Fe de la Comunitat Valenciana

25/04/2023

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

CONTROL DE FIRMAS

	FECHA	FIRMA
ELABORADO POR Comité Técnico de Seguridad de la Información IIS La Fe	27/02/2023	**Javier Ripoll Esteve** *Presidente Comité de Seguridad de la Información* **Alfredo Marco Moreno** *Secretario Comité Técnico de Seguridad de la Información* *Documento firmado digitalmente.* *Código de verificación en el pie de página*
REVISADO POR Comité de Seguridad de la Información IIS La Fe	12/04/2023	**Javier Ripoll Esteve** *Secretario Comité de Seguridad de la Información* **Ainhoa Genovés Martínez** *Presidenta Comité de Seguridad de la Información* *Documento firmado digitalmente.* *Código de verificación en el pie de página*
APROBADO POR Junta de Gobierno IIS La Fe	20/04/2023	**Ainhoa Genovés Martínez** *Directora Gerente IIS La Fe* *Documento firmado digitalmente.* *Código de verificación en el pie de página*
RATIFICADO POR Patronato IIS La Fe	25/04/2023	**Ainhoa Genovés Martínez** *Directora Gerente IIS La Fe* *Documento firmado digitalmente.* *Código de verificación en el pie de página*

CONTROL DE VERSIONES

VERSIÓN	FECHA	AUTOR	CAMBIOS
1.0	25/04/2023	Comité técnico de Seguridad de la Información	Versión inicial del documento

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L **URL de validació:**https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

Contenido

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

1 APROBACIÓN Y ENTRADA EN VIGOR

Texto elaborado por el Comité Técnico de Seguridad de la Información del IIS La Fe y remitido al Comité de Seguridad de la Información del Instituto de Investigación Sanitaria La Fe (en adelante IIS La Fe) el día 15 de marzo de 2023. Revisado por el Comité de Seguridad de la Información del IIS La Fe y remitido a la Junta de Gobierno del IIS La Fe el día 12 de abril de 2023. Aprobado por la Junta de Gobierno del IIS La Fe el día 20 de abril de 2023 y ratificado por el Patronato del IIS La Fe el día 25 de abril de 2023.

Esta 'Política de Seguridad de la Información', en adelante Política, será efectiva desde su fecha de ratificación, por parte del Patronato del IIS La Fe, hasta que sea reemplazada por una nueva Política.

2 INTRODUCCIÓN

El IIS La Fe depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad de la información tratada o los servicios prestados y estando siempre protegidos contra las amenazas o los incidentes con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información tratada y los servicios prestados.

Para hacer frente a estas amenazas, se requiere de una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que las Áreas de Gestión, Plataformas Científico-Tecnológicas y los Grupos de Investigación deben 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 ciberincidentes para garantizar la continuidad de los servicios prestados.

De este modo, todas las Áreas de Gestión, Plataformas Científico-Tecnológicas y los Grupos de Investigación del IIS La Fe tienen presente que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por tanto, para el IIS La Fe, el objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible, según lo establecido en el artículo 8 del ENS, con la aplicación de las medidas que se relacionan a continuación.

2.1 Prevención

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, el IIS La Fe implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de la identificación de posibles amenazas y el tratamiento de los riesgos derivados que se evalúen como inaceptables. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

Para garantizar el cumplimiento de la Política, el IIS La Fe:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo el análisis de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros, con el fin de obtener una evaluación independiente.

2.2 Detección

El IIS La Fe establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo dispuesto en el artículo 10 del ENS (vigilancia continua y reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS, Existencia de líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

2.3 Respuesta

El IIS La Fe establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4 Recuperación

Para garantizar la disponibilidad de los servicios, el IIS La Fe dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

3 MISIÓN DEL IIS LA FE

El IIS La Fe es un equipo multidisciplinar con vocación de servicio cuya misión es generar conocimiento biomédico, clínico y sanitario, promoviendo su efectiva traslación para mejorar la calidad de vida del paciente y la sociedad.

El IIS La Fe tendrá como finalidad impulsar, promover y favorecer la investigación científica y técnica en el seno del Hospital Universitario y Politécnico La Fe de Valencia y su Centro de Investigaciones.

Tanto para el cumplimiento de sus fines específicos, como para su funcionamiento como Fundación del sector público instrumental de la Generalitat Valenciana, la Fundación para la Investigación del Hospital y Politécnico de La Fe de la Comunitat Valenciana (en adelante Fundación La Fe) hace uso de información y de sistemas automatizados para su tratamiento, que deben ser convenientemente protegidos, supervisados y auditados.

4 PRINCIPIOS BÁSICOS

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

- **Alcance estratégico:** La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos del IIS La Fe, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.
- **Responsabilidad determinada:** En los sistemas TIC se identificará el **Responsable de la Información**, que determina los requisitos de seguridad de la información tratada; el **Responsable del Servicio**, que determina los requisitos de seguridad de los servicios prestados; el **Responsable del** Sistema que tiene responsabilidad sobre el/los sistema(s) de información que soportan los servicios y la información que éstos manejan, y el Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
- **Seguridad integral:** La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, 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 Riesgos:** La gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.
- **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- **Mejora continua:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
- **Seguridad por defecto:** Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

5 OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

El IIS La Fe establece como objetivos de la seguridad de la información los siguientes:

- Garantizar la calidad y protección de la información.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
- Gestión de activos de información: Los activos de información de IIS La Fe se encontrarán inventariados y categorizados y estarán asociados a un responsable.
- Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona, que acceda o pueda acceder a los activos de información, conozca sus responsabilidades y, de este modo, se reduzca el riesgo derivado de un su uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
- Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información, que contienen dichas áreas, estarán suficientemente protegidos frente a amenazas físicas o ambientales.
- Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad,

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

operación y actualización de las TIC. La información que se transmita, a través de redes de comunicaciones, deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

- Control de acceso: Se limitará el acceso a los activos de información, por parte de usuarios, procesos y otros sistemas de información, mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.
- Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Gestión de los incidentes de seguridad: Se implementarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- Garantizar la prestación continuada de los servicios: Se implementarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de los servicios que soportan, de acuerdo con las necesidades de nivel de servicio de sus usuarios.
- Protección de datos: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por los tratamientos de datos personales.
- Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información y protección de datos.

6 ALCANCE

Esta política se aplicará a los sistemas de información del IIS La Fe, relacionados con el ejercicio de sus competencias, y a cuantas personas tengan relación con los mismos. Esto incluye a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con el IIS La Fe. Todos ellos tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y su Normativa de Seguridad derivada, siendo responsabilidad del Comité Técnico de Seguridad disponer los medios necesarios para que la información llegue al personal afectado.

7 MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades del IIS La Fe está integrado por las siguientes normas:

- Ley 50/2002, de 26 de diciembre, de Fundaciones.
- Ley 9/2008, de 3 de junio, de la Generalitat Valenciana, de modificación de la Ley 8/1998, de Fundaciones de la Comunitat Valenciana.
- Ley 8/1998, de 9 de diciembre, de la Generalitat Valenciana, de Fundaciones de la Comunitat Valenciana.
- Decreto 68/2011, de 27 de mayo, del Consell, por el que se aprueba el Reglamento de Fundaciones de la Comunitat Valenciana.
- Ley 1/2015, de 6 de febrero, de Hacienda Pública, del Sector Público Instrumental y Subvenciones.
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- Ley 1/2022, de 13 de abril, de la Generalitat, de Transparencia y Buen Gobierno de la Comunitat Valenciana.

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Real Decreto 1098/2001, d 12 de octubre, por el que se aprueba el Reglamento general de la Ley de Contratos de las Administraciones Públicas.
- Ley 17/2022, de 5 de septiembre, por la que se modifica la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.
- Ley 14/2007, de 3 de julio, de Investigación Biomédica.
- Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los Ensayos Clínicos con Medicamentos, los Comités de Ética de la Investigación con medicamentos y el Registro Español de Estudios Clínicos.
- Ley 49/2002, de 23 de diciembre, del Régimen Fiscal de las Entidades sin Fines Lucrativos y de los incentivos fiscales al Mecenazgo.
- Ley 38/2003, de 17 de noviembre, General de Subvenciones.
- Real Decreto 887/2006, de 21 de julio, por el que se aprueba el Reglamento de la Ley 38/2003, de 17 de noviembre, General de Subvenciones.
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores.
- Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones vigentes sobre la materia.
- Ley 24/2015, de 24 de julio, de Patentes.
- Ley 34/2022, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la Información del Sector Público.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

8 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

8.1 Criterios utilizados

La Junta de Gobierno del IIS La Fe, teniendo en cuenta lo establecido en el antedicho Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) y las pautas establecidas en las correspondientes guías CCN-STIC que lo desarrollan, emprenderá las siguientes acciones:

- Designará roles de seguridad: **Responsable del Servicio, Responsable de la Información, Responsable de la Seguridad, Responsable del Sistema.**
- Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información. Este órgano se constituirá como un órgano colegiado y se denominará **Comité de Seguridad de la Información.**

8.2 Roles y Órganos de la Seguridad de la Información

En el IIS La Fe, en el marco del ENS, se crean los siguientes roles y órganos de Seguridad de la Información:

- **Responsable de la Información**: recae esta responsabilidad en la persona que ocupe el cargo de la Dirección Gerente de la Fundación La Fe.
- **Responsable del Servicio**: recae esta responsabilidad en la persona que ocupe el cargo de Responsable Superior de Gestión.
- **Responsable de Seguridad de la Información**: recae esta responsabilidad en la persona que ocupe el cargo de Coordinador/a del Área de Informática del IIS La Fe.
- **Responsable del Sistema**: recae esta responsabilidad en el técnico/a del Área de Informática designado por el Coordinador del Área de Informática del IIS La Fe.
- **Comité de Seguridad de la Información** (COMSEGINF)
    - Presidencia: Responsable de la información.
    - Secretario/a: Responsable de Seguridad de la Información.
    - Vocales:
        - Miembros permanentes:
            - Responsable del Servicio.
            - Responsable del Sistema.
            - Director/a Científico/a.
            - Coordinador/a Área Jurídica.
            - Coordinador/a Área Calidad.
            - Coordinador/a Área PRL.
            - Coordinador/a Área Gestión Económica.
            - Coordinador/a Área Desarrollo de Personas.
            - Coordinador/a Área de Comunicación y Difusión de la Ciencia.
            - Técnico/a Jurídico especializado en Protección de Datos.

        - Miembros no permanentes:

          El Comité de Seguridad podrá invocar la presencia en sus reuniones tanto de otros miembros del IIS La Fe como de especialistas externos, de los sectores público, privado, académico y/o de investigación cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

El Delegado de Protección de Datos o la persona en quien delegue podrá participar en las reuniones del Comité de Seguridad de la Información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación.

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

En todo caso, si excepcionalmente un asunto se sometiese a votación, se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

8.3 Responsabilidades roles asociados al Esquema Nacional de Seguridad

8.3.1 Responsable de la Información

- Establecer y elevar para su aprobación al Comité de Seguridad de la Información los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información) y a los Servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del RD ENS, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información de la que es responsable, especialmente la incorporación de nueva Información a su cargo. El cual dará traslado de dichos cambios al Comité de Seguridad de la Información en su próxima reunión.

8.3.2 Responsable del servicio

- Dictaminar respecto a los derechos de acceso a la información y los servicios.
- Aceptar los niveles de riesgo residual que afectan a la información y los servicios.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios a su cargo. El cual dará traslado de dichos cambios al Comité de Seguridad de la Información en su próxima reunión.

8.3.3 Responsable de la Seguridad

- Determinar las medidas de seguridad aplicables, en función de las valoraciones de la información tratada y los servicios prestados.
- 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.
- Determinar y aprobar la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad.
- Participar en la elaboración e implementación 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 al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.
- Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.

8.3.4 Responsable del Sistema

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando 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.
- Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad de la Información.
- Participar 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, en su caso, 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.
    - Informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
    - Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

El Responsable del Sistema gozará de absoluta independencia jerárquica en el ejercicio de las competencias atribuidas por la presente política. El Comité de Seguridad de la Información mediará y resolverá cualquier conflicto que pudiera surgir garantizando la seguridad de la información y el correcto funcionamiento del sistema.

8.4 Delegado de Protección de Datos

- Informar y asesorar al IIS La Fe, y a los usuarios que se ocupen del tratamiento, de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.
- Supervisar el cumplimiento de lo dispuesto en normativa de seguridad y de las políticas internas del IIS La Fe, en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisará su aplicación.
- Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

8.5 Comité de Seguridad de la Información (COMSEGINF)

Atribuciones del Comité de Seguridad de la Información:

a) Estar, permanentemente, informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.
b) Estar, permanentemente, informado de la relación de Entidades de Certificación acreditadas y organizaciones, públicas y privadas, certificadas.
c) Estar, permanentemente, informado de la relación de esquemas de certificación de la seguridad con los que la Administración Pública tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.
d) Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, a las que su presidente, deberá dar cumplida respuesta.
e) 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.
f) Atender las inquietudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas, informando regularmente del estado de la seguridad de la información a la Dirección.
g) Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Áreas de Gestión, Plataformas Científico-Tecnológicas y/o Grupos de Investigación, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
h) Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.
i) Revisar la Política de Seguridad de la Información previa aprobación por el Órgano Superior.
j) Aprobar la Normativa de Uso de Medios electrónicos para todo el personal.
k) Aprobar el Mapa de Normativa con la lista de Normativa y Procedimientos de seguridad para la implantación del ENS.

Periodicidad de las reuniones y adopción de acuerdos:

1. Durante el desarrollo del Proyecto de Adecuación al ENS, para evaluar el desarrollo del mismo y posibilitar su adecuado seguimiento, el Comité de Seguridad de la Información se reunirá, al menos, una vez al trimestre.
2. Una vez alcanzada la Certificación de Conformidad con el ENS de los servicios prestados por el IIS La Fe, el Comité de Seguridad de la Información se reunirá, al menos, dos veces al año con carácter semestral, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.
3. En cualquier caso, las reuniones se convocarán por su Presidencia, a través del Secretario/a, a su iniciativa o por mayoría de sus miembros permanentes.
4. Las decisiones se adoptarán por consenso de los miembros permanentes.

8.6 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 en las interconexiones y conectividad y otras funciones conexas o concordantes. Para su composición se propone:

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

- **Presidencia del Comité Técnico de Seguridad de la Información:** recae esta responsabilidad en la persona que ocupe el rol de Responsable de Seguridad.
- **Secretario/a:** Responsable del Sistema.
- Vocales:
    - Miembros permanentes:
        - Coordinador/a Gestión Económica
        - Técnico/a Jurídico especializado en Protección de datos.
        - Subdirector/a científico/a o gestor/a o técnico/a con quien delegue.
        - Gestor del Área Jurídica a elección del Coordinador/a Área Jurídica.
        - Coordinador/a Área de Calidad o gestor/a o técnico/a con quien delegue
        - Coordinador/a Área de Comunicación o gestor/a o técnico/a con quién delegue.
        - Coordinador/a Área Desarrollo de personas o gestor/a o técnico/a con quien delegue

      Además de los vocales permanentes nombrados en este punto, se podrá proponer la incorporación de otros vocales para cubrir cualquier perfil necesario, siempre y cuando se apruebe por el Comité de Seguridad de la Información.

    - Miembros no permanentes:
        - El Comité Técnico de Seguridad de la Información podrá invocar la presencia en sus reuniones tanto de otros miembros del IIS La Fe como de especialistas externos, de los sectores público, privado, académico y/o de investigación cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

Las funciones del Comité Técnico de Seguridad de la Información serán, entre otras que les puedan ser encomendadas por el Comité de Seguridad de la Información:

a) 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.
b) 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.
c) 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 traslado al Comité de Seguridad de la Información para su revisión y posterior aprobación del órgano superior.
    - Elaborar la normativa de Seguridad de la Información para su aprobación por el Comité de Seguridad de la Información.
    - 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 protección de datos.
    - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
    - 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 de ellos.

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

- Promover la realización de las auditorías periódicas ENS y RGPD que permitan verificar el cumplimiento de las obligaciones del IIS La Fe en materia de seguridad de la Información y protección de datos.

Periodicidad de las reuniones y adopción de acuerdos:

1. El Presidente del Comité Técnico de Seguridad de la Información convocará las reuniones de trabajo de sus miembros a través del Secretario/a, por iniciativa propia o por la de la mayoría de sus miembros permanentes. Además, recabará los acuerdos alcanzados, de los que dará cuenta al Comité de Seguridad de la Información, para su aprobación, en su caso.
2. El Comité Técnico de Seguridad de la Información 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 de Seguridad de la Información serán sometidas a análisis, debate y aprobación, si procede, por parte del Comité de Seguridad de la Información.

Se reunirá, al menos, una vez al mes y siempre antes de las celebraciones del Comité de Seguridad de la Información.

8.7 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 IIS La Fe
- Subdirección de Sistemas de Información del Hospital La Fe (en adelante Informática del Hospital La Fe).
- 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 del IIS La Fe:

- 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.
- Operaciones de seguridad sobre los dispositivos de defensa.
- 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 Subdirección de Sistemas de Información del Hospital La Fe:

- Análisis y correlación de eventos de seguridad y registros de actividad de los sistemas.

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

- 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.
- Gestión de vulnerabilidades (análisis y determinación de las acciones de subsanación/parcheado) de aplicaciones y servicios.

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

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 del IIS La Fe 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 lado, colaborar con el CSIRT-CV e Informática del Hospital La Fe en las tareas de operativa diaria.

8.8 Procedimientos de designación

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los responsables identificados en esta Política, se realizará por el Director/a Gerente de la Fundación La Fe.

El nombramiento se revisará cada 4 años o cuando el puesto quede vacante.

9 DATOS PERSONALES

El IIS La Fe, conforme a su Política de Privacidad, tratará los datos de manera lícita, leal y transparente en relación con el interesado, recogerá los datos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. Dichos datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; exactos y, si fuera necesario, actualizados, mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas de conformidad con los dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) así como lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

10 OBLIGACIONES DEL PERSONAL

Todo el personal del IIS La Fe, comprendido dentro del ámbito del ENS, atenderá a una o varias sesiones de concienciación en materia de seguridad y protección de datos, al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todo el personal, en particular al de nueva incorporación.

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

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

Las responsabilidades de seguridad de la información de todo el personal del IIS La Fe estarán claramente definidas, documentadas y comunicadas.

11 GESTIÓN DE RIESGOS

Todos los sistemas afectados por la presente Política de Seguridad de la Información están sujetos a un análisis de riesgos con el objetivo de identificar posibles amenazas y tratar los riesgos derivados que se evalúen como inaceptables. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de la Seguridad será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

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

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis y evaluación de riesgos.
- El Comité de Seguridad de la Información procederá a la selección de medidas de seguridad a aplicar par la mitigación de los riesgos evaluados como inaceptables, que deberán ser proporcionales a los mismos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los Anexos I y II del Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, Guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

En particular, para realizar el análisis de riesgos, como norma general se utilizará una metodología reconocida de análisis y gestión de riesgos.

12 GESTIÓN DE INCIDENTES

Prevención de incidentes de seguridad y brechas de datos personales

Para evitar o prevenir que la información o los servicios se vean perjudicados por incidentes de seguridad, se deberán implantar las medidas de seguridad determinadas por el ENS, así como cualquier medida de seguridad adicional identificada como resultado de la evaluación de amenazas y riesgos.

Monitorización y detección de incidentes brechas de datos personales

Habida cuenta que los servicios que presta IIS La Fe pueden degradarse rápidamente, debido a incidentes o brechas de datos personales, que van desde una disminución hasta el cese del nivel de prestación, se deberá monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia, según establece el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa, de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que puedan informar a los responsables, tanto regularmente como cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

Respuesta ante incidentes de seguridad o brechas de datos personales

Las pautas a seguir para la respuesta ante los incidentes de seguridad o brechas de datos personales son las siguientes:

- Establecer los debidos mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar a las personas que actuarán como puntos de contacto en las comunicaciones respecto a los incidentes que afecten al IIS La Fe.
- Notificar e intercambiar la información necesaria con el CCN-CERT del Centro Criptológico Nacional relacionada con los incidentes críticos, de muy alto o alto impacto, de conformidad con lo dispuesto en el artículo 33 del ENS.
- En caso de tratarse de un incidente o brecha de seguridad con afectación a datos personales, poner en conocimiento del Delegado de Protección de Datos el incidente para que determine las actuaciones a realizar y, en su caso, evalúe si debe ser comunicado a la Agencia Española de Protección de Datos, como autoridad responsable de la materia, cuando el riesgo pueda afectar gravemente a los derechos y libertades fundamentales de los afectados.

Recuperación y planes de continuidad

Para garantizar la disponibilidad de los servicios críticos se deberán desarrollar, probar y mejorar planes de continuidad de los sistemas de información y las comunicaciones, como parte del plan integral de continuidad de los servicios.

13 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas y procedimientos de seguridad, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas). Corresponde al Comité de Seguridad de la Información su revisión anual y/o mantenimiento, proponiendo, en caso de que sea necesario mejoras a la misma.

El cuerpo normativo sobre seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que, cada norma de un determinado nivel de desarrollo, se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: constituido por la presente Política de Seguridad de la Información, la Normativa Interna del Uso de los Medios Electrónicos y las directrices generales de seguridad aplicables al IIS La Fe.
b) Segundo nivel normativo: constituido por las normas de seguridad derivadas de las anteriores.
c) Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde a la Junta de Gobierno del IIS La Fe la aprobación de la Política de Seguridad de la Información y la Normativa Interna del Uso de los Medios Electrónicos del IIS La Fe. Estos documentos serán ratificados por el Patronato del IIS La Fe. El Comité de Seguridad de la Información es el órgano responsable de la aprobación y difusión de los restantes documentos, para que los conozcan las partes afectadas.

Del mismo modo, la presente Política de Seguridad de la Información complementa la Política de Privacidad del IIS La Fe, en materia de protección de datos.

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L

Todas las personas vinculadas al IIS La Fe tienen la obligación de conocer y cumplir la Normativa de Seguridad, la Política de Seguridad de la Información y, en particular, la Normativa Interna del Uso de los Medios Electrónicos. Será responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información esté disponible y pueda ser consultada por cualquier persona con acceso a los sistemas de información del IIS LA Fe. La documentación en soporte papel será custodiada por el Área de Informática.

14 TERCERAS PARTES

Cuando el IIS La Fe, preste servicios a otros organismos o maneje información de otros organismos, se les hará participe de esta Política de Seguridad de la Información. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el IIS La Fe, utilice servicios de terceros o ceda información a terceros, se les hará participe de esta Política de Seguridad y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Todo ello sin perjuicio de que, cuando un tercero preste servicios al IS La Fe en el ámbito del ENS, se le requerirá estar en posesión de la correspondiente declaración o certificación de conformidad con el ENS, con el mismo alcance y categoría que los servicios prestados.

Cuando algún aspecto de esta Política de Seguridad de la Información 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. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

15 MEJORA CONTINUA

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas.

Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

a) Revisión de la Política de Seguridad de la Información.
b) Revisión de los servicios e información y su categorización.
c) Ejecución con periodicidad anual del análisis de riesgos.
d) Realización de auditorías internas o, cuando procedan, externas.
e) Revisión de las medidas de seguridad.
f) Revisión y actualización de las normas y procedimientos.

CSV:NEVZJ5ZB:PKFVSV8L:J55KAI7L URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=NEVZJ5ZB:PKFVSV8L:J55KAI7L