POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE VHIO

FIRMAS DE RESPONSABILIDAD

REDACCIÓN			
Nombre	**Responsabilidad**	**Firma**	**Fecha**
Alfred Gutiérrez	Head of IT		10/06/2024

REVISIÓN			
Nombre	**Responsabilidad**	**Firma**	**Fecha**
ISec Auditors	ISec Auditors	ISec Auditors	10/05/2025

APROBACIÓN			
Nombre	**Responsabilidad**	**Firma**	**Fecha**
Sergi Cuadrado	Gerente adjunto		10/09/2025

HISTÓRICO DE MODIFICACIONES

Versión	Fecha	Motivo de la modificación
1.0	Junio 2024	Primera Versión del Documento
1.1	Mayo 2025	Revisión Isec Auditors

ÍNDICE DE CONTENIDOS

1. PROPÓSITO

La presente Política establece las directrices y líneas de actuación en materia de Seguridad de la Información que regirán el modo en que Vall d'Hebron Instituto de Oncología gestionará y protegerá su información y sus servicios, así como su comunicación a los grupos de interés y la implementación en toda la organización.

2. OBJETIVO

La Política de Seguridad de la Información define las directrices y principios establecidos por Vall d'Hebron Instituto de Oncología, para garantizar la protección de la información, así como el cumplimiento de los objetivos de seguridad definidos, asegurando así la confidencialidad, integridad y disponibilidad de los sistemas de información y por supuesto, garantizando el cumplimiento de todas las obligaciones legales aplicables.

3. ALCANCE

Esta política se aplica a todos los sistemas de información de Vall d'Hebron Instituto de Oncología y a todos los miembros de la organización, sin excepciones.

Esta política está alineada y se complementa con el resto de las políticas corporativas y normativas internas de Vall d'Hebron Instituto de Oncología.

La presente política está alineada con los principios y requisitos establecidos en la norma internacional ISO/IEC 27001:2022 y el Esquema Nacional de Seguridad (ENS) regulado por el Real Decreto 311/2022. Ambos marcos proporcionan un enfoque complementario para garantizar la protección integral de la información y la gestión adecuada del riesgo.

4. REFERENCIAS

Documento	
[1]	ISO 27001:2022 en su apartado: 5.2 "Política".
[2]	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 Abril del 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD).
[3]	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
[4]	Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), aplicable a los sistemas de información de las entidades del sector privado cuando prestan servicios o proveen soluciones a las entidades del sector público.

5. DEFINICIONES

Términos	**Definición y actividad**
Sistema de Información	Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
Riesgo	Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
Gestión de riesgos	Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
Sistema de Gestión de Seguridad de la Información (SGSI)	Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

Disponibilidad	Por disponibilidad entendemos aquella información a la que podemos acceder cuando la necesitamos a través de los canales adecuados siguiendo los procesos correctos.
Integridad	Cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.
Confidencialidad	Cualidad de la información para no ser divulgada a personas o sistemas no autorizados.
Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien garantiza la fuente de la que proceden los datos.
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) puedan ser trazadas de forma indiscutible hasta dicha entidad.
Activo de información	Algo que una organización valora y por lo tanto debe proteger
Parte interesada	Persona u organización que puede afectar, verse afectada o percibirse como afectada por las decisiones o actividades que realiza nuestra organización.

6. RESPONSABILIDAD

Es responsabilidad de todo el equipo humano de Vall d'Hebron Instituto de Oncología y las partes interesadas conocer y cumplir esta política de acuerdo con su rol cuando traten con información de la organización o sus clientes.

Es responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

El responsable de seguridad revisará esta política anualmente o cuando haya cambios significativos que así lo aconsejen, y la someterá de nuevo a aprobación por gerencia.

Las revisiones comprobarán la efectividad de la política, valorando los efectos de los cambios tecnológicos y de negocio.

Gerencia será responsable de aprobar las modificaciones necesarias en el texto cuando se produzca un cambio que afecte a las situaciones de riesgo establecidas en el presente documento.

7. PRINCIPIOS BÁSICOS

La Información es un activo muy importante para Vall d'Hebron Instituto de Oncología, y es necesario garantizar la confidencialidad, integridad y disponibilidad de esta de acuerdo con los estándares reconocidos de gestión de la Seguridad de la Información.

Los sistemas de información serán clasificados en función de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad conforme a las categorías BÁSICA, MEDIA o ALTA establecidas por el ENS. Esta clasificación determinará la aplicación de medidas de seguridad.

Se dispone de un inventario actualizado de activos de información, que se encuentran etiquetados y protegidos según la naturaleza de la información que gestionan.

Se adoptan medidas para identificar y proteger los activos de Información frente a accesos no autorizados, modificaciones, comunicaciones o destrucciones, ya sean intencionadas o fortuitas, garantizando que son utilizados únicamente para propósitos aprobados por gerencia.

El personal y colaboradores de la organización disponen de los recursos materiales, formación continuada en tecnologías y habilidades, así como procesos de desarrollo para detectar necesidades individuales, acorde con esta política y con el fin de conseguir los objetivos de negocio.

La implicación en la protección de estos activos y la implantación y mantenimiento de los controles de seguridad adecuados es una responsabilidad de todo el equipo humano de Vall d'Hebron Instituto de Oncología.

Todas las políticas, procedimientos y controles establecidos por la organización disponen de un histórico de versiones, un responsable asignado y un periodo de vigencia definido para garantizar su trazabilidad y actualidad.

El cumplimiento de la normativa legal y reglamentaria aplicable a todos los niveles, así como la voluntad de adaptarse a futuras normas, requisitos del cliente y sociales, es un compromiso y una responsabilidad de todos.

La mejora continua se desarrolla en el marco de un Sistema de Gestión, el cual la gerencia se compromete a liderar siguiendo los principios de la norma ISO 27001 y el ENS, y que aplica a toda la Organización. Todo ello basado en la gestión de las personas, la gestión por procesos y la mejora continua; garantizando su eficacia y eficiencia.

8. ORGANIZACIÓN DE SEGURIDAD

La seguridad de la información se estructura bajo un marco organizativo claro que define responsabilidades, autoridad y funciones. El Comité de Seguridad de la Información lidera la implantación y mejora del SGSI y sistema ENS. Se asignan responsables para los distintos dominios de seguridad, incluyendo responsables de activos, usuarios autorizados, responsables de incidentes y personal técnico. Esta estructura permite coordinar los recursos necesarios y garantizar una toma de decisiones eficaz ante eventos relacionados con la seguridad.

9. FORMACIÓN Y CONCIENCIACIÓN

Todo el personal debe recibir formación en seguridad de la información desde su incorporación y de forma periódica. Esta formación deberá ser adaptada a las funciones de cada puesto. Se promoverán campañas de concienciación y simulacros para fomentar la seguridad.

10. GESTIÓN DE INCIDENTES

Se dispone de procedimientos establecidos para detectar, comunicar, registrar, analizar y responder ante incidentes de seguridad de la información. Estos procedimientos incluyen criterios de clasificación, análisis de impacto, acciones correctivas y comunicación con las partes interesadas. El registro de incidentes servirá de base para la mejora del SGSI y sistema ENS, la prevención futura y la toma de decisiones informadas.

Se realizará un análisis periódico de los riesgos asociados a los activos de información, así como una evaluación de vulnerabilidades técnicas y organizativas. Este análisis alimentará el plan de tratamiento de riesgos y las decisiones relacionadas con la mejora de la seguridad.

11. CONTINUIDAD DE NEGOCIO

Se desarrollarán y mantendrán planes de continuidad de negocio y recuperación ante desastres que aseguren el restablecimiento de los servicios críticos en tiempos definidos. Estos planes estarán alineados con los resultados del análisis de riesgos y serán probados y revisados regularmente para garantizar su efectividad.

12. LÍNEAS ESTRATÉGICAS Y COMPROMISOS

A partir de los principios básicos expuestos, Vall d'Hebron Instituto de Oncología define las siguientes áreas de actuación estratégicas:

Política de Seguridad de la Información: proporcionar el soporte y la gestión necesaria para la seguridad de la información respetando los requerimientos legales. La política de Vall d'Hebron Instituto de Oncología está alineada con los objetivos de la organización, lo que garantiza el compromiso con la Seguridad de la Información.

Organización de la Seguridad de la Información: establecer un marco organizativo de referencia definiendo roles y responsabilidades de Seguridad de la Información que permitan la definición e implementación de un Plan de Tratamiento del Riesgo específico para la Seguridad de la Información y la evaluación de su efectividad para reducir los riesgos identificados.

Seguridad en Recursos Humanos: informar y concienciar al personal desde su incorporación a Vall d'Hebron Instituto de Oncología y de forma continua, cualquiera que sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. Incluye el establecimiento de las medidas necesarias de la Seguridad de la Información antes de la contratación y en el cese o cambio de puesto de trabajo.

Gestión de Activos: proteger adecuadamente los activos de la organización de acuerdo a su sensibilidad.

Control de Acceso: asegurar el acceso a los sistemas de información únicamente al personal autorizado.

Criptografía: utilizar sistemas y técnicas criptográficas para la protección de la información en base a la realización de análisis de riesgo, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

Seguridad física y ambiental: proteger los activos físicos de Vall d'Hebron Instituto de Oncología y la información sensible que gestionan mediante el establecimiento de perímetros de seguridad y áreas protegidas.

Gestión de las operaciones: garantizar la administración y gestión de las plataformas y servicios vinculados al tratamiento de información.

Seguridad de las comunicaciones: asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.

Adquisición de sistemas, desarrollo y mantenimiento: garantizar la seguridad por defecto y desde el diseño en aplicaciones desarrolladas internamente o desarrolladas por terceros por encargo de Vall d'Hebron Instituto de Oncología durante la etapa de desarrollo o implementación del software.

Relación con proveedores: implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados con los acuerdos de entrega de servicios de terceros.

Gestión de los incidentes de seguridad: garantizar que los eventos de seguridad de la información y las vulnerabilidades asociadas a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el menor tiempo posible.

Continuidad del Negocio: asegurar la continuidad de los procesos de Negocio mediante la aplicación de controles que eviten o minimicen la materialización de riesgos de impacto crítico.

Cumplimiento: garantizar el cumplimiento de los requerimientos legales de seguridad que se aplican al diseño, operación, uso y gestión de los sistemas de información.

13. SEGUIMIENTO Y CONTROL

Gerencia se compromete a revisar la Política de Seguridad de la Información periódicamente, adaptándola a nuevas exigencias organizativas, del entorno o del mercado que puedan surgir, así como a comunicarla a la Organización y a que esté a disposición de las partes interesadas en todo momento.

Los Objetivos de Seguridad de la Información son coherentes con esta política y están alineados con el modelo de procesos de Vall d'Hebron Instituto de Oncología y son revisados anualmente por gerencia y actualizados en función de su evolución y entorno.

En caso de detectar incumplimientos o violaciones de esta política, se tomarán las acciones disciplinarias o correctivas correspondientes, conforme a lo establecido en la normativa interna y la legislación aplicable.

14. VIGENCIA

Esta política entra en vigor tras su aprobación por gerencia y permanecerá vigente hasta su próxima revisión formal. La revisión se realizará como mínimo una vez al año o ante eventos significativos.