Política de Seguridad de la Información de HM Hospitales

Contenido

1. Introducción

Este documento expone la Política de Seguridad de la Información de HM HOSPITALES, como el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, en el marco de la norma UNE-EN ISO/IEC 27001 y el Esquema Nacional de Seguridad (ENS).

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de HM HOSPITALES. Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su conocimiento, procesado o tratamiento.

La Seguridad de la Información es la protección de este activo, con la finalidad de asegurar la calidad de la información y la continuidad del negocio, minimizar el riesgo y permitir maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información es un proceso que requiere medios técnicos y humanos, y una adecuada gestión y definición de los procedimientos, y en el que es fundamental la máxima colaboración e implicación de todo el personal de HM HOSPITALES.

La Dirección de HM HOSPITALES, consciente del valor de la información, está profundamente comprometida con la política descrita en este documento.

2. Definiciones

- **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:** Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten, especialmente la información crítica.
- **Integridad:** La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
- **Confidencialidad:** La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.
- **Autenticidad**: Se debe asegurar la identidad u origen de la información.
- **Trazabilidad**: Se debe asegurar para ciertos datos quién hizo qué y en qué momento.

3. Propósito

El propósito de esta Política de la Seguridad de la Información es proteger los activos de información de HM HOSPITALES, asegurando para ello la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información y de las instalaciones, sistemas y recursos que la procesan, gestionan, transmiten y almacenan, siempre de acuerdo con los requerimientos del negocio y la legislación vigente.

4. Alcance

La presente Política de Seguridad de la Información es de aplicación a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de HM HOSPITALES para los procesos descritos.

El personal sujeto a esta política incluye a todas las personas con acceso a la información descrita, independientemente del soporte automatizado o no en el que se encuentre ésta y de si el usuario es empleado o no de HM HOSPITALES. Por lo tanto, también se aplica a cualquier otra tercera parte que tenga acceso a la información o los sistemas de HM HOSPITALES.

Para garantizar que el proceso de seguridad implantado será actualizado y mejorado de forma continua, se implantará y documentará un Sistema de Gestión de la Seguridad de la Información. De esta forma, el contenido de la Política de Seguridad de la Información será desarrollado en normas y procedimientos complementarios de seguridad.

5. Fundamentos de esta Política

El objetivo último de la seguridad de la información es garantizar que una organización pueda cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información.

Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

Seguridad como proceso integral

La seguridad debe entenderse como un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.

Se promoverá la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Gestión de la seguridad basada en los riesgos

El análisis de los riesgos es parte esencial y continua del proceso de seguridad. La gestión de esos riesgos permitirá el mantenimiento de un entorno controlado, con dichos riesgos a niveles aceptables, y se realizará mediante la aplicación de medidas de seguridad de manera proporcionada a la naturaleza de la información tratada y de los servicios a prestar.

Prevención, detección, respuesta y conservación

La seguridad del sistema contempla medidas que implementen los aspectos de prevención, detección y respuesta ante incidentes de seguridad, y de conservación de la información y servicios en caso de que el incidente se produzca.

Existencia de líneas de defensa

HM HOSPITALES implementa una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Vigilancia continua y reevaluación periódica

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

HM HOSPITALES implementa controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Las medidas de seguridad se evaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Diferenciación de responsabilidades

HM HOSPITALES ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge más adelante en este documento.

En los sistemas de información se diferenciará 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 la responsabilidad sobre la prestación de los servicios; y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad. En los supuestos de tratamiento de datos personales además se identificará el responsable de tratamiento y, en su caso, el encargado de tratamiento.

6. Requisitos de seguridad

Esta política de seguridad se desarrollará aplicando los siguientes requisitos:

Organización e implantación del proceso de seguridad

La seguridad de la información compromete a todos los miembros de la organización. HM HOSPITALES identifica los responsables y establece sus responsabilidades al efecto en los apartados de “Roles, responsabilidades y deberes” y “Terceras Partes” de este documento. Esta

Política de Seguridad y las Normas de Uso de los Sistemas de Información serán conocidas por todas las personas comprendidas en el ámbito de aplicación de este documento.

Análisis y gestión de los riesgos. Inclusión de los riesgos con datos personales

Conocer los riesgos y elaborar una estrategia para gestionarlos adecuadamente es primordial para HM HOSPITALES, ya que únicamente si se conoce el estado de seguridad podrán tomarse las decisiones adecuadas para mitigar los riesgos a los que se enfrenta.

Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el RGPD y en la LOPDGDD o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. El responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizará un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos. Del resultado de ese análisis pueden derivarse medidas adicionales a implantar.

HM HOSPITALES adopta una metodología elaborada de acuerdo con lo dispuesto por las Autoridades de Control en diferentes guías respecto el análisis de los riesgos, realizando un análisis detallado de los riesgos que afecten a los activos recogidos en un inventario de activos, que queda documentado en un documento de Análisis de Riesgos.

La entidad determina los niveles de riesgo a partir de los cuales toma acciones de tratamiento sobre los mismos. Un Riesgo se considera aceptable cuando implementar más controles de seguridad se estima que consumiría más recursos que el posible impacto asociado.

El Responsable de 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.

Este análisis se repetirá:

- Al menos anualmente y cuando cambien la información manejada y/o los servicios prestados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

Una vez llevado a cabo el proceso de evaluación de riesgos, la Dirección de HM HOSPITALES es la responsable de aprobar los riesgos residuales y los planes de tratamiento de riesgo.

En el caso de las medidas implantadas en el ENS, si el análisis de riesgos establece medidas más importantes, se añadirán éstas a las descritas en el ENS.

Gestión de personal

Todo el personal de HM HOSPITALES relacionado con la información y los sistemas es formado e informado de sus deberes y obligaciones en materia de seguridad, esencialmente mediante los procedimientos de seguridad que en cada caso procedan y mediante las Normas de Uso de los Sistemas de Información. Sus actuaciones son supervisadas según los roles establecidos para verificar que se siguen los procedimientos definidos.

Los accesos de los usuarios son únicos y se verifican de forma periódica sus derechos y las actividades que tienen que ver con la seguridad de la información para corregir o exigir responsabilidades en su caso.

Profesionalidad, concienciación y formación

La seguridad de los sistemas es gestionada y revisada por personal de HM HOSPITALES cualificado y personal externo especializado, que recibe y actualiza la formación necesaria para

garantizar la seguridad de la información en todo el ciclo de vida de los sistemas de información: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento. Los requisitos de cualificación (formación y experiencia) serán siempre establecidos por HM HOSPITALES.

La presente Política de Seguridad de la Información debe ser conocida por todos los usuarios internos y externos y por las empresas que accedan, gestionen o traten datos de HM HOSPITALES.

El conjunto de políticas, normas y procedimientos complementarios a esta Política de Seguridad de la Información también deberán ser adecuadamente comunicados y puestos en conocimiento de las personas, empresas e instituciones afectadas o implicadas en cada caso.

Se definirán, periódicamente, programas de comunicación, concienciación y formación y se pondrá a disposición de los usuarios las Normas de Uso de los Sistemas de Información.

HM HOSPITALES promoverá la formación técnica en seguridad de la información necesaria, especialmente para los Responsables de Seguridad y de Sistemas.

Autorización y control de los accesos

El acceso a los sistemas de información es controlado, monitorizado y limitado a los usuarios, procesos, dispositivos y sistemas de información con las mínimas funcionalidades permitidas y/o autorizadas.

Se establecerán y gestionarán las autorizaciones necesarias para las tareas críticas.

Protección de las instalaciones

Los sistemas de HM HOSPITALES y su infraestructura de comunicaciones están situados en áreas protegidas debidamente, dotadas de medidas de seguridad físicas, de redundancia, continuidad y ambientales, y con un procedimiento de control de acceso físico.

Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos, HM HOSPITALES tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del Responsable de Seguridad.

Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores, y a lo dispuesto en el apartado de “Terceras partes” más adelante en este documento.

Mínimo privilegio y seguridad desde el diseño y por defecto

En HM HOSPITALES los sistemas se diseñan y configuran siempre pensando en la Seguridad desde el Diseño y por Defecto. El sistema proporciona la mínima funcionalidad requerida porque las funciones de operación, administración y registro de actividad son las mínimas necesarias, y HM HOSPITALES se asegura que sólo son accesibles por las personas, y desde emplazamientos o equipos autorizados.

Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario. Para ello, se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Todos los proyectos relacionados o que afecten a los sistemas de información deberán incluir, en su proceso de análisis, una evaluación de los requisitos de seguridad y definir un modelo de seguridad consensuado con el Responsable de seguridad de la Información.

En el diseño, desarrollo, instalación y gestión de los sistemas de información y en los proyectos se tendrán en cuenta y aplicarán los conceptos de seguridad desde el diseño, codificación segura y los controles y medidas de seguridad que proceda según el documento de aplicabilidad aprobado por HM HOSPITALES.

Integridad y actualización del sistema

En HM HOSPITALES los sistemas se evalúan de manera periódica para conocer en todo momento su estado de seguridad, tomando en consideración las especificaciones de los fabricantes, las vulnerabilidades, las deficiencias de su configuración, las actualizaciones que procedan y la detección temprana de incidentes, y gestionando de esta manera la integridad de los mismos.

Todos los elementos de los sistemas requieren autorización previa a su instalación.

Protección de la información almacenada y en tránsito

La información se clasifica de acuerdo con la sensibilidad requerida en su tratamiento y según los niveles de seguridad y protección exigibles.

HM HOSPITALES presta especial atención a la información almacenada o en tránsito a través de entornos inseguros. Esto incluye a la información almacenada o tratada en equipos portátiles, tabletas, smartphones, dispositivos periféricos, soportes de información, así como a las comunicaciones sobre redes abiertas o con cifrado débil, donde se aplican las medidas de seguridad que garanticen que la información se trata acorde a su clasificación.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Prevención ante otros sistemas de información interconectados

HM HOSPITALES protege el perímetro de acceso a su sistema, en particular en las conexiones a través de Internet, analizando siempre los riesgos derivados de la interconexión con otros sistemas, y estableciendo las medidas que garanticen el nivel de seguridad necesario.

Registro de actividad y detección de código dañino

HM HOSPITALES ha habilitado registros de la actividad de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales y demás disposiciones que resulten de aplicación.

HM HOSPITALES implementa un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones.

Al objeto de preservar la seguridad de los sistemas de información, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de

limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, se podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Incidentes de seguridad

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, HM HOSPITALES implementa las medidas de seguridad establecidas, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales, se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

HM HOSPITALES establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- 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.
- Para garantizar la disponibilidad de los servicios, HM HOSPITALES dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Los usuarios disponen de canales establecidos para informar de forma inmediata de cualquier incidente o anomalía detectada.

Continuidad de la actividad

HM HOSPITALES realiza las copias de seguridad que garantizan la recuperación de la información, y establece los mecanismos adecuados para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

En este sentido se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos y datos electrónicos producidos en el ámbito de sus competencias.

Mejora continua del proceso de seguridad

El sistema de gestión de seguridad implantado es actualizado y mejorado de manera continua, según establecen las certificaciones, tal y como está descrito más adelante en este documento.

7. Requisitos legales y marco normativo

- 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).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- 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.
- UNE-ISO/IEC 27001:2023 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.
- UNE-ISO/IEC 27002:2023 Seguridad de la información, ciberseguridad y protección de la privacidad. Control de la seguridad de la información. (ISO/IEC 27002:2022).

Así mismo, el Responsable de Seguridad será responsable de identificar las guías de seguridad del Centro Criptológico Nacional (CCN) que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

8. Roles, responsabilidades y deberes

Usuarios

Toda persona o sistema que acceda a la información tratada, gestionada o propiedad de HM HOSPITALES se considerará un usuario. Los usuarios son responsables de su conducta cuando acceden a la información o utilicen los sistemas informáticos de HM HOSPITALES. El usuario es responsable de todas las acciones realizadas utilizando sus identificadores o credenciales personales.

Los usuarios tienen la obligación de:

- Cumplir la Política de Seguridad de la Información y las normas, procedimientos e instrucciones complementarias.
- Proteger y custodiar la información de HM HOSPITALES, evitando la revelación, emisión al exterior, modificación, borrado o destrucción accidental o no autorizadas o el mal uso independientemente del soporte o medios por el que haya sido accedida o conocida.
- Conocer y aplicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y el resto de políticas, normas, procedimientos y medidas de seguridad aplicables.
- Generar incidencias o tareas respecto a la Seguridad de la Información.

Los usuarios que incumplan la Política de Seguridad de la Información o las normas y procedimientos complementarios podrán ser sancionados de acuerdo con lo establecido en los contratos que amparen su relación con HM HOSPITALES y con la legislación vigente y aplicable.

Responsable de la Información (Esquema Nacional de Seguridad)

El Responsable de la Información es quien determina los requisitos de la información tratada.

El Responsable de la Información tiene las siguientes responsabilidades:

- Velar por el buen uso de la información y, por tanto, de su protección.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información tratada, valorando las consecuencias de un impacto negativo.

Responsable del Servicio (Esquema Nacional de Seguridad)

El responsable del servicio tendrá las siguientes responsabilidades generales:

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad del servicio, de acuerdo con el Responsable de Seguridad y el Responsable del Sistema.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.

Dirección

La Dirección de HM HOSPITALES está profundamente comprometida con la política descrita en este documento y es consciente del valor de la información y del grave impacto económico y de imagen que puede producir un incidente de seguridad.

En el contexto del Esquema Nacional de Seguridad, la Dirección asume las responsabilidades descritas para el Responsable de la Información y el Responsable del Servicio. La Dirección hablará a través del Comité de Dirección.

HM Hospitales es propietaria de los activos de información, y la Dirección responsable de los riesgos.

La Dirección asume además las siguientes responsabilidades:

- Demostrar liderazgo y compromiso con respecto al Sistema de Gestión de Seguridad de la Información
- Asegurar que se establece la política y los objetivos de seguridad de la información y que estos son compatibles con la dirección estratégica de la organización.
- Informar de los cambios en el contexto de la organización que puedan afectar a la seguridad de la información al Comité de Seguridad de la Información y al DPD.

- Aprobar y comunicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y la importancia de su cumplimiento a todos los usuarios, internos o externos, a los clientes y a los proveedores.
- Reunirse al menos una vez al año dentro del ámbito del Comité de Seguridad, y cuando cualquier evento o solicitud extraordinaria lo demande, con los Responsables de Seguridad y de Sistemas, para ser informado sobre el SGSI y actualizar la estrategia en materia de Seguridad de la Información.
- Fomentar una cultura corporativa de seguridad de la información.
- Apoyar la mejora continua de los procesos de seguridad de la información.
- Asegurar que estén disponibles los recursos necesarios para el cumplimiento de la Política de Seguridad de la Información, de las Normas de Uso de los Sistemas de Información y para el funcionamiento del Sistema de Gestión de Seguridad de la Información.
- Definir el enfoque para el análisis y la gestión de los riesgos de seguridad de la información y los criterios para asumir los riesgos y asegurar la evaluación de los mismos al menos con una periodicidad anual.
- Asegurar que se realizan auditorías internas de seguridad de la información y que se revisan sus resultados para identificar oportunidades de mejora.
- Definir y controlar el presupuesto para seguridad de la información.
- Aprobar los planes de formación y las mejoras y proyectos relacionados con la Seguridad de la Información.
- Aprobar la documentación hasta su segundo nivel de normas y procedimientos.
- Determinar las medidas, sean disciplinarias o de cualquier otro tipo, que pudieran aplicarse a los responsables de violaciones de seguridad.

Responsable de Seguridad

El responsable de la seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios y supervisa la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones

La persona con el cargo de Responsable de Seguridad de la Información asumirá las siguientes funciones:

- Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información, con la responsabilidad y autoridad para asegurarse de que el Sistema de Gestión de la Seguridad de la Información cumple con los requisitos del Esquema Nacional de Seguridad y de la Norma UNE-ISO/IEC 27001.
- Supervisar el cumplimiento de la presente Política, de sus normas, procedimientos derivados y de la configuración de seguridad de los sistemas.
- Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables del Servicio y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS, declarando la aplicabilidad de dichas medidas.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.
- Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación a las normas especificadas en colaboración con el Responsable de Sistemas.
- Realizar, con la colaboración del Responsable del Sistema, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable del Sistema, aceptar los riesgos residuales calculados en el análisis de riesgos.

- Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información y analizar los informes de auditoría, elaborando las conclusiones a presentar al Responsable del Sistema para que adopte las medidas correctoras adecuadas.
- Coordinar el proceso de Gestión de la Seguridad, en colaboración con el Responsable de Sistemas.
- Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.
- Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período, en coordinación con el Responsable de Sistemas.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el Anexo II del ENS.
- Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, en coordinación con el Responsable del Sistema, aportando información puntual para la toma de decisiones.

Respecto a la documentación, y apoyándose en el Responsable del Sistema, son funciones del Responsable de Seguridad:

- Proponer al Comité de Seguridad para su aprobación la documentación de seguridad de segundo nivel (Normas de Seguridad TIC –STIC– y Procedimientos Generales del Sistema de Gestión de la Seguridad de la Información –SGSI–) y firmar dicha documentación.
- Aprobar la documentación de seguridad de tercer nivel (Procedimientos Operativos STIC e Instrucciones Técnicas STIC).
- Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma. Distribuirá la documentación del SGSI entre las personas necesarias.

Para el desarrollo de cualquiera de sus funciones el Responsable de Seguridad podrá recabar la colaboración del Responsable del Sistema.

Delegado de Protección de Datos

Siguiendo lo indicado en el RGPD y en la LOPDGDD, el Delegado de Protección de Datos tendrá como mínimo las siguientes funciones:

- Informar y asesorar al responsable del tratamiento y a sus empleados de las obligaciones que les incumben en relación con el RGPD y otras disposiciones de protección de datos.
- Supervisar el cumplimiento de lo dispuesto en dicho Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, 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 supervisar su aplicación de conformidad con el artículo 35 RGPD.
- Atender las consultas que los interesados realicen a la organización, ya sea para cuestiones relativas al tratamiento de sus datos o para el ejercicio de sus derechos.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

Responsable del Sistema

El Responsable del Sistema, por sí o a través de recursos propios o contratados, se encarga de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

Serán funciones del Responsable del Sistema las siguientes:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes.
- Seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación y cambios.
- Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, de acuerdo con el Responsable de Seguridad.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de Seguridad y la Dirección.
- Realizar con la colaboración del Responsable de Seguridad, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable de Seguridad, aceptar los riesgos residuales calculados en el análisis de riesgos.
- Elaborar en colaboración con el Responsable de Seguridad, la documentación de seguridad de tercer nivel (Procedimientos Operativos STIC e Instrucciones Técnicas STIC).

El Administrador de la Seguridad del Sistema

Las funciones que desempeñará son las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad de los sistemas de información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema en particular, los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los procedimientos operativos de seguridad.
- Aplicar los cambios de configuración del sistema de información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente, así como 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 del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

- Informar a los respectivos Responsables 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.

Comité de Seguridad de la Información

Compuesto por los siguientes miembros:

Permanentes:

- Técnico de Seguridad
- Responsable de Sistemas
- Responsable de Seguridad

Ac hoc:

- Dirección
- SSII/TD: Jefe Dpto. Seguridad y Sistemas, Técnico de Seguridad e Infraestructuras y Sistemas.
- TRC – Centro de Operaciones Seguridad
- Área Jurídico
- Área RRHH
- Área Calidad
- Delegado Protección de Datos

Se reúne al menos trimestralmente para coordinar la seguridad de la información a nivel de la organización.

Sus funciones son las siguientes:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
  - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
  - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
  - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
  - Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.
  - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
  - Revisar regularmente la presente Política de Seguridad de la Información para su aprobación por el órgano competente.
  - Elaborar la Normas de Uso de los Sistemas de Información de Seguridad de la Información para su aprobación en coordinación con la Dirección.

- 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 de carácter personal. Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas sobre la UNE-EN ISO/IEC 27001, ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la organización en materia de Seguridad de la Información.

9. Procedimiento de designación y resolución de conflictos

La Dirección de HM HOSPITALES asigna, renueva y comunica las responsabilidades, autoridades y roles en lo referente a la Seguridad de la Información, determinando en cada caso los motivos y el plazo de vigencia. También se asegurará de que los usuarios conocen, asumen y ejercen las responsabilidades, autoridades y roles asignados, resolviendo los conflictos que se generen en relación a cada responsabilidad en Seguridad de la Información.

El Responsable de la Seguridad será distinto del Responsable del Sistema, no debiendo existir dependencia jerárquica entre ambos.

10. Datos de carácter personal

La organización sólo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

De este modo, conforme a lo establecido en el RGPD y en la LOPDGDD se han adaptado las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos.

11. Terceras partes

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

Cuando HM HOSPITALES utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de las Normas de Uso de Sistemas de Información existente que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad ENS 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.

12. Desarrollo del SGSI, revisión y auditorías

El Comité de Seguridad ha aprobado el desarrollo de un Sistema de Gestión de Seguridad de la información (SGSI) que es establecido, implementado, mantenido y mejorado conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad y de la UNE-EN ISO/IEC 27001. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados. Existe un procedimiento de gestión documental que establece las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

La Política y las Normas de Seguridad de la Información se adaptarán a la evolución de los sistemas y de la tecnología y a los cambios organizativos y se alinearán con la legislación vigente y con los estándares y mejores prácticas del Esquema Nacional de Seguridad y de la UNE-EN ISO/IEC 27001, prestando especial atención a las guías publicadas por el Centro Criptológico Nacional como desarrollo de las medidas y controles de seguridad.

Las medidas de seguridad y los controles físicos, administrativos y técnicos aplicables se detallarán en el Documento de Aplicabilidad, y serán proporcionales a la criticidad de la información a proteger y a su clasificación.

El Comité de Seguridad de la Información revisará esta política anualmente o cuando haya cambios significativos que así lo aconsejen, y la someterá de nuevo a aprobación por la Dirección. Las revisiones comprobarán la efectividad de la política, valorando los efectos de los cambios tecnológicos y de negocio.

El Sistema de Gestión de Seguridad se auditará anualmente (UNE-EN ISO/IEC 27001) o cada dos años (Esquema Nacional de Seguridad), según un plan de auditorías desarrollado por el Responsable de Seguridad.

Aprobado por: **CIO /Comité de Seguridad**

Fecha: **Septiembre 2024**

Firma: **Jesús Sánchez**
Dirección Corporativa Transformación Digital y Sistemas