



Política de Seguridad de la Información

Politica-Seguridad-Informacion-ENS-v.20251017

Clasificación | Público

Elaborado por: Juan **Juan Pablo Nieto Muñoz**

Creado: viernes, 17 de octubre de 2025

Modificado: viernes, 17 de octubre de 2025

Aviso: La información contenida en este documento pertenece a Juaneda Hospitales. Dependerá de la clasificación de la información del documento el que cualquier forma de divulgación, reproducción, copia o distribución total o parcial de la misma quede prohibida, no pudiendo ser utilizada para otros fines sin la autorización de Juaneda Hospitales.

Control de versiones

Fecha	Versión	Autor	Descripción
17/10/2025	1.0	Juan Pablo Nieto	Creación

Politica-Seguridad-Informacion-ENS-v.20251024	
Revisado por: D. Juan <u>Juan Pablo Nieto Muñoz</u>	Aprobado por: D. <u>Juan De Dios Garcia Guerrero</u>
Nivel de seguridad: Público	

Índice

1 Introducción	4
2 Misión y Servicios Prestados	5
3 Principios Básicos	5
4 Objetivos de la Seguridad de Información	6
5 Alcance	8
6 Marco Normativo	8
7 Organización de la Seguridad de la Información	8
7.1 Criterios de la Seguridad de la Información	8
7.2 Comité de Seguridad de la Información	8
7.3 Designación y resolución de conflictos	9
8 Datos personales y riesgos que se derivan del tratamientos	10
9 Obligaciones del personal	10
10 Documentación complementaria	10
11 Terceras partes	11
12 Resolución de conflictos	11
13 Aprobación y entrada en vigor	11

1 Introducción

Juaneda Hospitales, depende de los sistemas TIC (Tecnologías de la Información y las Telecomunicaciones) 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 una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), así como realizar un seguimiento continuo de los niveles de prestación de los servicios, monitorizar y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los ciber incidentes para garantizar la continuidad de los servicios prestados.

De este modo, todas las unidades de Juaneda Hospitales tienen presente que la seguridad tecnológica 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 tecnológicos.

Por tanto, 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, con la aplicación de las medidas que se relacionan a continuación.

Se ha de comentar que en el ENS a menudo se indica en múltiples puntos “Política de Seguridad de la organización”. Debe de atenderse y evaluarse en cada caso cuándo se trata o se refiere al documento de “Política de Seguridad de la Organización” y cuándo al argot técnico utilizado como “Políticas de seguridad”, dónde este último se refiere como “Política de Seguridad” a aquella configuración de software o hardware que establezca unas normas o pautas a seguir, para que se cumpla en unos determinados casos de uso en concreto

2 Misión y Servicios Prestados

Juaneda Hospitales como órgano sanitario que realiza servicios con el sector privado y público sanitario, para la gestión de sus intereses, y en el ámbito de sus competencias sirve con objetividad los intereses generales y actúa de acuerdo a los principios de eficacia, jerarquía, descentralización y coordinación, promueve toda clase de actividades y presta los servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de los ciudadanos.

El organismo, presta los servicios que se regulan en el documento de categorización del sistema por el que se cumple las normativas de seguridad.

3 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:

- a) Seguridad como proceso integral.
- b) Gestión de la seguridad basada en los riesgos.
- c) Prevención, detección, respuesta y conservación.
- d) Existencia de líneas de defensa.
- e) Vigilancia continua.
- f) Reevaluación periódica.
- g) Diferenciación de responsabilidades.

Y por ello, y se desarrollará aplicando los siguientes requisitos mínimos:

- a) Organización e implantación del proceso de seguridad
- b) Análisis y gestión de los riesgos
- c) Gestión de personal
- d) Profesionalidad
- e) Autorización y control de los accesos
- f) Protección de las instalaciones
- g) Adquisición de productos de seguridad y contratación de servicios seguridad
- h) Mínimo privilegio
- i) Integridad y actualización del sistema
- j) Protección de la información almacenada y en tránsito
- k) Prevención ante otros sistemas de información interconectados
- l) Registros de la actividad y detección de código dañino
- m) Incidentes de seguridad
- n) Continuidad de la actividad
- o) Mejora continua del proceso de seguridad

4 Objetivos de la Seguridad de Información

La organización, 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 la organización se encontrarán inventariados y categorizados y estarán asociados a un responsable.
 - Seguridad ligada a las personas: Se implementarán 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, 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 sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.
- Protección de datos:
 - Se adoptarán las medidas técnicas y organizativas que corresponda implementar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad.
 - Dar a conocer los usuarios de Juaneda Hospitales las normas internas de seguridad que afectan al desarrollo de sus funciones en materia de protección de datos en cumplimiento normativa de Protección de Datos de Carácter Personal, y por consiguiente contribuir al buen uso de los medios técnicos e informáticos propiedad de Juaneda Hospitales.
- 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.
 - Configurarse como un posible instrumento de diligencia a nivel probatorio en caso de que se pudieran derivar acciones judiciales en materia de responsabilidad penal de las personas jurídicas. De tal forma, servir como instrumento de diligencia y control en aras del correcto cumplimiento del programa de prevención de delitos.

5 Alcance

Esta Política se aplicará a los sistemas de información de Juaneda Hospitales, relacionados con el ejercicio de sus competencias y a todos los usuarios con acceso autorizado a los mismos. 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 de Seguridad TIC o tecnológico disponer los medios necesarios para que la información llegue al personal afectado.

6 Marco Normativo

El marco normativo que aplica es aquel que está regido a través de todas aquellas normas que integren la seguridad de la información en el ámbito del servicio que presta la organización y su tecnología, en especial el Esquema Nacional de Seguridad (ENS) y cualquier norma que derive o esté tratada en este.

7 Organización de la Seguridad de la Información

7.1 Criterios de la Seguridad de la Información

La organización, teniendo en cuenta los artículos que describe el ENS, establece las siguientes acciones para organizar la Seguridad de la Información:

- i. Designará roles de seguridad: Responsables unificados de Servicios y de la Información, Responsable de la Seguridad, Responsable del Sistema y Delegado de Protección de Datos.
- ii. Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información. Este órgano se denominará Comité de Seguridad de la Información.

7.2 Comité de Seguridad de la Información

En la organización, se ha creado el Comité de Seguridad de la Información que estará compuesto por los siguientes miembros:

- Dirección

Estos miembros se clasifican en permanentes o no permanentes atendiendo a la obligatoriedad de la participación del Comité de Seguridad de la Información:

Miembros permanentes:

- Dirección
- Responsable de Sistema (RSIS)
- Responsable de Seguridad de la Información (RSEG)

- Asesores que se consideren oportunos para los temas en cuestión con voz, pero sin voto.

Miembros no permanentes:

- Responsables del Servicio y de la Información.
- Delegado de Protección de datos.
- Representantes de la organización, especialistas externos de los sectores público, privado, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

Los Responsables de la Información y los Servicios serán convocados por la presidencia en función de los asuntos a tratar, en representación de los distintos ámbitos o áreas de seguridad TIC. Cada área estará representada por un vocal con voto, sin perjuicio de que acudan varios representantes de la misma.

El Delegado de Protección de Datos participará con voz, pero sin voto 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. En todo caso, si un asunto se sometiera a votación, se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

El Secretario/a del Comité realizará las convocatorias y levantará actas de las reuniones del Comité de Seguridad. A las sesiones del Comité de Seguridad podrán asistir en calidad de asesores las personas que en cada caso estime pertinentes su Presidente.

La definición de estos roles y obligaciones de las diferentes figuras que conforman el comité de seguridad de la información, se encuentran en un anexo a esta política.

7.3 Designación y resolución de conflictos

- 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 a través de un acta de constitución inicial.
- Los roles nombrados se renovarán anualmente de forma automática. Las bajas o modificaciones en los roles designados, se comunicarán al Comité y se seguirán los cauces establecidos para la designación del nuevo responsable.
- Tal y como se regula en el artículo 13.3 del RD del ENS, se estipula que no puede existir dependencia jerárquica entre el RSEG y el RSIS, salvo excepciones justificadas, lo que conlleva a disponer de medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades.

8 Datos personales y riesgos que se derivan del tratamientos

El Legislador en el apartado 1.f) del artículo 12 del RD del ENS, intenta transmitir aquella referencia al correcto cumplimiento en materia de datos de carácter personal.

Por ello, para su correcta adecuación y cumplimiento de la LOPD-GDD y RGPD, se publicará el registro de actividades de su tratamiento y se realizará la gestión de riesgos a través de Análisis de Riesgos y EIPD, en el caso que fuese necesario esta, en la organización.

Todos los sistemas afectados por la presente Política de Seguridad están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos.

Las fases de este proceso se realizarán según lo dispuesto en los Anexos I y II del RD del ENS.

9 Obligaciones del personal

Todo el personal, tanto externo como interno, que interactúe con el sistema de información deberá de cumplir con la presente política de seguridad de la información.

10 Documentación complementaria

El cuerpo normativo se desarrollará en tres niveles:

- a) Primer nivel normativo: constituido por la presente Política de Seguridad de la Información.
- b) Segundo nivel normativo: constituido por las normas de seguridad derivadas de las anteriores con el objetivo de indicar el uso correcto de aspectos concretos del sistema de gestión de seguridad de la información.
- c) Tercer nivel normativo: constituido por procedimientos de seguridad, 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 dirección, la aprobación de la Política de Seguridad de la Información y siendo el Comité de Seguridad de la Información el órgano responsable de la aprobación y difusión de los restantes documentos propios de la organización, todo ello tal y como se establece en el artículo 12 del RD ENS.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

11 Terceras partes

Cuando la organización, 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 la organización 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 atañe 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 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 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.

Para cualquier relación con terceras partes, se establecerá un canal de comunicación con esta llamado Punto operacional de Comunicación (POC).

12 Resolución de conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de seguridad de la información corresponderá, en última instancia, al Comité de Seguridad de la Información la resolución de conflictos en calidad de máximo responsable de la organización.

13 Aprobación y entrada en vigor

Esta Política de Seguridad de la Información, será efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Texto aprobado el día __ de ____ de _____ vía Firma Electrónica del Director de Transformación Tecnológica en representación del Comité de Seguridad de la Información por Juaneda Hospitales.