ORG.1 - Política de Seguridad

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 ciberincidentes para garantizar la continuidad de los servicios prestados.

De este modo, todas las unidades administrativas de Juaneda Hospitales 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 TIC.

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 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”, donde 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.

Misión y servicios prestados

Juaneda Hospitales, como Órgano de Gobierno Municipal, para la gestión de sus intereses y en el ámbito de sus competencias y como Administración pública, 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 habitantes del municipio.

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

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:

- Seguridad como proceso integral.
- Gestión de la seguridad basada en los riesgos.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua.
- Reevaluación periódica.
- Diferenciación de responsabilidades.

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

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registros de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

Objetivos de la seguridad de la información

La organización establece como objetivos de la seguridad de la información los siguientes:

- Dar a conocer a 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 de la 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.
- 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.
- 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 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.
- 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.

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 disponer los medios necesarios para que la información llegue al personal afectado.

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, en especial el Esquema Nacional de Seguridad (ENS) y cualquier norma que derive o esté tratada en este.

Organización de la seguridad de la información

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:

- 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.
- 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.

Definición de roles y responsabilidades asociados al ENS

Responsables de Información y de los Servicios (RS)

Serán funciones de los Responsables de la Información y de los Servicios:

- Establecer 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.
- 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 la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo. El cual dará traslado de dichos cambios al Comité de Seguridad de la Información en su próxima reunión.
- Tiene la responsabilidad última del uso que se haga de determinados servicios e información y, por tanto, de su protección.

Responsable de la Seguridad de la Información (RSEG)

Serán funciones del Responsable de Seguridad:

- 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 y elaborar documentación del sistema.
- Aprobar la Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad TIC.
- Participar en la elaboración e implantación 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 poner en conocimiento al Comité las modificaciones que se hayan realizado a lo largo del periodo en curso.

- Participar en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política de Seguridad de la Información, para su aprobación por Dirección.

Actuará como Secretario del Comité de Seguridad de la Información, realizando las siguientes funciones:

- Convocar las reuniones del Comité de Seguridad de la Información.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

Responsable del Sistema (RSIS)

Serán funciones del 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 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.
- 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.
- Coordinar 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.

Delegado de Protección de Datos (DPD)

Serán funciones del Delegado de Protección de Datos:

- Informar y asesorar a la organización, 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 de la organización, 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.

El Delegado de Protección de Datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:

- Recabar información para determinar las actividades de tratamiento.
- Analizar y comprobar la conformidad de las actividades de tratamiento.
- Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
- Recabar información para supervisar el registro de las operaciones de tratamiento.
- Asesorar en el principio de la protección de datos por diseño y por defecto.
- Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.
- Priorizar actividades en base a los riesgos.
- Asesorar al Responsable de Tratamiento sobre áreas a acometer auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

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 clasificarán en permanentes o no permanentes atendiendo a la obligatoriedad de la participación en el 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 y 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 dirección 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 sometiese a votación, se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

Roles del Comité de Seguridad de la Información

- **Responsable de Sistema (RSIS):** Responsable del departamento de Sistemas
- **Responsable de Seguridad de la Información (RSEG):** Responsable de Seguridad de la Información y Proyectos TI / TD
- **Delegado de Protección de Datos:** Responsable de Seguridad de la Información y Proyectos TI / TD

Responsables del Servicio y de la Información:

- Historia Clínica: Director Médico Asistencial
- Servicio de HC Laboratorio: Responsable del departamento de Laboratorio
- Servicio de HC Radiología: Responsable del departamento de Radiología
- Servicio de HC Hemodiálisis: Responsable del departamento de Hemodiálisis
- Servicio de HC Radioterapia: Responsable del departamento de Radioterapia
- Servicio de HC Banco de Sangre: Responsable del departamento de Banco de Sangre / Hemoterapia

Atribuciones del Comité de Seguridad de la Información

Serán funciones del Comité de Seguridad:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución en lo que respecta a la seguridad de la información.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar documentación de seguridad de la información.
- 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.
- Estar permanentemente informado de la relación de Entidades de Certificación acreditadas y organizaciones, públicas y privadas, certificadas.
- 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.
- 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.
- 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.
- 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.

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes departamentos, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.
- Revisar la Política de Seguridad de la Información previa aprobación por el Órgano Superior.
- Aprobar el Plan de Adecuación para la implantación del ENS.

Periodicidad de las reuniones y adopción de acuerdos

El Comité de Seguridad de la Información se reunirá, al menos, una vez al año, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera una mayor frecuencia en las reuniones.
Las decisiones se adoptarán por consenso de los miembros permanentes.

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 disponer de medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades.

Datos personales y riesgos que se derivan del tratamiento

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 tratamiento y se realizará la gestión de riesgos a través de Análisis de Riesgos y EIPD, en el caso de que fuese necesario, 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.

Obligaciones del personal

Todo el personal, tanto externo como interno, que interactúe con el sistema de información deberá cumplir con la presente Política de Seguridad de la Información.

Documentación complementaria

La presente Política de Seguridad de la Información será complementada con documentos más precisos (normas, guías y procedimientos de seguridad) que ayuden a llevar a cabo lo propuesto.

El cuerpo normativo se desarrollará en tres niveles:

- **Primer nivel normativo:** constituido por la presente Política de Seguridad de la Información.
- **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.
- **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.

Terceras partes

Cuando la organización preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes 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 partícipes 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.

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).

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.

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 6 de mayo de 2026 vía acta de comité de seguridad de Juaneda Hospitales ·