Hospital Universitario Infanta Cristina

ANEXO POLÍTICA DE GESTIÓN DEL HOSPITAL UNIVERSITARIO INFANTA CRISTINA

HOSPITAL UNIVERSITARIO INFANTA CRISTINA depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a las dimensiones de seguridad que le son de aplicación: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, y uso previsto y valor de la información tratada o los servicios prestados.

Para defenderse de 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 se deban aplicar las medidas mínimas de seguridad exigidas por la Legislación de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Este Anexo Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** se integrará a la normativa básica del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**, incluyendo su difusión previa, y la instrumentación de las sanciones correspondientes por incumplimiento del presente texto, así como de los documentos relacionados a esta.

1. Objetivo

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 y reaccionando con presteza a los incidentes.

El Anexo Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** establece los principios básicos y requisitos mínimos de seguridad necesarios para proteger la información, así como la tecnología utilizada para su procesamiento, estableciendo las directrices para la implantación de medidas organizativas, técnicas y legales y define los responsables de su desarrollo, implantación y gestión.

La implantación de dichas medidas se realizará de forma preventiva, reactiva, dinámica y mediante mecanismos de detección, que garanticen en todo momento la preservación de la información, y el cumplimento de las leyes en vigor que afecten a su uso y tratamiento.

2. Referencias y marco normativo

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Norma UNE-ISO/IEC 27001:2023. Sistema de la información , ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.
- Norma UNE-ISO/IEC 27002:2023. Seguridad de la información, ciberseguridad y protección de la privacidad. Control de la seguridad de la información.
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).
- Reglamento (UE) 910/2014 del Parlamento Europeo y de Consejo de 23 de Julio de 2014 relativo a la

identificación electrónica y de los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

- Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo de 11 de diciembre de 2018 por la que se establece el Código Europeo de las Comunicaciones Electrónicas.
- 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.

3. Alcance

El alcance del Anexo Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** se centra en la información y los recursos de procesamiento de la información de todos los Sistemas de Información que usa, administra, o custodia el **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**.

Asimismo, el Anexo Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** cumple con las especificaciones del Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad).

4. Principios de actuación

El **HOSPITAL UNIVERSITARIO INFANTA CRISTINA,** en Parla (Madrid), es un centro de la red pública de hospitales de la Comunidad de Madrid. Tiene como misión la de diagnosticar y tratar las enfermedades de sus pacientes con el fin de procurar su pronta recuperación y el retorno a su vida diaria habitual y a su entorno social, con estándares de óptima calidad y con un compromiso especial por sus pacientes.

Nuestros principios fundacionales son la seriedad, calidad y ética profesional en el tratamiento de los servicios que prestamos, manteniendo siempre las bases de reserva y confidencialidad que estos asuntos requieren.

Es por ello que la Gerencia del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** se compromete a llevar a cabo, difundir y hacer cumplir los principios de su Política de Seguridad de la Información haciendo partícipes de la misma a sus partes interesadas.

Nuestra Política de Seguridad de la Información se basa en los principios y valores adquiridos a través de nuestra experiencia y dos pilares básicos:

4.1 Relativos al Sistema Integrado de Gestión

Se fundamenta en:

- La satisfacción de las necesidades reales de los grupos de interés y en especial de los pacientes y familiares. Considerando la seguridad como un aspecto relevante de nuestra actuación.
- Cumplir estrictamente con los requisitos legales y regulaciones aplicables al sector y otros que el **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** suscriba.
- Velar porque los principios sean asumidos por los profesionales que trabajan en el **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** y que se incorporen como pautas de conducta habitual con una actitud abierta y positiva hacia la mejora continua y permanente del Sistema de Gestión de Seguridad de la Información.
- Asegurar un compromiso manifiesto de la Gerencia del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** para la difusión, consolidación y cumplimiento de la presente Política.

- Mantener la Política de Seguridad de la Información de nuestro centro sanitario actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

4.2 Relativos a la Seguridad de la Información

Se fundamenta en:

- Constituir la seguridad de la información como una herramienta que permita identificar y minimizar los riesgos y amenazas a los cuales se expone la información del Hospital.
- Identificar, clasificar y establecer los mecanismos de protección necesarios para todos los activos pertenecientes al **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Definir e implantar controles para proteger la información contra violaciones de autenticidad, accesos no autorizados y pérdida de integridad, que garanticen la disponibilidad de los servicios ofrecidos por el **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**.
- Adquirir un compromiso de responsabilidad por parte de todas las personas internas y externas de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Instar al uso, única y exclusivamente, de software autorizado, que haya sido adquirido legalmente por el Hospital o por otras administraciones que nos autoricen su uso.
- Transmitir la responsabilidad de todas las personas internas y externas de informar de los Incidentes de seguridad, eventos sospechosos o mal uso de los recursos que pudieran identificarse.

Adicionalmente, el **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** cuenta con políticas específicas y un conjunto de estándares y procedimientos que soportan esta Política de Seguridad de la Información.

5. Destinatarios

La presente Política de Seguridad de la Información del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**, será de aplicación y de obligado cumplimiento para todo el personal adscrito a él que, preste servicios en el mismo independiente de la forma de contratación y vinculación con el mismo, de manera permanente o eventual, que en el desempeño de sus funciones o parte de ellas desarrolle su trabajo fuera de sus instalaciones, en adelante los usuarios.

6. Organización de la seguridad en el Hospital

La estructura organizativa encargada de la gestión de la seguridad de la información en el ámbito de los sistemas de información del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**, estará compuesta por:

6.1 Comité de Seguridad de Sistemas de Información

El Comité de Seguridad es un órgano, cuya competencia será velar por e impulsar la seguridad de la información y protección de los datos de carácter personal del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**.

6.2 Ámbito de responsabilidad

El Comité se responsabiliza de alinear todas las actividades del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** en materia de seguridad de la información y protección de datos de carácter personal. En concreto:

- coordina las actividades relacionadas con los sistemas de información y comunicaciones del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**,
- es responsable de la redacción del Anexo Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**,
- es responsable de la creación y aprobación de las normas que emanan del uso de los sistemas de información del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**,
- aprueba los procedimientos de actuación y calificación en lo relativo al uso de los sistemas de información y
- es responsable de velar por el correcto cumplimiento de las medidas de seguridad, en materia de protección de datos de carácter personal.

6.3 Funciones del Comité de Seguridad de Sistemas de Información

A nivel de gestión de la seguridad:

- elaborar la estrategia de evolución del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**. en lo que respecta a la seguridad de la información y protección de datos,
- promover la mejora continua del sistema de gestión de la seguridad de la información del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**,
- elaborar y revisar periódicamente, y al menos, una vez al año, el Anexo Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**,
- aprobar la normativa interna de seguridad de la información del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**, así como su armonización respecto a la establecida por parte de la CSCM,
- elaborar planes de mejora de la seguridad de la información del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**,
- elevar los Planes de Contingencia a la Comisión de Dirección para su aprobación,
- mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** de acuerdo con lo establecido en la Política de Seguridad de la Consejería de Sanidad,
- elaborar procedimientos de Seguridad de la Información dentro de la actividad del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**, con la finalidad de implantar lo dictado en las normas de seguridad de la información de la CSCM y
- analizar y proponer salvaguardias que prevengan incidentes similares en el futuro.

A nivel de coordinación de la seguridad:

- coordinar la seguridad de la información a nivel de hospital,
- atender a las solicitudes e instrucciones del Comité de Seguridad de la Información de la CSCM y
- coordinar los esfuerzos e interactuar con el Comité de Seguridad de la CSCM en todo lo referente a la seguridad de los sistemas de información.

A nivel de control de la seguridad:

- informar regularmente del estado de seguridad de la información al Comité de Seguridad de la Información de la Consejería de Sanidad de la Comunidad de Madrid,

- impulsar planes de formación y concienciación en materia de seguridad de la información y protección de datos a todo el personal que preste sus servicios en el **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**,
- aprobar las medidas correctivas derivada de las Auditorias de sobre la seguridad de la información,
- velar y supervisar la efectiva implantación de las medidas de seguridad necesarias en el desarrollo de todos los proyectos, desde su especificación inicial hasta su puesta en operación y
- monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones respecto de ellos.

El Comité asume la figura de Responsable de Seguridad, y con ello todas las funciones propias del mismo en materia de protección de datos, entre las que se encuentran:

- representar al **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**, por delegación del Responsable del Fichero, en lo relacionado al cumplimiento de la normativa legal sobre el tratamiento de datos de carácter personal,
- gestionar y coordinar la efectiva puesta en marcha de las medidas de seguridad, así como verificar cumplimiento de las mismas,
- promover la difusión de la documentación de seguridad de la información entre el personal del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**,
- revisar, al menos de forma trimestral, las incidencias registradas, proponiendo las medidas correctoras que limiten su ocurrencia en el futuro,
- solicitar periódicamente a los responsables de seguridad delegados (los cuales son definidos más adelante) que le reporten sobre el estado de implantación de las medidas de seguridad exigidas por la normativa de protección de datos de carácter personal.

6.4 Composición del Seguridad de Sistemas de Información

El Comité estará compuesto por los siguientes miembros:

a) Presidente: cargo que será ocupado por el titular de la Dirección Gerencia del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**, quien asumirá las siguientes competencias:
   - convocar las reuniones periódicas del Comité,
   - dirigir el Comité, proponiendo los distintos puntos a tratar en las reuniones periódicas,
   - realizar el seguimiento de los distintos proyectos y equipos de trabajo que hayan surgido como respuesta a objetivos estratégicos y tácticos,
   - comunicar al resto de comités de la CSCM las directrices claras a tener en cuenta en relación a los proyectos en curso y requisitos de seguridad que les puedan afectar, y
   - nombrar, a propuesta del Secretario, al resto de los miembros del Comité.

b) Vicepresidente: cargo que será desempeñado por Jefe de Servicio de Sistemas de la Información, quien desempeñará las funciones del presidente en ausencia de éste. Igualmente.

c) Secretario: será ocupado por el Jefe de Sección de Gabinete Jurídico del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**.
   - convocar las reuniones periódicas, así como las extraordinarias del Comité,
   - preparar los temas a tratar en las reuniones del comité, aportando información puntual para la toma de decisiones,
   - elaborar el acta de las reuniones y

- ser responsable de la comunicación directa o delegada de las decisiones del Comité.

d) Vocales:

- Representante de Atención al Paciente.
- Representante del área de Asesoría Jurídica.
- Representante de Recursos Humanos.
- Representante de Admisión y Documentación Clínica.

Dichos representantes son nombrados por el Presidente del Comité.

e) Invitados: a las reuniones del Comité podrá acudir, con voz, pero sin voto, convocados por el presidente, aquellas personas que, por razón de su actividad o conocimientos, tengan relación con los asuntos a tratar.

6.5 Funcionamiento

El Comité se reunirá como mínimo cuatro veces al año y de forma extraordinaria, siempre que el Presidente lo considere pertinente, así como de forma inmediata tras un incidente de seguridad que afecte a la seguridad de la información del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**, o a los datos de carácter personal custodiados por el mismo.

Los temas que se adopten en las reuniones deberán estar alineados con la definición de los objetivos de seguridad que se traten de alcanzar dentro de cada plan de mejora de acciones correctivas y preventivas, así como los objetivos por los cuales se constituye el Comité y las competencias que ostenta.

Después de cada reunión el Secretario levantará acta, que deberá ser firmado en todo caso, por el Presidente o el Vicepresidente.

6.6 Función diferenciada

En el Sistema de Información del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** se diferencian el Responsable de la Información, el Responsable del Servicio y el Responsable de la Seguridad.

- El Responsable de la Información determinará los requisitos de la información tratada y será asumido por la Jefa de Sección de Gabinete Jurídico del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**.
- El Responsable del Servicio determinará los requisitos de los servicios prestados y será asumido por el Comité de Seguridad del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**, siendo el representante la Gerencia, y la sustituta la Jefa de Admisión.
- El Responsable de Seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios y será asumido por Jefe de Servicio de Sistemas de la Información del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**.
- El Responsable de Sistema se encargará del funcionamiento operativo del sistema de información y será asumido por la Gerencia del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**.

Ante cualquier conflicto entre las partes este se elevará al Comité de Seguridad, qué será quien determine la manera más efectiva de proceder.

6.7 Designación del POC (Point of Contact)

Un POC (siglas en inglés de Point of Contact) es la persona o unidad identificada como responsable de recibir,

gestionar y coordinar la comunicación con terceros (por ejemplo, proveedores, organismos externos o CERT/CSIRT) en caso de que se produzca un incidente de seguridad.

Sus funciones principales son:

- actuar como intermediario oficial en la comunicación de incidentes con proveedores o servicios subcontratados,
- coordinar respuestas técnicas, operativas y administrativas durante un incidente,
- asegurar la trazabilidad y registro de las comunicaciones, y
- estar disponible para responder en los tiempos definidos en el procedimiento de gestión de incidentes.

El POC será asumido por Jefe de Servicio de Sistemas de la Información del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**.

7. Directrices de Seguridad de la Información

Las directrices del Anexo Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** serán desarrolladas de acuerdo a los estándares internacionales previstos en la Norma ISO/IEC 27001, el Código de Buenas Prácticas para la Gestión de la Seguridad de la Información, así como en el Esquema Nacional de Seguridad y Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**.

- Organización e implantación del proceso de seguridad.

  La seguridad de la información y protección de los datos deberá comprometer a todos los miembros del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**. En el presente documento se identifican a los responsables de velar por el cumplimiento del mismo y ponerla en conocimiento de todos los miembros de la organización administrativa.

- Análisis y Gestión de riesgos.

  Este proceso comprende las fases de categorización de los sistemas y servicios, identificación de los activos, responsables, análisis de los riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas. De ser necesario, se elaborará un Plan de Tratamiento de Riesgos.

  Este análisis se repetirá:

  - regularmente, al menos una vez al año,
  - cuando cambien los sistemas,
  - cuando cambien los servicios prestados,
  - cuando ocurra un incidente grave de seguridad y/o
  - cuando se reporten vulnerabilidades graves.

  Será el Comité de Seguridad el encargado de que se lleve a cabo el preceptivo análisis de riesgos. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, las cuales serán reevaluadas y actualizadas periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

- Gestión de Personal.

  Todos los miembros del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** deberán ser formados e informados de sus deberes y obligaciones en materia de seguridad y protección de datos de carácter personal. Sus

actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.

Su formación y concienciación será necesaria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El personal relacionado con la información y los sistemas, ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.

El significado y alcance del uso seguro del sistema se concretará y plasmará en las normas internas de seguridad del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**.

Será el Comité de Seguridad el encargado de fomentar la concienciación de los usuarios de los sistemas para alcanzar un grado de madurez en la formación seguridad de la información, por lo que deberá disponer de los medios necesarios para que la información llegue a los afectados.

Con la periodicidad establecida por el Comité y, al menos, una vez al año, se llevarán a cabo formaciones en aquellos temas que se haya detectado que se encuentran en mayor situación de olvido, o que, por la criticidad de la información, es necesario incidir en la importancia de adoptar buenas prácticas en su tratamiento y custodia. Se establecerá un programa de concienciación continua para atender a todos los miembros del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**, en particular a los de nueva incorporación.

El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** y a todas las actividades, de acuerdo al principio de Seguridad Integral recogido en el Artículo 5 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

Así mismo, se definirán las exigencias de confidencialidad y no divulgación de datos para todos los miembros del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**, esta exigencia se definirá formalmente y todo el personal deberá firmar como prueba de recepción.

- Profesionalidad.

  La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

  El personal del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**.

  Se hace necesario que, de manera objetiva y no discriminatoria, las organizaciones que presten servicios de seguridad al **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados.

- Autorización y control de los accesos.

  El acceso a los sistemas de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

  Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe 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 determinada actividad.

- Protección de las instalaciones.

  Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

Por ello, en primer lugar, se ha de establecer un perímetro físico de seguridad que proteja la información de la organización para prevenir incidencias, y garantizar el funcionamiento del resto de medidas.

El acceso a los locales, mediante vías de acceso autorizadas y controladas, barreras arquitectónicas como paredes o ventanas, elementos adicionales como áreas de descarga controladas, debe ser gestionado para proteger las zonas que contienen instalaciones informáticas o permiten el acceso a las mismas.

Dentro del perímetro de seguridad, se deben identificar las ubicaciones que almacenan soportes que puedan contener datos confidenciales o especialmente protegidos, estas ubicaciones dispondrán de una identificación personal de los usuarios que permita validar si disponen de autorización para su acceso.

Se deben validar las medidas de seguridad físicas de acceso al perímetro de seguridad, compuestas por puertas, cerraduras, alarmas, vigilancia, y formalizarlas en instrucciones de acceso a los locales, que deberán ser comunicadas a todo el personal.

- Adquisición de productos de seguridad.

  En la adquisición de productos de seguridad para las tecnologías de la información y las comunicaciones que se utilizarán en el **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**, será obligatorio que dichos productos cuenten con la certificación de las funcionalidades de seguridad relacionadas con su objeto de uso. Además, cualquier proveedor que tenga acceso a información sensible deberá aceptar y cumplir con la normativa de seguridad establecida y publicada por el hospital.

  La certificación de los productos deberá cumplir con las normas y estándares de seguridad funcional más reconocidos a nivel internacional.

- Seguridad por defecto.

  Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto, lo que se traduce en:

  - el sistema proporcionará la mínima funcionalidad requerida para que la organización sólo alcance sus objetivos, y no alcance ninguna otra funcionalidad adicional,
  - las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados,
  - en un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue,
  - el uso ordinario del sistema será sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario y
  - automatizando la actualización del sistema en la medida de lo posible.

  Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

  Se deberá conocer en todo momento el estado de 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.

- Protección de la información almacenada y en tránsito.

  En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los siguientes dispositivos: equipos portátiles, tabletas, dispositivos periféricos,

soportes de información (pen-drive, disco duro) y comunicaciones sobre redes abiertas o con cifrado débil.

Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por el **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** en el ámbito de sus competencias.

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 en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

- Prevención ante otros sistemas de información interconectados.

  El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, o a través de redes, con otros sistemas, y se controlará su punto de unión.

- Registro de actividad.

  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, de función pública o laboral, y demás disposiciones que, de aplicación, se registrarán las actividades 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.

- Incidentes de seguridad.

  Deben registrarse los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán para la mejora continua de la seguridad del sistema, y detección de vulnerabilidades.

  Se establecerá un sistema de detección y reacción frente a código dañino.

- Continuidad de la actividad.

  Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

- Mejora continua del proceso de seguridad.

  El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

- Cuerpo Normativo.

  Las directrices de seguridad de la información indicadas en el presente Anexo a la Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**, se desarrollarán en un conjunto de documentos entre los que destacan, Políticas, Normativas, Guías, Procedimientos e Instrucciones de Trabajo.

  La documentación sigue la siguiente estructura:

  - el presente documento del Anexo Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** del que emana el resto de documentos,
  - un documento de normativas que especifica los principios básicos y los requisitos mínimos de seguridad explicitados en el Esquema Nacional de Seguridad y enumera la relación de guías que es preciso desarrollar para lograr el cumplimiento de los citados principios básicos y requisitos mínimos

de seguridad,

- varios documentos guía donde se describe las actuaciones a desarrollar para implantar las medidas de seguridad enumeradas en el Esquema Nacional de Seguridad y
- varios documentos de procedimientos operativos de seguridad, registros, instrucciones de trabajo, manuales, etc., que se desarrollan como consecuencia de aplicar las guías.

8. Proceso de revisión

El Anexo Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de administración electrónica, a la evolución tecnológica y al desarrollo de la información.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comité de Seguridad revisará el presente texto, que se someterá, de haber modificaciones, a la aprobación del Comité de Seguridad del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**.

9. Terceros

Cuando el **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** utilice servicios de terceros o ceda información a terceros, se les hará participes de la Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** y del presente Anexo a la Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** 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 este texto.

Cuando algún aspecto de la Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** y del presente Anexo a la Política de Gestión del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA** 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.

Gerencia del **HOSPITAL UNIVERSITARIO INFANTA CRISTINA**.

06 de noviembre de 2025 - Versión: 03

Firmado digitalmente por: SANTANO MAGARIÑO ALMUDENA
Fecha: 2025.11.10 13:19