EUROPEAN UNION AGENCY
FOR CYBERSECURITY

DIRECTRICES SOBRE CONTRATACIÓN PARA LA CIBERSECURIDAD EN LOS HOSPITALES

Prácticas recomendadas para la seguridad de los servicios sanitarios

FEBRERO DE 2020

ACERCA DE ENISA

La misión de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) es lograr un elevado nivel común de ciberseguridad en toda la Unión, apoyando activamente a los Estados miembros y a las instituciones, órganos y agencias de la Unión en la mejora de la ciberseguridad. Contribuimos al desarrollo y la aplicación de políticas, apoyamos el desarrollo de capacidades y la preparación, facilitamos la cooperación operativa a escala de la Unión, mejoramos la fiabilidad de los productos, servicios y procesos de TIC mediante la aplicación de programas de certificación de la ciberseguridad, y posibilitamos el intercambio de conocimientos, la investigación, la innovación y la sensibilización, a la vez que desarrollamos las comunidades transfronterizas. Nuestro objetivo es reforzar la confianza en la economía conectada, impulsar la resiliencia y la confianza en la infraestructura y los servicios de la Unión y proteger digitalmente a nuestra sociedad. Puede encontrar más información sobre ENISA y su labor en www.enisa.europa.eu.

DATOS DE CONTACTO

Si desea ponerse en contacto con los autores, envíe un mensaje a eHealthSecurity@enisa.europa.eu.
Las consultas de los medios de comunicación acerca de este documento deben realizarse a través de press@enisa.europa.eu.

AUTORES

Dr. Athanasios Drougkas, Dimitra Liveri, Antigone Zisi, Pinelopi Kyranoudi

AGRADECIMIENTOS

Por proporcionar información valiosa que ayudó a dar forma al informe (en orden alfabético):

Tomáš Bezouška, Ministerio de Salud, República Checa

Konstantinos Chondropoulos, Administración del Tercer Distrito Sanitario de Macedonia, Grecia

Dimitrios Glynos, Census Labs, Grecia

Manuel Jimber del Río, Servicio Andaluz de Salud, España

Dr. Luis Martí-Bonmati, Hospital Universitari i Politècnic La Fe, España

Dr. Julio Mayol, Hospital Clínico San Carlos, España

Dr. Germán Seara, Hospital Clínico San Carlos, España

Elena Sini, Humanitas Research Hospital, Italia

Centro Criptológico Nacional, España

AVISO LEGAL

Las correspondientes fuentes de terceros se citan donde procede. ENISA no acepta responsabilidad alguna por el contenido de las fuentes externas, incluidos los sitios web externos a los que se hace referencia en esta publicación.

Esta publicación tiene un carácter meramente informativo. Debe ser accesible de forma gratuita. Ni ENISA ni ninguna persona que actúe en su nombre aceptan responsabilidad alguna en relación con el uso que pueda hacerse de la información incluida en la presente publicación.

AVISO DE DERECHOS DE AUTOR

ISBN 978-92-9204-312-4, DOI 10.2824/943961

ÍNDICE

RESUMEN

A medida que la ciberseguridad se convierte en una prioridad para los hospitales, es esencial que se integre de manera global en los diferentes procesos, componentes y fases que influyen en el ecosistema de las TIC de la asistencia sanitaria. La contratación es un proceso clave para configurar el entorno de las TIC de los hospitales modernos y, como tal, debe estar a la vanguardia para alcanzar los objetivos de ciberseguridad.

El presente informe tiene por objeto proporcionar a los responsables de la contratación de los hospitales y a los CISO/CIO un conjunto completo de herramientas y prácticas recomendadas que puedan adaptarse al proceso de contratación de los hospitales con el fin de garantizar el cumplimiento de los objetivos de ciberseguridad. En este contexto, en el informe se describen las prácticas recomendadas en tres fases distintas del ciclo de vida de la contratación: la **planificación**, el **aprovisionamiento** y la **gestión**. Las consideraciones relativas a la ciberseguridad son pertinentes para las tres fases, y en el presente informe se ofrece una guía fácil de utilizar para que los hospitales mejoren su proceso de contratación desde la perspectiva de la ciberseguridad.

El presente informe proporciona el contexto para abordar la ciberseguridad en la contratación definiendo sus tres fases e identificando 10 tipos de contratación (activos, productos, servicios, etc.) para los que son pertinentes las consideraciones relativas a la ciberseguridad; enumera las normas del sector con los aspectos de la ciberseguridad relevantes para estos tipos de contratación y destaca los principales problemas de ciberseguridad en cada caso. También se presenta un esquema de las amenazas y una lista de los principales riesgos asociados a la contratación. Toda esta información va acompañada de guías rápidas que proporcionan las claves para que los hospitales sepan utilizarla en su proceso de contratación.

El informe concluye con un amplio conjunto de prácticas recomendadas de ciberseguridad en la contratación. Estas prácticas recomendadas pueden ser prácticas generales aplicables a lo largo del ciclo de vida de la contratación, o pueden ser específicas de alguna de las fases. Todas las prácticas recomendadas están vinculadas a los tipos de contratación para los que son pertinentes y a las amenazas que pueden mitigar, lo que da lugar a un conjunto de prácticas fáciles de filtrar para los hospitales que desean centrarse en aspectos concretos. En general, se insta a los hospitales a adoptar estas prácticas recomendadas de ciberseguridad en la contratación:

- **Prácticas generales:**
  - Involucrar al departamento de informática en la contratación
  - Gestión de vulnerabilidades
  - Desarrollar una política de actualizaciones de *hardware* y *software*
  - Comunicación inalámbrica segura
  - Establecer políticas de pruebas
  - Establecer planes de continuidad de negocio
  - Tener en cuenta los aspectos de interoperabilidad
  - Permitir la auditoría y el registro
  - Usar la encriptación

- **Fase de planificación:**
  - Realizar una evaluación de riesgos
  - Prever las necesidades con antelación
  - Identificar las **amenazas**

- Segregar y segmentar la red
- Establecer **criterios de selección** para los proveedores
- Crear una licitación dedicada para la nube

- **Fase de aprovisionamiento**
  - Demandar certificación
  - Llevar a cabo una **EIPD**
  - Abordar los sistemas heredados
  - Proporcionar formación en materia de ciberseguridad
  - Desarrollar planes de respuesta a incidentes
  - Involucrar al proveedor en la gestión de incidentes
  - Organizar las operaciones de mantenimiento
  - Segurizar el acceso remoto
  - Demandar parcheado

- **Fase de gestión**
  - Concienciar sobre la ciberseguridad
  - Realizar un inventario de activos y la gestión de la configuración
  - Mecanismos de **control de acceso** específicos para productos sanitarios
  - Programar **pruebas de penetración** con frecuencia o después de un cambio en la arquitectura/sistema

1. INTRODUCCIÓN

La asistencia sanitaria está cada vez más conectada, ya que las empresas de tecnología médica fabrican actualmente más de 500 000 tipos diferentes de productos sanitarios; por ejemplo, los llamados *wearables* (dispositivos digitales vestibles), los dispositivos implantables y los dispositivos médicos estacionarios 1. Se prevé que el mercado del «Internet de las Cosas Médicas» crezca de 11 000 millones en 2017 a 40 000 millones en 2022 solo en Europa, mientras que el valor del mercado europeo de tecnología médica se estimaba en unos 115 000 millones en 20172. Al mismo tiempo, un estudio demostró que los hospitales estadounidenses tenían, en promedio, entre 10 y 15 dispositivos conectados por cama, lo que da una idea de cómo la proliferación de soluciones de tecnología médica ha cambiado por completo el panorama de las TIC en las organizaciones sanitarias de todo el mundo. Todos estos dispositivos los fabrican diferentes empresas, y todos deben comunicarse eficazmente entre sí para brindar atención al paciente. La creciente interconexión de los productos sanitarios y el uso de conexiones remotas para su mantenimiento; la necesidad de vigilar continuamente a los pacientes (incluso a los que no están ingresados en el hospital); el uso de teléfonos inteligentes para que pacientes y médicos accedan a la información sobre la salud; junto con la incapacidad de los departamentos informáticos (TI) para aplicar parches y la habitual falta de presupuesto para los servicios y soluciones de ciberseguridad hacen que el sector de la atención sanitaria sea especialmente vulnerable[3]. La ciberseguridad debe tenerse en cuenta en los primeros días de la compra de activos (infraestructura, programas informáticos, sistemas, dispositivos, etc.) para las instituciones sanitarias.

Durante el ataque WannaCry de 2017, un programa de secuestro de datos se propagó exponencialmente aprovechando una vulnerabilidad presente solo en el 5 % de los ordenadores del Sistema Nacional de Salud del Reino Unido (NHS), que todavía estaban funcionando con *software* anticuado y sin soporte.

1.1 OBJETIVOS

Este estudio se centra en una parte del amplio ecosistema sanitario: el hospital. Se considera que el hospital es un conjunto de activos (infraestructura, programas informáticos, sistemas, dispositivos, etc.), y que la ciberseguridad debe abordarse explícitamente en todos sus diferentes componentes. En general, el objetivo de este estudio es proporcionar a los profesionales de la salud en los hospitales directrices sobre cómo mejorar su proceso de contratación para cumplir los objetivos de ciberseguridad. Estas directrices abarcan múltiples temas, y van desde las prácticas organizativas recomendadas para las propias organizaciones sanitarias hasta qué información solicitar a los proveedores como «pruebas» de ciberseguridad a la hora de adquirir sistemas y contratar servicios.

1.2 ÁMBITO DE APLICACIÓN

Este estudio se centra en los hospitales: las organizaciones de atención sanitaria más complejas y críticas y los principales actores en el ámbito de la contratación. Los hospitales también se enfrentan a menudo a la falta de recursos, por lo que este informe pretende ser una guía para los profesionales de la salud. Muchas de las prácticas y recomendaciones serán útiles también para otras organizaciones sanitarias, ya que los procesos de contratación pueden ser muy similares. Las directrices de contratación propuestas en este informe hacen referencia a todo proceso de contratación de las organizaciones sanitarias que pueda repercutir en la ciberseguridad.

[1] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf
[2] https://www.medtecheurope.org/wp-content/uploads/2019/04/The-European-Medical-Technology-Industry-in-figures-2019-1.pdf
[3] Lynne Coventry and Dawn Branley, 'Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward', Maturitas 113 (julio de 2018): 48–52, https://doi.org/10.1016/j.maturitas.2018.04.008.

1.3 PÚBLICO OBJETIVO

Este informe está dirigido a los profesionales de la salud que ocupan puestos técnicos en los hospitales, en particular, a los cargos de nivel superior: CIO[4], CISO, CTO, equipos de TI y responsables de compras de las organizaciones de salud.

Este informe puede ser de interés para los fabricantes de productos sanitarios que son proveedores de hospitales; en este caso los productos pueden ser (entre otros) productos sanitarios, sistemas de información clínica, equipos de redes, servicios en la nube, etc. Cuando estos fabricantes ofrezcan servicios o productos, conocerán los requisitos de seguridad que el hospital espera que cumplan y podrán aportar pruebas para demostrarlo.

1.4 METODOLOGÍA

La información que se presenta en este informe es el resultado del análisis de los datos obtenidos a través de una serie de entrevistas. Las entrevistas se realizaron con expertos en la materia que trabajan en hospitales, encargados de formular políticas o reguladores (ministerios de salud), fabricantes de productos sanitarios y expertos en ciberseguridad que se centran en la atención sanitaria. El informe fue validado por los expertos que participaron en la encuesta/entrevistas, así como por el Grupo de Expertos en Seguridad de la Sanidad Electrónica de ENISA[5].

Esta metodología permitió a ENISA colaborar activamente con los interesados, además de:

- identificar los tipos de contratación y los activos correspondientes que sean pertinentes para los objetivos de ciberseguridad de los hospitales,
- identificar posibles amenazas, riesgos y desafíos relacionados con la contratación en organizaciones hospitalarias,
- enumerar las prácticas recomendadas relacionadas con la contratación de servicios de atención sanitaria a fin de cumplir los objetivos de ciberseguridad, y
- relacionar las prácticas recomendadas propuestas con los tipos de contratación para los que pueden utilizarse y las amenazas para las que son pertinentes.

1.5 CONTEXTO

1.5.1 Política europea

La legislación desempeña un papel importante en la definición de los requisitos de ciberseguridad que deben describirse en las especificaciones técnicas al obtener productos y servicios en un hospital. A continuación se presentan algunas de las normas más destacadas:

1.5.1.1 La Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (NISD)

La Directiva sobre la seguridad de las redes y de la información (NISD) 2016/1148/UE, que entró en vigor en mayo de 2018, tiene dos objetivos principales: la aplicación de unos requisitos mínimos de seguridad y el establecimiento de notificaciones de ciberseguridad tanto para los operadores de servicios esenciales como para los proveedores de servicios digitales. En la mayoría de los Estados miembros, los

La legislación europea introduce una obligación de notificación a los hospitales. En algunos casos, la notificación debe seguir la cadena de

[4] Responsable Principal de Información - CIO, Responsable General de Seguridad de la Información - CISO, Responsable General de Tecnología - CTO, etc.
[5] https://resilience.enisa.europa.eu/ehealth-security

proveedores de servicios de salud, es decir, los hospitales, se identifican como operadores de servicios esenciales. Por lo tanto, estas organizaciones deberán tener en cuenta la Directiva y la legislación nacional correspondiente al contratar un producto o servicio.

suministro. Esto debe preverse durante el proceso de contratación.

La Directiva va más allá de la aplicación de los requisitos de seguridad, ya que otorga a los organismos reguladores la facultad de auditar a los operadores de servicios esenciales para garantizar que el nivel de ciberseguridad de las organizaciones es aceptable y conforme a las disposiciones de la Directiva. En los ecosistemas hospitalarios, esto puede traducirse en requisitos de ciberseguridad para todos los productos, por lo que debería incluirse como una disposición en el proceso de contratación. Un dispositivo/sistema/servicio vulnerable puede tener una gran repercusión en la ciberseguridad del hospital como operador de un servicio esencial.

1.5.1.2 Reglamento sobre productos sanitarios (MDR)

El Reglamento sobre productos sanitarios (MDR) es un nuevo reglamento que incluye disposiciones específicas relacionadas con la seguridad informática (*hardware*, *software*, etc.) para todos los productos sanitarios. Los requisitos generales de seguridad y funcionamiento definidos en el MDR (productos sanitarios/SW) incluyen:

- repetibilidad, fiabilidad y funcionamiento según el uso previsto
- los principios del ciclo de vida del desarrollo, la gestión de riesgos, la verificación y la validación
- el uso de *software* en combinación con plataformas de computación móvil
- medidas de seguridad informática, incluida la protección contra el acceso no autorizado

El Grupo de Coordinación de Productos Sanitarios (MDCG) publicó en diciembre de 2019 la **Guía sobre Ciberseguridad para Productos Sanitarios** («Guidance on Cybersecurity for medical devices»)[6] con el fin de proporcionar a los fabricantes orientación sobre cómo cumplir todos los requisitos esenciales del MDR. Estos requisitos de ciberseguridad, enumerados en el Anexo I del Reglamento sobre productos sanitarios, se refieren a aspectos tanto previos como posteriores a la comercialización. El MDCG está compuesto por representantes de todos los Estados miembros y está presidido por un representante de la Comisión Europea. El MDCG asesora a la Comisión y ayuda a ésta y a los Estados miembros a garantizar una aplicación armonizada de los reglamentos sobre productos sanitarios.

1.5.1.3 Reglamento General de Protección de Datos (RGPD)

El Reglamento General de Protección de Datos (GDPR)[7] entró en vigor el 25 de mayo de 2018. Establece las normas para el tratamiento y la libre circulación de los datos personales, y se aplica a todos los ámbitos de los sectores público y privado; sin embargo, se definen algunas excepciones específicas para los datos relativos a la salud, con el fin de proteger los derechos de los interesados y la confidencialidad de sus datos personales sobre la salud y, al mismo tiempo, preservar los beneficios del tratamiento de datos para la investigación y la salud pública.

EL RGPD trata los datos relacionados con la salud como una «categoría especial» de datos personales que se consideran sensibles por naturaleza, e impone un nivel de

[6] https://ec.europa.eu/docsroom/documents/38941
[7] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

protección más elevado para su procesamiento. Las organizaciones que procesan datos sobre la salud tienen las siguientes obligaciones (entre otras):

- aplicar las medidas técnicas y organizativas adecuadas para garantizar la seguridad de los sistemas de tratamiento, los servicios y los datos personales,
- realizar una evaluación de Impacto relativa a la Protección de Datos, y
- informar de las violaciones de los datos que puedan suponer un riesgo para los derechos y libertades de las personas en un plazo de 72 horas después de haber tenido conocimiento de ellas.

En el párrafo 12 del artículo 4 del RGPD se define la «violación de los datos personales» como una infracción de seguridad que provoca la destrucción, la pérdida, la alteración o la divulgación no autorizada de los datos personales transmitidos, almacenados o procesados, o bien el acceso no autorizado a los mismos; hay que señalar que si un incidente de violación de datos afecta también a la continuidad de los servicios de salud, debe notificarse de conformidad con la Directiva SRI.

1.5.2 Política internacional

1.5.2.1 Ley de Transferibilidad y Responsabilidad del Seguro Sanitario de 1996 (HIPAA)[8]

Esta ley requirió que el Secretario del Departamento de Salud y Servicios Humanos de los Estados Unidos (HHS) desarrollara normas que protegieran la privacidad y la seguridad de cierta información sobre salud. Las Normas de Seguridad para la Protección de la Información Electrónica Protegida sobre la Salud (Security Rule) establecen un conjunto nacional de normas de seguridad para la protección de determinada información sobre la salud que se conserva o transfiere en formato electrónico. La «Security Rule» pone en práctica las protecciones que contiene la «Privacy Rule» abordando las salvaguardias técnicas y no técnicas que las organizaciones denominadas «entidades cubiertas» deben establecer para asegurar la «información médica electrónica protegida» (e-PHI) de los individuos.

1.5.2.2 Guía de la FDA sobre ciberseguridad[9]

Esta guía ha sido elaborada por la FDA para ayudar a la industria a identificar las cuestiones relacionadas con la ciberseguridad que los fabricantes deben abordar en el diseño y el desarrollo de sus productos sanitarios, así como en la preparación de las presentaciones previas a la comercialización de esos productos.

Si un fabricante tiene como objetivo los mercados internos, el producto debe cumplir tanto con la legislación europea como con la internacional.

1.6 ESTRUCTURA DEL INFORME

El estudio está estructurado de la siguiente manera:

Sección 2: Definición del contexto en torno a los Procesos de Contratación de Servicios de Salud y sus variantes con una visión general de los conceptos tratados y los retos de seguridad relacionados.

[8] https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm
[9] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissionsmanagement-cybersecurity-medical-devices

Sección 3: Análisis de amenazas y riesgos que contiene un esquema de las amenazas y ejemplos de casos de ataques al sector de la salud.

Sección 4: Descripción de las prácticas recomendadas de contratación en función de las amenazas y tipos de contratación.

Anexo A: Lista de las normas relevantes de la industria

Cada sección del informe va acompañada de una descripción de la forma en que los hospitales pueden utilizar la información proporcionada en la sección para abordar la ciberseguridad en sus procesos de contratación. Las descripciones pertinentes se proporcionan en cuadros de texto como este.

2. LA CONTRATACIÓN EN LOS HOSPITALES

2.1 PROCESO DE CONTRATACIÓN

Comprender dónde encaja la ciberseguridad en las diferentes fases del ciclo de vida de las contrataciones y adquisiciones. En esta sección se indican las consideraciones de ciberseguridad que deben tenerse en cuenta al planificar la contratación, en el proceso de aprovisionamiento y en las fases de posventa..

Dado que el ecosistema hospitalario está compuesto por una serie de componentes informáticos, la ciberseguridad debe examinarse por separado en todos estos componentes. La ciberseguridad debería formar parte de todas las diferentes etapas del proceso de contratación. En esta sección se presentan las etapas comunes del proceso de contratación y adquisición de productos y servicios (incluidos los productos sanitarios, los sistemas de información y las infraestructuras), junto con algunas consideraciones relativas a cada etapa del proceso.

Figura 1: Ciclo de vida del proceso de contratación para los hospitales

- Fase de planificación: Inicialmente, el hospital analiza sus necesidades y anota los requisitos de sus departamentos internos. Por ejemplo, en el caso de contratar un nuevo servicio en la nube, el CTO debe identificar las necesidades y comprender qué tipo de utilidad ofrecerá este servicio.
- Fase de aprovisionamiento: Posteriormente, los requisitos se traducen en especificaciones técnicas y, en colaboración con la oficina de contratación y compras, se inicia el proceso de aprovisionamiento (por ejemplo, se publica una licitación). El hospital recibe las ofertas, y el comité (incluidos el CTO/ CISO y miembros del equipo de TI) las evalúa y selecciona los productos más apropiados. Se llevan a cabo negociaciones con el contratista y se adjudica el contrato.
- Fase de gestión: Por último, el contrato (gestión y supervisión) se asigna al propietario del negocio dentro del hospital. El gestor asignado es responsable de finalizer la licitación y de recibir cualquier información de los usuarios sobre el funcionamiento real del equipo/sistema/servicio.

A lo largo de las diferentes fases del ciclo de vida de la contratación, el hospital debe considerar la ciberseguridad un criterio importante a la hora de contratar o adquirir el producto/servicio. Estas son algunas de las posibles consideraciones:

- Fase de planificación: Se evalúan los riesgos de ciberseguridad asociados a una nueva adquisición/contratación y se definen los requisitos de ciberseguridad específicos para la misma.
- Fase de aprovisionamiento: Los requisitos de ciberseguridad se traducen en especificaciones técnicas y características de seguridad de los productos, y las responsabilidades de los proveedores en relación con los aspectos de la ciberseguridad se aclaran e incluyen en los contratos.
- Fase de gestión: Determinados aspectos de la ciberseguridad como los incidentes y las nuevas vulnerabilidades se vigilan continuamente y se aplican medidas correctivas (como los parches) para mantener un alto nivel de seguridad. Del mismo modo, al final del ciclo de vida de los productos, se requiere un borrado seguro por razones de privacidad, ya que los dispositivos tienen almacenada la información de los pacientes.

2.2 TIPOS DE CONTRATACIÓN/ADQUISICIÓN

Las consideraciones relativas a la ciberseguridad son pertinentes para diferentes tipos de adquisiciones/contrataciones. Consulte la siguiente lista para determinar si el tipo específico de contratación/adquisición que está planificando o gestionando podría tener implicaciones en materia de ciberseguridad que deban abordarse.

Como se ha mencionado a lo largo del presente documento, el hospital es un ecosistema compuesto por varios componentes, y la ciberseguridad debería ser una prioridad para todos ellos. En este capítulo hemos creado un esquema para clasificar los tipos de contrataciones/adquisiciones e investigar cómo se aborda la ciberseguridad en cada uno de ellos.

Figura 2: Tipos de contratación/adquisición (esquema de activos)

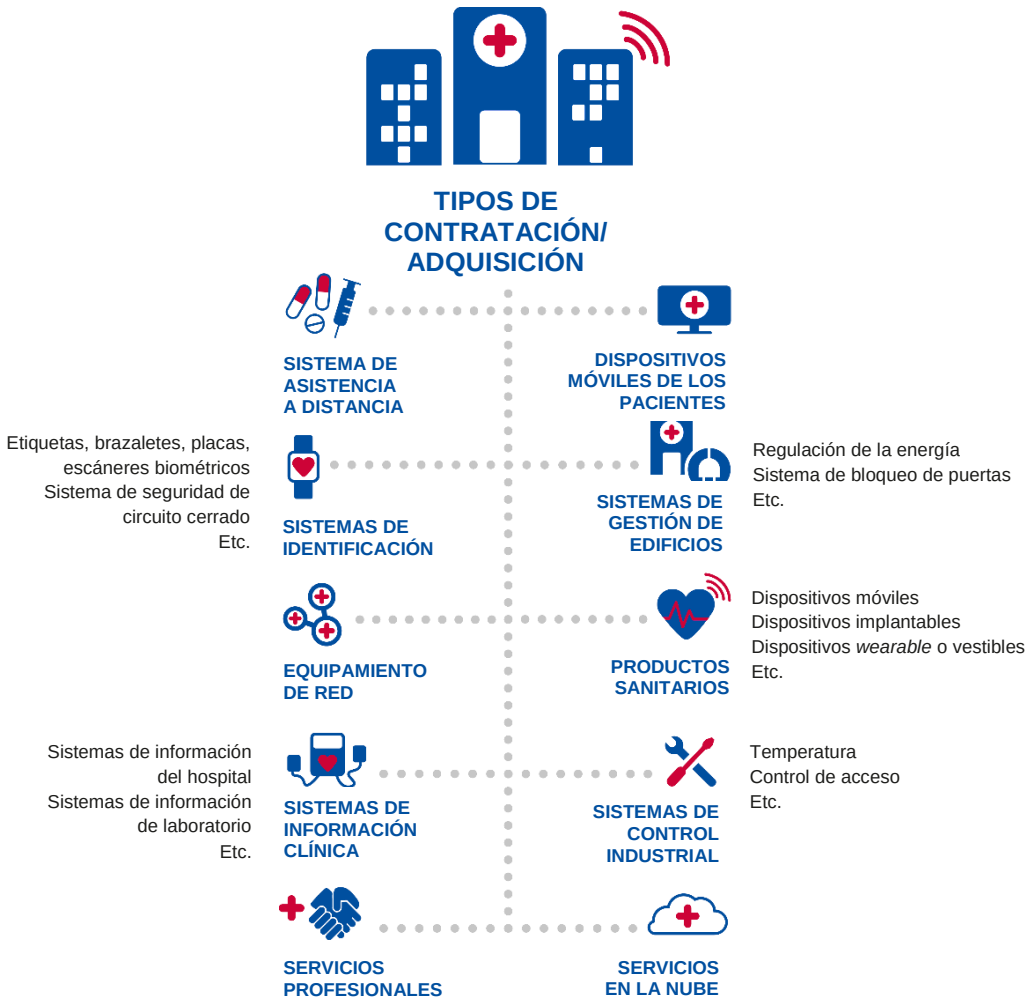


Tabla **1:** Tipos de contratación/adquisición

Tipo de contratación/adquisición	Descripción
Sistemas de información clínica	Incluye la adquisición de cualquier tipo de *software* orientado a la atención médica: - Sistemas de Información Hospitalaria y Registro Médico Electrónico (HIS-EMR), - Sistema de Información de Laboratorio (LIS), - Sistema de Información de Radiología, Sistema de Comunicación y Archivado de Imágenes (RIS- PACS), - Farmacia, - Bases de datos de fármacos - Administración del cuidado - *Software* de dietas, - Sistema informatizado de entrada de órdenes médicas (CPOE), - Análisis de grandes volúmenes de datos, etc. El sistema de información clínica **debe encontrarse** en el edificio médico o en un centro de datos bajo el control total del departamento de informática del centro médico. Los sistemas basados en la nube tienen su propia categoría.
Productos sanitarios	Cualquier componente de *hardware* dedicado al tratamiento, control o diagnóstico de enfermedades: equipos de radiología, radioterapia, medicina nuclear, equipos de quirófano o de cuidados intensivos, robots para cirugía, equipos electromédicos, bombas de infusión, dispositivos de espirometría, láseres médicos, equipos de endoscopia, etc. Incluye dispositivos implantables en el paciente[10] (*holters*, marcapasos, bombas de insulina, implantes cocleares, estimuladores cerebrales, desfibriladores cardíacos, estimuladores gástricos, etc.[11]) o vestibles/*wearable* (*holters* externos de electrocardiograma o de presión, monitores de glucosa, etc.), siempre que se comuniquen por medios electrónicos con los sistemas informáticos del hospital.
Equipamiento de red	Líneas de red (coaxiales, ópticas), pasarelas, *routers*, conmutadores, cortafuegos, VPN, IPS, IDS, etc.
Sistemas de asistencia a distancia	Instalaciones o dispositivos para proporcionar asistencia fuera del entorno hospitalario, especialmente lo que hoy en día se denomina «servicios de atención domiciliaria desde el hospital». Puede incluir los dispositivos de comunicación a distancia «pulsar para obtener ayuda» utilizados para la asistencia a la población de edad avanzada que vive sola en casa.
Dispositivos móviles de los pacientes	Todos los programas informáticos que proporcionan asistencia sanitaria o recopilan datos médicos y no están directamente conectados a la red del hospital; por ejemplo: aplicaciones de telemedicina. No incluye los los dispositivos 'wearables' ya que están incluidos en una categoría aparte. Los dispositivos cliente móviles necesitan un protocolo definido para conectarse a la red del hospital.
Sistemas de identificación	Sistemas para identificar de forma unívoca a los pacientes o al personal médico (escáneres biométricos, lectores de tarjetas, etc.) y garantizar la identificación y/o la autorización para acceder a los sistemas informáticos.
Sistemas de gestión de edificios	Un sistema de BMS o de gestión de edificios permite el control centralizado de los inmuebles sanitarios. Incluye las líneas de electricidad, agua, gas, gases medicinales, mobiliario, etc., excepto las líneas de red, que se incluyen en la categoría de «equipamiento de red». Los sistemas de gestión de edificios (BMS) se incluyen en la siguiente categoría de contratación, ya que son, principalmente, sistemas de control.

[10] Las prótesis de rodilla o cadera o las lentes intraoculares también son ejemplos de «productos sanitarios», pero no se incluyen en este estudio. Para una definición detallada de «producto sanitario», véase el Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo de 5 de abril de 2017 sobre los productos sanitarios (2017), http://data.europa.eu/eli/reg/2017/745/oj.

[11] Aliya Tabasum et al., 'Cybersecurity Issues in Implanted Medical Devices', in 2018 International Conference on Computer and Applications (ICCA) (2018 International Conference on Computer and Applications (ICCA), Beirut: IEEE, 2018), 1–9, https://doi.org/10.1109/COMAPP.2018.8460454.

Sistemas de control industrial	Sistemas que controlan todos los aspectos físicos de los centros, como sistemas de regulación de energía, sistemas de bloqueo de puertas, sistemas de seguridad de circuito cerrado, sistemas de HVAC[12], sistemas de alarma, agua, calefacción, unidades de energía auxiliar, acceso de seguridad, ascensores, extinción de incendios, etc. Hoy en día, el control de todos estos sistemas se gestiona a través de programas informáticos: Sistemas de gestión de edificios (BMS). Los BMS pueden adquirirse por separado o como parte de un proyecto de renovación de un edificio,
Servicios profesionales	Todo tipo de servicios, subcontratados o no, prestados por profesionales o empresas: servicios médicos, de transporte, de contabilidad, de ingeniería, de informática, jurídicos, de mantenimiento, de limpieza, de catering, etc.
Servicios en la nube	Cualquier sistema de información clínica o de otro tipo que no esté ubicado en el edificio médico o en un centro de datos bajo el control total del departamento de informática del centro médico.

2.3 NORMAS Y DIRECTRICES DE LA INDUSTRIA

Ya existe una serie de reglamentos, normas internacionales y prácticas recomendadas sobre sistemas, productos y servicios de atención sanitaria que incluyen criterios básicos de ciberseguridad. Consulte esta sección para ver si existe una norma industrial relacionada con el tipo específico de contratación/adquisición que está planificando o gestionando.

Existen varias normas internacionales y prácticas recomendadas en el mercado relacionadas con la contratación y adquisición de productos y servicios sanitarios. En la siguiente sección se enumeran las normas y protocolos existentes que guardan relación directa *o indirectamente* con la contratación.

Un estándar de la industria muy relevante para la ciberseguridad y la contratación es el ***Manufacturer Disclosure Statement for Medical Device Security*** (**MDS2**) («Declaración de divulgación del fabricante para la seguridad de los productos sanitarios»). El formulario MDS2 proporciona a los fabricantes de productos sanitarios un medio para revelar las características relacionadas con la seguridad de sus productos. El formulario MDS2 incluye un conjunto de preguntas sobre la seguridad de los productos sanitarios, y permite la comparación de las características de seguridad entre diferentes productos y fabricantes.

A día de hoy, la ISO está desarrollando más de 25 nuevas normas para la informática sanitaria. Estas son algunas de las más interesantes:

- **ISO/DTR 22696** Informática sanitaria - Guía para la identificación y autentificación de dispositivos personales de salud conectables,
- **ISO/DTR 21332** Informática sanitaria - Consideraciones de la computación en la nube para la seguridad y privacidad de los sistemas de información sanitaria,
- **ISO/WD 13131** Informática sanitaria - Servicios de telesalud - Directrices de planificación de la calidad,
- **ISO/AWI 22697** Informática sanitaria - Aplicación de la gestión de la privacidad a la información personal sobre la salud

Además, existe una serie de directrices, normas y prácticas recomendadas a nivel de la UE y de los Estados miembros. En la figura 3 se muestra un breve resumen del panorama normativo.

[12] Sistemas de calefacción, ventilación y aire acondicionado

Figura 3: Reglamentos, normas internacionales y prácticas recomendadas en materia de sistemas de atención sanitaria

A continuación se enumeran las normas internacionales más relevantes que tratan de normalizar los requisitos mínimos para el diseño seguro, la fabricación y la gestión de riesgos de diversos tipos de contratación/adquisición. Se presentan con más detalle en el Anexo A.

Tabla 2: Esquema de las normas por tipo de contratación/adquisición

Normas	Sistemas de información clínica	Productos sanitarios	Equipamiento de red	Sistemas de asistencia a distancia	Dispositivos cliente móviles	Sistemas de identificación	Sistemas de gestión de edificios	Sistemas de control industrial	Servicios profesionales	Servicios en la nube
ISO 80001			X	X	X	X	X		X	
ISO 13972			X	X	X	X	X		X	
ISO 13485		X	X	X	X	X	X		X	
ISO 14971		X	X	X	X	X	X		X	
ISO / IEC 20000	X		X	X	X	X	X		X	
ISO 27000	X		X	X	X	X	X		X	
ISO 27799	X		X	X	X	X	X		X	
ISO 22857	X		X	X	X	X	X		X	
ISO 27019			X	X	X	X	X	X	X	
ISO 27017										X
IEC 62304	X		X	X	X	X	X		X	
IEC 60364-7-710			X	X	X	X	X	X	X	
ISA/IEC 62443			X	X	X	X	X	X	X	
DICOM			X	X	X	X	X		X	
HL7			X	X	X	X	X		X	
MDS2		X		X	X					
NIST-SP 800-66	X		X	X	X	X	X		X	
NIST CSF	X		X	X	X	X	X		X	
HTMs			X	X	X	X	X	X	X	

2.4 DESAFÍOS EN MATERIA DE CIBERSEGURIDAD

Muchos sistemas, productos o servicios contratados o adquiridos por los hospitales introducen o se caracterizan por presentar importantes problemas de ciberseguridad. Consulte esta sección para obtener información sobre los principales desafíos e identifique cuáles son los más importantes según el tipo específico de contratación/adquisición que está planificando o gestionando. Trabaje conjuntamente con sus departamentos de informática, seguridad o riesgos para identificar las mejores formas de abordar cada desafío.

Según lo que averiguamos en las entrevistas con las partes interesadas, el tipo de contratación/adquisición más difícil fue la de «productos sanitarios» (100 % de las respuestas), seguida de la de «sistemas de control industrial» y la de «sistemas de información clínica». Como señaló un entrevistado, las amenazas que plantean más problemas suelen estar asociadas a las contrataciones/adquisiciones en las que el departamento de informática no suele participar.

Otros desafíos interesantes no incluidos en la lista pero señalados por los interesados fueron los «servicios de mantenimiento» y los desafíos relacionados con el *software* libre cedido por algunos proveedores médicos.

Sobre la base de la información obtenida en las entrevistas con los interesados, se identificaron varios desafíos clave relacionados con las contrataciones y adquisiciones en las organizaciones de atención sanitaria. Estos desafíos se han agrupado sobre la base de los tipos de contratación previamente definidos.

Sistemas de información clínica

- **Vulnerabilidad de los componentes**: Los sistemas de información de las organizaciones sanitarias suelen constar de diferentes componentes de distintos proveedores. Además, estos sistemas interactúan y comparten archivos y datos, por lo que una vulnerabilidad de un componente puede afectar a otros.
- **Creciente interoperabilidad**: La especialización del *software* y las nuevas tendencias como los grandes volúmenes de datos (*big data*) y los sistemas de análisis crean la necesidad de compartir los datos de los pacientes entre los diferentes sistemas. Este proceso debe realizarse de forma segura, utilizando protocolos adecuados y transmitiendo solo los datos necesarios al receptor adecuado.
- **Funcionamiento continuo a pleno rendimiento**: Las organizaciones de atención sanitaria suelen funcionar 24/7, y los recursos son escasos, por lo que interrumpir una modalidad o incluso los procesos de un ordenador puede repercutir gravemente sobre el servicio. Cuando se detecta un incidente, a veces es muy difícil aislar el equipo y, por lo tanto, esto facilita la propagación. En esos casos, durante el proceso de contratación se debería exigir a los proveedores planes de contingencia y redundancia.

Productos sanitarios

- **Procesos de fabricación**: Aunque este tema lo han controlado tradicionalmente de forma estricta los proveedores de productos sanitarios, en realidad es muy común que haya terceros proveedores de programas informáticos y componentes electrónicos en su cadena de suministro. Esto introduce nuevos desafíos para los fabricantes: no solo tienen que comprobar los materiales, la durabilidad o la esterilización, sino que ahora también tienen que probar el *software* y los componentes electrónicos para asegurarse de que son resistentes y seguros antes de comercializar el producto.

- **Equipamiento alquilado**: Especialmente cuando se plantea el uso de equipamiento médico caro, es común alquilar dispositivos que tal vez se hayan utilizado previamente en otras organizaciones de salud, por lo que a menudo vienen con una configuración predeterminada. Al contratar servicios de alquiler se deben establecer medidas para evitar los riesgos de esta práctica.
- **Dispositivos obsoletos**: Los equipos médicos suelen ser muy caros; se prevé que estos dispositivos estén en servicio durante muchos años. Debido a este largo ciclo de vida, los compradores a veces pueden tener dificultades para obtener apoyo de mantenimiento de los fabricantes. Por esta razón, las vulnerabilidades no siempre se pueden corregir, y por lo tanto pueden facilitar los ciberataques.
- **Funcionalidades ocultas**: El equipamiento médico siempre es complejo de manejar y configurar. Ni los médicos ni el departamento de informática suelen estar formados para manejar los nuevos equipos. Lo habitual es dejarlos con la configuración estándar[13], por lo que evitar las contraseñas predeterminadas y asegurarse de que las funcionalidades desconocidas no se activen es otro reto en estos entornos. Los dispositivos pueden tener aplicados procedimientos operativos (por ejemplo, solicitudes de fecha/hora, comunicación de datos técnicos y de mantenimiento al fabricante, solicitudes de mantenimiento, actualizaciones automáticas, etc.) desconocidos para el comprador que podrían activar alertas de seguridad en el sistema IPS del hospital. Esa interconectividad ofrece un abanico de oportunidades para que las personas malintencionadas accedan a la infraestructura informática de la organización.
- **Actualizaciones / gestión del ciclo de vida**: Los dispositivos más recientes suelen ofrecer la opción de control remoto. Esto permite a los proveedores reducir los costes de mantenimiento y realizar otras operaciones. Pero esta opción, si se ignora o se descuida, puede suponer una puerta trasera en la organización, ya que a menudo se establece sin conocimiento del departamento de informática.

Sistemas de gestión de edificios - Sistemas de control industrial

- **Soluciones híbridas TI/TO**: Las soluciones híbridas hacen posible la convergencia entre el mundo digital y el mundo físico; van desde los edificios inteligentes hasta los gemelos digitales, e incluyen por ejemplo sistemas de localización en tiempo real de pacientes y activos valiosos, lavanderías de hospitales, sistemas de farmacia o módulos de cirugía. Por supuesto, esto abre un nuevo escenario para las amenazas y riesgos a los que las organizaciones de salud se deben enfrentar.

Redes

- **Protocolos desprotegidos**: Al igual que en otros sectores, los protocolos se han diseñado teniendo en cuenta los casos de uso, pero no los casos de abuso. Por otra parte, los datos sobre la salud son muy persistentes: si se filtran, podría tener un impacto permanente en los pacientes. Es crucial mejorar la seguridad de los protocolos utilizados para intercambiar los datos de los pacientes.

Servicios profesionales

- **Factores humanos**: La concienciación de los usuarios permite a las organizaciones sanitarias mejorar su nivel de protección casi exponencialmente. No obstante, en el ámbito de la atención sanitaria, la presión y la necesidad de

[13] Clemens Scott Kruse et al., 'Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends', *Technology and Health Care* 25, no. 1 (21 de febrero de 2017): 1–10, https://doi.org/10.3233/THC-161263.

prestar atención sanitaria urgente a veces hace que los usuarios no sigan del todo las prácticas recomendadas en materia de ciberseguridad[14].

- **Seguridad del paciente**: En las organizaciones sanitarias se dan dos circunstancias específicas que hacen que los sistemas de información sean diferentes del resto: (1) Los datos de los pacientes son permanentes, no se pueden cambiar si se vulnera la privacidad (como se podría hacer con el número de la tarjeta de crédito, por ejemplo); y (2) los ciberataques pueden volverse físicos y costar vidas humanas. Los médicos se esfuerzan mucho para mejorar la seguridad de los pacientes, y los productos sanitarios y los servicios informáticos deben considerarse otra capa en lo que respecta a la seguridad del paciente[15]. Esta debería ser la clave de los requisitos de ciberseguridad específicos de la fase de contratación/adquisición.

[14] Ross Koppel et al., 'Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?', *Studies in Health Technology and Informatics* 208 (2015): 215–20.
[15] ECRI Institute, '2019 Top 10 Health Technology Hazards Executive Brief' (ECRI Institute, 2018).

3. LA CIBERSEGURIDAD EN LA CONTRATACIÓN

3.1 ESQUEMA DE LAS AMENAZAS

Los diferentes tipos de contratación están asociados a diversas amenazas para las TIC de un hospital. Consulte el esquema de amenazas de esta sección junto con su departamento informático, de seguridad o riesgos para identificar qué amenazas tienen más probabilidad de afectar a su organización. Esta actividad debería formar parte de las tareas informáticas del hospital independientemente de las posibilidades de contratación. A continuación, puede dar prioridad a las prácticas recomendadas de contratación que figuran en el capítulo 4 y que pueden mitigar las amenazas identificadas.

La fuente de las amenazas es el otro factor de riesgo que debe tenerse en cuenta al analizar los riesgos. Una fuente de amenazas se caracteriza por: (i) la intención y el método destinados al aprovechamiento de una vulnerabilidad; o (ii) una situación y un método que puedan utilizar accidentalmente una vulnerabilidad[16]. Algunos ejemplos de fuentes de amenaza son: una persona, una organización, un cliente, un hacker activista, un usuario, un usuario/administrador con privilegios de acceso, el fallo de un dispositivo de almacenamiento, el fallo de un control de temperatura, el fallo de un sistema operativo, un incendio. Tenga en cuenta que la lista de fuentes de amenazas es bastante amplia. El apéndice D de la publicación especial 800-30 del NIST que hemos mencionado anteriormente, la «Guía para la realización de evaluaciones de riesgos», contiene una tabla (D-2) con un útil esquema de las fuentes de amenazas.

Sobre la base de los últimos informes de ENISA sobre «Smart Hospitals»/hospitales inteligentes (2016)[17] y el informe sobre el panorama de las amenazas de 2018[18], este estudio analiza las principales amenazas cibernéticas con un enfoque específico en la atención sanitaria (por ejemplo, el hackeo de equipos médicos y las amenazas a las que estos están expuestos).

[16] Joint Task Force Transformation Initiative, 'Guide for Conducting Risk Assessments' (Gaithersburg, MD: National Institute of Standards and Technology, 2012), https://doi.org/10.6028/NIST.SP.800-30r1.
[17] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals
[18] European Union and Agency for Network and Information Security, ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends., 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport.

Figura 4: Panorama general de las amenazas para la asistencia sanitaria

El esquema de las amenazas propuesto se compone de cinco grupos que se describen con más detalle a continuación:

3.1.1 Fenómenos naturales

Amenaza	Descripción
Fenómenos naturales	Los incendios, las inundaciones o los terremotos son amenazas poco frecuentes pero posibles para la infraestructura y el equipamiento en general (dispositivos, componentes de la red, etc.). Habitualmente, las máquinas de tomografía computarizada, los equipos de resonancia magnética, los equipos de radioterapia y otros dispositivos muy costosos suelen instalarse en la planta baja o en el sótano de los hospitales (ya sea por la normativa vigente o simplemente por su peso y dimensiones), y se ven especialmente afectados por este tipo de fenómenos. Cabe señalar que los fallos a causa de inundaciones o incendios, como una rotura de tuberías que inunde el sótano o la habitación de un paciente, pueden tener una repercusión diferente a la de un desastre debido a fenómenos naturales (incendio forestal, tormenta, tsunami, etc.), y podrían acabar afectando a todo el hospital y su entorno o a sus proveedores.

3.1.2 Fallo en la cadena de suministro

Amenaza	Descripción
Fallo del proveedor de servicios en la nube	No todos los servicios están alojados en los servidores de los hospitales. La contabilidad, la gestión laboral y el control de inventario pueden subcontratarse y depender de servicios de terceros en la nube. Casi todos los dispositivos médicos personales de IoT funcionan en la nube. De hecho, algunos hospitales, especialmente los regionales o los pequeños centros asociados, pueden tener todo su sistema de registro electrónico de expedientes médicos ubicado en otro sitio. Estos servicios, si no están adecuadamente preparados para trabajar sin conexión, pueden causar graves trastornos en la prestación de servicios médicos.
Fallo del proveedor de la red	Un fallo en la red puede tener efectos devastadores. La mayoría de los principales centros hospitalarios forman un eje entre el edificio principal y sus centros asociados, en su mayoría radiológicos o centros de salud y ambulatorios. La redundancia y el diseño de la topología son cruciales para mitigar este tipo de amenaza.
Corte de electricidad	Un corte de electricidad puede tener importantes repercusiones dependiendo del equipo afectado. Las unidades de cuidados intensivos, las salas de operaciones, los servidores y los clientes suelen estar protegidos por fuentes de alimentación ininterrumpida o baterías, pero otros equipos como las máquinas de resonancia magnética o de tomografía computarizada pueden verse más afectados.
Fallo del fabricante del dispositivo médico / ausencia de responsabilidad	Todos los dispositivos médicos pueden tener errores de diseño en sus sistemas. Estos errores latentes pueden dar la cara en determinadas circunstancias durante el uso normal del dispositivo. La mayoría de las veces, estos errores son conocidos y no pueden mitigarse porque el dispositivo no permite actualizaciones. Si los empresas que fabrican estos equipos son adquiridas por empresas más grandes o cierran puede haber problemas con las actualizaciones o reparaciones del dispositivo. Además, la información de seguridad compartida con terceros puede verse comprometida.

3.1.3 Errores humanos

Amenaza	Descripción
Error de configuración del sistema médico	No cambiar las contraseñas predeterminadas de fábrica es uno de los errores más comunes que da a los atacantes acceso a los dispositivos una vez que han obtenido acceso a la red. Otros errores de este tipo pueden ser, por ejemplo, configurar nuestro dispositivo para permitir conexiones entrantes desde cualquier dirección o comunicarse usando protocolos no encriptados.
Falta de registros de auditoría	Los registros son una parte crucial de la estrategia «asegurar-probar-analizar-mejorar». Si damos por hecho que tarde o temprano nuestro sistema se verá comprometido, los registros son una de las herramientas más útiles que podemos usar para rastrear cómo los atacantes obtuvieron acceso a nuestro sistema. También podemos evaluar cuánta información ha estado en peligro. Mantener los registros seguros es una de las tareas más importantes en relación con la seguridad, aunque su ausencia no compromete la seguridad ya aplicada. En algunas circunstancias, los registros pueden ser obligatorios por ley para el funcionamiento normal del sistema (por ejemplo, el acceso al historial médico)
Control de acceso no autorizado / falta de procesos	Debido a la diversidad de profesionales que trabajan en los hospitales (personal médico, de enfermería, administración) se deben establecer procedimientos de control de acceso. Dado que la prioridad de todo el personal sanitario es la atención a los pacientes, a menudo se dan soluciones provisionales cuando se trata de controlar el acceso (incluidos todos los tipos de control de acceso, desde los edificios hasta los sistemas y las cuentas). Esto plantea grandes amenazas para el sistema interconectado del hospital.
Incumplimiento (BYOD)	Los empleados de hoy en día quieren tener la libertad de trabajar desde cualquier lugar y cualquier dispositivo a cualquier hora del día. Estas personas utilizan cada vez más sus dispositivos móviles personales para realizar tareas del trabajo. Desde una perspectiva empresarial, habilitar BYOD es una estrategia útil[19]. Sin embargo, *bring-your-own-device*/BYOD («trae tu propio dispositivo») también puede suponer un riesgo considerable para las organizaciones. El departamento informático recibe una gran presión para encontrar una manera de habilitar de forma segura la estrategia BYOD. De lo contrario, se pueden producir brotes de *malware*, incumplimiento de los requisitos normativos y exposición corporativa a raíz del robo de dispositivos personales.
Error del personal médico / del paciente	Siempre existe la posibilidad de que se produzca un error humano al introducir los datos por cualquiera de las dos partes, en particular al introducir el número del historial médico. A veces, dos pacientes pueden tener nombres idénticos y la información clínica de uno de ellos puede introducirse por error en la del otro. Esto es de vital importancia cuando la información proporcionada da lugar a decisiones clínicas que pueden afectar a la salud del paciente: por ejemplo, un paciente con el mismo nombre que otro podría ser diagnosticado erróneamente de cáncer. En el peor de los casos, el paciente podría recibir una cirugía que no necesita (amputaciones) o radio/quimioterapia. Por el contrario, un paciente con cáncer podría tardar demasiado en recibir su tratamiento por un informe de falsa normalidad. Aunque la repercusión no es a gran escala porque solo afecta a uno o dos pacientes, el impacto global en la reputación de la empresa u organización sanitaria puede ser muy alto.

[19] BYOD and GDPR: Managing the compliance conundrum. En PrivSec Report, 11 de enero de 2019.

3.1.4 Acciones malintencionadas

Amenaza	Descripción
***Malware*:** - **Virus** - **Programas de secuestro (*ransomware*)** - **BYOD**	En las organizaciones sanitarias, los sistemas informáticos están muy interconectados y son difíciles de aislar sin generar una interrupción del servicio, lo que propicia el *malware*. Las empresas con un gran número de dispositivos pueden tener dificultades para actualizar sus licencias debido a los elevados costes. El *adware* es una de las formas más fáciles de distribuir *malware* y la que los usuarios ignoran con más frecuencia[20]. El *ransomware* es quizás la amenaza más conocida por las organizaciones sanitarias, debido principalmente al caso WannaCry. El *ransomware* normalmente realiza ataques indiscriminados de bajo coste. Es muy fácil infectar la infraestructura sanitaria debido a dos factores; (i) no es fácil mantener actualizada la infraestructura de *software* porque es muy difícil conseguir encontrar el intervalo de tiempo perfecto para realizar tareas de mantenimiento que supongan una interrupción del servicio, (ii) las máquinas que ejecutan *software* heredado que solo funciona en un sistema operativo específico o con una versión determinada de ciertos controladores son un blanco fácil para estos ataques. Muchos de estos dispositivos heredados que no pueden actualizarse actúan como reservorios para el *malware*, lo que contribuye a su propagación a través de la red. Las empresas que permiten a los usuarios utilizar sus propios dispositivos (BYOD) sin políticas apropiadas están expuestas a riesgos adicionales.
Hackeo*:** ***Cryptojacking* / *Medjacking	El equipamiento médico requiere normalmente comunicaciones en tiempo real, y los médicos necesitan también una respuesta rápida del sistema cuando buscan datos de los pacientes o información de las pruebas. Dedicar tiempo de procesamiento o la capacidad de comunicación a la minería de criptomonedas maliciosa afecta al rendimiento y, por supuesto, a la prestación de los servicios sanitarios. La diferencia entre el *cryptojacking* y el *medjacking* es básicamente el tipo de *hardware* involucrado. En el primer caso, se trata de la infraestructura informática general, y en el segundo, nos referimos a los equipos médicos basados en sistemas informáticos.
Ingeniería social: - ***Phishing*** - ***Baiting*** - **Clonación de dispositivos**	El correo electrónico (*phishing*, *spam* y *spear-phishing*) es el principal vector de ataque para las infecciones de *malware*. Según Verizon DBIR334, el correo electrónico fue el vector de ataque para el 92,4 % del *malware* detectado[21]. La mayoría de las organizaciones todavía permiten el acceso a cuentas web de correo privado en la mayoría de los ordenadores del hospital. Las direcciones de correo electrónico de los médicos son fáciles de recopilar a través de los directorios públicos de los hospitales, las presentaciones de las páginas web, etc. En nuestra investigación, encontramos tanto casos de uso de cuentas de correo electrónico profesionales para asuntos personales como casos de uso de cuentas de correo electrónico personales para asuntos profesionales. La lucha contra el *phishing* no es fácil: concienciar bien a todos los usuarios es muy difícil. Se han sugerido múltiples factores: la mayoría del personal del ámbito sanitario no tiene ningún conocimiento técnico; un ambiente estresante con alta presión, trabajo por turnos[22], rotación de personal y la falta de coordinación entre el equipo informático y el personal médico[23] [24].

[20] ENISA Threat Landscape Report 2018. Enero de 2019.
[21] ENISA Threat Landscape Report 2018. Enero de 2019.
[22] Annalena Welp et al., 'Teamwork and Clinician Burnout in Swiss Intensive Care: The Predictive Role of Workload, and Demographic and Unit Characteristics', *Swiss Medical Weekly*, 24 de marzo de 2019, https://doi.org/10.4414/smw.2019.20033.
[23] Koppel et al., 'Workarounds to Computer Access in Healthcare Organizations'.
[24] Sean W Smith and Ross Koppel, 'Healthcare Information Technology's Relativity Problems: A Typology of How

Amenaza	Descripción
	La clonación de dispositivos (tarjetas de identificación) requiere un alto nivel de especialización y acercarse a la víctima para clonar su identificación. La identificación de dos factores ha hecho que este tipo de amenaza sea muy poco probable.
Robo: **- Equipos** **- Datos**	El coste de los dispositivos médicos es muy elevado. El robo de equipamiento médico es un delito muy común. Los dispositivos robados suelen venderse en el mercado de segunda mano de los países subdesarrollados o para usos veterinarios por una fracción de su precio. Los dispositivos portátiles de tamaño pequeño y mediano, como los equipos de ultrasonido, electrocardiógrafos, desfibriladores, bombas de infusión o monitores de constantes vitales están entre los más robados. Los dispositivos no deben exponer los datos médicos a menos que el usuario haya iniciado sesión adecuadamente. Por desgracia, la mayoría de ellos usan las credenciales de fábrica. La falta de participación del departamento de seguridad informática en la configuración y la gestión del equipamiento médico y la falta de conciencia sobre el riesgo por parte del personal puede dar lugar a filtraciones de información que podrían a su vez afectar a la reputación, la privacidad del paciente e incluso la seguridad del paciente, y dar pie a las sanciones correspondientes.
Manipulación de equipos médicos/productos sanitarios	Las comunicaciones desprotegidas entre los dispositivos médicos y los servidores pueden dar lugar a la manipulación de la información. Los sofisticados ataques de intermediario (*man-in-the-middle*, MITM) pueden cambiar los datos provenientes de los monitores de constantes vitales o el laboratorio, los informes de patología o incluso imágenes DICOM provenientes de tomografías, resonancias magnéticas o sistemas de ultrasonido al enviarse al servidor PACS.
Skimming	El *skimming* (robo de información de tarjetas de crédito) puede ocurrir por accesos no autorizados a los datos administrativos de los pacientes. Es poco probable que ocurra en los sistemas de salud pública en los que normalmente no hay que pagar, sino que la información que se utiliza son los números de la seguridad social. Ese no es el caso en las entidades privadas. Cuando la protección de los datos administrativos pasa a ser secundaria frente a la protección de los expedientes médicos, se puede producir un acceso no autorizado con mayor facilidad. Los grandes centros comerciales y los sistemas de comercio electrónico parecen ser el objetivo de este tipo de delincuentes organizados. En los últimos años se han realizado grandes esfuerzos por parte de algunas organizaciones públicas y privadas para prevenir el fraude en este ámbito, aunque es un tema que no se trata en el presente informe.
Ataques de denegación de servicio	La denegación de servicio es un ciberataque muy común que puede inhabilitar los servidores de una organización sanitaria, especialmente porque suelen ser reacias a utilizar la infraestructura pública en la nube, por lo que la capacidad de los servidores es limitada. La repercusión puede ser alta, dependiendo del tipo de sistemas afectados.
Ataques basados en la web	El uso extendido de los servicios web no documentados con fines de interoperabilidad y la demora en la aplicación de las actualizaciones, así como el esfuerzo por mantener la configuración del sistema sin cambios y de reducir el tiempo de inactividad en la medida de lo posible, facilitan que los ciberdelincuentes se aprovechen de las vulnerabilidades conocidas.

Patients' Physical Reality, Clinicians' Mental Models, and Healthcare Information Technology Differ', *Journal of the American Medical Informatics Association* 21, no. 1 (enero de 2014): 117–31, https://doi.org/10.1136/amiajnl-2012-001419.

Amenaza	Descripción
Ataques de aplicaciones web	La Inyección SQL y la denegación de servicio representan el 68,8 % de los ataques de aplicaciones web, mientras que en las instituciones gubernamentales representan solo el 26 %, y el 27,7 % a nivel mundial. La Inyección SQL por sí sola representa el 46 % en el caso de la asistencia sanitaria, porcentaje similar al de las empresas energéticas y manufactureras, otro entorno en el que el equipamiento industrial es muy común[25].
Amenaza interna	El personal del hospital puede actuar como una amenaza interna desde cualquier puesto (médicos, enfermeros, administrativos, personal de mantenimiento, etc.), pero los pacientes y sus acompañantes pueden actuar también desde el interior del hospital, dado que no se puede restringir el acceso a determinadas zonas.
Manipulación / daño físico	El equipo médico puede ser muy costoso, y muchas veces se concede acceso físico a personal no autorizado o sin la suficiente formación (o directamente sin ninguna formación en absoluto), lo que permite manipulaciones, daños, robos o la pérdida de equipos o de los datos que contiene.
Robo de identidad	Pueden sufrir un robo de identidad los empleados o los pacientes. El primer caso puede ser peligroso porque hacerse pasar por un médico o un enfermero permite, por ejemplo, recetar medicamentos sin un criterio adecuado o diagnosticar a un paciente de una determinada enfermedad. En el segundo caso una persona podría engañar al sistema de atención sanitaria e introducir también diagnósticos erróneos.
Ciberespionaje	El interés de las industrias farmacéuticas multinacionales u otros grupos de interés por los resultados de las investigaciones clínicas o los datos de los pacientes puede ser una de las motivaciones de este tipo de amenazas. Se han documentado casos en los que se han probado nuevas tecnologías en un hospital y otras naciones han espiado con la intención de copiar la nueva tecnología o tratamiento.
Alteración mecánica de los componentes	Los dispositivos de imagen como las máquinas de resonancia magnética y los escáneres TC incluyen componentes mecánicos que se controlan a distancia. Una brecha de seguridad puede otorgar el control a un individuo malintencionado, que puede provocar un movimiento no deseado de estos componentes. Esto puede afectar directamente al paciente.

[25] Positive Technologies, 'Web Application Attack Statistics: Q2 2017', septiembre de 2017, http://blog.ptsecurity.com/2017/09/web-application-attack-statistics-q2.html.

3.1.5 Fallos del sistema

Amenaza	Descripción
Fallo de *software*	Cualquier componente de *software* puede tener errores. En dispositivos como las bombas de infusión, unidades electroquirúrgicas, ventiladores, láseres de uso médico o dispositivos que utilizan radiaciones ionizantes para funcionar —equipo de radiología y radioterapia— que podrían generar daños físicos si se produjera un error se adoptan medidas de seguridad especiales. Se han aprendido lecciones de los graves incidentes ocurridos en el pasado[26]. La regla general es: se deben tomar todas las medidas para que no se pueda administrar una sobredosis bajo ninguna circunstancia. Estos dispositivos se someten a exhaustivas pruebas antes de salir al mercado. El fabricante actualiza el *software* en pocas ocasiones. Los servidores son más propensos a fallar, no solo por los fallos en el diseño de su *software* dedicado, sino porque dependen de otras plataformas de *software* (sistemas operativos, marcos de programación, bases de datos) que también pueden fallar. De hecho, la experiencia nos ha demostrado que muchos errores ocurren después de una actualización de *software*. Los fallos en los servidores médicos tienen lugar normalmente como errores latentes y, en algunas ocasiones, pueden interrumpir el servicio. Habitualmente desaparecen después de reiniciar el servidor. El análisis de los registros generados es crucial para encontrar la causa del error. Los fallos que no causan averías en el servidor o interrupción del servicio (por ejemplo, la pérdida de las citas de los pacientes o de su información clínica) suelen detectarse varios meses después de que se produzcan. Se deben realizar varias pruebas especiales para asegurar que el sistema hace lo que se espera que haga. Como estos sistemas funcionan 24/7, encontrar intervalos de tiempo de inactividad para ejecutar las pruebas puede ser muy difícil, si no imposible. Los frecuentes fallos de los servidores empeoran la atención médica y merman la confianza en la institución.
***Firmware* anticuado**	La falta de procedimientos para actualizar el firmware de todos los dispositivos (médicos o no) en el hospital es una gran amenaza para las organizaciones de salud y, en particular, los hospitales. Los sistemas y programas heredados ofrecen puertas traseras a los individuos malintencionados, que pueden acceder a datos sanitarios sensibles.
Fallo del dispositivo	Un fallo que dé lugar simplemente a una capacidad limitada/reducida puede afectar gravemente a los procesos que dependen, por ejemplo, de la recopilación en tiempo real de datos de los pacientes, como los dispositivos de medición de la glucosa;
Fallo de los componentes de la red	El ecosistema interconectado de un hospital tiene que ser resistente, ya que existe una gran necesidad de analizar los datos en tiempo real. Si un componente falla, un sistema puede dejar de estar disponible, lo que puede tener efectos en cascada sobre otros sistemas (por ejemplo, el historial médico del paciente)
Mantenimiento insuficiente	La falta de actualizaciones o de parches es otra amenaza muy común que puede tener un gran impacto en la organización sanitaria y facilitar la propagación del *malware*. Las cuestiones operacionales pueden quedar sin resolver y poner en peligro la salud de los pacientes.

[26] Más información en "Overview of some major incidents in radiotherapy and their consequences", Hamish Porter. British Institute of Radiology. Septiembre de 2012.

3.2 RIESGOS EN LA CONTRATACIÓN

Cada tipo de contratación/adquisición lleva aparejados sus propios factores de riesgo. Consulte la siguiente lista para identificar los principales riesgos asociados al tipo específico de contratación que está planificando o gestionando. Trabaje conjuntamente con sus departamentos de informática, seguridad o riesgos para identificar las mejores formas de abordar cada riesgo.

Cada tipo de contratación/adquisición lleva aparejados sus propios factores de riesgo. Es importante que los administradores de las organizaciones sanitarias comprendan estos factores de riesgo y los efectos negativos que podrían tener sobre la infraestructura informática, la salud y la información de los pacientes, el diagnóstico y la calidad del servicio.

En la siguiente tabla se ilustran algunos factores de riesgo relacionados con cada tipo de contratación/adquisición. No se trata de una lista exhaustiva de factores de riesgo. Junto a cada factor de riesgo presentamos ejemplos de posibles consecuencias negativas.

Tabla 3: Riesgos en la contratación

Tipo de contratación/adquisición	Factores de riesgo	Consecuencia negativa
Sistemas de información clínica	Infraestructura incapaz de manejar el sistema	Lentitud del nuevo sistema debido a una CPU de servidor de baja capacidad o una memoria insuficiente. Errores de disco debido a la falta de espacio en el disco. Ancho de banda de la red incapaz gestionar el tráfico de datos, con efectos sobre todas las comunicaciones de la red de la organización.
	Sistema mal diseñado o mal programado	Resultados erróneos debido a una mala programación. Errores del sistema por falta de validaciones de entrada. Larga curva de aprendizaje del usuario debido a interfaces de usuario mal diseñadas. Errores del usuario debido a interfaces de usuario mal diseñadas.
	Falta de consideraciones de seguridad	Una mala gestión de las contraseñas (p. ej. contraseñas almacenadas sin medidas de seguridad) permite a los intrusos robar los datos de los pacientes. Fraude y errores debido a la falta de separación de funciones. Oportunidad para los atacantes debido a la falta de validaciones de entrada, p. ej., Inyección SQL. La falta de registros de las transacciones (*logging*) permite a los atacados ocultar sus acciones.
Sistemas de control industrial	Contraseña de servicio conocida (publicada)	Los atacantes pueden controlar los dispositivos BMS debido a que las credenciales de inicio de sesión del administrador conocidas (publicadas) no se han cambiado durante la instalación.

Tipo de contratación/adquisición	Factores de riesgo	Consecuencia negativa
		Una vez que el atacante controla el dispositivo, lo utiliza para lanzar ataques de denegación de servicio contra la infraestructura de la organización.
	Uso de protocolos de red inseguros	Debido al uso de protocolos de red inseguros (HTTP), los atacantes pueden entrar en la red de la organización.
	BMS instalado con puertos abiertos y expuestos	Los puertos abiertos de un dispositivo pueden utilizarse como vector de ataque.
	Mala protección de la seguridad física de los controladores de los dispositivos BMS y las estaciones de trabajo.	Los atacantes pueden obtener acceso físico a las consolas para instalar *malware* o sabotear los dispositivos.
Productos sanitarios	Falta de controles de autenticación	El intruso manipula la consola del dispositivo para producir resultados erróneos.
	Datos sin cifrar	La transmisión de datos sin cifrar permite a los atacantes alterar los resultados del sensor.
	Uso de protocolos de red inseguros	Los atacantes entran en la red de la organización.
Dispositivos médicos móviles conectados	Uso de un *smartphone* vulnerable	Los atacantes pueden interferir en el correcto funcionamiento del dispositivo médico.
Sistemas de identificación	Datos sin cifrar	Debido a la transmisión de texto sin cifrar, los atacantes pueden acceder a la identificación de los usuarios y a las instalaciones.
Servicios en la nube	Mala aplicación	Información confidencial publicada debido a las deficientes medidas de seguridad del lado del cliente. Sistema no disponible debido a los ataques de denegación de servicio.

4. PRÁCTICAS RECOMENDADAS DE CIBERSEGURIDAD PARA LA CONTRATACIÓN

Cómo utilizar las prácticas recomendadas de este capítulo:
***Paso 1:** Identificar el tipo de contratación/adquisición que se está planificando/gestionando (Cap. 2) **Paso 2:** (Opcional) Identificar las amenazas que más interesa mitigar (Cap. 3)*
***Paso 3:** Identificar las prácticas recomendadas de contratación pertinentes para el tipo de contratación identificado (y las amenazas)*
***Paso 4:** Evaluar en qué fase del ciclo de vida de la contratación debe abordarse la ciberseguridad. Comprender la descripción y los objetivos que deben alcanzarse en las prácticas recomendadas seleccionadas en la fase correspondiente.*
***Paso 5:** Utilizando los gráficos proporcionados, determinar en qué fases de la contratación puede aplicarse cada práctica recomendada*
***Paso 6:** Véanse los ejemplos indicativos de cómo aplicar cada práctica o prueba que se pueda solicitar al proveedor; adaptarse a las prácticas/metodología propias de contratación según sea necesario.*

En este capítulo se ofrecen recomendaciones de prácticas para mejorar la ciberseguridad en la contratación/adquisiciones. Las prácticas recomendadas se clasifican en función de la fase del ciclo de vida de la contratación, y para cada una de ellas se incluyen ejemplos, tipo de adquisición abordada, amenaza mitigada y pruebas. Las prácticas generales se aplican a las tres etapas del ciclo de vida. En algunos casos, una práctica recomendada puede aplicarse a dos fases, en cuyo caso se incluye dentro de la fase en la que debe aplicarse primero o en la que es más pertinente.

La lista de prácticas recomendadas que figura a continuación no es en absoluto exhaustiva, pero ofrece información muy valiosa a los profesionales de informática en el ámbito sanitario responsables de la compra de equipos en hospitales. Este conjunto de prácticas recomendadas es el resultado colectivo de todas las aportaciones recibidas de los profesionales de la salud entrevistados. El lector puede adaptar la lista en función de las prioridades de su organización.

4.1 PRÁCTICAS RECOMENDADAS GENERALES

GP 1. Involucrar al departamento de informática en la contratación

	Involucrar al departamento de informática en las diferentes etapas de la contratación/adquisición para garantizar que se tienen en cuenta los conocimientos especializados sobre ciberseguridad
Ejemplos/pruebas	• Involucrar al personal informático en la redacción de los requisitos de ciberseguridad • Consultar al departamento de informática para integrar las consideraciones de ciberseguridad al planificar nuevas contrataciones o adquisiciones • Hacer que los requisitos de ciberseguridad formen parte de la solicitud de propuestas • Debería formar parte de la política de contratación y adquisiciones de las organizaciones de salud incluir a los departamentos informáticos en todos los comités de adquisición/contratación de sistemas, servicios o dispositivos
Tipos de contratación y adquisiciones relacionadas	Todas
Amenazas relacionadas	Todas

GP 2. Poner en práctica un proceso de identificación y gestión de vulnerabilidades

	Asegurarse de que se tienen en cuenta las vulnerabilidades antes de adquirir nuevos productos o contratar servicios, y de que se vigilen las vulnerabilidades de los productos o servicios existentes durante todo su ciclo de vida
Ejemplos/pruebas	• Establecer un proceso de gestión de vulnerabilidades para vigilar y abordar las vulnerabilidades de los productos y servicios de TIC • La información sobre las vulnerabilidades existentes puede obtenerse del fabricante o de fuentes públicas, como la base de datos de vulnerabilidades del NIST[27] • Abordar en consecuencia las nuevas vulnerabilidades que se identifiquen e incluir cláusulas en la solicitud de

[27] https://nvd.nist.gov/vuln/search

	propuestas/contrato sobre la responsabilidad de los proveedores en el tratamiento de las vulnerabilidades mediante la aplicación de los parches oportunos • Las organizaciones de atención sanitaria pueden plantearse la posibilidad de exigir en sus solicitudes una lista de los materiales (BOM[28]) utilizados en los sistemas o productos adquiridos. Esto puede ser útil para el seguimiento de los sistemas vulnerables en la infraestructura de una organización de atención sanitaria sobre la base de la información sobre vulnerabilidades disponible de forma pública.
Tipos de contratación y adquisiciones relacionadas	Sistemas de información clínica, productos sanitarios, equipamiento de red, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, sistemas de control industrial, servicios en la nube
Amenazas relacionadas	Todas

GP 3. Desarrollar una política de actualizaciones de *hardware* y *software*

	Desarrollar una política de actualizaciones para garantizar que se aplican los últimos parches al sistema operativo y al *software* y que se actualiza el *software* antivirus.
Ejemplos/pruebas	• Crear un registro / inventario de activos informáticos de todo el *software* y el *hardware* en funcionamiento, incluidas las versiones instaladas. • Mantenerse al día sobre los nuevos parches publicados. • Informar al CISO/ISO de estas novedades. • Probar el parche propuesto en algunas máquinas antes de tomar la decisión de aplicarlo en todas. • Determinar el momento más adecuado para aplicar los parches en cada segmento de la red. • Determinar las soluciones para las máquinas en las que no se puedan aplicar parches. • Documentar el procedimiento de actualización. • Definir la participación de terceros proveedores. • Definir las medidas que se tomarán para revertir la situación si las máquinas parcheadas no funcionan como se esperaba

[28] La práctica de pedir a los proveedores una lista de materiales (BOM) del *software* y el *hardware* real utilizados en un sistema permite a cualquier tercero rastrear de forma independiente si un determinado dispositivo puede ser susceptible de sufrir una vulnerabilidad conocida. Es común que la información de dicha lista de materiales se facilite a los organismos notificados, de modo que estos puedan publicar avisos sobre ciertos sistemas y dispositivos médicos. No obstante, para los administradores de la atención sanitaria también puede ser beneficioso tener acceso a esa información a fin de hacer un seguimiento de los componentes vulnerables en toda su infraestructura.

Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, sistemas de información clínica, equipamiento de red, sistemas de atención a distancia, dispositivos móviles de los pacientes, sistemas de identificación, sistemas de control industrial, servicios en la nube
Amenazas relacionadas	Acciones malintencionadas, fallo en la cadena de suministro, fallos en el sistema

GP 4. Mejorar los controles de seguridad para la comunicación inalámbrica

	El acceso a las redes Wi-Fi del hospital debe ser limitado y controlarse estrictamente. Se debe vigilar el número de dispositivos conectados y, en el caso de los dispositivos médicos/productos sanitarios, se debe verificar y restringir. El personal no autorizado no debe tener acceso a la red Wi-Fi.
Ejemplos/pruebas	• De forma predeterminada, contraseñas Wi-Fi fuertes (mantener un registro de la frecuencia con la que se cambia la contraseña). Esto debería estar vinculado a una política • Hacer obligatoria la autenticación de dos factores • Los dispositivos médicos/productos sanitarios que requieren comunicación inalámbrica disponen de una red inalámbrica dedicada con un estricto control de acceso y una política de apoyo dedicada • Se prohíbe el acceso desde dispositivos públicos
Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, dispositivos cliente remotos, sistemas de identificación, servicios en la nube
Amenazas relacionadas	Acciones malintencionadas, error humano

GP 5. Establecer políticas de pruebas

	La organización sanitaria debe establecer un mínimo de pruebas de seguridad para productos o sistemas adquiridos, en función del tipo de producto/sistema. También es importante señalar que un producto recién adquirido o recién configurado debe someterse a una prueba de penetración en su entorno real. De igual manera, las medidas de reparación que se adopten deben estar en consonancia con los parámetros operacionales del entorno real.

Ejemplos/pruebas	• Para cualquier tipo de producto o sistema, la organización sanitaria define un conjunto de pruebas de seguridad y una serie de umbrales. • Las políticas de pruebas abarcan todas las etapas de la contratación/adquisición y pueden incluir auditorías periódicas de seguridad y pruebas de penetración de los sistemas que ya se encuentran en el entorno de producción • Las pruebas y los umbrales se comunican a los proveedores y forman parte de la solicitud de propuestas • Los criterios de aceptación se definen sobre la base de las pruebas de seguridad antes de la finalización de la contratación/adquisición • La solicitud de propuestas/el contrato establece las responsabilidades específicas de los proveedores en relación con los resultados de las pruebas de seguridad de los sistemas en producción • El CISO debe revisar y aprobar todas las políticas de pruebas • La facturación de algunos sistemas depende de la carga. Trate este tema con el proveedor antes de realizar pruebas de carga que puedan suponer un coste • Prepare siempre un plan de contingencia por si el servidor, el sistema de comunicaciones o el dispositivo médico/producto sanitario deja de funcionar durante una prueba • Si la carga de prueba tiene el potencial de detener permanentemente un dispositivo médico/producto sanitario o sistema médico, verifique si su plan de mantenimiento cubre un reinicio del dispositivo/sistema.
Tipos de contratación y adquisiciones relacionadas	Sistemas de información clínica, productos sanitarios, equipamiento de red, sistemas de atención a distancia, dispositivos móviles de los pacientes, sistemas de identificación, sistemas de gestión de edificios, sistemas de control industrial, servicios en la nube
Amenazas relacionadas	Acciones malintencionadas, fallos del sistema, errores humanos

GP 6. Establecer planes de continuidad de negocio

	Deben establecerse planes de continuidad de negocio siempre que el fallo de un sistema pueda afectar a los servicios básicos del hospital, y la función del proveedor en tales casos debe estar bien definida

Ejemplos/pruebas	• En la solicitud de propuestas debe quedar claro cuáles serán los servicios de asistencia que prestará el proveedor en caso de interrupción del servicio, incluidos el coste de los servicios del proveedor (durante y después de la garantía) y el tiempo de respuesta (acuerdo de nivel de servicio) • Se deben prever diferentes situaciones de desastre cuando se planifique la continuidad de la actividad, y si la estrategia de continuidad incluye la asistencia por parte del proveedor; esto debe ser indicarse claramente en la solicitud de propuestas y en el contrato final • Los costes y los requisitos de nivel de servicio para los servicios de continuidad de la actividad deben quedar claros durante el proceso de solicitud de propuestas • Si el fallo de un sistema recién adquirido puede poner en peligro la capacidad del hospital para prestar servicios básicos, el plan de continuidad de la actividad debe establecer la estrategia (sustituir el dispositivo o cambiar los componentes defectuosos), los medios y los procedimientos necesarios para que la organización pueda mantener sus servicios más importantes en las peores circunstancias
Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, sistemas de información clínica, equipamiento de red, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, sistemas de control industrial, servicios en la nube
Amenazas relacionadas	Acciones malintencionadas, fallo en la cadena de suministro, fallos en el sistema

GP 7. Tener en cuenta los problemas de interoperabilidad

	La interoperabilidad es uno de los mayores riesgos de ciberseguridad para las organizaciones sanitarias. El ecosistema informático del hospital está compuesto por diferentes componentes: dispositivos médicos/productos sanitarios, equipos de red, sistemas de atención a distancia, etc. Algunos componentes son más antiguos que otros (sistemas heredados), y la conexión con los nuevos componentes podría dar lugar a brechas de seguridad.
Ejemplos/pruebas	• El proveedor debe indicar cómo se integra la solución propuesta en el sistema preexistente. Si es necesario, deberá incluir en la oferta la documentación técnica que explique cómo se llevará a cabo la integración • El proveedor también debe asegurarse de que vigila la transmisión (al menos durante un período de tiempo predefinido) para evitar la pérdida de datos
Tipos de contratación y adquisiciones relacionadas	Sistemas de información clínica, productos sanitarios, sistemas de atención a distancia, dispositivos móviles de los pacientes, sistemas de identificación, sistemas de control industrial, servicios en la nube

Amenazas relacionadas	Fallos del sistema, errores humanos, acciones malintencionadas

GP 8. Planificar pruebas de todos los componentes

	Los sistemas de información deben probarse a fondo para garantizar que cumplen lo prometido: verificar la facilidad de uso, comprobar la corrección de los resultados bajo carga y comprobar si hay fallos de seguridad (política de contraseñas débil, Inyección SQL). La realización de pruebas debería ser un requisito en la contratación/adquisiciones, así como la supervisión durante las pruebas. Las pruebas deben estar en consonancia con las políticas de pruebas
Ejemplos/pruebas	• El proveedor debe incluir escenarios de prueba para los dispositivos/sistemas ofrecidos. Debe explicar cómo realizar las pruebas y cómo se coordinarán. Definir puntos de referencia para cada prueba • Los informes de las pruebas podrían compartirse dentro de un círculo de confianza • Prepare siempre un plan de contingencia por si el servidor, el sistema de comunicaciones o el dispositivo médico/producto sanitario deja de funcionar durante una prueba • Si la carga de prueba tiene el potencial de detener permanentemente un dispositivo médico/producto sanitario o sistema médico, verifique si su plan de mantenimiento cubre un reinicio del dispositivo/sistema.
Tipos de contratación y adquisiciones relacionadas	Sistemas de información clínica, productos sanitarios, dispositivos cliente remotos, sistemas de identificación, servicios en la nube, sistemas de control industrial, sistemas de atención a distancia, sistemas de gestión de edificios, dispositivos cliente móviles
Amenazas relacionadas	Acciones malintencionadas, errores humanos, fallos del sistema, fallo de la cadena de suministro

GP 9. Activar los registros de auditoría

	Los registros son una parte crucial de la estrategia «asegurar-probar-analizar-mejorar». Si damos por hecho que tarde o temprano nuestro sistema se verá comprometido, los registros son una de las herramientas más útiles que podemos usar para rastrear cómo los atacantes obtuvieron acceso a nuestro sistema. También podemos evaluar cuánta información ha estado en peligro. Mantener los registros seguros es una de las tareas más importantes en relación con la seguridad, aunque su ausencia no compromete la seguridad ya aplicada

Ejemplos/pruebas	• Crear un Sistema Central de Registros seguro para mantener una copia de los registros de forma que estos archivos estén a salvo en una ubicación segura fuera de las instalaciones de la organización. • El mantenimiento de un sistema de registro externo también es útil por otras razones. Por ejemplo, si tienes un servidor que se ha bloqueado y no responde, puedes comprobar los registros de errores del núcleo en tu servidor *syslog* centralizado • El proveedor podría permitir el acceso a los registros para fines de auditoría
Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, sistemas de control industrial
Amenazas relacionadas	Acciones malintencionadas, fallo en la cadena de suministro, fallos en el sistema

GP 10. Cifrar datos personales sensibles en reposo y en tránsito

Gestión  Planificación Aprovisionamiento	Como mínimo, definir una política para los sistemas, servicios o dispositivos que procesan las categorías especiales de datos personales del artículo 9 del RGPD. Este tipo de información debe estar siempre cifrada (siempre que se almacene o se transmita). Para todas las demás categorías de datos personales, se requiere el cifrado siempre que los datos salgan de la organización. Tenga presente que, en muchos casos, este requisito no recae en el proveedor del sistema, servicio o dispositivo, sino en la propia organización. Los datos podrían copiarse a un disco externo para almacenarse en un sitio alternativo. En este caso, es responsabilidad de la organización proporcionar el mecanismo de cifrado Si los datos tienen que salir de las instalaciones de la organización como proceso de comunicaciones de sistema a sistema (enviando los resultados de los datos a un centro de procesamiento remoto), es responsabilidad del proveedor proporcionar un protocolo de comunicaciones seguro y cifrado
Ejemplos/pruebas	• Defina si los datos deben estar cifrados, ya sea mientras están almacenados o durante su transmisión. Incluya este requisito en la solicitud de propuestas. En la oferta del proveedor, busque los algoritmos y métodos de cifrado. En esta etapa se debe informar al responsable de la protección de datos. • El proveedor debe definir explícitamente métodos de cifrado para los datos en reposo, los datos en tránsito y para diferentes tipos de datos (datos sanitarios sensibles frente a datos personales) • A veces los dispositivos no son capaces de cifrar la información que proporcionan. Deben proporcionarse pasarelas adecuadas para el cifrado entre los dispositivos y nuestra red

Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, sistemas de información clínica, equipamiento de red, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, sistemas de control industrial, servicios en la nube
Amenazas relacionadas	Acciones malintencionadas, fallo en la cadena de suministro, fallos en el sistema

4.2 PRÁCTICAS PARA LA FASE DE PLANIFICACIÓN

GP 11. Realizar una evaluación de riesgos como parte del proceso de contratación/adquisiciones

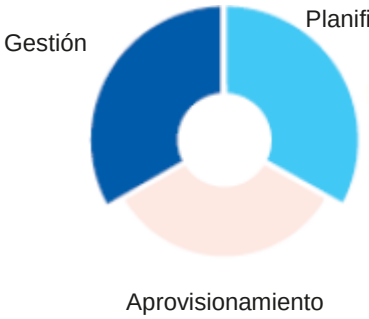
	Como parte del proceso de contratación, las organizaciones sanitarias deben realizar evaluaciones de riesgos.
Ejemplos/pruebas	• Antes de iniciar un nuevo proceso de contratación/adquisición, las organizaciones sanitarias deben evaluar el impacto de la nueva adquisición en su seguridad informática (por ejemplo, nuevo riesgo, aumento/disminución de la probabilidad o impacto de un riesgo existente) • Tras identificar los riesgos asociados a la adquisición de un sistema, servicio o dispositivo, debe diseñarse una estrategia para hacerles frente e integrarla durante el proceso (incluyendo los cambios en el presupuesto, en las especificaciones, etc.) • Los riesgos deben identificarse en una etapa temprana del proceso de adquisición • Las adquisiciones pueden cancelarse (o bien deben examinarse soluciones alternativas) en caso de que hagan aumentar considerablemente las amenazas a la seguridad informática
Tipos de contratación y adquisiciones relacionadas	Todas
Amenazas relacionadas	Todas

GP 12. Planificar con antelación los requisitos de red, *hardware* y licencia

	Evalúe si los nuevos sistemas, servicios o dispositivos requieren *software* de terceros o si el sistema utilizará el software actual pero necesitará licencias adicionales. Coteje los requisitos de *hardware* (espacio en disco, ancho de banda, capacidad de la CPU, memoria) facilitados por los proveedores durante la solicitud de propuestas con la capacidad actual y ya planificada para determinar si es necesario realizar actualizaciones y/o compras adicionales antes de la instalación para adaptarse al nuevo sistema.

Ejemplos/pruebas	• Algunos dispositivos vienen con su propio *software* libre, otros requieren la adquisición de *software* adicional de la misma compañía. Pida a su departamento jurídico que verifique las condiciones de las licencias y su alcance • Investigue si el *software* puede usarse directamente sin cambios o necesita configurarse • Compruebe si las licencias tienen que renovarse y si las actualizaciones están incluidas • Asegúrese de que tiene espacio disponible en su centro de datos para alojar los nuevos servidores • Algunos de sus proveedores externos de servicios informáticos pueden necesitar espacio de su centro de datos. Reserve algo de espacio para necesidades futuras no previstas (y el servidor IPS/IDS por ejemplo) • Asegúrese de que su sistema de energía existente (incluidas las unidades de energía auxiliar) tiene suficiente capacidad. Habitualmente existe una falta de enchufes disponibles para los nuevos dispositivos • Planifique cómo se conectarán físicamente los nuevos dispositivos a su red
Tipos de contratación y adquisiciones relacionadas	Sistemas de información clínica, equipamiento de red, sistemas de identificación, sistemas de control industrial.
Amenazas relacionadas	Fallo en la cadena de suministro, fallos del sistema, fenómenos naturales, errores humanos

GP 13. Identificar las amenazas relacionadas con los productos adquiridos o los servicios contratados

	Las amenazas a la ciberseguridad deben tenerse en cuenta al planificar la adquisición de un nuevo sistema, producto o servicio, y la identificación de las amenazas debe ser continua durante el ciclo de vida de la adquisición
Ejemplos/pruebas	• Utilice un enfoque estructurado para identificar con precisión las amenazas • Incluya a todos los interesados al evaluar las amenazas asociadas a una nueva adquisición • El proceso de modelización de amenazas de la organización sanitaria debe actualizarse si procede tras la adquisición de un nuevo producto o la contratación de un nuevo servicio
Tipos de contratación y adquisiciones relacionadas	Todas
Amenazas relacionadas	Todas

GP 14. Segregar y segmentar la red

	A veces no se pueden mitigar las vulnerabilidades inherentes de los dispositivos conectados a la red: por ejemplo, los dispositivos heredados que funcionan con Windows NT y no se pueden actualizar a un sistema operativo más reciente. Para proteger la infraestructura informática existente de estos dispositivos, se deben aplicar controles compensatorios. Es importante aislar todos los dispositivos conectados del resto de la red. Para ello, aplique la segmentación de la red. Con la segmentación de la red, el tráfico puede aislarse y/o filtrarse para limitar y/o impedir el acceso entre zonas de la red
Ejemplos/pruebas	• En la solicitud de propuestas, el hospital debe proporcionar un resumen de la topología actual de la red y exigir a los futuros proveedores que proporcionen una nueva topología teniendo en cuenta las prácticas de segregación de la red • El proveedor debe proporcionar información sobre el perímetro de seguridad de la red en función de los dispositivos médicos/productos sanitarios conectados. Esta información debe incluirse en la solicitud de propuestas
Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, sistemas de información clínica, equipamiento de red, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, sistemas de control industrial, servicios en la nube
Amenazas relacionadas	Acciones malintencionadas, fallo en la cadena de suministro, fallos en el sistema

GP 15. Determinar los requisitos de la red

	Después de crear la topología de la red y los componentes (cómo se conectan los dispositivos a los sistemas), los profesionales del hospital también deben enumerar los requisitos de seguridad de cada uno de los diferentes componentes para garantizar la interoperabilidad y evitar lagunas (requisitos de ancho de banda, etc.). El hospital necesita saber de antemano las características de seguridad que quieren que tenga el equipamiento de red

Ejemplos/pruebas	• Compruebe sus interruptores. Asegúrese de que tiene espacio disponible para conectar los nuevos servidores y dispositivos • Cree nuevas redes virtuales si es necesario • ¿Hay suficientes enchufes de pared o los dispositivos se comunicarán de forma inalámbrica? • ¿El ancho de banda es suficiente? Verifique si se van a instalar nuevas líneas o si el *router* inalámbrico ofrece suficiente velocidad y capacidad • Es posible que algunos dispositivos utilicen protocolos diferentes de los TCP/IP. Compruebe si necesitarán pasarelas especiales para comunicarse con su red • Algunos dispositivos no cifran las comunicaciones por defecto. Compruebe si los dispositivos ofrecen funciones de cifrado o si tiene que proporcionarlas usted mismo a través de una pasarela antes de que los datos entren en su red. • Asegúrese de que su dispositivo no inicia comunicaciones no previstas con terceros • ¿Necesitan los dispositivos externos una pasarela dedicada o un cortafuegos? • Compruebe y documente los puertos en uso • Diseñe una topología redundante por si falla la línea principal de comunicaciones
Tipos de contratación y adquisiciones relacionadas	Sistemas de información clínica, equipamiento de red, sistemas de identificación, sistemas de control industrial, servicios en la nube, sistemas de atención a distancia, dispositivos cliente móviles.
Amenazas relacionadas	Fallo en la cadena de suministro, fallos en el sistema, fenómenos naturales

GP 16. Establecer criterios de elegibilidad para los proveedores

	Establecer requisitos básicos de seguridad y traducirlos en criterios de elegibilidad al seleccionar los proveedores.

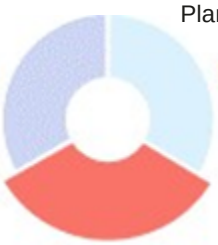
Ejemplos/pruebas	• En las adquisiciones/contrataciones, las organizaciones de atención sanitaria deben establecer unos requisitos mínimos para componentes comunes, p. ej. ordenadores personales, sistemas operativos, protocolos de comunicación (por ejemplo, HTTP no permitido), mecanismos de autenticación (autenticación de un solo factor o de dos factores), bases de datos, cifrado, etc. Los fabricantes que no cumplan con los requisitos mínimos no pueden participar en el proceso de selección • Determine los requisitos mínimos de certificación de seguridad de los proveedores para los diferentes tipos de contratación/adquisiciones (por ejemplo, para la prestación de servicios de seguridad, el proveedor debe tener la certificación ISO 27001) • Incluya los requisitos mínimos de seguridad en el documento de la solicitud de propuestas (criterios de elegibilidad)
Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, sistemas de información clínica, equipamiento de red, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, sistemas de control industrial, servicios en la nube
Amenazas relacionadas	Acciones malintencionadas, fallo en la cadena de suministro, fallos en el sistema

GP 17. Crear una licitación específica para la contratación de servicios en la nube

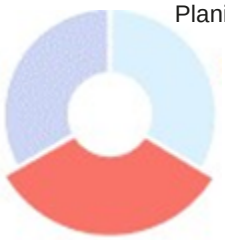
	Al contratar servicios en la nube, especialmente en el caso de los hospitales, se debe redactar una solicitud de propuestas específica teniendo en cuenta los requisitos reglamentarios. En varios Estados miembros, el gobierno ha publicado directrices sobre lo que debe garantizarse al contratar servicios en la nube
Ejemplos/pruebas	• El proveedor de servicios en la nube debe indicar de forma específica dónde se almacenan los datos del hospital. El hospital debe exigir que los datos sensibles permanezcan dentro de la UE (para que se aplique la normativa de protección de datos de la UE). El proveedor también debe explicar qué mecanismos de cifrado utiliza • El proveedor prueba la redundancia y la continuidad de la actividad en caso de incidente. También debe compartir el proceso de notificación de incidentes (según los requisitos de la Directiva SRI) • El proveedor podría compartir los resultados de las auditorías y las pruebas de penetración con el hospital, con carácter confidencial
Tipos de contratación y adquisiciones relacionadas	Servicios en la nube
Amenazas relacionadas	Acciones malintencionadas, fallo en la cadena de suministro

4.3 PRÁCTICAS PARA LA FASE DE APROVISIONAMIENTO

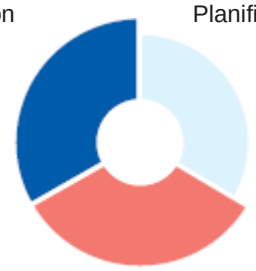
GP 18. Exigir certificados de ciberseguridad

Planificación Gestión  Aprovisionamiento	Las organizaciones de atención sanitaria deben dar prioridad a la adquisición de activos que estén certificados según los programas/normas de ciberseguridad.
Ejemplos/pruebas	• Los productos sanitarios adquiridos deben cumplir con el Reglamento sobre los productos sanitarios (se debe pedir al fabricante que proporcione pruebas) • En las adquisiciones se debe dar prioridad a los productos que hayan sido certificados con arreglo a los programas de certificación de ciberseguridad de la UE, si procede • En el caso de los servicios externos, como los servicios en la nube, es importante exigir que el proveedor cuente con certificados de seguridad acreditados, p. ej., ISO 27001/ ISO 27018/ CCM, etc. • Al examinar los certificados, es importante comprender el alcance del mismo y el alcance del servicio que se va a contratar. Un proveedor de servicios en la nube podría contar con el certificado ISO 27001 en algunas partes del servicio (atención al cliente) pero no en otras que podrían ser más importantes para la organización • Si están disponibles en internet, las organizaciones sanitarias deben revisar los certificados de los proveedores que vienen con el informe completo de la entidad certificadora en el que se detallen las conclusiones. El capítulo del informe relativo al ámbito de aplicación suele detallar cada uno de los servicios incluidos en el volumen de suministro. Estos documentos se ponen a disposición del contratante para dar garantías sobre los servicios ofrecidos
Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, sistemas de información clínica, equipamiento de red, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, sistemas de control industrial, servicios en la nube
Amenazas relacionadas	Acciones malintencionadas, fallo en la cadena de suministro, fallos en el sistema

GP 19. Realizar evaluaciones del impacto de la protección de datos para los nuevos productos o servicios

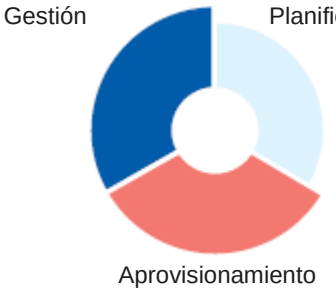
Gestión Planificación  Aprovisionamiento	Evaluar las repercusiones en las cuestiones de protección de datos y el cumplimiento de las normas cuando se planifique la adquisición de un nuevo sistema o la contratación de un servicio.
Ejemplos/pruebas	• Siempre que el sistema, dispositivo o servicio que se esté considerando procese grandes volúmenes de categorías especiales de datos, deberá realizarse una evaluación del impacto sobre la protección de datos • Documente la necesidad de que un determinado proveedor procese datos personales y limítelos a lo necesario • Documente de forma exhaustiva el tipo de datos que debe procesar el nuevo producto/sistema y aplique las limitaciones correspondientes en los requisitos de la solicitud de propuestas
Tipos de contratación y adquisiciones relacionadas	Sistemas de información clínica, productos sanitarios, equipamiento de red, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, servicios profesionales, servicios en la nube
Amenazas relacionadas	Acciones malintencionadas, errores humanos

GP 20. Establecer pasarelas para mantener conectados los sistemas/máquinas obsoletos

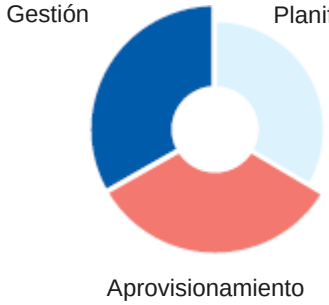
Gestión Planificación  Aprovisionamiento	Siempre que un dispositivo médico/producto sanitario deba utilizar una versión antigua de un sistema operativo que se sabe que tiene vulnerabilidades, debe mantenerse fuera de la red; deberá desarrollarse una pasarela de PC para comunicarse con este dispositivo con el fin de obtener los datos y pasarlos a la red cifrados. A veces todo un segmento completo de la red debe comunicarse a través de esta pasarela. (por ejemplo, todos los equipos de laboratorio). Esta pasarela proporciona un excelente control fronterizo en caso de problemas dentro de estos grupos. El bloqueo de la pasarela aísla todas las máquinas del grupo. Siga esta recomendación siempre que las máquinas dentro del segmento no necesiten comunicarse con el resto de la red, excepto con uno o dos servidores CIS.
Ejemplos/pruebas	• Debido al *hardware* u otros requisitos, algunos dispositivos médicos/productos sanitarios no permiten actualizaciones (por ejemplo, algunos equipos de ultrasonido pueden funcionar con versiones antiguas de Windows) • Los dispositivos médicos tienen una larga vida útil. Los controladores utilizados para comunicarse con la máquina pueden no estar disponibles en las versiones más recientes del sistema operativo, por lo que las versiones antiguas del sistema operativo deben mantenerse para acceder a los datos de la máquina • A veces, los centros comunitarios o de día utilizan dispositivos desechados por hospitales pero que siguen siendo útiles para entornos que no son tan exigentes

Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, sistemas de control industrial
Amenazas relacionadas	Acciones malintencionadas, fallo en la cadena de suministro, fallos en el sistema

GP 21. Proporcionar formación en materia de ciberseguridad relacionada con las prácticas de seguridad de la organización al personal y a los consultores externos

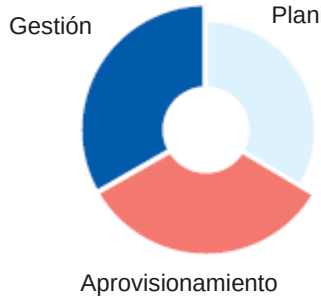
	Asegurarse de que el personal interno o los contratistas/consultores externos que trabajan en las instalaciones estén adecuadamente formados en las prácticas de seguridad de la organización sanitaria.
Ejemplos/pruebas	• El personal técnico debe recibir periódicamente formación en materia de seguridad en relación con los sistemas que utiliza o mantiene • El personal técnico debe recibir una formación específica de seguridad *ad hoc* cuando necesite utilizar o mantener un producto recién adquirido • El personal general (médicos, personal de enfermería, etc.) debe recibir formación sobre las políticas y los procedimientos de seguridad de la información de la organización. • Los contratistas/consultores externos contratados para trabajar en las instalaciones deben recibir formación obligatoria sobre las políticas de seguridad de la organización de atención sanitaria y las prácticas de seguridad relacionadas con su función
Tipos de contratación y adquisiciones relacionadas	Todas
Amenazas relacionadas	Acciones malintencionadas, errores humanos

GP 22. Desarrollar planes de respuesta a incidentes

	Desarrollar planes de respuesta a incidentes que cubran los productos o sistemas recientemente adquiridos.

Ejemplos/pruebas	• Desarrolle un plan de respuesta que establezca lo que el personal de la organización debe hacer en caso de que se produzca un incidente de ciberseguridad y las correspondientes funciones y responsabilidades • Asegúrese de que se aplican las actualizaciones críticas, incluidos los parches de *software*, y de mantener el *software* antivirus actualizado • Determine los canales de comunicación apropiados en caso de incidentes, inclusive entre el hospital y el proveedor • Realice pruebas periódicas de los planes de respuesta a incidentes para todos los productos/sistemas y al menos una prueba de los planes de respuesta a incidentes para los productos/sistemas recién adquiridos
Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, sistemas de información clínica, equipamiento de red, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, sistemas de control industrial, servicios en la nube
Amenazas relacionadas	Acciones malintencionadas, fallo en la cadena de suministro, fallos en el sistema

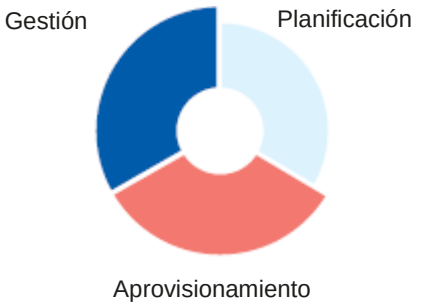
GP 23. Involucrar al proveedor/fabricante en la gestión de incidentes

	Los sistemas y dispositivos acaban fallando, debido a una codificación inexacta, un manejo inadecuado o, simplemente, por el desgaste. En la solicitud de propuestas debe quedar claro cuáles serán los servicios de asistencia del proveedor en estos casos, el coste de los mismos (el primer año y los años posteriores) y el tiempo de respuesta (acuerdo de nivel de servicio) esperado.
Ejemplos/pruebas	• El proveedor debe incluir en la oferta los detalles de su papel en la gestión de incidentes (según de quién sea la responsabilidad) • El proveedor debe mencionar en la oferta los casos en los que informará al hospital, teniendo en cuenta las obligaciones reglamentarias • Se debe describir y formalizar la participación de otros órganos nacionales, como los Equipos de Respuesta ante Emergencias Informáticas específicos de cada sector
Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, sistemas de información clínica, equipamiento de red, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, sistemas de control industrial, servicios en la nube
Amenazas relacionadas	Acciones malintencionadas, fallo en la cadena de suministro, fallos en el sistema

GP 24. Programar y supervisar las operaciones de mantenimiento de todos los equipos

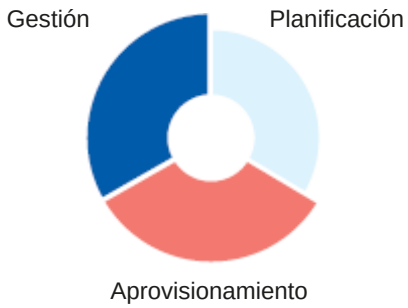
	De acuerdo con la política de actualización de *hardware* y *software*, las operaciones de mantenimiento deben realizarse para todos los diferentes tipos de equipos, incluidos los que forman parte del sistema de gestión de edificios. El personal de mantenimiento debe asegurar un nivel adecuado de funcionalidad de los equipos y decidir si hay que aplicar actualizaciones o parches, etc.
Ejemplos/pruebas	• El proveedor debe incluir el calendario indicativo de mantenimiento en su propuesta. Se debe describir el papel de los profesionales de la informática del hospital (supervisión del funcionamiento) • Registros de mantenimiento • Si una operación de mantenimiento revela la necesidad de aplicar parches o actualizaciones, se deberá iniciar otro procedimiento
Tipos de contratación y adquisiciones relacionadas	Sistemas de información clínica, equipamiento de red, productos sanitarios, sistemas de gestión de edificios, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, sistemas de control industrial, servicios en la nube
Amenazas relacionadas	Errores humanos, fallos del sistema, desastres naturales

GP 25. El acceso remoto debe minimizarse y controlarse

	Cada proveedor debe tener un protocolo definido para acceder a la red del hospital. El acceso debe predefinirse, aprobarse y supervisarse. En caso de emergencia, se debe activar una alerta específica. Las políticas deben mencionar cuándo y cómo puede acceder el proveedor a los dispositivos. El acceso remoto debe ser solo para fines de mantenimiento. No se deben recopilar datos personales durante este proceso. La información que está permitido que salga del sistema y sea procesada por el proveedor debe estar claramente definida en el contrato. Los *routers* y las pasarelas deben configurarse de manera que las comunicaciones externas con el proveedor se limiten al dispositivo que tienen que controlar únicamente.
Ejemplos/pruebas	• Revise los archivos de configuración de todos los componentes de la red y los dispositivos médicos/productos sanitarios • Habilite la autenticación de dos factores para el acceso remoto a los escáneres PET/TC y a las máquinas de resonancia magnética • Habilite el acceso remoto solo a través de VPN • Controle estrictamente el acceso: el proveedor solo debe tener acceso al dispositivo que ha suministrado y en los intervalos de tiempo preestablecidos • Estas cláusulas deben explicarse en la propuesta del proveedor
Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, sistemas de información clínica, equipamiento de red, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, sistemas de control industrial, servicios en la nube

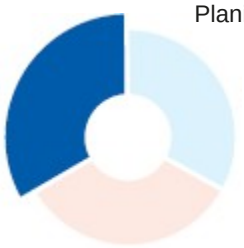
Amenazas relacionadas	Acciones malintencionadas, fallo en la cadena de suministro, fallos en el sistema, errores humanos

GP 26. Exigir la aplicación de parches para todos los componentes

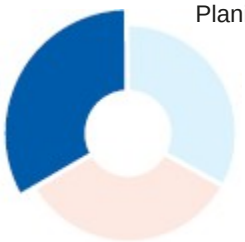
	Los parches son un requerimiento básico que el hospital exigirá al proveedor. Los parches no se pueden aplicar en cualquier momento, debe seguirse un procedimiento. La información sobre los parches debe incluirse en la solicitud de propuestas.
Ejemplos/pruebas	• El proveedor debe explicar el procedimiento para la aplicación de parches en su oferta. También debe describir el papel de los profesionales informáticos del hospital en este proceso. El proceso debe ser explícito para cada componente • El proveedor debe presentar también un plan de redundancia por si un parche no funcionara según lo previsto; debe existir un plan de retroceso • El parche propuesto debe probarse en algunas máquinas antes de tomar la decisión de aplicarlo a todas. Los resultados de la prueba deben entregarse a los profesionales informáticos del hospital
Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, sistemas de información clínica, equipamiento de red, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, sistemas de control industrial, servicios en la nube
Amenazas relacionadas	Acciones malintencionadas, fallo en la cadena de suministro, fallos en el sistema

4.4 PRÁCTICAS PARA LA FASE DE GESTIÓN

GP 27. Aumentar la conciencia en materia de ciberseguridad entre el personal

Gestión Planificación  Aprovisionamiento	Asegurarse de que el personal sea consciente de los riesgos de ciberseguridad asociados a los productos o servicios recientemente adquiridos.
Ejemplos/pruebas	• Adaptar las campañas de sensibilización periódicas o puntuales para incluir productos adquiridos o servicios contratados recientemente • Realizar campañas de sensibilización sobre los riesgos asociados a los productos o servicios recién adquiridos/contratados • Realizar campañas específicas de sensibilización sobre buenas prácticas de higiene cibernética cuando los productos o servicios recién adquiridos/contratados introduzcan cambios en los métodos de trabajo cotidiano del personal clínico (por ejemplo, la migración de los servicios a la nube o la digitalización de los procesos)
Tipos de contratación y adquisiciones relacionadas	Todas
Amenazas relacionadas	Todas

GP 28. Realizar un inventario de activos y la gestión de la configuración

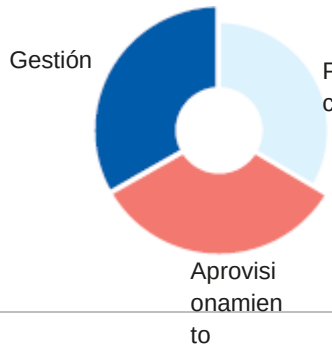
Gestión Planificación  Aprovisionamiento	Asegurarse de que el inventario informático se actualiza adecuadamente cuando se añada o elimine algún componente del entorno de las TIC, y de que existan y se gestionen adecuadamente las configuraciones básicas de seguridad para los componentes TIC.
Ejemplos/pruebas	• Asegúrese de que existe un proceso de gestión de activos informáticos y de que el inventario de activos se actualice cuando se añada, modifique o elimine un nuevo componente • Asegúrese de que existen configuraciones de seguridad básicas para los componentes informáticos y de que se actualizan según corresponda

	• Cree configuraciones básicas de seguridad para cualquier nuevo tipo de producto/sistema que se adquiera antes de que se empiece a utilizar en un entorno de producción
Tipos de contratación y adquisiciones relacionadas	Sistemas de información clínica, productos sanitarios, equipamiento de red, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación
Amenazas relacionadas	Acciones malintencionadas, errores humanos, fallos del sistema

GP 29. Establecer mecanismos de control de acceso específicos para productos sanitarios

	Los dispositivos médicos/productos sanitarios como los escáneres PET/TC, los robots quirúrgicos, etc. también deben protegerse físicamente. El acceso solo debe permitirse al personal especializado, y cada persona debe tener una cuenta dedicada. El departamento informático debe supervisar la política de control de acceso de cada dispositivo. Al adquirir dispositivos, el proveedor debe tener en cuenta estas normas.
Ejemplos/pruebas	• Control de acceso basado en roles, cuentas dedicadas para los que manejan dispositivos médicos/productos sanitarios con controles estrictos (bloqueo de acceso después de 2 intentos de acceso erróneos, autenticación de 2 factores, etc.) • Establezca medidas de control de acceso físico para los dispositivos médicos/productos sanitarios (acceso mediante biometría). La descripción técnica debe incluir esta disposición
Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, sistemas de gestión de edificios, sistemas de identificación
Amenazas relacionadas	Acciones malintencionadas, error humano

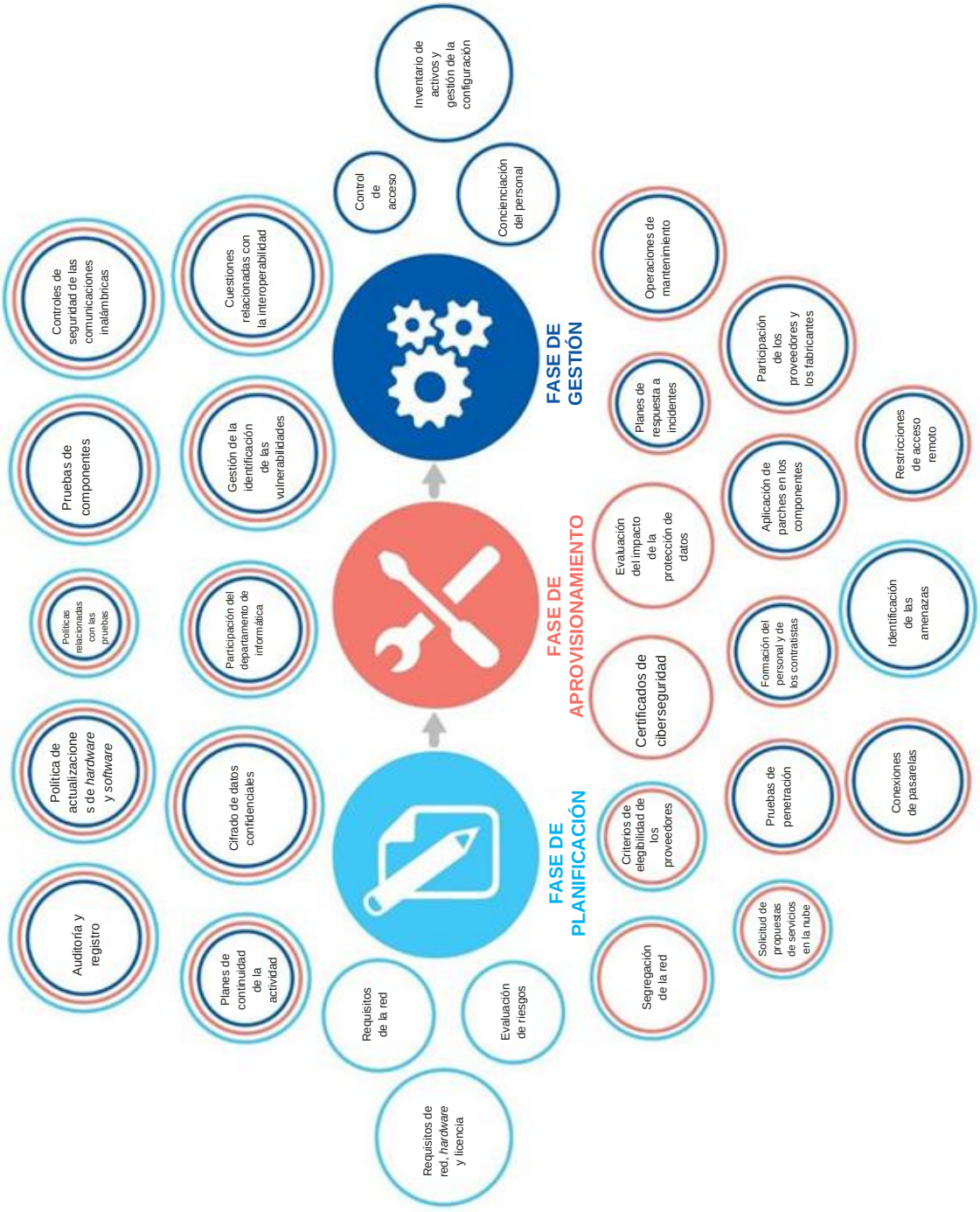
GP 30. Programar las pruebas de penetración con frecuencia o después de un cambio en la arquitectura/sistema

	El proveedor reconoce el derecho del hospital a llevar a cabo los controles de seguridad necesarios (por ejemplo, auditorías de seguridad, pruebas de penetración) bajo su propia autoridad, y garantizará a la institución o al representante autorizado del hospital el acceso ilimitado a los documentos necesarios. Se debe incluir una cláusula específica en la solicitud de propuestas. También es importante señalar que un producto recién adquirido o recién configurado debe someterse a una prueba de penetración en su entorno real.

Ejemplos/pruebas	• Es importante que los productos y sistemas se prueben una vez que se hayan instalado y configurado en su entorno operativo real. Cualquier medida que se plantee para solucionar algún problema deberá tener en cuenta los parámetros operacionales específicos de este entorno. • El proveedor deberá (si así lo exige la solicitud de propuestas) ofrecer opciones para la realización de pruebas de penetración por parte de un tercero. Esto debería incluir tanto las pruebas de caja negra como las de caja blanca. El proveedor debe incluir el coste de estas pruebas en la oferta • El hospital tiene derecho a solicitar los resultados de las auditorías realizadas por el proveedor. El proveedor debe informar en caso de una prueba y contribuir a la transparencia
Tipos de contratación y adquisiciones relacionadas	Productos sanitarios, sistemas de información clínica, equipamiento de red, sistemas de atención a distancia, dispositivos cliente móviles, sistemas de identificación, sistemas de control industrial, servicios en la nube
Amenazas relacionadas	Acciones malintencionadas, fallo en la cadena de suministro, fallos en el sistema

5. PANORAMA GENERAL

Figura 5: Prácticas recomendadas de ciberseguridad para la contratación y las adquisiciones en hospitales



ANEXO A: NORMAS DE LA INDUSTRIA

Tabla 4: Normas relacionadas con la fabricación de productos sanitarios

Norma	Descripción
ISO 13485	La norma ISO 13485 define los requisitos que debe cumplir un sistema de gestión de la calidad para el diseño y la fabricación de productos sanitarios. Esta norma se basa en cierta medida en la ISO 9001. La norma ISO 13485 solo exige que la organización certificada demuestre que el sistema de calidad se aplica y se mantiene eficazmente, y a menudo se considera el primer paso para lograr el cumplimiento de los requisitos reglamentarios europeos.
ISO 14971	La norma ISO 14971 establece el estándar recomendado para gestionar los riesgos de los productos sanitarios y determinar la seguridad de los mismos durante todo el ciclo de vida. Esta actividad la exigen normativas de nivel superior (directivas de la Unión Europea 93/42/CEE, 90/385/CEE y 98/79/CEE) y otras normas sobre sistemas de gestión de la calidad, como la ISO 13485. El informe técnico **ISO/TR 24971**, también de la ISO, proporciona orientación sobre la aplicación de esta norma.
MDS2	El estándar ANSI/NEMA HN 1-2019, *Manufacturer Disclosure Statement for Medical Device Security*, consiste en el formulario MDS2 y las instrucciones para completarlo. El MDS2 actualizado pide a los fabricantes de productos sanitarios que utilicen una nueva hoja de cálculo, incluida en el documento, para describir las características de seguridad de sus productos con el fin de facilitar los esfuerzos de las organizaciones sanitarias para realizar evaluaciones de riesgos y proteger los datos creados, recibidos, transmitidos o mantenidos por sus productos sanitarios. Las organizaciones sanitarias pueden utilizar los datos del nuevo formulario MDS2 para comparar equipos de diferentes fabricantes y tomar decisiones de compra informadas que cumplan con sus políticas de seguridad y privacidad.

Tabla 5: Normas relativas a la adquisición y gestión de sistemas de información sanitaria

Norma	Descripción
ISO / IEC 20000	La serie ISO/IEC 20000 es la norma internacionalmente reconocida para la gestión de servicios TI. La norma ISO 20000 especifica los requisitos para «establecer, aplicar, mantener y mejorar continuamente un sistema de gestión de servicios [...] incluida la planificación, el diseño, la transición, la prestación y la mejora de los servicios».
ISO 27000	La serie ISO/IEC 27000 ofrece recomendaciones sobre las mejores prácticas de gestión de la seguridad de la información.

Norma	Descripción
ISO 27799	La norma ISO 27799 define las directrices para la interpretación y la aplicación en la informática sanitaria de la norma ISO/IEC 27002 y es un complemento de esa norma internacional. Mediante la aplicación de la norma ISO 27799:2016, las organizaciones sanitarias podrán garantizar un nivel mínimo de seguridad adecuado a sus circunstancias y que mantendrá la confidencialidad, la integridad y la disponibilidad de la información personal sobre salud.
IEC 62304	La norma internacional IEC 62304 es una norma que especifica los requisitos del ciclo de vida para el desarrollo de *software* médico y *software* dentro de los productos sanitarios. Está armonizada por la Unión Europea (UE) y los Estados Unidos (EE.UU.) y, por lo tanto, puede utilizarse como referencia para cumplir los requisitos reglamentarios de ambos mercados. El informe técnico **ISO/TR 24971**, también de la ISO, proporciona orientación sobre la aplicación de esta norma.
NIST-SP 800-66	Publicación especial 800-66 Rev. 1: es una guía para aplicar la normativa de seguridad de la Ley de Transferibilidad y Responsabilidad del Seguro Sanitario (HIPAA), y trata sobre las consideraciones de seguridad y los recursos que pueden aportar valor al aplicar los requisitos de esta ley.
NIST CSF	El NIST CSF (*NIST CyberSecurity Framework*) ofrece un marco normativo de orientación en materia de seguridad informática para que las organizaciones del sector privado de los Estados Unidos puedan evaluar y mejorar su capacidad de prevenir, detectar y responder a los ataques cibernéticos.
ISO 22857	La norma ISO 22857:2013 *Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health data* proporciona orientación sobre los requisitos de protección de datos para facilitar la transferencia de datos personales de salud a través de las fronteras nacionales o jurisdiccionales. Es normativa solo con respecto al intercambio internacional o transjurisdiccional de datos personales de salud. No obstante, puede ser informativa con respecto a la protección de la información sobre la salud dentro de los límites nacionales/jurisdiccionales y ser de ayuda para los órganos nacionales o jurisdiccionales que participan en la elaboración y aplicación de los principios de protección de datos.

Tabla 6: Normas relacionadas con la comunicación entre dispositivos de atención médica y el intercambio de información médica

Norma	Descripción
ISO 80001	La norma ISO 80001 es la recomendada para la gestión de riesgos en las redes informáticas que incorporan productos sanitarios. Define las funciones, responsabilidades y actividades necesarias para que la gestión de riesgos de la red informática aborde la seguridad, la eficacia y la seguridad de los datos y los sistemas (las propiedades clave). Esta norma no especifica los niveles de riesgo aceptables, aunque las actividades de gestión de riesgos se derivan de la norma antes mencionada, la ISO 14971.

Norma	Descripción
ISO 15225:2016 (revocada)	En la norma ISO 15225:2016 se especifican las normas y directrices para una estructura de datos de la nomenclatura de los productos sanitarios, a fin de facilitar la cooperación y el intercambio de los datos utilizados por los órganos reguladores a nivel internacional entre las partes interesadas. Se incluyen directrices para conjuntos mínimos de datos y su estructura. Estas directrices se proporcionan a los diseñadores de sistemas que establecen bases de datos que utilizan el sistema de nomenclatura aquí descrito. Los requisitos que contiene esta norma internacional debían aplicarse a la elaboración y el mantenimiento de una nomenclatura internacional para la identificación de los productos sanitarios.
ISO 13972	La ISO 13972:2016 *Health informatics — Detailed clinical models, characteristics and processes* define los *Detailed Clinical Models*/Modelos Clínicos Detallados (DCM) en los términos de un modelo lógico subyacente.
Normas eHealth del ETSI	El Instituto Europeo de Normas de Telecomunicaciones (ETSI) es una organización de normalización de la industria de las telecomunicaciones (fabricantes de equipos y operadores de redes) independiente y sin ánimo lucro que opera en Europa y tiene su sede en Francia. El Proyecto ETSI (EP) eHEALTH está «comprometido con la creación de un mercado basado en normas técnicas para la salud. Promoverá un clima de innovación basado en normas técnicas para garantizar la interoperabilidad, la eficiencia, la seguridad y la privacidad en la prestación de servicios sanitarios en todo el mundo».
HL7	HL7 (*Health Level Seven*) es un conjunto de normas internacionales elaboradas por HL7international que están cada vez más extendidas. HL7 proporciona un marco amplio y normas conexas para la transferencia de datos clínicos y administrativos de manera uniforme y coherente entre las aplicaciones informáticas de las organizaciones de salud. **HL7 es el estándar ISO/HL7 27931:2009** [HL7 RIM R1 - 2003] *Data Exchange Standards - Health Level Seven Version 2.5*, un protocolo de aplicación para el intercambio electrónico de datos en entornos sanitarios.
DICOM	*Digital Imaging and Communications in Medicine* (DICOM) es la norma más utilizada para la comunicación y gestión de la información de imágenes médicas y datos relacionados. DICOM se utiliza sobre todo para almacenar y transmitir imágenes médicas a los sistemas de archivado y transmisión de imágenes (PACS, por sus siglas en inglés) de múltiples fabricantes. DICOM define los formatos de las imágenes médicas que pueden intercambiarse con los datos y la calidad necesarios para el uso clínico. Su norma ISO derivada, la **ISO 12052:2017**, en el ámbito de la informática sanitaria, aborda el intercambio de imágenes digitales e información relacionada con la producción y gestión de dichas imágenes, tanto entre equipos de imágenes médicas como entre los sistemas relacionados con la gestión y la comunicación de esa información.
NIST NISTIR 7497.	NIST NISTIR 7497: también conocido como The Health Information Exchange (HIE) Security Architecture define las directrices para proporcionar un enfoque sistemático para diseñar una arquitectura de seguridad técnica para el intercambio de información de salud.

Tabla 7: Normas relativas al suministro de sistemas de control industrial

Norma	Descripción
ISO 27019	La norma ISO/IEC TR 27019:2013 proporciona principios rectores basados en la norma ISO/IEC 27002 para la gestión de la seguridad de la información aplicada a los sistemas de control de procesos tal y como se utilizan en la industria de servicios energéticos.
IEC 60364-7-710	La norma IEC 60364-7-710 se aplica a las instalaciones eléctricas de los centros médicos, para garantizar la seguridad de los pacientes y del personal médico. Se trata principalmente de hospitales, clínicas privadas, consultorios médicos y dentales, centros de salud y salas médicas especializadas.
UK Health Technical Memoranda **(Memorandos Técnicos de Salud del Reino Unido, HTM)**	Los Memorandos Técnicos de Salud (HTM) ofrecen una guía exhaustiva sobre el diseño, la instalación y el funcionamiento de las tecnologías de construcción e ingeniería especializadas que se utilizan en la prestación de servicios sanitarios. La serie incluye nueve temas centrales: 00 Políticas y principios (aplicables a todos los Memorandos) 01 Descontaminación 02 Gases medicinales 03 Sistemas de calefacción y ventilación 04 Sistemas de agua 05 Seguridad contra incendios 06 Servicios eléctricos 07 Medio ambiente y sostenibilidad 08 Servicios especializados
ISA/IEC 62443	Desarrollada por el comité ISA99, la norma «ISA-62443-4-2, Seguridad para los sistemas de automatización y control industrial: Requisitos técnicos para la seguridad de los componentes de IACS» proporciona los requisitos técnicos de ciberseguridad para los componentes que forman los IACS (sistemas de automatización y control industrial), específicamente los dispositivos integrados, los componentes de red, los *hosts* y las aplicaciones de *software*. La norma, que se basa en los requisitos de seguridad del sistema IACS de la «ISA/IEC 62443-3-3, Requisitos de seguridad del sistema y niveles de seguridad», especifica las funciones de seguridad que permiten a un componente mitigar las amenazas para un nivel de seguridad determinado sin la asistencia de medidas compensatorias.

TP-03-19-825-ES-N

ACERCA DE ENISA

La misión de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) es lograr un elevado nivel común de ciberseguridad en toda la Unión, apoyando activamente a los Estados miembros y a las instituciones, órganos y agencias de la Unión en la mejora de la ciberseguridad. Contribuimos al desarrollo y la aplicación de políticas, apoyamos el desarrollo de capacidades y la preparación, facilitamos la cooperación operativa a escala de la Unión, mejoramos la fiabilidad de los productos, servicios y procesos de TIC mediante la aplicación de programas de certificación de la ciberseguridad, y posibilitamos el intercambio de conocimientos, la investigación, la innovación y la sensibilización, a la vez que desarrollamos las comunidades transfronterizas. Nuestro objetivo es reforzar la confianza en la economía conectada, impulsar la resiliencia y la confianza en la infraestructura y los servicios de la Unión y proteger digitalmente a nuestra sociedad. Puede encontrar más información sobre ENISA y su labor en www.enisa.europa.eu.

ENISA
Agencia de la Unión Europea para la Ciberseguridad

Oficina de Atenas
1 Vasilissis Sofias Str
151 24 Marousi, Attii, Grecia

Oficina de Heraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Grecia

enisa.europa.eu

ISBN 978-92-9204-312-4
DOI: 10.2824/943961