Seguridad de dispositivos basados en Internet de las cosas médicas (IoMT)

Mejores Prácticas en Ciberseguridad

B.01

Volumen B:
Un enfoque técnico

BID

INCD
Israel National
Cyber Directorate

Códigos JEL: D82, H12, I19, K24, L86, L96, M15, O20, O21, O33

Palabras clave: ciberseguridad, amenazas cibernéticas, riesgos cibernéticos, protección de datos, seguridad de sistemas, seguridad de dispositivos, dispositivos médicos, Internet de las cosas, Internet de las cosas médicas, sector salud

Este documento fue originalmente publicado por la Dirección Nacional de Ciberseguridad de Israel (INCD) en idioma hebreo. Su traducción al idioma español fue realizada por el equipo de ciberseguridad de la División de Capacidad Institucional del Estado (IFD/ICS) del Banco Interamericano de Desarrollo (BID), y se incluye como capítulo de la colección "Mejores Prácticas en Ciberseguridad".

El lector debe tener presente que la ciberseguridad es un campo que evoluciona rápidamente. Aunque estos documentos reflejan principios establecidos, podrían actualizarse periódicamente según sea necesario para reflejar los avances en este campo. Adicionalmente, si bien se ha hecho lo posible para presentar las recomendaciones y recursos de manera que sean universalmente aplicables a las organizaciones de todo el mundo, el lector puede encontrar referencias que son específicas al ecosistema cibernético y contexto de Israel (tales como las sumas indicadas en Nuevos Shekels Israelíes [NIS], o referencias a la normativa israelí o a sus organismos gubernamentales).

El documento original se encuentra disponible en el siguiente enlace: **https://www.gov.il/he/pages/iomt**. Tenga en cuenta que allí figura la siguiente renuncia de responsabilidad:

"El presente documento ha sido redactado por el Dirección Nacional de Ciberseguridad con el fin de fomentar la ciberseguridad en la economía israelí. Todos los derechos reservados para el Estado de Israel - Dirección Nacional de Ciberseguridad. El documento ha sido elaborado para beneficio del público. La copia del documento o su incorporación en otros documentos estará sujeta a las siguientes condiciones: el reconocimiento de la autoría de la Dirección Nacional de Ciberseguridad en el formato que aparece a continuación; la utilización de la última versión del documento; la no realización de modificaciones en el documento. El documento contiene información de carácter profesional, cuya implementación requerirá el conocimiento de los sistemas y la adaptación a las características de estos por parte de un profesional en el ámbito de la ciberseguridad. Cualquier comentario o referencia se puede enviar por correo electrónico a: tora@cyber.gov.il."

Índice

Prólogo

La transformación digital y el reto de la ciberseguridad

A medida que la transformación digital continúa expandiéndose por todo el mundo, los gobiernos, las organizaciones, los individuos e incluso los objetos están cada vez más conectados a Internet. Aunque la digitalización ha demostrado ofrecer beneficios innegables, como la prestación eficiente de servicios públicos, el crecimiento económico y la conectividad esencial para el desarrollo de innumerables actividades, también contribuye a una creciente exposición colectiva a los riesgos de ciberseguridad. Un importante motor de este fenómeno en los últimos tiempos ha sido la pandemia mundial de la COVID-19. Como resultado de las generalizadas políticas de distanciamiento social, el número de transacciones de comercio electrónico y las comunicaciones personales en línea experimentaron un crecimiento repentino y pronunciado en un corto período de tiempo, junto con el número de empleados que comenzaron a teletrabajar por primera vez. En esta situación sin precedentes, muchos usuarios de Internet se enfrentaron a nuevas interacciones en línea sin ser suficientemente conscientes de los riesgos de seguridad que estas conllevan. Las organizaciones también tuvieron que adaptarse rápidamente a los desafíos, estableciendo flujos de trabajo totalmente remotos, a menudo sin contar con todas las medidas de seguridad necesarias ni con la orientación adecuada para los empleados.

Sin duda, los ciberdelincuentes no tardaron en explotar la incertidumbre y vulnerabilidad de los usuarios desprevenidos. Proliferaron los intentos de suplantación de identidad (*phishing*) y otras estafas de ingeniería social, aprovechando la necesidad mundial de información relacionada con la pandemia y el uso masivo de herramientas, como las aplicaciones de videoconferencia. En abril de 2020, Google informó de más de 18 millones de correos electrónicos diarios de *software* malicioso (*malware*) y *phishing* relacionados con la COVID-19 en solo una semana. Los *hackers* enviaban correos electrónicos de *phishing* haciéndose pasar por la Organización Mundial de la Salud (OMS), y difundieron masivamente enlaces maliciosos a falsas reuniones de videoconferencia y archivos adjuntos que contenían *malware*. Además, el Informe de Seguridad 2021 de Check Point mostró que durante los primeros meses de 2020 se detectaron casi un millón de intentos de ataque diarios contra las conexiones del protocolo de escritorio remoto (RDP), ampliamente utilizado entre las organizaciones para las conexiones remotas de los empleados. De hecho, los ataques al RDP fueron la forma más popular de ciberataque, superando incluso a los correos electrónicos de *phishing*. Durante la segunda mitad del año, a medida que más organizaciones reforzaban la seguridad de sus plataformas remotas, los *hackers* centraron sus esfuerzos en explotar las vulnerabilidades de los activos privados de los empleados y los dispositivos de acceso remoto para penetrar en sus organizaciones. Aunque estas amenazas se vieron maximizadas por este contexto global, no son novedosas ni desaparecerán; las personas siguen viviendo en un entorno de riesgo elevado, que es especialmente grave en regiones del mundo donde las políticas y tecnología de ciberseguridad están menos desarrolladas, y donde falta educación y concienciación ciudadana en torno a este tema. En otras palabras, aunque los cambios debidos a la pandemia de la COVID-19 acabarán por asentarse, estos han evidenciado la urgente necesidad de reforzar las protecciones individuales y colectivas contra los riesgos cibernéticos.

Reforzar la ciberseguridad es esencial para salvaguardar los derechos de los ciudadanos en la esfera digital, como la privacidad y la propiedad, promover la confianza de las personas en las tecnologías digitales y apoyar el crecimiento económico mediante una transformación digital segura. En particular, los ciudadanos deben tener la seguridad de que los sistemas digitales que utilizan para sus actividades personales o profesionales, y también los que involucran sus datos personales, cuentan con las medidas de seguridad adecuadas para garantizar la integridad, confidencialidad y disponibilidad de su información y de los servicios de los que dependen. Además, los fallos de ciberseguridad tienen un impacto económico importante. Un reciente informe de McAfee estimó que la ciberdelincuencia cuesta a la economía mundial unos US$600.000 millones anuales, es decir, el 0,8% del producto interno bruto (PIB) global.

Israel, líder en ciberseguridad a nivel mundial

El ecosistema de innovación y emprendimiento de Israel es reconocido globalmente como uno de los más vibrantes del mundo, lo cual le ha ganado el nombre de *Startup Nation*. Según los indicadores de ciencia y tecnología de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) de marzo de 2021, Israel es el país de la OCDE que invierte un mayor porcentaje de su PIB (4,9%) en investigación y desarrollo (I+D). Cuenta con un total de más de 300 centros de innovación, investigación y desarrollo de compañías multinacionales; de ellos, docenas están dedicadas a la ciberseguridad.

No es sorpresa entonces que el 40% de la inversión privada a nivel mundial en ciberseguridad tenga lugar en Israel, que posee también el segundo ecosistema privado más grande del mundo en esta área después de Estados Unidos. Según datos de 2021, durante ese año se invirtieron US$8,8 billones en alrededor de 131 compañías israelíes del sector, y más de 40 fueron adquiridas por un total de US$3,5 billones. El país cuenta con más de 500 *startups* de ciberseguridad y, en 2021, el 33% de la población de "unicornios" del mundo eran israelíes. En total, se estimó su exportación de productos de ciberseguridad para 2020 en US$6,85 billones.

La Dirección Nacional de Ciberseguridad de Israel (INCD) es responsable de asegurar el ciberespacio nacional y de establecer y promover la resiliencia cibernética en el país. La INCD opera a nivel nacional para elevar constantemente el nivel de seguridad de las organizaciones y ciudadanos, prevenir y gestionar los ciberataques, y reforzar las capacidades de respuesta en caso de una emergencia cibernética. Su posición como parte de la oficina del Primer Ministro demuestra claramente la centralidad e importancia de sus competencias para el país. Sus objetivos también incluyen la preparación y capacitación del sector privado israelí y del público en general para protegerse de las ciberamenazas mediante la adopción de tecnologías ciberseguras, la publicación de mejores prácticas, la formación del personal y el aumento de la concienciación. Se encarga además de establecer y reforzar la base científica y tecnológica de ciberseguridad mediante el desarrollo de un capital humano altamente cualificado, el apoyo a la investigación académica de vanguardia, la participación en una avanzada I+D tecnológica y el fomento de la ciberindustria. La INCD dedica sus esfuerzos a mantener un ciberespacio protegido, seguro y abierto para todos los habitantes y empresas del Estado de Israel y a facilitar su crecimiento y su base científica e industrial.

¿Cuál es el estado de la ciberseguridad en la región de América Latina y el Caribe?

El Banco Interamericano de Desarrollo (BID) realiza periódicamente estudios sobre la evolución de las capacidades de sus Estados miembros para defenderse de las crecientes amenazas en el ciberespacio. El *Reporte regional de madurez en ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe*, elaborado en colaboración con la Organización de los Estados Americanos (OEA), mostró que los países se encontraban en diferentes etapas de desarrollo en su preparación para enfrentar los desafíos de la ciberseguridad, pero en general aún tenían un amplio margen de mejora.

Mientras que, en 2016, año de la primera edición del informe, el 80% de los países de la región no contaba con una estrategia nacional de ciberseguridad, esta cifra se redujo al 60% en 2020. Además, solo unos pocos países gestionan la exposición de sus infraestructuras críticas —como energía, sanidad, telecomunicaciones, transporte, suministro de agua y finanzas— a ciberataques. Como revela el Reporte de 2020, solo siete de los 32 países evaluados contaban con un plan de protección cibernética de infraestructuras críticas. Esta es una de las conclusiones más preocupantes, si se tiene en cuenta el impacto catastrófico que los ataques a estos sectores podrían tener no solo en las economías nacionales, sino en la vida de todos sus ciudadanos.

En cuanto a la capacidad de los países para gestionar y responder a los incidentes de ciberseguridad, el mismo estudio relevó que el 63% de los países contaba con equipos de respuesta a incidentes de seguridad, como Equipos de Respuesta a Emergencias Informáticas (CERT) o Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT). Sin embargo, de los 20 países que sí los tenían, solo tres habían alcanzado una madurez avanzada en su capacidad de coordinar dichas respuestas. De hecho, 23 de los 32 países se encontraban todavía en una fase inicial de madurez en este tema. Este hallazgo llamó la atención sobre la necesidad de que los países refuercen la capacidad de sus equipos para coordinar eficazmente sus respuestas a los ciberincidentes. Además, el informe examinó la disponibilidad de oportunidades educativas y de formación en ciberseguridad y descubrió que menos de la mitad de los países de la región ofrecían educación formal en ciberseguridad, como posgrados, maestrías o títulos técnicos. No hace falta decir que contar con suficientes profesionales formados es esencial para diseñar e implementar las políticas y medidas de ciberseguridad necesarias para garantizar la resiliencia de un país frente a ciberataques cada vez más sofisticados y complejos.

¿Qué hace el BID para apoyar a la región?

Durante los últimos años, el BID ha apoyado activamente a la región en el desarrollo de la capacidad en ciberseguridad, el diseño e implementación de una política pública de ciberseguridad a nivel nacional y el fortalecimiento de las capacidades sectoriales en ciberseguridad. Este apoyo adopta diversas formas. El BID ha puesto a disposición de los países de América Latina y el Caribe (ALC) asistencia financiera por valor de decenas de millones de dólares para desarrollar capacidades nacionales de ciberseguridad a través de más de 15 operaciones de inversión en el sector público, así como una importante financiación adicional para garantizar la ciberseguridad en los proyectos de inversión en transformación digital.

También proporciona orientación técnica y lleva a cabo proyectos de ciberseguridad en toda la región en forma de consultorías, diagnósticos y proyectos de fortalecimiento de la ciberseguridad hechos a medida, en temas que incluyen la protección cibernética de infraestructuras críticas, cibercrimen y análisis forense, diseño y fortalecimiento de los CSIRT y de los Centros de Operaciones de Seguridad (SOC), y estrategias nacionales y sectoriales de ciberseguridad. Además, el BID ha realizado importantes esfuerzos para proporcionar oportunidades a los profesionales de ALC, a fin de reforzar y actualizar sus habilidades en este campo, ofreciendo regularmente talleres y actividades de formación. Estos han incluido cursos ejecutivos de ciberseguridad de dos semanas de duración, ofrecidos conjuntamente con la Universidad Hebrea de Jerusalén en Israel, así como cursos a medida sobre protección de infraestructuras críticas y otros dirigidos a sectores específicos. Por último, el BID ha elaborado varias publicaciones de gran impacto sobre cuestiones de ciberseguridad a nivel nacional y sectorial, y sigue actualizando y ampliando periódicamente este cuerpo de conocimientos.[1]

1. Véase el sitio del Grupo de Datos y Gobierno Digital (DDG) de la División de Capacidad Institucional del Estado (ICS) del BID, disponible en: **https://www.iadb.org/es/quienes-somos/topicos/modernizacion-del-estado/datos-y-gobierno-digital**.

El BID y la INCD: uniendo esfuerzos

Los retos de la ciberseguridad, como los de la propia Internet, son de naturaleza global, por lo que compartir el conocimiento y herramientas para afrontarlos beneficia a la población en su conjunto. Reconociendo esta realidad, la INCD y el BID se han asociado para poner la experticia israelí a disposición de los países de ALC. La colaboración entre ambas instituciones ha proporcionado un fuerte apoyo a la región, en forma de capacitaciones ejecutivas y técnicas sobre temas avanzados de ciberseguridad, conferencias de vanguardia para funcionarios públicos de ALC y profesionales en el campo, y proyectos innovadores de asistencia técnica. La presente publicación es un producto más de esta colaboración. Consiste de una serie de guías metodológicas de ciberseguridad para organizaciones desarrollada por la INCD a la luz de su análisis sobre riesgos, métodos de ataque, incidentes cibernéticos y estándares globalmente aceptados. Estas guías han sido traducidas al español y al inglés, en una actividad conjunta de ambas organizaciones, con el objetivo de permitir el acceso a este cuerpo de conocimiento por parte de audiencias de toda la región de ALC, y así contribuir a aumentar su resiliencia cibernética.

Esta colección ofrece una orientación práctica sobre una serie de cuestiones metodológicas y técnicas relevantes para el fortalecimiento de la ciberseguridad en las organizaciones de cualquier tipo, con base en los más reconocidos estándares mundiales.

El reto de proteger el espacio digital seguirá creciendo, junto con la necesidad de contar con experiencia probada para afrontarlo. Las reflexiones aquí contenidas pretenden servir como recurso para potenciar la tan necesaria formación profesional en ciberseguridad que se observa actualmente en ALC. Estas guías contribuirán a elevar los estándares organizacionales, a promover mayor conciencia y cultura de ciberseguridad dentro de las organizaciones y en el público en general, y a informar a los tomadores de decisiones, gerentes y líderes en sus iniciativas de ciberseguridad. Confiamos en que estas guías servirán de hoja de ruta para los profesionales y líderes de ALC, trabajando juntos para construir un futuro más seguro y próspero.

Listado de siglas

Sigla	Definición
2FA	Autenticación de dos factores
DDoS	(Ataque) distribuido de denegación de servicio
IoMT	Internet de las cosas médicas
IoT	Internet de las cosas
MFA	Autenticación multifactor
MITM	Ataque de intermediario
RFID	Identificación por radiofrecuencia
VLAN	Red de área local virtual

/01. Introducción

El término Internet de las cosas (IoT, por sus siglas en inglés) se refiere a la comunicación inalámbrica entre objetos. Esta comunicación funcional permite recopilar e intercambiar información en la red para diversas necesidades, como seguimiento y monitoreo remoto, eficiencia, ahorro y optimización, entre otras. Los componentes de IoT suelen incluir un puerto/alimentación a un sensor o actuador para la conexión de red en canales de Internet como wifi, bluetooth, Zigbee, etcétera.

En los últimos años ha habido un desarrollo en el uso de dispositivos IoT debido, entre otras cosas, a la disponibilidad y amplia cobertura inalámbrica, una mejora significativa en las capacidades de procesamiento de información incluso en componentes diminutos basados en volúmenes de almacenamiento muy grandes, nube y tecnologías de bajo costo, etc. Estos componentes se utilizan en diversas industrias (automotriz, aviación, armamento, agricultura sanitaria, entre otras) y brindan capacidades de almacenamiento de información y comunicación, con lo que generan capacidades tecnológicas avanzadas de gestión remota, monitoreo, procesamiento de información con fines de optimización, etcétera.

Gráfico 1. Arquitectura modular en capas de IoT

Capa de contenido
Dispositivos de interfaz de usuario (por ejemplo, pantallas, tabletas, lentes inteligentes).

Capa de servicio
Aplicaciones, *software* para analizar datos y transformarlos en información.

Capa de red
Protocolos de comunicaciones, wifi, computación en la nube.

Capa de dispositivo
Hardware: sistema ciberfísico (CPS, por sus siglas en inglés), máquinas, sensores.

/02. Objetivo de esta publicación

El objetivo de esta publicación es ayudar a las organizaciones del sector de la salud a reducir la superficie de ataque, mediante la realización de endurecimiento y controles para fortalecer los equipos médicos basados en Internet de las cosas médicas (IoMT, por sus siglas en inglés). También se propone establecer un banco de control específico (véase la sección 5) para proteger los componentes en el entorno de red y la red misma (evitar la posibilidad de uso de componentes para atacar y saltarse la red), y controles para reducir los riesgos cibernéticos de entornos externos.

/03.
Público objetivo de la publicación

Las principales destinatarias de este documento son las personas a cargo de la ciberseguridad en el sector de la salud. Esta publicación ayuda a las organizaciones y usuarios a reducir los riesgos cibernéticos mediante la integración de la configuración y los controles de dispositivos médicos basados en IoT en la organización. El documento también está dirigido al Director de Seguridad de la Información (CISO, por sus siglas en inglés), a las entidades a cargo de la arquitectura de protección cibernética/tecnológica, a practicantes de la ciberseguridad y a equipos de sistemas. Asimismo, puede servir como plataforma para los requisitos de seguridad de los fabricantes y proveedores del sector de la salud.

/04.
Riesgos cibernéticos en componentes de IoMT en el sector sanitario y médico

Uno de los sectores a los que se dirige la tecnología IoT es el sanitario y médico, por eso otro término común es Internet de las cosas de asistencia médica (IoHT, por sus siglas en inglés). El uso de estos componentes conectados e inteligentes se expresa en la funcionalidad y diferentes necesidades de este sector. Desde actividades de monitoreo remoto y de indicadores de salud para pacientes y enfermos, el control de activos en una extensión geográfica local o más amplia en la industria de la salud (para determinar la ubicación exacta de los activos de información para pacientes, como sillas de ruedas), hasta el control de instalaciones y monitoreo del entorno de los pacientes, edificios y demás.

Debido a la mejora funcional y las capacidades del campo de IoMT, los hospitales e instituciones médicas estuvieron entre los primeros en adoptar tecnologías basadas en IoMT, tanto en quirófanos como en salas de atención a pacientes, a raíz de la necesidad de utilizar plataformas y servicios en la nube que permitan compartir información de manera eficiente entre las organizaciones sanitarias y los proveedores de información (Chacko y Hayajneh, 2018). El uso de esta tecnología IoMT permite monitorear los índices de los pacientes e incluye una variedad de capacidades y usos, tales como monitoreo de marcapasos, bombas de infusión, bombas de insulina (que permiten la administración continua de insulina de acuerdo a los índices), monitoreo de implantes cocleares, entre otros.

Algunas de estas tecnologías solamente envían información, mientras que otras también la reciben. La asimilación de esta capacidad tecnológica tiene un efecto significativo en los procedimientos médicos, e impacta la naturaleza del tratamiento en los hospitales y el sistema de salud. Un ejemplo es el hecho de que los pacientes no tienen que estar en el complejo hospitalario para su seguimiento, sino que pueden ser equipados con componentes portátiles que incluyen capacidades de IoMT mientras se lleva a cabo el seguimiento y la supervisión de manera remota. Los componentes se pueden dividir de la siguiente manera: componentes que se pueden conectar al paciente (portátiles), componentes que se utilizan para medir índices mediante el tacto pero que no son portátiles de forma permanente/prolongada, componentes de medición esenciales que no conciernen al paciente, y componentes operativos que son esenciales para el paciente pero no tanto para el diagnóstico (CSA, 2020). Este modelo permite atribuir controles y recursos según los riesgos asociados a la capacidad del componente para influir en el paciente y modificar los datos.

Cuadro 1. Grado de integración entre el paciente y el componente de IoMT

Grados de separación	Definición	Responsabilidad de soporte del dispositivo
0 grados	El dispositivo se implanta en el paciente.	Proveedor y/o médico o equipo médico
1 grado	El dispositivo toca al paciente.	Proveedor o personal de ingeniería clínica
2 grados	El dispositivo no toca al paciente, pero toma medidas de los signos vitales, fluidos o datos del paciente.	Proveedor o personal de ingeniería clínica
3 grados	El dispositivo no toca al paciente, pero puede estar haciendo algo aún vital para el diagnóstico adecuado del paciente.	Proveedor o personal de ingeniería clínica
4 grados	El dispositivo está separado del paciente y es una herramienta operativa más que un dispositivo de diagnóstico o clínico.	Proveedor o personal de tecnología de la información (TI)

Fuente: CSA (2020).

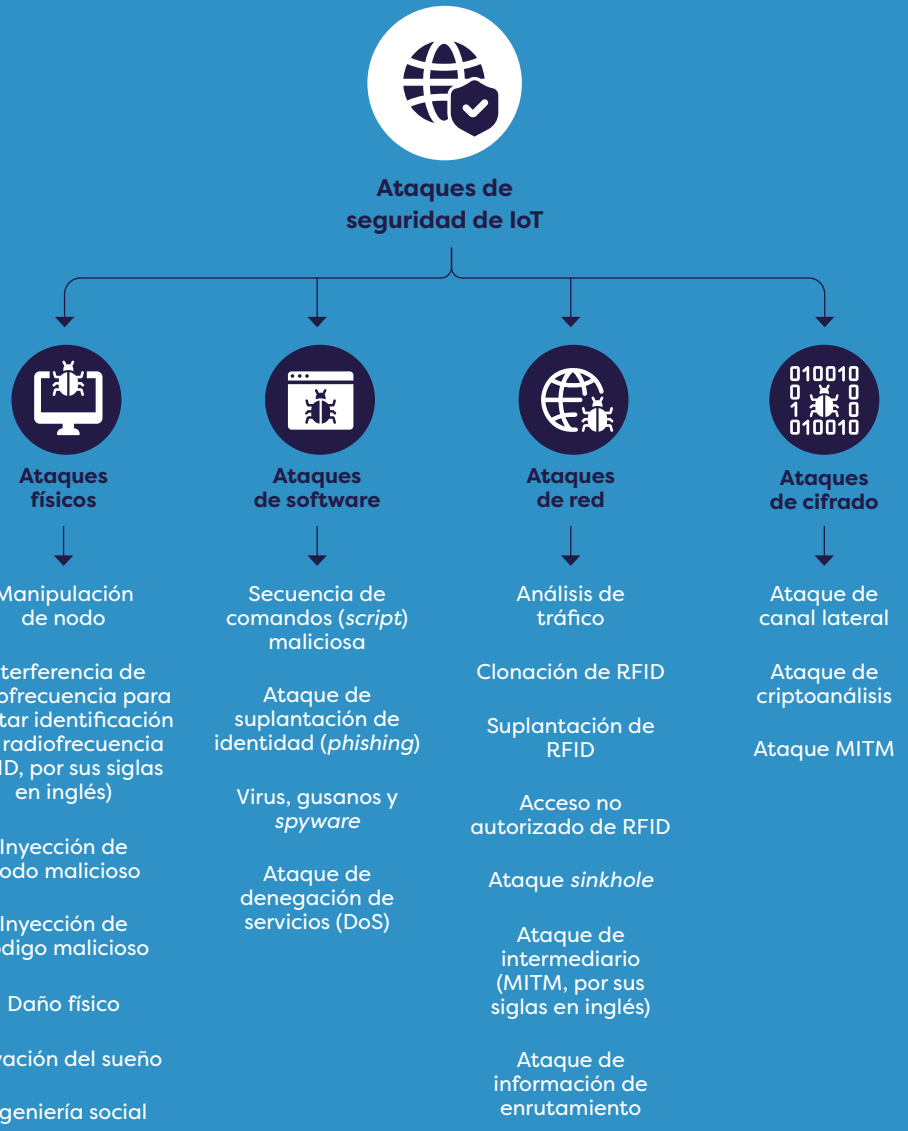
La disponibilidad y tráfico de información sensible y atractiva en la red la exponen a riesgos cibernéticos. Los dispositivos médicos en general, y los basados en componentes de IoMT en particular, no siempre incluyen configuraciones de seguridad y, como tales, pueden no solo poner en peligro el tratamiento o dañarlo y afectar al paciente, sino vulnerar los sistemas de información y la infraestructura de computación médica. Las capacidades de un ciberataque se manifiestan en una variedad de vulnerabilidades, como el secuestro de datos (*ransomware*) con fines de ataque, bloqueo y destrucción; y violación de la confidencialidad, integridad y disponibilidad de datos (según la tríada CIA [por sus siglas en inglés]).

Hasta la fecha, no hay evidencia en la literatura profesional sobre un ciberataque a partir de componentes de dispositivos basados en IoMT en el sistema de salud. Sin embargo, las capacidades para atacar y manipular componentes de IoMT se han demostrado en bastantes estudios y artículos. En un estudio realizado en 2015, el investigador de seguridad Billy Rios, que también colabora con el Departamento de Seguridad Nacional (DHS, por sus siglas en inglés) de Estados Unidos, demostró un cambio remoto de dosis en una bomba de insulina. Este ataque al canal de contraseñas se basó en un análisis de las especificaciones del fabricante que llevó a piratear cientos de componentes (CSA, 2020). Otros posibles ataques contra componentes se centran en intentos maliciosos para generación de carga y ataques distribuidos de denegación de servicio (DDoS, por sus siglas en inglés). Esto se hace conectando los componentes de IoMT al *software* (*botnets*) que controlan y vinculan los componentes para crear una conexión con los servidores de la organización o fuera de ella.[2]

Junto con el tema de la seguridad, también está el **tema de la privacidad**. Estos componentes procesan información médica y algunos de los datos son privados y sensibles. También almacenan documentación histórica y transmiten información sobre las actividades diarias, incluyendo ubicaciones y rutas, hallazgos y cuadros médicos, tales como una condición que empeora o mejora, entre otras cuestiones. En consecuencia, es esencial proteger la información en esta dimensión.

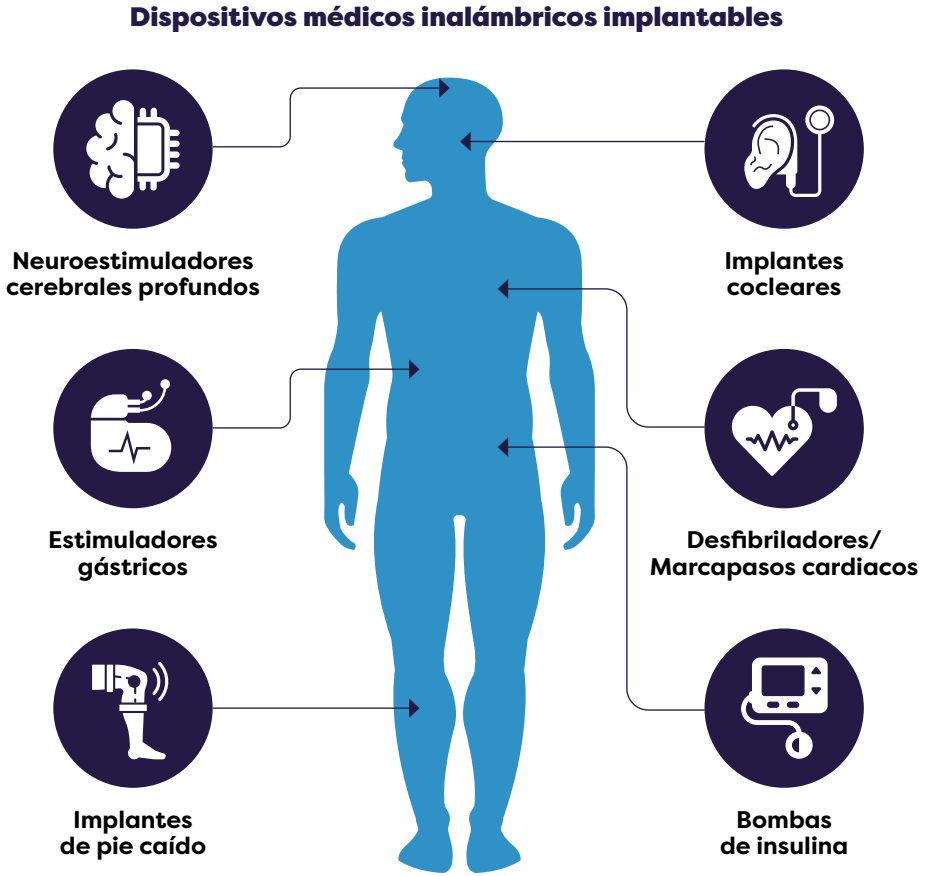
2. El *software* malicioso (*malware*) Mirai ha logrado esclavizar alrededor de 493.000 componentes de IoT. Para obtener más información sobre este tema, visite: **https://pacetoday.com.au/threat-iot-devices-rises-493000-hacked-mirai/**.

Gráfico 2. Variedad de métodos de ataque por segmentación: ataques físicos, de *software*, red y cifrado



Fuente: Atlam y Wills (2019).

Gráfico 3. Componentes médicos de IoMT en el cuerpo de un paciente



A veces existen preferencias funcionales que comprometen la seguridad en el uso de dispositivos IoMT en el sistema de salud. Sin embargo, la viabilidad, atractivo y facilidad de implementación de estos ataques contra componentes IoMT, demostrados en bastantes informes y estudios, plantean la necesidad de un cambio en la percepción de la seguridad en la forma de adquisición, asimilación y respuestas de seguridad en las instituciones médicas y el sistema de salud. Entre otras cuestiones, deberían establecerse requisitos para los fabricantes, desde las fases de desarrollo y equipamiento hasta el ciclo de vida del producto (BSI, 2018).

/05.

Recomendaciones de controles para reducir los riesgos cibernéticos en los sistemas de IoMT

Como punto de partida en los procesos de defensa, conviene recordar que no existe una tecnología única que se pueda aplicar a todo tipo de sistemas. Por lo tanto, la ciberseguridad de los componentes de IoMT impone requisitos sobre su protección y sobre la protección frente a ellos (por ejemplo, un evento en el que los componentes se utilicen para crear consultas y cargar en los servidores, ataques de *ransomware*, etc.). Cabe mencionar que se trata de una industria en desarrollo con una variedad de componentes de IoMT de varios fabricantes y proveedores, de los cuales no todos tienen la misma configuración de seguridad. Estos hechos dificultan la estandarización y gestión uniforme de los componentes. En consecuencia, es necesario proteger e implementar los componentes y sus entornos combinando diferentes controles (de política, tecnológicos, físicos, etc.).

La protección también se encuentra en la configuración de implementación del propio componente (tanto como sea posible), pero además se basa en los requisitos de protección de la red y el endurecimiento de los entornos informáticos y terminales a los que está conectado el equipo (INCD, 2018).[3]

El banco de control presentado en el cuadro 2 es específico y adecuado para el entorno de IoMT. Los controles están orientados a los componentes, entornos informáticos, sistemas de interfaz y tecnologías. El éxito de la implementación y asimilación de los controles de seguridad para reducir los riesgos depende de la organización. La selección de los controles debe realizarse manteniendo un equilibrio adecuado con los requisitos y la funcionalidad del componente, la disponibilidad y la seguridad del paciente.

El cuadro 2 incluye los siguientes campos:

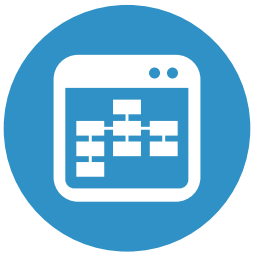
- Número de ID del control.
- Categoría del control.
- Explicación complementaria aplicable, que también incluye los posibles requisitos para los procesos de desarrollo de componentes de IoMT.
- Detalles de las aplicaciones del control y ejemplos, con el fin de transmitir contenido y experiencia en el control.

3. El documento ***Reducción de los riesgos de ciberseguridad en los puntos finales de la organización*** se encuentra disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad a través del siguiente enlace: **https://publications.iadb.org/es/reduccion-de-los-riesgos-de-ciberseguridad-en-los-puntos-finales-de-la-organizacion-mejores**.

Cuadro 2. Banco de control para entornos IoMT

ID del control	Categoría	Explicación complementaria (también aplicable como requisitos de desarrollo)	Detalles de la aplicación del control y ejemplos
5.1	**Política de componentes de IoMT**	Las políticas de la organización para proteger los entornos de IoMT deben redactarse, administrarse y revisarse.	• Considerar procesos de registro ordenados, aspectos regulatorios, regulación de factores de responsabilidad, división de responsabilidades, etc. • Validar esta política una vez cada dos años.
5.2	**Política de componentes de IoMT**	Se deben definir las reglas de uso adecuadas del equipo y usar etiquetas adhesivas específicas en los componentes. También debe haber una señalización adecuada en las proximidades de los componentes, incluidas las explicaciones.	• Incluir en la etiqueta la política de uso de estos componentes (por ejemplo, no conectar medios desmontables, etc.).
5.3	**Proceso de endurecimiento de los componentes de IoMT**	Tras la aceptación e implementación del uso del dispositivo, se debe ejecutar un proceso estructurado para fortalecer los componentes de IoMT de acuerdo con las recomendaciones del fabricante y los estándares internacionales.	• Realizar adaptaciones a los requisitos de la Administración de Alimentos y Medicamentos (FDA, por sus siglas en inglés). • Garantizar la actualización de los componentes en las diferentes versiones. • Eliminar funciones que no son necesarias para la operación y la gestión. • Endurecer los sistemas según los estándares del fabricante.
5.4	**Diseño y protección de la arquitectura de red**	Se deben tomar medidas para una planificación segura con las entradas adecuadas para evitar daños e impedir que se amplíe la superficie de ataque de la red utilizando los componentes de IoMT.	• Examinar la posibilidad de aislar los componentes de IoMT en una red de área local virtual (VLAN, por sus siglas en inglés) administrada dedicada para reducir la utilización del espacio de ataque basado en IoMT, y también aumentar la posibilidad y capacidad de monitoreo para este entorno. • Alternativamente, aislar áreas en casos de ciberataques (*ransomware*, etc.). Este entorno también generará capacidades de gestión y seguimiento a través del sistema de gestión de información y eventos de seguridad (SIEM, por sus siglas en inglés) para eventos sospechosos (implementación de herramientas como sistema de prevención de intrusiones [IPS, por sus siglas en inglés], sistema de detección de intrusiones [IDS, por sus siglas en inglés], etc.).
5.5	**Diseño y protección de la arquitectura de red**	Se tiene que examinar e implementar la inhabilitación de puertos específicos y/o conexiones de red de IoMT para la conectividad selectiva en la red corporativa e Internet.	• Verificar que el proveedor proporcione pautas para evitar esta comunicación.

ID del control	Categoría	Explicación complementaria (también aplicable como requisitos de desarrollo)	Detalles de la aplicación del control y ejemplos
5.6	**Diseño y protección de la arquitectura de red**	Se debe utilizar una comunicación confiable y segura entre los componentes de IoMT y la red corporativa.	• Versiones seguras actualizadas de protocolos de comunicación (protocolo seguro de transferencia de hipertexto [HTTPS, por sus siglas en inglés], protocolo simple de administración de red [SNMPv3, por sus siglas en inglés], etc.). Se deben seguir las nuevas versiones de acuerdo con el desarrollo de la tecnología.
5.7	**Insumos de protección física y prevención de daños en componentes**	Deben garantizarse los insumos adecuados para evitar el sabotaje y la manipulación (tales como cambios inhabilitantes), así como manejar la amenaza interna (INCD, 2019).[4] Todo esto, con énfasis en la distribución geográfica de los componentes en hospitales, clínicas y ambientes médicos, e incluso fuera de ellos (por ejemplo, dispositivos portátiles que lleve consigo el paciente).	• Se puede considerar la norma según la cual si se ha realizado una desconexión de la red corporativa o del medio deseado, se debe generar un aviso y aislar el componente de la red. • Sin embargo, se debe garantizar que la pérdida de comunicación no afecte la integridad del dispositivo, y que los dispositivos de IoMT continúen funcionando durante un período prolongado (se debe realizar actividad auxiliar según se requiera y una estimación puntual de la duración de la actividad después de la pérdida de comunicación).



4. El documento ***Recomendaciones de defensa: la amenaza interna*** se encuentra disponible dentro de esta serie de guías de buenas prácticas en ciberseguridad a través del siguiente enlace: **https://publications.iadb.org/es/recomendaciones-de-defensa-la-amenaza-interna-adaptacion-de-la-organizacion-en-el-ciberespacio**.

ID del control	Categoría	Explicación complementaria (también aplicable como requisitos de desarrollo)	Detalles de la aplicación del control y ejemplos
5.8	**Permisos y componentes de usuario**	Preferiblemente, deben seleccionarse componentes de IoMT que aíslen código, procesos y datos confidenciales originados en procesos en partes del *firmware*, mientras se retiene la información ingresada (*inputs*) para evitar el acceso no autorizado para realizar cambios.	• Es aconsejable verificar las características de los componentes en la documentación del fabricante.
5.9	**Autenticación de usuario**	Se debe implementar un sistema de registro que registra eventos y cruza la funcionalidad y los datos existentes y generados.	• Por ejemplo: alerta al cambiar de red, al modificar datos, etc. Los registros también deben mantenerse en un almacenamiento persistente y con capacidad de recuperarse (para evitar la manipulación y los cambios).
5.10	**Reducir la superficie de ataque de contraseñas**	Para evitar el acceso no autorizado al componente.	• Reemplazar la contraseña del fabricante para evitar el uso de contraseñas predeterminadas. • Seleccionar y usar una contraseña compleja (habilitando un mecanismo de cumplimiento [*enforcement*] al momento de elegir una contraseña). • Establecer un bloqueo de contraseña tras varios intentos fallidos de inicio de sesión. • Al activar un mecanismo de recuperación de contraseña, asegurarse de que no haya retroalimentación sobre la cuenta y el usuario.

ID del control	Categoría	Explicación complementaria (también aplicable como requisitos de desarrollo)	Detalles de la aplicación del control y ejemplos
			• Establecer una protección contra mecanismos de adivinación de contraseñas (como ataques de fuerza bruta). • Bloquear o deshabilitar el dispositivo tras varios intentos fallidos de ingresar la contraseña.
5.11	**Evitar el acceso no autorizado**	Junto con las entradas lógicas (*logical inputs*), también se deben utilizar las entradas físicas (*physical inputs*) para evitar accesos no autorizados o manipulaciones alrededor de los componentes mediante ataques de canal lateral (*side-channel attacks*) (Yan, 2019).	
5.12	**Impedir la capacidad de inyectar archivos**	Se debe impedir la capacidad de inyectar códigos de secuencias de comandos en sitios cruzados (XSS, por sus siglas en inglés), falsificación de petición en sitios cruzados (CSRF, por sus siglas en inglés) o lenguaje de consulta estructurado (SQL, por sus siglas en inglés). Todo esto como medida para prevenir consultas de obtención de datos.	
5.13	**Actualizaciones de *software***	La organización controlará el proceso de actualización del *software* dentro de períodos de tiempo razonables, que se definirán en la política de la organización o de acuerdo con la urgencia y necesidad, para prevenir riesgos que surjan en el medio, incluyendo procesos de manipulación de información y ataques MITM.	• Coordinar directamente el procedimiento para transferir actualizaciones de forma segura a la organización o al componente de IoMT (esto es después de comparar las firmas de archivos: consultar el ID 5.14 más abajo). • En la medida de lo posible, distribuir las actualizaciones a través de un servidor dedicado en la organización. Esto, luego de recibir los archivos de actualización y verificar las firmas con el proveedor/fabricante.
5.14	**Actualizaciones de *software***	Es preciso realizar un proceso de actualización de *software* seguro por el aire (OTA).	• Verificar la recepción del archivo de una fuente confiable y un servidor seguro. • Transferir el archivo de actualización en un proceso seguro y encriptado. • Verificar la autenticidad en la firma del archivo (verificación del archivo de firma). • Solicitar actualizaciones de seguridad al proveedor para los defectos graves que se publiquen.

ID del control	Categoría	Explicación complementaria (también aplicable como requisitos de desarrollo)	Detalles de la aplicación del control y ejemplos
5.15	**Actualizaciones de *software***	Es necesario guardar la última versión de *firmware* y los ajustes de configuración como parte del proceso de recuperación de la versión del fabricante (crisis/evento cibernético y recuperación de una falla o desastre).	• Realizar revisiones periódicas entre versiones existentes y la última referencia.
5.16	**Entorno de soporte y pruebas**	Se debe asignar un entorno dedicado (computadora o red separada de la red corporativa) para soporte de procesos, resolución de problemas y soporte de fallas de componentes.	• Llevar a cabo el proceso de soporte de forma controlada y bajo la gestión de la institución médica. • Asignar una sesión temporal al proceso de soporte remoto. • Iniciar la conexión al entorno de soporte por parte del cliente/organización y requerir autenticación de dos factores (2FA, por sus siglas en inglés) o multifactor (MFA, por sus siglas en inglés). • Antes de devolver el componente o la modificación a la red, garantizar el cumplimiento de las políticas y controles.
5.17	**Codificación de información**	Se deben usar componentes con capacidad funcional para eliminar información y datos sin procesar después del uso, y al cambiar de uso o consumidor (eliminar información en la transferencia de paciente a paciente).	• Por ejemplo, un evento en el que se puede aplicar este control es cuando se transfiere de un paciente a otro.
5.18	**Acoplamiento de información para identificar componentes de IoMT en línea**	Se tienen que examinar datos e identificadores que circulan por Internet y explorar alternativas para el cambio de dicha información públicamente expuesta para que ya no esté presente en los componentes IoMT de la organización con el objeto de reducir las áreas de ataque.	• Por ejemplo, evitar la posibilidad de búsqueda en páginas web por nombre de fabricante, nombre de componente (cambio de nombre de componente), contraseñas predeterminadas, etc. (Hoelscher, 2023).
5.19	**Contacto de la red**	Es preciso desactivar la capacidad de hacer referencia a enlaces selectivos, para prevenir cambios funcionales, robo de información sobre pacientes, etc.	
5.20	**Prevenir los riesgos cibernéticos en los repositorios de datos**	Se deben aplicar los controles adecuados para reducir los riesgos cibernéticos en los procesos de conexión no autorizados, como los puertos USB y los componentes de IoMT.	• Aplicar bloqueo lógico o físico al componente, para evitar la posibilidad de insertar código hostil y manipular el componente y la información (incluido el robo de datos y registros médicos, información personal, confidencial, etc.).
5.21	**Asignar entradas de escaneo de archivos dañinos**	Se deben asegurar los procesos de escaneo en el equipo designado. También, implementar parches de seguridad y procesos de mantenimiento de actualizaciones de antivirus.	• Utilizar e instalar el sistema de antivirus de acuerdo con las instrucciones del fabricante (para evitar daños en el rendimiento).
5.22	**Reducir el riesgo de daños en los procesos de trabajo**	Es necesario verificar los procesos de trabajo e implementar escenarios que aseguren la prevención de daños a los procesos de trabajo críticos en la red, proceso operativo, entidades y seguridad o productividad de la organización.	• Por ejemplo, aplicar configuraciones apropiadas en el componente y la red para asegurar que el componente no será manipulado con el propósito de cargar información y denegar el servicio (véase también el el ID 5.24 más abajo).

ID del control	Categoría	Explicación complementaria (también aplicable como requisitos de desarrollo)	Detalles de la aplicación del control y ejemplos
5.23	**Entradas para reducir riesgos en la comunicación inalámbrica**	Se tienen que implementar mecanismos de seguridad para las redes inalámbricas instaladas en una VLAN dedicada y separada de los otros sistemas, y también calibrar la potencia de transmisión de la señal inalámbrica de forma tal que las señales no se reciban en un radio amplio fuera del edificio/piso.	• Implementar mecanismos de autenticación e identificación para usuarios y dispositivos en la red y limitar el servicio únicamente a personas autorizadas. De vez en cuando, cambiar las contraseñas como parte del proceso de actualización de los usuarios autorizados.
5.24	**Enfrentar un ataque DDoS**	Es necesario verificar e implementar infraestructura resiliente frente a ataques DDoS que puedan afectar al componente y/o a través de él a los usuarios y/o la red.	• Configurar un cortafuegos en el componente que servirá como búfer de protección externo e interno.
5.25	**Cifrado**	Se deben usar componentes que combinen capacidad criptográfica para proteger la confidencialidad y confiabilidad de la información tanto en el proceso de tránsito (*transit*) como en los procesos de reposo (*rest*).	• Elegir algoritmos de cifrado estándar y claves de cifrado seguras, siempre asegurando no comprometer el rendimiento.
5.26	**Validación de entrada y salida de datos**	Se debe realizar un proceso de verificación en cada módulo de acuerdo con una lista blanca (*whitelist*).	
5.27	**Protección de la información médica de los pacientes**	El acceso a la información médica de los pacientes (incluso en entornos de nube) requiere el uso de sólidos mecanismos de identificación y autenticación.	• Usar mecanismos 2FA/MFA.

ID del control	Categoría	Explicación complementaria (también aplicable como requisitos de desarrollo)	Detalles de la aplicación del control y ejemplos
5.28	**Protección de la información médica e información personal frente a terceros**	Se debe habilitar y definir la gestión y el control de la transferencia de información de los sistemas IoMT a terceros.	• Examinar el significado de la información y el canal de transferencia de información que se pasa a un tercero, tanto en términos de seguridad como de protección de la privacidad (BITAG, 2016). La transferencia de datos de pacientes (a clientes, empleados y otros) requiere notificación y aprobación por consentimiento.
5.29	**Protección de la información: privacidad y prevención de la divulgación de información**	Se deben asegurar y garantizar entradas apropiadas para evitar el uso de lenguaje informativo que contengan conocimiento potencialmente explotable/ sensible al devolver un mensaje de error.	• Evitar la visualización de datos sobre la naturaleza del error, direcciones, versión del servidor web e información relacionada con el paciente.
5.30	**Protección de la información sensible en registros**	Tiene que asegurarse de que la información generada durante el procesamiento de la información se inserte inmediatamente en el archivo personal (también como una copia impresa) para evitar la pérdida de información personal.	• Durante el proceso de liberación, asegurarse de que la información producida por los documentos se haya ingresado en el archivo médico.
5.31	**Protección y privacidad de la información del usuario**	Se debe generar la capacidad para ejercer los derechos de información en los servicios de IoMT y para ejercer sus derechos sobre la información, acceso, supresión, corrección y movilidad de datos, limitación de procesamiento, resistencia al procesamiento, etc.	

ID del control	Categoría	Explicación complementaria (también aplicable como requisitos de desarrollo)	Detalles de la aplicación del control y ejemplos
5.32	**Documentación y seguimiento**	Los procesos de monitoreo deben determinarse e implementarse para los componentes y eventos críticos que el sistema documentará (registro de eventos).	• Definir el comportamiento y la configuración normales, y recolectar *logs* y anomalías de cada elemento con el objeto de correlacionar y generar alertas por cambios de ajustes, configuración, etc. • El proceso de revisión de alertas es un componente importante en la protección, detección de brechas de seguridad e intentos de ataque y capacidades de recuperación. En consecuencia, hay que realizar auditorías y revisiones periódicas de los controles de seguridad para garantizar un proceso eficiente.
5.33	**Supervivencia y resiliencia**	Se tienen que usar tecnologías y componentes que contengan capacidades mecánicas integradas y mecanismos de autodiagnóstico y reparación para la recuperación ante percances o fallas.	
5.34	**Validación de la funcionalidad médica**	Se debe establecer un proceso ordenado (como parte de un control) de pruebas médicas funcionales del componente con el fin de detectar eventos excepcionales (informes inexactos/ falsos, incumplimiento de índices, etc.).	• Esto se puede hacer comparándolo con un componente o sistema con la misma funcionalidad, pero hay que asegurarse de que no haya dependencia entre los componentes.
5.35	**Realización de pruebas de resiliencia**	Es necesario realizar pruebas de resiliencia periódicas.	• El propósito de la prueba es verificar la robustez de la red y los componentes. La prueba se centrará en los riesgos cibernéticos durante la manipulación de la red y el deterioro de la funcionalidad de los componentes, la capacidad de atacar desde la red a los componentes y desde los componentes a la red.

Referencias

- Alsubaei, F., A. Abuhussein, V. Shandilya y S. Shiva. 2019. IoMT-SAF: Internet of Medical Things Security Assessment Framework. Disponible en: **https://www.researchgate.net/publication/336340918_IoMT-SAF_Internet_of_Medical_Things_Security_Assessment_Framework**.

- Atlam, H. F. y G. B. Wills. 2019. IoT Security, Privacy, Safety and Ethics. En: M. Farsi et al. (eds.), *Digital Twin Technologies and Smart Cities*. Springer Nature Switzerland. Disponible en: **https://www.researchgate.net/publication/332859761_IoMT_Security_Privacy_Safety_and_Ethics**.

- BITAG (Broadband Internet Technical Advisory Group). 2016. Internet of Things (IoT) Security and Privacy Recommendations. Noviembre. Disponible en: **https://securityandtechnology.org/wp-content/uploads/2020/07/Internet-of-Things-IoT-Security-and-Privacy-Recommendations.pdf**.

- BSI (Federal Office for Information Security [Alemania]). 2018. Cyber Security Requirements for Network-Connected Medical Devices. BSI-CS 132. Noviembre. Disponible en: **https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/Medical_Devices_CS-E_132.pdf?__blob=publicationFile&v=2**.

- Chacko, A. y T. Hayajneh. 2018. Security and Privacy Issues with IoT in Healthcare. *EAI Endorsed Transactions on Pervasive Health and Technology* 4 (14). Disponible en: **https://www.researchgate.net/publication/326568227_Security_and_Privacy_Issues_with_IoMT_in_Healthcare/link/5b5922cea6fdccf0b2f7d79b/download**.

- CSA (Cloud Security Alliance). 2020. Managing the Risk for Medical Devices Connected to the Cloud. Disponible en: **https://cloudsecurityalliance.org/artifacts/managing-the-risk-for-medical-devices-connected-to-the-cloud**/.

- ENISA (Agencia de la Unión Europea para la Ciberseguridad). 2017. Baseline Security Recommendations for IoT. Disponible en: **https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot**.

- GSMA. 2017. IoT Security Guidelines for Endpoint Ecosystems. Version 2.0. Octubre. Disponible en: **https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf**.

- Hoelscher, P. 2023. How to Find and Remove Your Device from the Shodan IoT Search Engine. *Comparitech*. 4 de agosto. Disponible en: **https://www.comparitech.com/blog/vpn-privacy/remove-device-shodan/**.

- INCD (Dirección Nacional de Ciberseguridad de Israel). 2017. Metodología de ciberdefensa para organizaciones. Disponible en: **https://publications.iadb.org/es/metodologia-de-ciberdefensa-para-organizaciones-version-10-mejores-practicas-en-ciberseguridad**.

- ———. 2022. Recomendaciones de defensa: la amenaza interna. Adaptación de la organización en el ciberespacio. Disponible en: **https://publications.iadb.org/es/recomendaciones-de-defensa-la-amenaza-interna-adaptacion-de-la-organizacion-en-el-ciberespacio**.

- ———. 2024. Reducción de los riesgos de ciberseguridad en los puntos finales de la organización. Disponible en: **https://publications.iadb.org/es/reduccion-de-los-riesgos-de-ciberseguridad-en-los-puntos-finales-de-la-organizacion-mejores**.

- IoT Security Foundation. 2018a. IoT Security Architecture and Policy for the Home: A Hub Based Approach. Release 1. Noviembre. Disponible en: **https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Security-Architecture-and-Policy-for-the-Home-a-Hub-Based-Approach.pdf**.

- ———. 2018b. IoT Security Compliance Framework. Release 2. Diciembre. Disponible en: **https://web.archive.org/web/20200504004918/https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf**.

- Makhdoom, I., M. Abolhasan, J. Lipman, R. Liu, y W. Ni. 2018. Anatomy of Threats to the Internet of Things. *IEEE Communications Surveys & Tutorials*. Disponible en: **https://www.researchgate.net/publication/328043031_Anatomy_of_Threats_to_The_Internet_of_Things**.

- NIST (Instituto Nacional de Estándares y Tecnología [Estados Unidos]). 2018a. NIST Releases Draft NIST Internal Report (NISTIR) 8222, Internet of Things (IoT) Trust Concerns. Septiembre. Disponible en: **https://www.nist.gov/news-events/news/2018/09/nist-releases-draft-nist-internal-report-nistir-8222-internet-things-iot.**

- ———. 2018b. NIST Releases Special Publication 500-325, Fog Computing Conceptual Model. Marzo. Disponible en: **https://www.nist.gov/news-events/news/2018/03/nist-releases-special-publication-500-325-fog-computing-conceptual-model**.

- Yan, Y. 2019. Side Channel Attacks on IoT Applications. Universidad de Bristol. Disponible en: **https://research-information.bris.ac.uk/ws/portalfiles/portal/210500367/Final_Copy_2019_03_19_Yan_Y_PhD.pdf**.

El término Internet de las cosas (IoT, por sus siglas en inglés) se refiere a la comunicación inalámbrica entre objetos que permite recopilar e intercambiar información en la red para diversas necesidades. Los sectores sanitario y médico se benefician con frecuencia de la tecnología IoT. Otro término común es Internet de las cosas médicas (IoMT, por sus siglas en inglés). El uso de estos componentes conectados e inteligentes se expresa en la funcionalidad y diferentes necesidades de este sector. Abarca desde actividades de monitoreo remoto y de indicadores de salud para pacientes y enfermos, el control de activos en una extensión geográfica local o más amplia, hasta el control de edificios y monitoreo del entorno de los pacientes, edificios y demás.

No obstante, la disponibilidad y tráfico de tal información sensible y atractiva en la red la expone a riesgos cibernéticos. Los dispositivos médicos en general, y los basados en componentes de IoMT en particular, no siempre incluyen configuraciones de seguridad y, como tales, pueden no solo poner en peligro el tratamiento y afectar al paciente, sino vulnerar los sistemas de información y la infraestructura de computación médica.

Con esto en mente, el objetivo de esta publicación es ayudar a las organizaciones del sector de la salud a reducir la superficie de ataque, mediante la realización de endurecimiento y controles para fortalecer los equipos médicos basados en IoMT. El documento también presenta un banco de control específico para proteger los componentes en el entorno de red y en la red misma, y controles para reducir los riesgos cibernéticos de entornos externos, ayudando a las instituciones y usuarios a reducir los riesgos cibernéticos presentes en los dispositivos médicos basados en IoT dentro de la organización.

El ciberespacio es un ámbito de oportunidades en términos de progreso tecnológico, conectividad, integración y conexión global a Internet. Pero también es terreno de amenazas y riesgos. Los ciberataques pueden dañar a las organizaciones e infligirles importantes daños económicos y de imagen. Para que una organización esté preparada para defenderse de las amenazas cibernéticas, debe dominar una gran cantidad de especializaciones: tecnológicas, organizativas y de procesos. La lista de capítulos presentada a continuación refleja el estado de la colección al momento de la publicación de este documento.

Volumen A: Un enfoque metodológico

Volumen B: Un enfoque técnico

- **B.01** Seguridad de dispositivos basados en Internet de las cosas médicas (IoMT)
- **B.02** Seguridad de infraestructuras Access Point Name (APN)
- **B.03** Endurecimiento de sistemas informáticos
- **B.04** Reducción de riesgos de ciberseguridad en cámaras de videovigilancia
- **B.05** Reducción de los riesgos de ciberseguridad en los puntos finales de la organización
- **B.06** Seguridad de sistemas de planificación de recursos empresariales (ERP)
- **B.07** Preparación y respuesta ante un ataque de *ransomware* en la organización
- **B.08** Reducción de riesgos de ciberseguridad en sistemas de control industrial (ICS)
- **B.09** Plantilla para inspección de riesgos de ciberseguridad en sistemas de control industrial (ICS)
- **B.10** Seguridad de infraestructuras de voz sobre protocolo de internet (VoIP)
- **B.11** Autenticación multifactor avanzada ante amenazas de ciberseguridad
- **B.12** Principales amenazas de ciberseguridad de las plataformas de asistencia remota a usuarios
- **B.13** Prevención y respuesta ante un secuestro de Border Gateway Protocol (BGP Hijacking)
- **B.14** Preparación ante ataques distribuidos de denegación de servicio (DDoS)
- **B.15** Reducción de riesgos de ciberseguridad en sistemas de gestión de edificios (BMS)
- **B.16** Ciberseguridad por medio de sistemas de gestión de dispositivos móviles (MDM/EMM)
- **B.17** Seguridad en la transferencia gestionada de archivos (MFT)
- **B.18** Aspectos de ciberseguridad de la distribución de publicidad por mensajes de texto (SMS)
- **B.19** Principios de operación del equipo de respuesta ante emergencias cibernéticas (CERT) israelí
- **B.20** Seguridad de los sistemas multimedia
- **B.21** Integración de principios de ciberseguridad en los procesos de respaldo y recuperación
- **B.22** Protección de los servicios de nube pública ante amenazas de *ransomware*

Volumen C: Desarrollo seguro de *software*