



PROTEGIENDO LA SALUD DIGITAL

Una guía de ciberseguridad
en el sector de salud

AUTORES: Pablo Alzuri, Florencia Cabral, Santiago Paz, Ariel Nowersztern y Pablo Libedinsky.
DISEÑO: www.souvenirme.com

Copyright © 2021 Banco Interamericano de Desarrollo. Esta obra se encuentra sujeta a una licencia Creative Commons IGO 3.0 Reconocimiento- NoComercial-SinObrasDerivadas (CC-IGO BY-NC-ND 3.0 IGO) (<http://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode>) y puede ser reproducida para cualquier uso no comercial otorgando el reconocimiento respectivo al BID. No se permiten obras derivadas. Cualquier disputa relacionada con el uso de las obras del BID que no pueda resolverse amistosamente se someterá a arbitraje de conformidad con las reglas de la UNCITRAL. El uso del nombre del BID para cualquier fin distinto al reconocimiento respectivo y el uso del logotipo del BID no están autorizados por esta licencia CC-IGO y requieren de un acuerdo de licencia adicional.

Nótese que el enlace provisto más arriba incluye términos y condiciones adicionales de esta licencia.

Las opiniones expresadas en esta publicación son de los autores y no necesariamente reflejan el punto de vista del Banco Interamericano de Desarrollo, de su Directorio Ejecutivo ni de los países que representa.





PROTEGIENDO LA SALUD DIGITAL

Una guía de ciberseguridad
en el sector de salud

Índice

PRÓLOGO	5
RESUMEN EJECUTIVO.....	6
INTRODUCCIÓN	8
¿QUÉ ES LA CIBERSEGURIDAD?	11
ESTADO DEL ARTE	13
7 PASOS PARA LA IMPLEMENTACIÓN DE CIBERSEGURIDAD.....	27
RECOMENDACIONES Y REFLEXIONES FINALES	31
AGRADECIMIENTOS	33
REFERENCIAS BIBLIOGRÁFICAS	34

Prólogo

El COVID-19 ha acelerado la digitalización de nuestras sociedades y la ciberseguridad ha pasado a ocupar un lugar central entre las preocupaciones del mundo. **La digitalización es clave para acelerar la recuperación económica y social, y por ello, es uno de los cinco ejes estratégicos de la Visión 2025, el plan del Grupo BID para impulsar el crecimiento inclusivo y sostenible post pandemia.** La necesidad de proteger este espacio digital creciente explica la importancia de entender el rol de la ciberseguridad en la transformación digital.

La ciberseguridad en el sector salud es particularmente relevante debido a la sensibilidad de la información que maneja. Las tecnologías que apoyan la Historia Clínica Electrónica (EHR), la telemedicina, y otros dispositivos médicos avanzados son sistemas críticos y desafortunadamente han sido víctimas de múltiples ataques en los últimos años. Los Datos Personales de Salud (PHI) son los datos más valorados en los mercados negros, con valores decenas de veces más altos que, por ejemplo, los números de tarjeta de crédito^a.

Durante 2020, en Estados Unidos **las fugas de datos del sector salud crecieron un 55%** según el Departamento de Salud y Servicios Humanos. De estas fugas, el 67% se debe a incidentes de ciberseguridad^b.

Según el estudio publicado por el Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos en 2020, la región de

América Latina y el Caribe sigue enfrentando importantes desafíos. En muchos países de esta región aún existen actividades e iniciativas de ciberseguridad ad-hoc sin visión estratégica. **Sólo 13 países tienen una estrategia nacional de ciberseguridad y sólo 9 un plan de protección de infraestructuras críticas.** Según el Global Cybersecurity Index de ITU, de 55 países del mundo que destacan por su compromiso con la ciberseguridad, solamente uno, Uruguay, pertenece a esta región.

Desde el BID somos muy conscientes de estos desafíos, y por ese motivo hemos desarrollado esta guía que apunta a facilitar el acceso a conocimiento y herramientas de apoyo para diagnosticar y mejorar el estado de la ciberseguridad en las organizaciones de salud y para proteger a los ciudadanos de nuestra región.

Miguel Porrúa

*Coordinador del Clúster de Datos
y Gobierno Digital*

Innovación para Servir al Ciudadano (ICS)
Instituciones para el Desarrollo (IFD)

Luis Tejerina

Especialista Líder
Protección Social y Salud (SPH)
Sector Social (SCL)

^a <https://www.securelink.com/blog/healthcare-data-new-prize-hackers/>

^b <https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY21Q1HealthcareBreachReport2021.pdf>

Resumen ejecutivo

El sector salud no sólo fue uno de los más atacados por los hackers en 2019¹, sino que es la industria que ha sufrido los ataques más dañinos en los últimos años. El costo promedio de un ciberataque en el sector salud en términos de pérdida de negocio, gastos de prevención, detección y recuperación equivale a 7,13 millones de dólares² en comparación con los 3,86 millones que, en promedio, cuestan los ciberataques en cualquier otra industria. En Brasil, por ejemplo, el costo promedio de un ciberataque se incrementó un 10.5% entre 2019 y 2020. Los Datos Personales de Salud (PHI) son los datos más cotizados en los mercados negros, con valores decenas de veces más altos que por ejemplo los números de las tarjetas de crédito³.

Asimismo, hay que tener presente que **el 80% de la información comprometida por estos ciberataques son datos personales** y que es en el sector salud donde más tiempo se tarda en detectar una posible vulneración de información: desde que tiene éxito un ataque hasta que la institución se da cuenta de que sus datos fueron vulnerados pasa un promedio de 329 días. Nuestra región, de hecho, presenta uno de los mayores tiempos de detección de ataques a nivel mundial.

Por todo ello y con el fin de fortalecer la seguridad de la información en las organizaciones es importante que cuenten con herramientas para enfrentar esta realidad, con base en la

implementación de marcos de trabajo, controles y guías. Los marcos de trabajo construyen un contexto que permite desarrollar distintas actividades de seguridad de la información o ciberseguridad según sea su naturaleza, de forma sistematizada y controlada, junto con la definición e incorporación de controles o medidas de seguridad, con perfil técnico y de gestión, apoyados en guías que definen herramientas prácticas y que abordan problemáticas específicas.

Acompasando esta realidad, los distintos gobiernos y organizaciones internacionales han definido marcos regulatorios, como el Reglamento General de Protección de Datos (GDPR), de la Comunidad Europea, y el Health Information Privacy (HIPAA), de Estados Unidos. Ambos marcos buscan reglamentar el manejo y la protección de los datos personales por parte de los distintos actores involucrados según sea el contexto y el HIPAA, en particular, tiene como alcance los datos personales de salud.

Esta guía, realiza una recopilación y clasificación del conocimiento existente a nivel global en lo que respecta a normas, marcos de trabajo, estándares, buenas prácticas y guías de implementación de ciberseguridad, con el fin de orientar al lector en su uso. También se propone una estrategia de 7 pasos esenciales para comenzar o fortalecer la ciberseguridad en una organización del sector salud.

¹ Verizon, 2020.

² IBM, 2020.

³ Neveux, Ellen, 2021.

LOS 7 PASOS PARA LA IMPLEMENTACIÓN DE CIBERSEGURIDAD PROPUESTOS SON:

1. Incluir la ciberseguridad como prioridad en la gestión estratégica de la organización.
2. Definir la estructura organizacional en ciberseguridad.
3. Definir los objetivos y las metas de ciberseguridad.
4. Realizar un diagnóstico de situación con análisis de brechas o GAP.
5. Elaborar un plan director de ciberseguridad.
6. Ejecutar el plan director.
7. Evaluar los resultados y el riesgo remanente.

Para realizar el diagnóstico de situación con análisis de brechas o GAP indicado en el paso 4, se propone utilizar la herramienta de autoevaluación desarrollada por el BID (detallada en los anexos de esta guía). Esta herramienta de autoevaluación, mediante un set de preguntas múltiple opción, realiza un diagnóstico respecto a las mejores prácticas de la industria basada en el marco de ciberseguridad del NIST⁴. **Esta herramienta ayuda a calcular las brechas y brinda recomendaciones que sirven como base para la elaboración del plan director.**

El plan director de ciberseguridad es el instrumento de gestión que se utilizará para cumplir los objetivos y metas de ciberseguridad. No es otra cosa que un programa con duración, alcance y presupuesto determinados, que agrupa todos los proyectos de ciberseguridad que deben realizarse para cumplir un conjunto de metas y objetivos y reducir el GAP existente.



Visite la herramienta: www.iadb.org/cibereval

⁴ National Institute of Technical Standards (NIST), 2018 (a).

Introducción

Si bien la ciberseguridad como tal se viene desarrollando desde hace varias décadas, su implementación no es todavía de uso común en el sector salud. Existen numerosos artículos en la web y en el mundo académico sobre este tema, como marcos de trabajo, definiciones de controles, guías y buenas prácticas. El estado del arte es amplio y variado, lo que supone un gran desafío a la hora de analizar el camino a tomar por una organización que debe abordar la temática y comprender de forma sencilla los aspectos y consideraciones a tener en cuenta.

En el contexto de la emergencia sanitaria, la adopción de las tecnologías de la información y comunicación (TIC) se ha acelerado en el sector salud. En muchos países de América Latina y el Caribe (ALC) el sector está ofreciendo una mejor calidad de servicio a los ciudadanos, avanzando en proyectos de acceso a servicios digitales de salud por medio de teleconsultas o telemedicina, brindando acceso a los ciudadanos a historias clínicas electrónicas, entre otros.

Con el aumento del uso de las TIC en ALC y, en particular, en el sector salud, crecen los riesgos de incidentes de ciberseguridad en el sector. El sector salud no sólo fue uno de los más atacados por los *hackers* en 2019⁵, sino que es la industria que ha sufrido los ataques más dañinos en los últimos años. A esto se suma que los datos que maneja el sector son

confidenciales y sumamente sensibles, por lo que el impacto no material puede ser también muy grave. La tendencia en términos de incidentes de ciberseguridad es creciente, como lo refleja la encuesta del *Healthcare Information and Management System Society* (HIMSS)⁶ donde se muestra que en el año 2018 y en Estados Unidos el 75,7% de las organizaciones encuestadas indicó haber tenido, al menos, un incidente de ciberseguridad significativo en los últimos 12 meses; únicamente el 21,2% indicó no haber tenido un incidente de seguridad significativo reciente en los últimos 12 meses, y el 3,2% indicó que no lo sabía.

En ALC la tendencia de los ciberataques también es creciente. En Brasil el costo promedio de un ciberataque se incrementó en un 10,5% entre 2019 y 2020⁷. Es importante notar que el 80% de la información comprometida son datos personales y que en el sector salud es donde más tiempo toma detectar una vulneración de la información. Desde el momento que un ataque tiene éxito hasta que la institución se da cuenta de que sus datos fueron vulnerados pasa un promedio de 329 días. Nuestra región, de hecho, presenta uno de los mayores tiempos de detección de ataques del mundo. En los últimos años han tenido lugar múltiples incidentes en la región, por ejemplo, exposición de datos sensibles en México⁸, Chile⁹ o Argentina¹⁰, entre otros.

⁵ Ver Verizon, 2020.

⁶ Ver Healthcare Information and Management System Society, HIMSS North America, 2018.

⁷ Ver IBM, 2020.

⁸ Ver DataBreaches.net. The Office of Inadequate Security, 2018.

⁹ Ver Carvajal, Víctor y Jara, Matías, 2016.

¹⁰ Ver Clarín Tecnología, 2018.

Con el objetivo de entender la importancia y la urgencia de una acción en este tema en el sector salud, analizaremos el caso de *WannaCry* en 2017 en el Reino Unido¹¹. Este incidente interrumpió los servicios en un tercio de los hospitales y en alrededor del 8% de las consultas de medicina general, lo que tuvo un impacto de unas 19.000 citas canceladas. Si bien es difícil estimar los costos de tecnologías de la información (TI), se calcula que tuvo un costo de 19 millones de libras por causa de la cancelación de citas y de 73 millones de libras que tuvieron que ser invertidos en los meses siguientes en el soporte o en consultores para restaurar datos y sistemas afectados por el ataque.

Otro punto relevante que se observa a nivel internacional es un uso creciente de nuevas tecnologías en el sector, en particular el internet de las cosas médicas (IoMT). Esto presenta nuevos desafíos para el sector y nuevos riesgos con posibles impactos en la seguridad de los pacientes. Si bien se considera que el índice de penetración del IoMT en ALC es bajo, se cree que la situación revertirá en los próximos años y, por ende, el sector deberá estar preparado para afrontar los nuevos retos.

Dado el creciente proceso de informatización de las TIC en el sector salud en ALC y los riesgos que esto conlleva, el presente material pretende servir de guía práctica para que los interesados puedan definir su estrategia de seguridad de la información, considerando la legislación vigente, las mejores prácticas de la industria y los estándares aplicables.

El documento también aborda el problema de la baja implementación de la ciberseguridad y proporciona una guía de implementación estratégica con siete pasos concretos para apoyar el desarrollo de la ciberseguridad en una institución del sector salud.

Adicionalmente, realiza una **recopilación y clasificación del conocimiento existente a nivel global en lo que respecta a normas, marcos de trabajo, estándares, buenas prácticas y guías de implementación** con el fin de orientar al lector en su uso para poner en práctica la estrategia de los 7 pasos propuesta. El paso 4 propone realizar un diagnóstico de situación con análisis de brechas o GAP, utilizando la herramienta de autoevaluación para el sector salud (detallada en los anexos de esta guía).

Este documento **está dirigido a las personas con responsabilidades de ciberseguridad y/o autoridades de tecnología de la información del sector salud**. Pretende desmitificar la ciberseguridad para que deje de ser considerada como un tema exclusivo del sector informático, afirmando la importancia del compromiso y la responsabilidad de todo el personal de salud.

Quienes deseen tener una visión estratégica han de leer, como mínimo, las secciones “**7 pasos para la implementación de ciberseguridad**” y “**Recomendaciones y reflexiones finales**”. Una lectura completa del documento es recomendada para aquellas personas que quieran profundizar técnicamente.

¹¹ Ver UK Department of Health & Social Care, 2018.

WANNACRY

WannaCry es un *ransomware* surgido en mayo de 2017 para *Microsoft Windows* que afectó a unas 230.000 computadoras en más de 150 países, incluyendo servicios críticos de salud, proveedores de telefonía, bancos, sistemas de transporte, universidades y empresas privadas, entre otros. Cifraba los archivos de la víctima, los retenía y pedía un rescate en Bitcoin bajo la promesa de liberarlos. Utilizaba las vulnerabilidades conocidas de *Microsoft Windows* (Eternal-Blue y DoblePulsar), que tenían un parche liberado casi dos meses antes, por lo que el incidente se podría haber evitado si los sistemas operativos hubiesen estado actualizados. Tenía un *KillSwitch* que consultaba un sitio web y, si el mismo estaba disponible, no continuaba con la propagación. Por esta razón las prácticas usuales para la contención de un incidente (aislar los equipos y redes afectadas) tuvieron un efecto negativo y aumentaron la propagación. La recomendación es siempre no ceder a este tipo de extorsiones y nunca efectuar un pago a los cibercriminales. En este caso particular se tiene la duda de si, incluso pagando, era posible recuperar los datos, debido a un defecto que tenía el propio *malware*. WannaCry fue el punto de inicio para otros tipos de *ransomware* y estrategias seguidas por los cibercriminales.

REFERENCIAS:

- latam.kaspersky.com/resource-center/threats/ransomware-wannacry
- assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf
- www.welivesecurity.com/la-es/2017/05/12/wannacry-ransomware-nivel-global/
- www.bbc.com/mundo/noticias-39929920
- blog.segu-info.com.ar/2017/05/wannacrypt-al-menos-15-paises-afectados.html
- www.welivesecurity.com/la-es/2021/05/12/wannacry-como-evoluciono-escena-ransomware/

¿Qué es la ciberseguridad?

La información de las empresas y los sistemas que la almacenan y procesan, son activos clave de las organizaciones. En el sector salud, en particular, se utiliza información personal muy sensible que es altamente codiciada por los ciberdelincuentes debido a su alto valor en el mercado negro¹². Por eso la ciberseguridad es un asunto que debe involucrar a toda la organización, desde el directorio hasta el último empleado.

La ciberseguridad o la seguridad informática es la rama que se dedica a la implantación de medidas con el fin de proteger los activos informáticos como los sistemas, redes, computadoras, documentos digitales, entre otros, de posibles ataques que afecten su integridad, confidencialidad y/o disponibilidad. Esto puede tener impactos en la continuidad asistencial de los usuarios del sistema de salud y/o en la imagen de las organizaciones.

La naturaleza de los ciberataques puede ser muy variada y evoluciona generando nuevas estrategias o mejoras en las existentes, por lo que al trabajar en medidas que mitiguen o eliminen el ataque de una forma eficaz se debe contar con personas, tecnología y procesos que lo acompañen. No considerar cualquiera de los aspectos antes mencionados implica que no se pueda brindar respuesta oportuna ante un incidente o ciberataque.

Comúnmente, las organizaciones invierten en tecnologías aisladas de protección, como pueden ser un antivirus o un dispositivo de red *firewall*, entre otras, considerando que con este tipo de herramientas se incrementan los niveles de seguridad. **Aunque este tipo de tecnologías contribuyen a la mejora, por sí solas no logran usualmente su objetivo.** Para comprender mejor el punto que estamos mencionando, podemos tomar como ejemplo los antivirus: una organización, a pedido del responsable del equipo de TI, adquiere una solución de antivirus corporativo para proteger los dispositivos como PCs, laptops o celulares de la organización. Esta medida en sí no garantiza que los dispositivos estén protegidos, simplemente implica contar con la herramienta, pero si, por ejemplo, no tenemos las personas para que puedan configurarla y desplegarla en todos los dispositivos de la organización, la medida no será suficiente y podrían quedar dispositivos sin protección que se conviertan en puntos vulnerables de entrada a la organización.

Ahora bien, **¿qué pasaría si días o semanas después de la instalación, el equipo técnico no contara con procesos y procedimientos de actualización y mantenimiento de la solución?** En este caso no serían capaces de detectar las nuevas firmas o virus, quedando los dispositivos sin protección alguna.

¹² Neveux, Ellen, 2021.

Por estas razones **la ciberseguridad necesita contar con un fuerte alineamiento estratégico, involucrar a toda la organización y ser gestionada de forma estructurada.** En este documento se verán distintas técnicas probadas de manera global que ayudarán a los líderes en la materia a realizarlo.

La realidad y el contexto de las organizaciones y sus servicios han ido mutando con el paso de los años. Hoy en particular, atravesando una

emergencia sanitaria, las instituciones de salud tienen que ofrecer sus servicios de forma rápida y accesible para un gran número de interesados.

Este fenómeno genera una exposición y abre a los posibles atacantes una numerosa variedad de brechas que ponen en riesgo la protección de los activos y la seguridad de las personas.

Estado del arte

En las últimas décadas se viene trabajando a nivel global en temas relacionados con la seguridad de la información y la ciberseguridad.

Si bien este trabajo tiene un fuerte componente técnico, fue acompañado con reglamentaciones y normativas que permiten la regulación tanto a nivel nacional como internacional.

Existen diferentes tipos de herramientas habituales y maduras que pueden ser utilizadas por los diferentes actores del ecosistema, ya sean reguladores, operadores o proveedores de servicios, entre otros. Podemos agrupar dichas herramientas en cuatro grupos: *frameworks*, controles, guías y marco regulatorio. Siempre es importante destacar que el uso conjunto de estas herramientas dará consistencia al sistema en su totalidad, desde la regulación, la implementación, la ejecución, y el control y monitoreo.

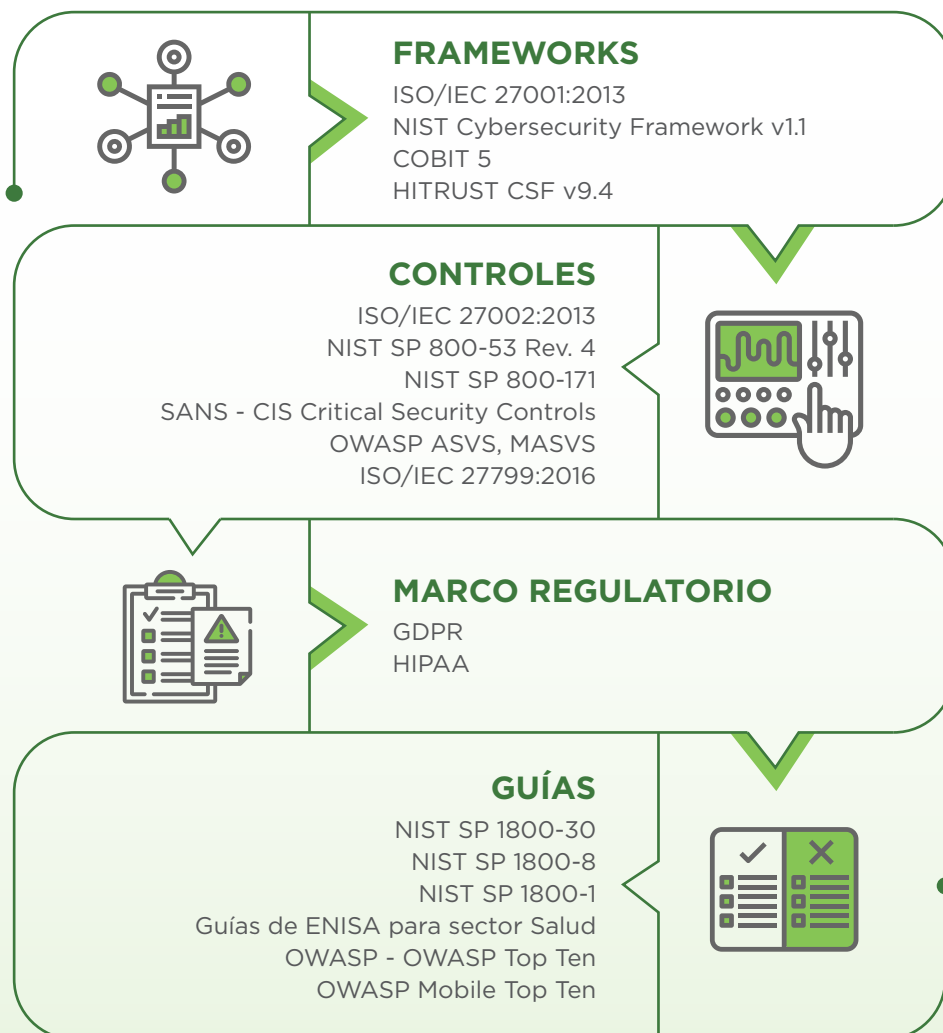
Los *frameworks* ponen a disposición de la organización **herramientas para desarrollar las distintas actividades de seguridad de la información de forma sistematizada y controlada.**

Los *frameworks* tienen enfoques diferentes, pero en general, brindan mecanismos para definir los objetivos de seguridad de la organización y los perfiles o niveles de madurez. Implementan un análisis de riesgo que define los controles que se deben implementar y que permite a las organizaciones tomar decisiones en los distintos niveles, ya sean técnicos, de gestión o de recursos para lograr dichos objetivos.

Los controles son medidas de seguridad técnicas o de gestión que tienen **la finalidad de conseguir determinados objetivos de seguridad de la información.** Por ejemplo, la publicación NIST SP 800-53 define actividades para garantizar la gestión de cuentas como parte de las medidas enfocadas en el control de acceso.

Por último, las guías son herramientas prácticas y abordan problemáticas específicas; por ejemplo, la guía NIST SP 1800-8 detalla cómo administrar activos, protegerse contra amenazas y mitigar vulnerabilidades en bombas de infusión inalámbricas y presentan conceptos útiles para abordar la temática de IoMT.

FIGURA 1 • Resumen de los principales *frameworks*, controles, normativa aplicable y guías



Dada la gran variedad de metodologías, estándares y buenas prácticas, uno de los principales desafíos es definir la *normativa aplicable*, los *frameworks*, *controles* y *guías* que se desean adoptar.

>> Framework

En este artículo nos centraremos en los cuatro *frameworks* de mayor adopción a nivel global¹³, tres de ellos para organizaciones en general y uno orientado al sector salud.

- **NIST-CSF¹⁴**

El *National Institute of Standard and Technology* (NIST) definió un marco que brinda medidas y controles a las organizaciones que suministran servicios críticos en Estados Unidos con el fin de identificar, evaluar y gestionar los riesgos de ciberseguridad.

Para esto define cinco funciones: identificar, proteger, detectar, responder y recuperar, que brindan una visión integral de la gestión de los riesgos de ciberseguridad. También define una comparativa con estándares y buenas prácticas de la industria.

FIGURA 2 • Framework de Ciberseguridad Versión 1.1



Fuente: <https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework>

Por otro lado, define niveles de implantación del marco que progresan desde el Nivel 1 (Parcial), Nivel 2 (Riesgo informado), Nivel 3 (Repetible) y Nivel 4 (Adaptable), para reflejar la gestión de los riesgos de ciberseguridad en función de los manejos de los riesgos en la organización.

Por último, define perfiles que identifican el estado actual de la organización (perfil actual) y el perfil objetivo, aquel lugar adonde quiere llegar la organización y que está alineado con los riesgos aceptados.

- **HITRUST CSF¹⁵**

HITRUST es una alianza creada en 2007 entre empresas internacionales como Google, AT&T o Amazon, entre otras. HITRUST CSF es un marco de privacidad y seguridad para organizaciones del sector salud. Tiene un enfoque basado en la gestión de riesgos de seguridad de la información y ofrece una panorámica clara del cumplimiento de la normativa aplicable a través de un mapeo, aunque la mayoría de las normas mapeadas no son aplicables para ALC. El CORE de HITRUST CSF se basa en las normas ISO/IEC 27001 y 27002. Define controles agrupados en categorías, aprovechando las categorías principales de las familias 27000 y agrega categorías específicas para evaluar un programa de gestión de seguridad de la información (SGSI) y gestión de riesgos.

HITRUST CSF permite a las organizaciones la posibilidad de certificarse con un agente externo que valide cómo está implementado y ejecutado su sistema de gestión de la seguridad de la información.

- **ISO/IEC 27001¹⁶**

La familia ISO 27000, creada por la *International Organization for Standardization*, es un estándar global para la seguridad de la información que especifica los requisitos necesarios para la implementación,

¹³ Ver Healthcare Information and Management System Society, HIMSS North America, 2018.

¹⁴ National Institute of Technical Standards (NIST), 2018 (a).

¹⁵ HITRUST, 2019.

¹⁶ International Standards Organization (ISO), 2013 (a).

mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La última versión existente durante la elaboración de este documento es la del año 2013, con correcciones en el año 2015, en la que se detallan 130 requerimientos.

Un punto importante a tener en cuenta es que esta familia de estándares permite a las organizaciones la posibilidad de certificarse con un agente externo que valide cómo está implementado y ejecutado su sistema de gestión de la seguridad de la información.

- **COBIT¹⁷**

La Asociación de Auditoría y Control de Sistemas de Información (ISACA) es una organización sin fines de lucro formada por más de 450.000 profesionales de más de 188 países y con diversos roles en tecnologías de la información. Uno de sus productos principales es COBIT (*Control Objectives for Information and Related Technologies*) del que actualmente están activas las versiones COBIT 5, del 2012, y COBIT 2019, del 2018.

COBIT es un marco de trabajo que tiene como objetivo asegurar una efectiva gobernanza de información y tecnologías. Si bien este *framework* no es específico para seguridad de la información, en su versión 2019 está alineado con diferentes *frameworks*, controles y guías de seguridad de la información. En particular, se alinea con la familia ISO/IEC 27000, NIST Cybersecurity Framework v1.1 y HITRUST® Common Security Framework, versión 9, de septiembre de 2017.

¹⁷ Information System Audit and Control Association (ISACA), 2019.

>> Controles

En este artículo nos centraremos en los seis grupos de controles más adoptados a nivel global, cinco de ellos para organizaciones en general y uno orientado al sector salud.

- **ISO/IEC**

Estas normas proporcionan directrices específicas que deben cumplir las organizaciones que desean implementar un sistema de gestión de seguridad de la información (SGSI).

Estos controles deben ser seleccionados por las organizaciones en función del nivel de aceptación del riesgo y la normativa aplicable.

- **ISO/IEC 27002¹⁸**

Esta norma fue publicada por primera vez en 2005. Hasta el año 2013 tuvo varias actualizaciones dependiendo el país y fueron realizadas correcciones en el año 2015. Su fin es brindar una guía con buenas prácticas que permitan mejorar el sistema de gestión de seguridad de la información de una organización a través de las categorías principales de seguridad (35) y controles específicos (114), agrupados en 14 cláusulas de control, tal como se muestra en la tabla 1.

Cada cláusula contiene una o más categorías de control y para cada una de ellas se define el objetivo y los controles necesarios para lograrlo. Esto se acompaña de una guía en donde se brindan directrices sobre cómo implementar dichos controles, así como información adicional de relevancia para el caso.

TABLA 1 • Cláusulas de control de la norma ISO/ICE 27002

Política de seguridad de la información	Seguridad de las operaciones
Organización de la seguridad de la información	Seguridad de las comunicaciones
Seguridad ligada a los recursos humanos	Adquisición, desarrollo y mantenimiento de los sistemas
Gestión de activos	Relaciones con los proveedores
Control de acceso	Gestión de incidentes de seguridad de la información
Criptografía	Aspectos de seguridad de la información en la gestión de la continuidad de negocio
Seguridad física y de ambiente	Cumplimiento

¹⁸ International Standards Organization (ISO), 2013 (b).

- **ISO/IEC 27799¹⁹**

Esta norma fue publicada en 2008 y actualizada en el 2016. A diferencia del resto de las normas, que son genéricas, la ISO/IEC 27799 ofrece una guía específica para implementar las mismas 14 cláusulas de control de la ISO/IEC 27002 (mostradas en la Tabla 1), pero para organizaciones del sector salud o que custodien datos de pacientes.

Más allá de que los datos personales son importantes y de que se debe resguardar su confidencialidad, integridad y disponibilidad, los datos de los pacientes, en particular, deben contar con resguardos adicionales ya que su afectación podría comprometer la seguridad física de las personas, razón por la que en la mayoría de los países son clasificados como información sensible y han de cumplir normativas específicas.

Otro punto importante es la disponibilidad de esa información puesto que para la eficiencia de la atención médica es crítico contar con dichos datos en cualquier situación y, en particular, durante desastres o emergencias. Por esta razón la guía aplica mayores restricciones a los controles y brinda información más precisa sobre cuál es la mejor manera de usarlos.

La norma ISO/IEC 27799 incluye 3 anexos. El primero hace referencia a las amenazas para la protección de la información de salud. El segundo anexo presenta un plan de acción práctico sobre cómo usar el estándar para implementar ISO/IEC 27002 en organizaciones del sector salud. El último anexo brinda una *checklist*

para realizar una autoevaluación de conformidad que sirve como apoyo a lo descrito en la cláusula de cumplimiento.

Para comprender con mayor claridad lo anteriormente mencionado consideremos el siguiente ejemplo: en el caso de la categoría de **Responsabilidad por los activos**, perteneciente a la cláusula de **Gestión de activos**, ambas normas tienen el objetivo de **identificar los activos de la organización y definir las responsabilidades de protección adecuadas**. Uno de los controles asociados es el Inventario de activos que, según especifica esta norma, debe cumplir los controles de definidos en ISO/IEC 27002:2013 8.1.1 y, adicionalmente, incorpora los siguientes controles:

- Contabilizar los activos de información de salud.
- Designar un custodio de esos activos de información de salud.
- Tener reglas de uso aceptable de estos activos que estén identificadas, documentadas e implementadas.

- **NIST**

El NIST realiza y actualiza publicaciones especiales en donde se define el catálogo de controles de seguridad y privacidad que deben cumplir todas las organizaciones federales y no gubernamentales de Estados Unidos, con el fin de gestionar los riesgos de seguridad de la información.

En particular, y asociado al *framework* de ciberseguridad (NIST-CSF) mencionado

¹⁹ International Standards Organization (ISO), 2016.

anteriormente en este documento, se destacan dos publicaciones: el NIST SP 800-53 y el NIST 800-171. Ambas publicaciones tienen como objetivo perfiles de empresas con características diferentes y comparten a grandes rasgos las principales familias de controles, aunque en distintos niveles de profundidad.

- **NIST SP 800-53²⁰**

Tuvo su última actualización en septiembre del 2020 generando el documento revisión número 5. El propósito de este documento es detallar las medidas que se deben implementar para salvaguardar los activos y la privacidad de las personas para los distintos tipos de sistemas y organizaciones federales.

El documento cuenta con tres capítulos. El primero es una introducción a la temática, el segundo describe los conceptos fundamentales sobre los controles de seguridad y privacidad, y el último profundiza en el catálogo de los controles. La tabla 2 detalla las 20 familias de controles propuestos.

Cada una de las familias de controles cuenta con un identificador de dos letras; por ejemplo, para control de acceso es AC. En cada familia se enumeran controles específicos; por ejemplo, AC-2 es gestión de cuentas. Para cada control se define una lista de actividades o tareas que se deben cumplir, que se enumeran en la lista ordenada (a, b, c, etc.). Este ejemplo se puede ver en la figura 3.

TABLA 2 • Familias de controles de la SP 800-53 del NIST

Control de acceso	Seguridad física y de ambiente
Entrenamiento y concientización	Planificación
Auditoría	Programa de gestión
Evaluación, autorización y seguimiento	Seguridad del personal
Gestión de configuración	Procesamiento y transparencia de datos personales identificables (PII)
Plan de contingencia	Evaluación de riesgos
Identificación y autenticación	Adquisición de sistemas y servicios
Respuesta a incidentes	Protección en los sistemas y comunicaciones
Mantenimiento	Integridad de los sistemas y la información
Protección de medios	Gestión de riesgo de la cadena de suministro

²⁰ National Institute of Technical Standards (NIST), 2020 (b).

FIGURA 3 • Gestión de cuentas de usuarios

AC-2	ACCOUNT MANAGEMENT
	Control:
	<ol style="list-style-type: none">Define and document the types of accounts allowed and specifically prohibited for use within the system;Assign account managers;Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;Specify:<ol style="list-style-type: none">Authorized users of the system;Group and role membership; andAccess authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];Monitor the use of accounts;Notify account managers and [Assignment: organization-defined personnel or roles] within:<ol style="list-style-type: none">[Assignment: organization-defined time period] when accounts are no longer required;[Assignment: organization-defined time period] when users are terminated or transferred; and[Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;Authorize access to the system based on:<ol style="list-style-type: none">A valid access authorization;Intended system usage; and[Assignment: organization-defined attributes (as required)];Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; andAlign account management processes with personnel termination and transfer processes.

Cada control tiene distintos apartados, como:

- Una explicación del control (*discussion*).
- Los controles relacionados (*related controls*).
- Un apartado de mejoras al control (*control enhancements*).

• **NIST SP 800-171²¹**

Fue liberado en febrero del 2020 generando el documento de revisión número 2, a su vez, actualizado en enero de 2021. En él se detallan las medidas a implementar para salvaguardar la información no clasificada (CUI, por sus siglas en inglés de *Controlled Unclassified Information*) para los distintos tipos de sistemas y organizaciones no federales. En el caso de la salud todos los documentos clínicos están dentro de esta clasificación.

²¹ National Institute of Technical Standards (NIST), 2020 (c).

El documento cuenta con tres capítulos. El primero es una introducción a la temática, el segundo describe los conceptos fundamentales sobre las 14 familias de controles de seguridad y en el último se profundiza en el catálogo de los controles. La tabla 3 detalla las 14 familias de controles propuestos. En cada una de las familias de controles se definen sub-controles agrupados en conjuntos de requerimientos básicos según la FIPS Publication 200²² y un segundo conjunto de requerimientos derivados de NIST 800-53. Por ejemplo, en la familia de control de acceso (figura 4) se entiende que limitar el acceso a los sistemas a usuarios autorizados es un requerimiento básico, mientras que emplear el principio de mínimo privilegio en las actividades que podrá realizar en dicho sistema o aplicación, en función de su responsabilidad para garantizar su actividad de negocio, se considera un requerimiento derivado.

Entre las principales diferencias encontradas en las publicaciones NIST SP 800-53 y NIST SP 800-171 está el nivel de profundidad que manejan algunas de las temáticas de suma importancia para las organizaciones. En particular, en la NIST SP 800-171 no se definen familias de controles para el plan de contingencia, el manejo de los datos personales (PII) o la gestión de riesgo de la cadena de suministro, entre otros.

Cuenta con varios anexos. El anexo D, en particular, mostrado en la figura 5, hace un mapeo de cada control con NIST 800-53 y con ISO/IEC 27001.

En el anexo E se explicita qué controles de la NIST SP 800-53 se deben implementar para cumplir los requerimientos básicos de la NIST SP 800-171.

TABLA 3 • Familias de controles de la SP 800-171 del NIST

Control de acceso	Protección de medios
Entrenamiento y concientización	Seguridad del personal
Auditoría	Protección física
Gestión de configuración	Evaluación de riesgos
Identificación y autenticación	Evaluación de seguridad
Respuesta a incidentes	Protección en los sistemas y comunicaciones
Mantenimiento	Integridad de los sistemas y la información

²² National Institute of Technical Standards (NIST), 2006.

FIGURA 4 • Control de acceso

3.1 ACCESS CONTROL	
Basic Security Requirements	
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.
Derived Security Requirements	
3.1.3	Control the flow of CUI in accordance with approved authorizations.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
3.1.8	Limit unsuccessful logon attempts.
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
3.1.11	Terminate (automatically) a user session after a defined condition.
3.1.12	Monitor and control remote access sessions.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
3.1.14	Route remote access via managed access control points.
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.

FIGURA 5 • Mapeo de controles - NIST 800-53 e ISO/IEC 27001

SECURITY REQUIREMENTS		NIST SP 800-53 Relevant Security Controls	ISO/IEC 27001 Relevant Security Controls
3.1 ACCESS CONTROL			
Basic Security Requirements			
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). 3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2	Account Management	A.9.2.1 User registration and de-registration
			A.9.2.2 User access provisioning
			A.9.2.3 Management of privileged access rights
			A.9.2.5 Review of user access rights
			A.9.2.6 Removal or adjustment of access rights
	AC-3	Access Enforcement	A.6.2.2 Teleworking
			A.9.1.2 Access to networks and network services
			A.9.4.1 Information access restriction
			A.9.4.4 Use of privileged utility programs
			A.9.4.5 Access control to program source code
			A.13.1.1 Network controls
			A.14.1.2 Securing application services on public networks
			A.14.1.3 Protecting application services transactions
			A.18.1.3 Protection of records

- **SANS CIS Critical Security Controls²³**

El Centro de Seguridad de Internet (CIS) es una organización independiente formada por expertos de TI de diferentes verticales de negocio. Su objetivo es promover las mejoras prácticas en ciberseguridad a nivel internacional.

En la versión 7.1 de *CIS Critical Security Controls* se definen un conjunto de controles (20) con buenas prácticas y acciones de defensa para mitigar los ataques más frecuentes a sistemas y redes. Dichos controles se organizan en tres grupos de implementación que se definen considerando, entre otros factores, la sensibilidad de los activos a proteger, el tamaño y la madurez de la organización.

Cada uno de ellos cuenta con una primera parte que explica la importancia de implementar el control y cuáles son sus implicaciones. Posteriormente aparece un conjunto de sub-controles en los que se detallan las distintas buenas prácticas asociadas a dicho

control y en qué grupo de implementación debe ser incluido. Por último, para cada caso se incluye un apartado con un diagrama de relaciones de entidades de sistemas, procedimientos y herramientas como apoyo a la ejecución de las distintas actividades.

La tabla 4 muestra cómo se presentan los controles y sub-controles en la versión 7.1 de CIS.

Analicemos, como ejemplo, el control 1: “Inventario y control de activos *hardware*”. Este control tiene 8 subcontroles, 5 de ellos para la función Identificar, 1 para Responder y 2 para Proteger. En el subcontrol 1.1 señala que se debe utilizar una herramienta de descubrimiento activo, proporciona una descripción detallada del mismo e indica que se debe incluir en los grupos de implementación 2 y 3. Recordemos que una herramienta de descubrimiento activo permite de manera proactiva, por medio de escaneos o técnicas similares, identificar equipos conectados a la red de la organización y actualizar el inventario de activos de *hardware*.

TABLA 4 • CIS Control 1: Inventario y control de activos *hardware*

CIS Control 1: Inventario y control de activos <i>hardware</i>							
Sub-control	Tipo de activo	Función de seguridad	Control	Descripción	Grupos de implementación		
1.1	Equipos	Identificar	Utilizar una herramienta de descubrimiento activo	Utilice una herramienta de descubrimiento activo para identificar equipos conectados a la red de la organización y actualizar el inventario de activos de <i>hardware</i> .		●	●
1.2	Equipos	Identificar	Utilizar una herramienta de descubrimiento pasivo de activos	Utilice una herramienta de descubrimiento pasivo para identificar dispositivos conectados a la red de la organización y actualizar automáticamente el inventario de activos.			●

²³ Centro de Seguridad de Internet (CIS), 2019.

- **OWASP ASVS²⁴ y MASVS²⁵**

Open Web Application Security Project (OWASP) es una fundación sin fines de lucro que trabaja para mejorar la seguridad de las aplicaciones web. Está compuesta por cientos de capítulos locales en todo el mundo y decenas de miles de miembros. OWASP genera múltiples proyectos de código abierto entre los que destacan el *Application Security Verification Standard (ASVS)* y *Mobile Application Security Verification Standard (MASVS)*. Estos proyectos para aplicaciones web o para dispositivos móviles, respectivamente, proveen una base para probar los controles técnicos de seguridad y también proporcionan a los desarrolladores una lista de requerimientos para desarrollo seguro.

Los posibles usos son:

- Como métricas, usando los controles y las pruebas sobre los mismos como criterios de evaluación.
- Como guía, usando los controles como guía para el desarrollo seguro.
- En la adquisición, usando los controles como requerimientos para evaluar el *software* o incluyéndose en los contratos.

²⁴ Open Web Application Security Project (OWASP), 2020 (a).

²⁵ Open Web Application Security Project (OWASP), 2020 (b).

>> Guías

La siguiente sección contiene una tabla con las principales guías aplicables en seguridad en

el sector salud. Esta tabla no es exhaustiva y su objetivo es servir de punto de partida para aquellos expertos que deseen profundizar en la materia.

TABLA 5 • Principales guías

Nombre de la guía	Descripción
NIST SP 1800-30 ²⁶	Guía práctica para una solución de telemedicina y monitoreo remoto de los pacientes (RPM).
NIST SP 1800-24 ²⁷	Guía sobre cómo proteger el ecosistema de imagenología, centrándose en los sistemas de comunicación y archivo de imágenes (PACS) en las organizaciones de prestación de servicios de salud (HDO).
NIST SP 1800-8 ²⁸	Guía detallada sobre cómo administrar activos, protegerse contra amenazas y mitigar vulnerabilidades en bombas de infusión inalámbricas. Se utiliza un enfoque de evaluación de riesgos, contempla los estándares de ciberseguridad actualmente disponibles y la ley HIPAA. Se basa en principios como defensa en profundidad. Si bien inicialmente parece estar enfocada a bombas de infusión inalámbricas, los conceptos vertidos son útiles para todo IoMT.
NIST SP 1800-1 ²⁹	Guía para protección de registros médicos en dispositivos móviles. Muestra cómo utilizar herramientas y tecnologías disponibles comercialmente, o de código abierto, que son consistentes con los estándares de ciberseguridad, para ayudar a las organizaciones que usan dispositivos móviles a compartir registros médicos electrónicos de manera más segura.
ENISA - Procurement Guidelines For Cybersecurity In Hospitals ³⁰	Guía para mejorar el ciclo de compra y apoyar en el cumplimiento de los objetivos de ciberseguridad en hospitales.
ENISA - Security and Resilience in eHealth Infrastructures and Services ³¹	Muestra el estado del arte e investiga el enfoque y los medios utilizados para proteger los sistemas de salud críticos en cada uno de los países miembros.
ENISA - Cyber security and resilience for Smart Hospitals ³²	Investiga y hace recomendaciones sobre los <i>smart hospitals</i> y sus problemas relacionados. Define los activos y clasifica sus amenazas, planteando escenarios de ataques en donde se analizan los efectos, la recuperación y las buenas prácticas.
ENISA - ICT security certification opportunities in the healthcare sector ³³	Investiga las directrices y regulaciones en la tecnología de la información en la salud y IoMT.
OWASP Top Ten ³⁴	Ranking de OWASP de los 10 riesgos más comunes en aplicaciones web.
OWASP Mobile Top Ten ³⁵	Ranking de OWASP de los 10 riesgos más comunes en aplicaciones para dispositivos móviles.

²⁶ National Institute of Technical Standards (NIST), 2021.

²⁷ National Institute of Technical Standards (NIST), 2020 (a).

²⁸ National Institute of Technical Standards (NIST), 2018 (c).

²⁹ National Institute of Technical Standards (NIST), 2018 (b).

³⁰ European Union Agency for Cybersecurity (ENISA), 2020.

³¹ European Union Agency for Cybersecurity (ENISA), 2015.

³² European Union Agency for Cybersecurity (ENISA), 2016.

³³ European Union Agency for Cybersecurity (ENISA), 2019.

³⁴ Open Web Application Security Project (OWASP), 2017.

³⁵ Open Web Application Security Project (OWASP), 2016.

>> Marco regulatorio

Existen normativas aplicables y/o de adopción que reglamentan el comportamiento y definen cómo deben actuar las organizaciones.

Con respecto a la seguridad de la información o ciberseguridad y, en particular, en el sector salud, existen normativas en función del país e, incluso, dependiendo de la ciudad o estado en el que se encuentra la organización.

Sin perjuicio de lo anterior, existen dos marcos regulatorios que en los últimos años han adquirido gran notoriedad a nivel global y han servido de inspiración para muchos países. Ambos tienen como objetivo reglamentar el uso de los datos de las personas físicas, definen cómo se deben tratar los datos, las responsabilidades ante un incidente de información y las multas por no cumplimiento, entre varios puntos. Se trata del Reglamento General de Protección de Datos (GDPR), de la Comunidad Europea³⁶, y la ley Health Information Privacy (HIPAA), de Estados Unidos de América³⁷.

El GDPR europeo tiene como alcance el tratamiento de datos de las personas físicas para organizaciones como empresas o sociedades que:

- Están establecidas en la Unión Europea (UE) independientemente de si el tratamiento de los datos se da o no allí.
- Ofrecen bienes o servicios a personas que se encuentran en la UE.

Esta reglamentación hace énfasis en que las organizaciones realicen un correcto análisis y evaluación de riesgos de los datos tratados durante todo su ciclo de vida, desde la captura hasta la destrucción de los mismos.

Las organizaciones serán responsables de garantizar a través de las medidas técnicas y organizativas, los derechos y las libertades de los individuos con respecto a sus datos. Entre varias definiciones, señala que se debe mantener informadas a las personas sobre el uso de sus datos con el fin de tener su consentimiento y notificar siempre que exista un posible caso de violación de la seguridad de sus datos.

En el caso del sector salud, se considera tratamiento de alto riesgo y, por ende, se definen actividades que las organizaciones deben cumplir, como, entre otras, realizar registros de actividad del tratamiento o definir roles específicos, como, por ejemplo, delegado de protección de datos (DPD). Existen actividades generales que siempre se deben cumplir, como la definición de políticas, planes de capacitación y concientización para las organizaciones, entre otras.

El objetivo del presente documento es hacer una introducción inicial a la temática y no un análisis completo de la normativa aplicable. Si bien la normativa descrita no es aplicable en ALC, consideramos importante introducirla pues ha sido usada como guía para la creación de leyes en los distintos países de esta región y, en los casos en que no existen, es deseable que las organizaciones la tengan como referencia. Para un análisis más profundo se puede tomar como insumo el *dashboard* (<https://socialdigital.iadb.org/en/sph/dashboard>) desarrollado por el BID en el que se presenta información sobre los marcos normativos a nivel nacional para la implementación de historias clínicas electrónicas (HCE) de 26 países de la región.

³⁶ El reglamento puede consultarse en Unión Europea, 2016 y en Comisión Europea (s.f.) puede consultarse información sobre las normas sobre protección de datos personales dentro y fuera de la UE.

³⁷ Para información relativa al "Health Insurance Portability and Accountability Act" puede consultarse el sitio respectivo del HHS en <https://www.hhs.gov/hipaa/index.html>.

7 pasos para la implementación de ciberseguridad

FIGURA 6 • 7 pasos para la implementación de ciberseguridad



Una vez descritas las diferentes herramientas disponibles para el desarrollo de la ciberseguridad en el sector, es importante enfocarnos en el proceso de implementación, que debe realizarse de una manera sistemática, estructurada y continua ya que el cambio no se conseguirá de la noche a la mañana.

Si bien existen diferentes abordajes para contemplar e incluir la seguridad de la información en una organización, proponemos una metodología simple cuyo objetivo es ser una guía estratégica para la dirección de la organización.

Presentamos un ciclo de mejora continua compuesto por 7 pasos y que se representa gráficamente en la figura 6.

A continuación, hacemos una breve descripción de cada uno de los pasos discutiendo sus implicaciones y beneficios para la organización:



INCLUIR LA CIBERSEGURIDAD COMO PRIORIDAD EN LA GESTIÓN ESTRATÉGICA DE LA ORGANIZACIÓN

Las organizaciones de salud tienen como fin salvar vidas. Para lograr este objetivo buscan garantizar la seguridad del paciente, lo que implica, entre tantas cosas, poner el foco en una adecuada gestión de la seguridad de la información y la ciberseguridad. Por esta razón la gestión estratégica de la organización debe incluir objetivos, metas e hitos que agreguen la ciberseguridad en la agenda de la organización. Un ejemplo puede ser que la institución defina como meta obtener la certificación ISO/IEC 27001 en los procesos críticos de la organización.



DEFINIR LA ESTRUCTURA ORGANIZACIONAL EN CIBERSEGURIDAD

Para cumplir los objetivos, metas e hitos definidos en el paso anterior y promover la gestión de la seguridad de la información, debe definirse una estructura organizacional adecuada que, como mínimo, establezca un responsable de seguridad de la información en la organización y un comité de seguridad de la información.

El comité de seguridad de la información deberá tener como sus principales objetivos:

- Definición de lineamientos estratégicos, junto con sus respectivos objetivos, metas e hitos anuales.
- Definición de responsabilidades generales.
- Definición, aprobación y seguimiento de políticas de seguridad de la información.
- Apoyo y seguimiento de los proyectos que se definirán en el Plan Director. Es responsabilidad del comité conseguir los recursos necesarios para que dichos proyectos tengan éxito.
- Ser el interlocutor y facilitador en materia de seguridad de la información para agentes externos a la organización.

Es recomendable que en esta etapa se defina con dicho comité toda la estructura de seguridad de la información. A modo de ilustración tomamos la gestión de la respuesta a incidentes, que se puede abordar de múltiples maneras como, por ejemplo, con un equipo de respuesta a incidentes, un centro de respuesta a incidentes centralizado o un centro de respuesta a incidentes descentralizado, entre otros. Para cada función de seguridad se debe definir la estructura que mejor se adapte a la organización y, para cada caso, también las dependencias jerárquicas, sus responsabilidades y la constitución del equipo con los perfiles asociados.



DEFINIR LOS OBJETIVOS Y LAS METAS DE CIBERSEGURIDAD

Se deben establecer claramente los objetivos y metas de seguridad de la información y ciberseguridad. En la definición de los mismos se deben tener en cuenta los objetivos organizacionales, como la necesidad de cumplimiento, la normativa nacional e internacional aplicables, las mejores prácticas de la industria y el perfil de riesgo organizacional. El perfil de riesgo organizacional se puede definir por varios factores entre los cuales destacan: el tamaño y recursos de la organización, la sensibilidad de los activos que maneja, el nivel de madurez actual y los umbrales aceptables de riesgo definidos. Es fundamental fijar las métricas e indicadores que se utilizarán para evaluar dichos objetivos y metas.



REALIZAR UN DIAGNÓSTICO DE SITUACIÓN CON ANÁLISIS DE BRECHAS O GAP

Una vez definidos los objetivos y las metas de seguridad de la información, se debe realizar un diagnóstico de la situación actual. Dicho análisis debe considerar las diferencias entre la situación actual y el objetivo (usualmente conocido como análisis de brechas o GAP).

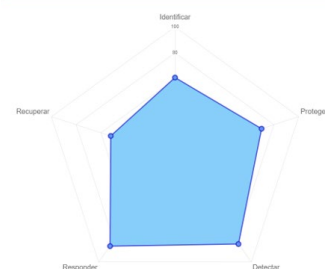
Dependiendo de los objetivos definidos, se pueden utilizar diferentes herramientas para la ejecución del diagnóstico. En caso de que se haya decidido adoptar un marco, se debe elaborar un análisis de brechas con el mismo, lo que puede efectuarse mediante consultorías especializadas o herramientas de evaluación (la mayoría de los marcos tienen herramientas de evaluación o autoevaluación).

Para los escenarios en los que se opta inicialmente por no adoptar un marco, el BID ha desarrollado diferentes herramientas para facilitar dicho diagnóstico. Entre ellas destaca una [herramienta de autoevaluación para el sector salud](#) (detallada en los anexos de este artículo), respecto a las mejores prácticas de la industria, y que está basada en el marco de ciberseguridad del NIST³⁸. Mediante un cuestionario simple



Inicio Ver resultado Eliminar datos Descargar datos Restaurar datos

Resultado de la autoevaluación de nivel AVANZADO.



Visite la herramienta: www.iadb.org/cibereval

esta herramienta ayuda a calcular las brechas y brinda recomendaciones que sirven como base para la elaboración del plan director.

Es importante incluir en el diagnóstico de situación un análisis de riesgos de seguridad de la información para priorizar entre las brechas detectadas los controles sugeridos y evaluar el riesgo remanente de aplicar dichos controles.



ELABORAR EL PLAN DIRECTOR DE CIBERSEGURIDAD

El responsable de seguridad de la información, con el apoyo y asesoramiento del comité de seguridad, deben elaborar un plan director. El plan debe incluir los objetivos de seguridad de la información, las metas específicas y un portafolio de proyectos y/o servicios. Debe reflejar con claridad el aporte de cada proyecto y/o servicio a las metas previamente definidas, y cómo se llega al resultado a través del logro de los distintos hitos definidos, junto a los indicadores de gestión para los proyectos y los servicios que permitan monitorear las variables estratégicas. Para asegurar la viabilidad del plan se deben incluir los costos estimados para los proyectos y/o servicios, incorporando la forma de financiamiento. Por último, se recomienda que el plan

³⁸ National Institute of Technical Standards (NIST), 2018 (a).

contemple la gestión de riesgos asociados a los proyectos y/o servicios.



EJECUTAR EL PLAN DIRECTOR

En esta etapa se busca hacer un monitoreo integral del plan director para asegurar su éxito. El responsable de seguridad de la información debe realizar un seguimiento de la ejecución del plan, analizando los indicadores de gestión y riesgos asociados, y debe informar al comité sobre cualquier desvío mayor con el fin de definir las medidas correctivas necesarias y los recursos correspondientes.



EVALUAR LOS RESULTADOS Y EL RIESGO REMANENTE

Los resultados obtenidos de la ejecución del plan deben ser evaluados de forma periódica analizando el impacto del mismo en la organización. En función de dicha evaluación se debe efectuar un análisis del estado de la situación, considerando los riesgos remanentes y, según el resultado, comenzar nuevamente el ciclo de mejora continua, volviendo al paso 4. Con una periodicidad mayor y ante cambios en la realidad de la organización, se necesita revisar la visión estratégica, ante lo que se debe comenzar nuevamente el ciclo de mejora continua, con el paso 1.

Recomendaciones y reflexiones finales

Las organizaciones de salud se han visto expuestas en las últimas décadas a numerosos ataques que han afectado la disponibilidad de sus servicios y la confidencialidad de los datos personales y clínicos de los pacientes. Por esta razón las organizaciones han visto la necesidad de priorizar y embarcarse en los temas de ciberseguridad. En este documento recomendamos que las organizaciones comiencen con un abordaje estratégico integral, como el sugerido en la sección “7 pasos para la implementación de ciberseguridad”.

Si bien los 7 pasos brindan un abordaje integral, **es recomendable revisar la metodología propuesta según el nivel de madurez de la organización.** Cada organización debe analizar si existe una estrategia que gradúe el nivel de profundidad en cada paso y con esto se logre un plan de mejora continua para llegar al nivel deseado por la organización a largo plazo.

Los 7 pasos están basados en la experiencia del equipo aplicando las mejores prácticas de la industria y está alineado con los marcos de trabajo (o *frameworks*) internacionales. Para lograr una implementación eficaz, eficiente y sostenible de la ciberseguridad en la organización, es importante que esta adopte un marco de trabajo de referencia y cuente con una estructura organizacional que le dé sustento. Como se presenta en el paso 2, es necesario definir roles claves como, por ejemplo, el CISO, el comité de seguridad de la información y las responsabilidades de ciberseguridad para todo el personal. En este contexto, uno de los principales desafíos que enfrentan las organizaciones

es elegir qué metodologías, estándares y buenas prácticas seguir en materia de seguridad de la información.

Dentro de la definición de los objetivos y metas de seguridad de la información y la ciberseguridad, la organización debe definir si necesita o desea tener una certificación; este punto guía la definición de qué marco de trabajo puede ser el más adecuado.

Consideramos que una muy buena opción es adoptar el NIST-CSF. El NIST-CSF plantea un enfoque basado en mejorar las medidas y controles de ciberseguridad, por lo que permite una rápida implementación y produce resultados medibles en el corto plazo; desde su diseño busca conseguir un balance adecuado de costos y resultados.

En caso de que la organización tenga necesidades de certificación, recomendamos la adopción de la familia de normas ISO/IEC 27000 o HITRUST CSF. Ambas sirven de guía para la adopción de un sistema de gestión de seguridad de la información. La ventaja de adoptar la familia de normas ISO/IEC 27000 es que, al ser un estándar de uso general (no particular para el sector salud), tiene un amplio nivel de penetración en las organizaciones y, por ende, resulta más fácil conseguir los recursos humanos para la adopción. En cambio, el HITRUST CSF es un estándar adaptado para el sector salud, lo que resulta ventajoso pues evita tener que adaptar algo de uso general a un sector específico.

Dependiendo del marco de trabajo seleccionado, se debe definir el conjunto de controles que se desea implementar. Todos los conjuntos de controles presentan niveles según los requerimientos y objetivos de seguridad de la información de la organización.

En el caso de utilizar el NIST-CSF recomendamos evaluar la adopción de los controles especificados en la publicación especial NIST SP 800-171 r2, dado que son los controles mínimos recomendados para organizaciones de salud.

Si se ha decidido alinearse con la familia de normas ISO/IEC 27000, recomendamos evaluar la adopción de los controles especificados para el sector salud en la norma ISO/IEC 27799. Si se optó por la alineación con HITRUST CSF, recomendamos utilizar los controles que el mismo define.

Sin perjuicio de lo anteriormente mencionado, cada organización debe tomar sus propias decisiones considerando aspectos como la complejidad de su adopción en la organización. Si la situación organizacional no acompaña la implementación de lo recomendado previamente, mientras se trabaja para construir dicha sinergia, sugerimos buscar otro enfoque e ir adoptando medidas técnicas. Para esto recomendamos utilizar estándares y guías con enfoque práctico como, por ejemplo, CIS Critical Security Controls.

Por último, pero no menos importante, para casos particulares se debe contemplar el uso de otro tipo de controles específicos como, por ejemplo, OWASP ASVS y MASVS para la especificación de requisitos de seguridad en aplicaciones o guías específicas de organismos internacionales como ENISA o NIST para temas tales como IoMT.

En ALC se están dando grandes pasos en la concientización en ciberseguridad, lo que está impulsando cambios normativos y regulatorios.

Si bien cada país está generando sus propias leyes, la mayoría toman como insumo experiencias previas, en particular HIPAA y GDPR. Por ello es importante ir definiendo medidas y controles compatibles con HIPAA y GDPR ya que esto contribuye con el cumplimiento de regulaciones locales e internacionales, actuales y futuras.

Por todo lo expuesto anteriormente, consideramos que la próxima década impulsará la adopción de buenas prácticas en materia de seguridad de la información a nivel organizacional y gubernamental en diferentes sectores críticos y, en particular, tendrá un gran impacto en el sector salud en ALC.

Agradecimientos



Cristina Pombo, Jennifer Nelson y Pablo Orefice.

Referencias bibliográficas

- **Carvajal, Víctor y Jara, Matías, 2016:** “Grave falla en la red del Minsal dejó expuesta información confidencial de pacientes”, CIPER, 5 de marzo de 2016, disponible en <https://www.ciperchile.cl/2016/03/05/grave-falla-en-la-red-del-minsal-dejo-expuesta-informacion-confidencial-de-pacientes/>.
- **Centro de Seguridad de Internet (CIS), 2019:** “CIS Critical Security Controls. Versión 7.1”, disponible en <https://www.sans.org/critical-security-controls>.
- **Clarín Tecnología, 2018:** “Ciberdelito. Pagan miles de dólares en criptomonedas para recuperar historias clínicas robadas”, en Clarin.com, 27 de enero de 2018, disponible en https://www.clarin.com/tecnologia/pagan-miles-dolares-criptomonedas-recuperar-historias-clinicas-robadas_0_ByjjB7qSM.html.
- **Comisión Europea, s.f.:** “Protección de datos. Normas sobre protección de datos personales dentro y fuera de la UE”, disponible en https://ec.europa.eu/info/law/law-topic/data-protection_es.
- **DataBreaches.net. The Office of Inadequate Security, 2018:** “Telemedicine company exposed data of more than 2 millions patients in Mexico”, 8 de agosto de 2018, disponible en <https://www.databreaches.net/telemedicine-company-exposed-data-of-more-than-2-millions-patients-in-mexico/>.
- **European Union Agency for Cybersecurity (ENISA), 2015:** “Security and Resilience in eHealth Infrastructures and Services”, disponible en <https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services>.
- **European Union Agency for Cybersecurity (ENISA), 2016:** “Cyber security and resilience for Smart Hospitals”, disponible en <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals>.
- **European Union Agency for Cybersecurity (ENISA), 2019:** “ICT security certification opportunities in the healthcare sector”, disponible en <https://www.enisa.europa.eu/publications/healthcare-certification>.
- **European Union Agency for Cybersecurity (ENISA), 2020:** “Procurement Guidelines for Cybersecurity in Hospitals”, disponible en <https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services>.
- **Healthcare Information and Management System Society (HIMSS), HIMSS North America, 2018:** “2018 HIMSS Cybersecurity Survey”, disponible en https://www.himss.org/sites/hde/files/d7/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf.

- **HITRUST, 2019:** “HITRUST Cybersecurity Framework”, disponible <https://hitrustalliance.net/product-tool/hitrust-csf/>.
- **IBM, 2020:** “Cost of a Data Breach Report 2020”, disponible en <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/>.
- **Information System Audit and Control Association (ISACA), 2019:** “COBIT 2019”, disponible en <https://www.isaca.org/resources/cobit>.
- **Information System Audit and Control Association (ISACA), 2019 (b):** “COBIT 5 Implementation”, disponible en <https://www.isaca.org/resources/cobit>.
- **International Standards Organization (ISO), 2013 (a):** “ISO/IEC 27001. Information Security Management”, technical standard, disponible en <https://www.iso.org/isoiec-27001-information-security.html>.
- **International Standards Organization (ISO), 2013 (b):** “ISO/IEC 27002. Code of Practice for Information Security Controls”, technical standard, disponible en <https://iso.org/standard/54533.html>.
- **International Standards Organization (ISO), 2016:** “ISO/IEC 27799 Health informatics. Information security management in health using ISO/IEC 27002”, technical standard, disponible en <https://www.iso.org/standard/62777.html>.
- **National Institute of Technical Standards (NIST), 2006:** “FIPS-200. Minimum Security Requirements for Federal Information and Information Systems”, disponible en <https://csrc.nist.gov/publications/detail/fips/200/final>.
- **National Institute of Technical Standards (NIST), 2018 (a):** “Framework for improving Critical Infrastructure Cybersecurity. Version 1.1”, disponible en <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
- **National Institute of Technical Standards (NIST), 2018 (b):** “SP1800-1. Securing Electronic Health Records on Mobile Devices”, disponible en <https://csrc.nist.gov/publications/detail/sp/1800-1/final>.
- **National Institute of Technical Standards (NIST), 2018 (c):** “SP1800-8. Securing Wireless Infusion Pumps in Healthcare Delivery Organizations”, disponible en <https://csrc.nist.gov/publications/detail/sp/1800-8/final>.
- **National Institute of Technical Standards (NIST), 2020 (a):** “SP1800-24. Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector”, disponible en <https://csrc.nist.gov/publications/detail/sp/1800-24/final>.
- **National Institute of Technical Standards (NIST), 2020 (b):** “NIST Special Publications 800-53, revision 5. Security and Privacy Controls for Information Systems and Organizations”, disponible en <https://nvd.nist.gov/800-53>.
- **National Institute of Technical Standards (NIST), 2020 (c):** “NIST Special Publications SP 800-171, revision 2. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”, disponible en <https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>.
- **National Institute of Technical Standards (NIST), 2021:** “SP1800-30. Securing Telehealth Remote Patient Monitoring Ecosystem (2nd Draft)”, disponible en <https://csrc.nist.gov/publications/detail/sp/1800-30/draft>.
- **Neveux, Ellen, 2021:** “Hackers, breaches, and the value of healthcare data”, disponible en <https://www.securelink.com/blog/healthcare-data-new-prize-hackers/>.
- **Open Web Application Security Project (OWASP), 2016:** “Top 10 Mobile Application Security Risks”, disponible en <https://owasp.org/www-project-mobile-top-10/>.

- **Open Web Application Security Project (OWASP), 2017:** “Top 10 Web Application Security Risks”, disponible en <https://owasp.org/www-project-top-ten/>.
- **Open Web Application Security Project (OWASP), 2020 (a):** “OWASP Application Security Verification Standard (ASVS) version 4.0.2”, disponible en <https://owasp.org/www-project-application-security-verification-standard/>.
- **Open Web Application Security Project (OWASP), 2020 (b):** “OWASP Mobile Application Security Verification Standard (MASVS) version 1.3”, disponible en <https://github.com/OWASP/owasp-masvs>.
- **UK Department of Health & Social Care, 2018:** “Securing cyber resilience in health and care. Progress update, October 2018”, disponible en https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf.
- **Unión Europea, 2016:** “Reglamento General de Protección de Datos. Y listado de empresas de protección de datos”, disponible en <https://rgpd.es/>.
- **U.S. Department of Health & Human Services, s.f.:** “Health Information Privacy”, disponible en <https://www.hhs.gov/hipaa/index.html>.
- **Verizon, 2020:** “Verizon 2020 Data Breach Investigations Report”, disponible en <https://enterprise.verizon.com/en-gb/resources/reports/dbir/2020/data-breach-statistics-by-industry/>.

