Ciberseguridad en el sector salud: un compromiso moral, legal y de sostenibilidad

"Cuando las barbas de tu vecino veas cortar, pon las tuyas a remojar". Así reza un antiguo refrán en un llamado a la precaución y a la prevención cuando alguien cercano experimenta una desgracia: debemos prepararnos para que no nos suceda lo mismo. Esta recomendación es oportuna ante la posibilidad de sufrir un ciberataque en las entidades del sector salud, similar en mayor o menor medida a los que ya han impactado a varias entidades del sector, públicas y privadas, en Colombia y en el mundo entero.

El desarrollo y la masificación en el uso de las tecnologías de la información y las comunicaciones (TIC) en los últimos años, así como la digitalización que convierte procesos analógicos y objetos físicos al formato digital, han encauzado la transformación digital o proceso mediante el cual una organización integra tecnología digital a todas las áreas empresariales. Desde el 2020, con la irrupción de la pandemia por COVID-19, se aceleró la digitalización de nuestras sociedades en el diario vivir.

Sin embargo, a la par del gran salto tecnológico y del desarrollo de nuevas capacidades y oportunidades en todas las esferas, automáticamente crecieron en forma exponencial los riesgos y vulnerabilidades en el ciberespacio, lo que ha aumentado la posibilidad de ser objeto de un ciberataque. Según cifras de TicTac (2022), cada minuto la economía mundial pierde USD 11,4 millones por delitos asociados con el cibercrimen. Se estima que en 2015 el costo global del cibercrimen ascendió a USD 10,5 billones. Además, para el 2031 se calcula que habrá un ataque de *ransomware* cada dos segundos a negocios, usuarios o dispositivos. Por otra parte, Surfshark (2022), en su estudio *"Cybercrime statistics"*, presenta un panorama de ciberdelincuencia a nivel global, en el que afirma que en países como Estados Unidos, Irán, Israel, Emiratos Árabes y Qatar el 50 % de los correos electrónicos de cada 100 usuarios son vulnerados por ciberdelincuentes.

Cuando en el horizonte de la humanidad irrumpió la pandemia, el sector salud tuvo que responder a obstáculos y desafíos innumerables, pero también a oportunidades de digitalización y transformación digital en su quehacer. Esto trajo consigo la ocurrencia de ciberataques y brechas de seguridad de la información. De

acuerdo con el estudio *"Healthcare breaches on the rise in 2022"*, hubo un aumento del 84 % de ciberataques en el sector en los últimos tres años. Asimismo, según el *Cyber Security Report* 2023, de Check Point Software, en 2022 el sector salud a nivel global registró 74 % más ciberataques que en 2021, el aumento más alto de incidentes de todas las industrias.

También se observa a nivel internacional un uso creciente de nuevas tecnologías en el sector salud, en particular el internet de las cosas médicas *(Internet of Medical Things* IoMT). Esto representa nuevos desafíos para el sector y nuevos riesgos con posibles impactos en la seguridad de los pacientes. Si bien se considera bajo el índice de penetración del IoMT en América Latina y el Caribe (ALC), se cree que la situación revertirá en los próximos años y el sector deberá prepararse para afrontar nuevos retos.

La información de las empresas y los sistemas que la almacenan y procesan son activos clave de las organizaciones. Además, en el sector salud en particular se utiliza información personal muy sensible, altamente codiciada por los ciberdelincuentes, debido a su alto valor en el mercado negro. Según el BID (2021), los Datos Personales de Salud 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. Por eso, la ciberseguridad es un asunto que debe involucrar a toda la organización, desde la alta dirección hasta el último

empleado. Se trata del único medio para proteger la empresa y su futuro.

Para entender la urgencia de una acción de ciberseguridad en el sector salud, se presenta el caso de *WannaCry* en 2017 en el Reino Unido, que interrumpió los servicios en un tercio de los hospitales y alrededor del 8 % de las consultas de medicina general, lo que causó unas 19.000 citas canceladas. Si bien es difícil estimar los costos de tecnologías de la información (TI), se calcula un costo de 19 millones de libras por cancelación de citas y de 73 millones de libras invertidos en los meses siguientes en soporte o consultores para restaurar datos y sistemas afectados en el ataque.

WannaCry es un *ransomware* surgido en mayo de 2017 para Microsoft Windows, que afectó 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. Este cifraba los archivos de la víctima, los retenía y pedía un rescate en bitcoins

La tecnología de la información en red existente en los hospitales permite intercambiar datos con rapidez y llevar a cabo procesos automatizados; sin embargo, al mismo tiempo eleva el riesgo de sufrir ataques por ciberdelincuentes.

para liberarlos. Utilizó vulnerabilidades conocidas de Microsoft Windows (Eternal-Blue y DoblePulsar), que tenían un parche liberado dos meses antes, por lo que el caso se podía evitar si los sistemas operativos estaban actualizados. La recomendación es siempre no ceder a la extorsión y nunca pagar a los cibercriminales.

Hasta Colombia llegaron los efectos del *WannaCry* que afectó la ciberseguridad mundial el 12 de mayo de 2017: el Instituto Nacional de Salud detectó rastros del código malicioso en cuatro de sus servidores, por lo que de inmediato acogió la recomendación de la cartera TIC y suspendió los servicios de su página web hasta el 15 de mayo como medida de prevención. La decisión no tuvo efectos significativos en la mayoría de los servicios, excepto en el de trasplantes, ya que la Red Nacional que centraliza la ubicación, asignación y los turnos de los trasplantes en el país usa los recursos del Instituto. Mientras retornó la normalidad, el servicio se prestó por vía telefónica.

Con el caso *WannaCry* se detectó que un blanco favorito de los ciberdelincuentes son los hospitales. La tecnología de la información en red existente en los hospitales permite intercambiar datos con rapidez y llevar a cabo procesos automatizados; sin embargo, al mismo tiempo eleva el riesgo de sufrir ataques por ciberdelincuentes. En los últimos años, aumentó el registro de ataques a la estructura digital de hospitales de todo el mundo. Dos ejemplos de febrero de 2016 fueron los siguientes:

- El Hollywood Presbyterian Medical Center de los Ángeles (EU), afectado por un *ransomware,* tuvo que pagar un rescate para liberar sus sistemas informáticos. Según declaraciones de sus directivas, se pagaron 40 bitcoins con un valor equivalente a unos 15.000 euros en ese momento. Los sistemas afectados volvieron a estar operativos después de una semana de cierre.

- Cuando los hospitales de Alemania recibieron ataques, se vieron obligados a utilizar métodos del siglo pasado: los datos de los pacientes se anotaban con papel y bolígrafo; los documentos se enviaban por fax y los pacientes tenían que recoger los resultados de las pruebas en persona, en lugar de recibirlos por correo electrónico.

De ahí que, si bien la digitalización y la transformación digital son claves para acelerar la recuperación económica y social, para impulsar el crecimiento inclusivo y sostenible en la postpandemia, también se convierte en una urgencia la implantación de la ciberseguridad como un componente esencial de la administración y la gestión estratégica en las organizaciones.

Para Microsoft, la ciberseguridad, también conocida como seguridad digital, es la práctica de proteger su información digital, dispositivos y activos; para Cisco, la ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Para el BID (2021), 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.

PROGRAMA DE OPTIMIZACIÓN DE LA HEMOSTASIA

El **P**rograma de **O**ptimización de la **H**emostasia o **HOP** por sus siglas en inglés está diseñado para mejorar la utilización de hemostáticos adyuvantes a través de un enfoque sistemático.

Proporciona orientación sobre la selección del hemostático adyuvante adecuado para la situación y sitio del sangrado concretos.

GESTIÓN DEL CRECIMIENTO

- Estandarización de proveedores
- Utilización de producto
- Consolidación del producto

SUS BENEFICIOS

1

Hasta 4 días
en promedio de reducción en la estancia hospitalaria.[1,2]

Hasta 25 minutos
podría reducirse el tiempo en quirófano.[2,3]

Hasta 40%
menos pacientes, podrían requerir una transfusión.[4-12]

2

El HOP se basa en un estudio cuantitativo y cualitativo a gran escala realizado por ETHICON en el cual se analizaron: [9]

11 ESPECIALIDADES
450 CIRUJANOS
7.864 SITUACIONES DE SANGRADO

3

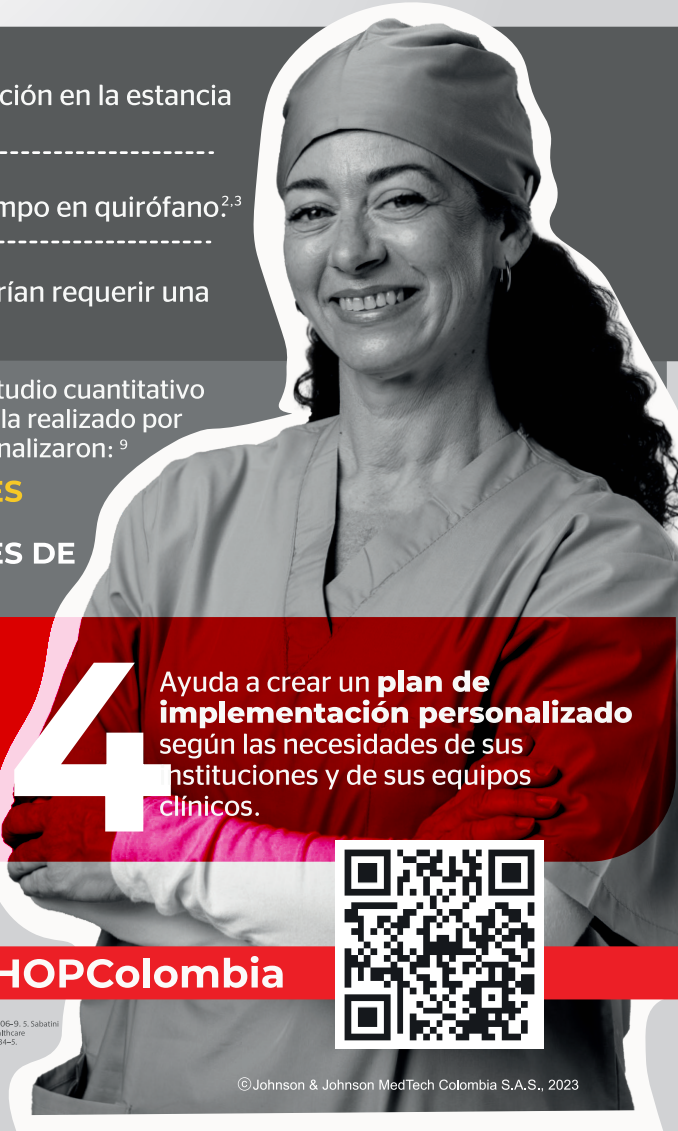
Beneficios del mundo real
(Instituciones de US)

15% de reducción en el costo invertido por cada hemostático.[9]

168.688 dólares de ahorro anual.[9]

4

Ayuda a crear un **plan de implementación personalizado** según las necesidades de sus instituciones y de sus equipos clínicos.



SUSCRÍBASE AL Programa de Optimización de la Hemostasia
Un enfoque sistemático para el control del sangrado

EN Ethicon.com/ProgramaHOPColombia

Referencias:
1.Notarnicola A et al. Blood Coagul Fibrinolysis. 2012;23(4):278–84. 2. Dancey AL et al. Plast Reconstr Surg. 2010;125(5):1309–17. 3. Pan HW et al. Ophthalmology.2011;118(6):1049–54. 4. Molloy DO et al. J Bone Joint Surg Br. 2007;89(3):306–9. 5. Sabatini et al. J OrthopTraumatol.2012; 13 (3): 145–151. 6. Wang et al. J Bone Joint Surg. 2001. 83-A (10): 1503 1505. 7. Randelli et al. Int J Immunopathol Pharmacol. 2013; 26 (1): 189–97. 8. Joseph et al. Eur J Vasc Endovasc Surg. 2004; 27, 540–552. 9. Ferko N et al. Healthcare Purchasing News. 2017; 41(11): 34–5. 10. Levy J et al. Anesth Analg. 2010;110(2): 354–64. 11. Liu L et al. PLoS One. 2013;8(5): e64261. 12. Massin P et al. Orthop Traumatol Surg Res. 2012;98(2): 180–5. 13. Ferko N et al. Healthcare Purchasing News. 2017;41(11):34–5.

ETHICON Johnson & Johnson SURGICAL TECHNOLOGIES

Programa de Optimización de la Hemostasia
Un enfoque sistemático para el control del sangrado

En Colombia aumentan los ciberataques de manera exponencial

Dado el aumento exponencial del fenómeno, un ciberataque puede representar una caja de Pandora para su organización. En estos momentos, mientras lee este informe, Usted a título personal o su empresa a escala institucional puede estar siendo víctimas de un ciberataque. No en balde la ciberseguridad pasó a ocupar un lugar preponderante entre las preocupaciones del mundo y a posicionarse en los primeros lugares entre los riesgos que se deben atender con urgencia en los próximos años. Por lo general, los ciberataques apuntan a acceder, modificar o destruir la información confidencial, extorsionar a los usuarios o interrumpir la continuidad del negocio. Actualmente, la implementación de medidas de seguridad digital se debe a que hay más dispositivos conectados que personas y los atacantes son cada vez más creativos.

Según la Cámara Colombiana de Informática y Telecomunicaciones, las denuncias por delitos informáticos se incrementaron en un 30 % en 2022 con respecto a 2021, y aunque la ciberseguridad se está convirtiendo en un tema prioritario para las empresas del país, cada vez son más las afectadas por ataques informáticos sin importar su tamaño o sector al que pertenezca.

La directora de la Dijín de la Policía, Olga Salazar, informó que en 2022 se bloquearon más de 20.000 páginas relacionadas con delitos cibernéticos. Asimismo, según el Centro Cibernético de la Policía, tan solo en 2023 el hurto vía medios informáticos tuvo un incremento del 1,8 % en todo el país con más de 20.000 casos, la transferencia no consentida de activos, con al menos 2.525 denuncias, y la suplantación de sitios web registra 3.346 casos. Bogotá concentra cerca del 32 % de los ciberdelitos registrados en 2023 en todo el territorio nacional, con 14.590 denuncias; le sigue Medellín, con más de 3.000 casos, y Cali, con por lo menos 2.500 denuncias.

Colombia y Brasil son los países de Latinoamérica que aparecen en el listado de los diez países del mundo con más ataques de *ransomware* en 2022, según el informe "Amenazas Cibernéticas 2023" de la empresa SonicWall, alertando sobre la importancia de la ciberseguridad para las organizaciones colombianas de todas las industrias en 2023.

En las últimas décadas se trabaja a nivel global en temas relacionados con la seguridad de la información y la ciberseguridad. En América Latina y el Caribe (ALC) se están dando grandes pasos en la concientización en ciberseguridad, lo que impulsa cambios normativos y regulatorios. Si bien cada país genera sus propias leyes, la mayoría toma como insumo experiencias previas y el Reglamento General de Protección de Datos (GDPR).

Existen dos marcos regulatorios de gran notoriedad a nivel global que han inspirado normas en muchos países. Ambos tienen como objetivo reglamentar el uso de los datos de las personas físicas, y definen cómo tratar los datos, responsabilidades ante un incidente de información y multas por incumplimiento, entre otros puntos. Se trata del Reglamento General de Protección de Datos (GDPR) de la Comunidad Europea y la ley *Health Information Privacy* (HIPAA) de Estados Unidos.

Por ello, es importante definir medidas y controles compatibles con HIPAA y GDPR, ya que esto contribuye al cumplimiento de regulaciones locales e internacionales, actuales y futuras. Se estima 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.

De acuerdo con reportes de la compañía de ciberseguridad LUMU, Colombia registró un incremento en 2022 de 133 %, comparado con 2021 en el número de empresas afectadas por *ransomware* y, aunque algunas tomaron cartas en el asunto, varias empresas afectadas aún no han podido recuperar el control de sus sistemas. En el sector salud fueron afectadas con tipos de *ransomware* algunas como: Salud Total, Procaps Laboratorios, Famisanar, Red de Salud de Ladera, Invima, Clínica Laura, Comfacundi y Keralty (Sanitas).

Si bien la ciberseguridad como tal se desarrolla desde hace varias décadas, su implementación no es todavía de uso común en el sector salud. Los ciberataques en el sector salud pueden impactar la continuidad de la atención a los usuarios o la imagen de las organizaciones. Es importante aclarar que todos los días se presentan ciberataques, algunos son efectivos y, en realidad, no es una sospecha que las organizaciones van a ser atacadas, sino que se trata de una certeza, por lo que la indicación obligada es estar preparado. Sin duda, la clave es prevención, prevención y prevención.

En el libro *Análisis de la Industria de la Ciberseguridad en Colombia*, se afirma que el tamaño del mercado de la ciberseguridad en Colombia alcanzó un valor de 243,86 millones de dólares en 2022. Además, indica que, durante el período de pronóstico de 2023-2028, se anticipa que el mercado refuerce a una CAGR del 14,70 % impulsado por la transformación digital de los segmentos industriales para la privacidad y protección de datos.

De acuerdo con información consignada en el Proyecto de Ley 010 de 2023-Senado, que se tramita actualmente en el Congreso de la República, Colombia es el segundo país de América Latina que recibe más ciberataques, solo superado por Brasil (IBM, 2022), y se encuentra en el puesto 69 del *ranking* global que mide el nivel de seguridad cibernética de los países (NCIS, 2022). Esta situación evidencia falencias en su política de ciberseguridad, como se detalla en la tabla 1.

Tabla 1. Nivel de seguridad cibernética en Colombia

Indicador	Porcentaje
Desarrollo de política de ciberseguridad	29 %
Análisis e información de amenazas de ciberataques	40 %
Educación y desarrollo profesional	67 %
Contribución a la ciberseguridad global	33 %
Protección de sus servicios digitales	0 %
Protección de sus servicios esenciales	17 %
Identificación digital y servicios de confianza	78 %
Protección de datos personales	100 %
Respuesta a ciberataques	50 %
Manejo de crisis cibernéticas	20 %
Operaciones militares en materia de ciberseguridad	67 %

Nota. Proyecto de Ley 010 de 2023-Senado. Elaboración propia con información del *National Security Index* (2022).

También se indica en el proyecto que, desde el 2022, el número de ataques cibernéticos en Colombia aumentó considerablemente en comparación con años anteriores. Según Fortinet (2023), el país en 2022 recibió 20.000 millones de intentos de ciberataques, lo que representa un crecimiento del 80 % frente a 2021. Dicho incremento va en consonancia con el panorama mundial pues, según el Informe de Riesgos Globales del Foro Económico Mundial (2023), los delitos cibernéticos aumentaron un 600 % después de la pandemia y es la octava amenaza mundial en términos de mayor impacto a la que se enfrenta hoy la humanidad.

Importantes infraestructuras críticas del Estado, tanto públicas como privadas, han sido víctimas de ciberataques y del robo masivo de información en el último año. Por ejemplo, Colsanitas (Grupo Keralty) perdió 0,7 terabytes de información incluyendo estados financieros, balances, presupuestos e información personal de sus usuarios (Portafolio, 2022); el Invima fue víctima de

La Fiscalía General de la Nación sufrió un ataque cibernético en el cual más de 10 TB de información sensible, incluyendo correos privados, fueron secuestrados por ciberdelincuentes.

tres ataques cibernéticos entre 2022 y 2023, en los que se estima que fueron capturados 700 GB de datos confidenciales de la entidad. La Fiscalía General de la Nación sufrió un ataque cibernético en el cual más de 10 TB de información sensible, incluyendo correos privados, fueron secuestrados por ciberdelincuentes. Y en mayo de 2023, la plataforma SECOP II, clave para trámites de contratación pública en el país, estuvo fuera de línea por 34 horas.

Algunas definiciones clave incluidas en el proyecto de Ley 010 de 2023 - Senado, son las siguientes:

- Ciberataque: incidente de ciberseguridad en el que una persona o grupo de ellas, conocidas o no, intenta destruir, exponer, alterar, deshabilitar, filtrar, robar, hacer uso o acceder de manera ilícita a un activo de información o de tecnologías de la información, y en el que puedan verse afectados también activos físicos de forma eléctrica o mecánica.

- Ciberespacio: ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información utilizado para la interacción entre usuarios y para almacenar, modificar e intercambiar datos.

- Ciberseguridad: conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que puedan utilizarse. Busca la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio.

- Delitos cibernéticos: aquellos que afectan la disponibilidad, integridad y confidencialidad de la información y los sistemas digitales. Estos solo pueden cometerse a través y en contra de un sistema informático.

- Delitos ciberhabilitados: aquellos que existían de forma previa a las TIC, pero que, con el desarrollo de estas, ahora se desarrollan también mediante la modalidad cibernética.

- Ecosistema digital: conjunto de infraestructuras y prestaciones (plataformas, dispositivos de acceso) asociadas a la provisión de contenidos y servicios a través de Internet. Este es un sujeto de análisis fundamental para la definición de políticas públicas, en áreas tan diversas como la digitalización de procesos productivos y la protección de la privacidad de los usuarios.

- **Equipo de respuesta a incidentes de seguridad informática:** grupo de especialistas multidisciplinarios capacitados para prevenir, detectar, gestionar y responder a incidentes de ciberseguridad, en forma rápida y efectiva, para actuar de acuerdo a procedimientos y políticas predefinidas, que colaboren en resolver la situación presentada.

- **Incidente:** cualquier evento adverso real o sospechado, intencionado o no intencionado, que puede cambiar el curso esperado de una actividad en el entorno digital.

- **Infraestructuras críticas:** sistemas y activos, físicos o virtuales, soportados por TIC, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.

- **Protección de Datos Personales:** acciones administrativas y operativas encaminadas a mantener la privacidad de las personas naturales en un Estado, de acuerdo con lo definido y exigido por el Régimen de Protección de Datos Personales.

- **Seguridad digital:** es la situación de normalidad y de tranquilidad en el entorno digital, a través de la apropiación de políticas, buenas prácticas, y mediante: (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa, que demanda la voluntad social y política de las partes interesadas.

- **Sistema de Información:** medio por el cual dispositivos, redes o plataformas almacenan, procesan o transmiten datos digitales, ya sea a través de redes de comunicaciones electrónicas, dispositivos o cualquier grupo de redes interconectadas o dispositivos o sistemas de información y plataformas relacionadas entre sí.

Métodos comunes para amenazar la ciberseguridad

- *Malware:* software malicioso, es una de las ciberamenazas más comunes. Es un software que un cibercriminal o un *hacker* crea para interrumpir o dañar el equipo de un usuario legítimo. Con frecuencia se propaga mediante un archivo adjunto de correo electrónico no solicitado o de una descarga de apariencia legítima. Es utilizado por los ciberdelincuentes para ganar dinero o con fines políticos. Hay varios tipos de *malware,* como:

  – Virus: un programa capaz de reproducirse, que se incrusta en un archivo limpio y se extiende por todo el sistema informático e infecta a los archivos con código malicioso.
  – Troyanos: se disfraza como software legítimo. Los cibercriminales engañan a los usuarios para que carguen troyanos a sus computadoras, donde causan daños o recopilan datos.
  – Spyware: programa que registra en secreto lo que hace un usuario para que los cibercriminales puedan usar esta información. Por ejemplo, puede capturar los detalles de las tarjetas de crédito.
  – *Ransomware:* malware que bloquea los archivos y datos de un usuario, con la amenaza de borrarlos o divulgarlos, a menos que se pague un rescate.

  - Adware: software de publicidad que puede utilizarse para difundir *malware*.
  - Botnets: redes de computadoras con infección de *malware* que los cibercriminales utilizan para realizar tareas en línea sin el permiso del usuario.

- **Inyección de código SQL:** Por sus siglas en inglés, *Structured Query Language*, se utiliza para tomar el control y robar datos de una base de datos. Los cibercriminales aprovechan las vulnerabilidades de las aplicaciones basadas en datos para insertar código malicioso mediante una instrucción SQL maliciosa. Esto les brinda acceso a la información confidencial de la base de datos.

- **Phishing:** los cibercriminales atacan a sus víctimas con correos electrónicos que parecen de una empresa legítima que solicita información confidencial. Estos ataques se utilizan a menudo para inducir a que las personas entreguen sus datos de tarjetas de crédito y otra información personal.

- **Ataque de tipo "Man-in-the-middle":** un cibercriminal intercepta la comunicación entre dos individuos para robar datos. Por ejemplo, en una red Wi-Fi no segura, un atacante podría interceptar los datos que se transmiten desde el dispositivo de la víctima y la red.

- **Ataque de denegación de servicio:** es cuando los cibercriminales impiden que un sistema informático satisfaga solicitudes legítimas sobrecargando las redes y los servidores con tráfico. Esto hace que el sistema sea inutilizable e impide que una organización realice funciones vitales.

Algunos ciberataques en entidades de salud en Colombia en 2022 y 2023

Ante el avance de la transformación digital de las empresas vinculadas al sector salud en Colombia y en el mundo entero, promovida en gran medida por la emergencia sanitaria mundial por COVID-19 y por los constantes avances tecnológicos en medicina, telecomunicaciones y en la industria 4.0, así como con la incorporación de sistemas IoT e IoMT (Internet de las cosas e Internet de las cosas médicas), paralelamente aumentan de manera automática los riesgos cibernéticos para la información y los datos altamente sensibles que manejan estas instituciones. La salud constituye una de las infraestructuras críticas de un país; por eso, es una preocupación mayor el aumento de ataques a instituciones del sector salud.

En Colombia, según la firma de ciberseguridad Fortinet, tan solo en el primer semestre de 2023 Colombia recibió 5.000 millones de intentos de ataques informáticos, lo que lo convierte en el cuarto país de América Latina y el Caribe que más ha estado expuesto a esa amenaza.

Invima recibió dos ataques cibernéticos en febrero y octubre de 2022

El 6 de febrero de 2022 la plataforma tecnológica que brinda servicios de nacionalización de alimentos y medicinas al parecer fue comprometida con un *ransomware*. Se deshabilitó el portal web y se desconectaron sus servidores físicos y virtuales. El Invima indicó que la protección de la información, privacidad y confidencialidad de los datos que maneja estaba asegurada por el acompañamiento del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) y las medidas implementadas por la propia entidad. Además, se advirtió una campaña de engaños con envíos de correos desde el dominio oficial de la entidad: invima.gov.co. El restablecimiento de las operaciones tardó más de 30 días y a ciertos procesos se les extendieron los términos legales.

El 3 de octubre de 2022 nuevamente la plataforma informática del Invima fue objeto de un ataque cibernético, que produjo la no disponibilidad de información y de los aplicativos externos, a excepción de la Ventanilla

Única de Comercio Exterior (VUCE). El equipo técnico del Instituto aseguró que la información, privacidad y seguridad de los datos bajo su cargo se encontraban protegidos. Nuevamente, se deshabilitó el portal web invima.gov.co y las conexiones con los servidores físicos y virtuales hasta controlar la situación. Asimismo, se adecuaron medidas administrativas para la autorización de medicamentos vitales no disponibles y la liberación de lotes.

En este ataque se amenazó al entonces director de la entidad, Francisco Rossi, con un plazo máximo de tres días para contactar a los *hackers* o, de lo contrario, "los 700 GB de datos confidenciales robados serán vendidos", evidenciando un ataque de *ransomware* o "secuestro de información". Además, en redes sociales se publicaron fotos de pasaportes de empleados del Invima, de otras entidades del gobierno y de personas de otros países que tendrían relación con el Instituto. Según informó en su momento Rossi, los ciberdelincuentes estaban pidiendo un pago entre dos y cinco millones de dólares en criptomonedas para que la página web volviera a funcionar sin problemas. Se identificó como responsable del ciberataque al grupo de piratas informáticos denominado Guacamayas, que no solo afectó al Invima sino también a las Fuerzas Militares colombianas con el robo al sistema militar de México, Chile, El Salvador y Perú. En 2023 se siguieron presentando retrasos en algunos trámites del Invima debido a fallas presentadas en el restablecimiento del servicio.

Salud Total EPS-S fue objeto de ataque informático externo

En comunicado oficial, Salud Total EPS-S informó que el domingo 1 de mayo de 2022 la plataforma tecnológica de la entidad fue objeto de un ataque informático externo, lo que ha

En Colombia, según la firma de ciberseguridad Fortinet, tan solo en el primer semestre de 2023 Colombia recibió 5.000 millones de intentos de ataques informáticos.

produjo una indisponibilidad en parte de la información relacionada con la operación. En consecuencia, siguiendo los protocolos establecidos por la EPS en el marco del sistema de continuidad del negocio, se deshabilitaron los servicios informáticos afectados, así como las conexiones con los servidores físicos y virtuales, con el objetivo principal de salvaguardar la información y establecer el estado de los aplicativos afectados.

La EPS desplegó todas las acciones preventivas y reactivas encaminadas a restablecer los aplicativos afectados y activaron las acciones penales procedentes a instancias de la Fiscalía General de la Nación, de conformidad con la legislación penal aplicable.

Ciberataque a EPS Sanitas buscaba afectar a sus 5,5 millones de usuarios y pedir rescate

En noviembre de 2022, luego de dos días de fallas en los servicios digitales que provocaron a su vez demoras o negativas en la asignación y atención de citas médicas, suspensión del servicio de citas prioritarias, no entrega de medicamentos ni resultados de exámenes médicos, y no atención al usuario por los diferentes canales, el Grupo Keralty, dueño de la EPS Sanita, informó que los servidores informáticos de las empresas del Grupo habían sido objeto de un ciberataque que generó fallas en sus sistemas.

El 20 de diciembre RamsonHouse, organización criminal de talla internacional, anunció tener en su poder 0,7 TB (terabytes) de información institucional, de los cuales había revelado trece archivos que contenían estados financieros, balances, presupuestos, así como información relativa a algunos usuarios. El 17 de enero de 2023, la EPS informó a sus afiliados que ya podían consultar servicios en línea y, en marzo, se informó que el grupo

de *hackers* publicó la mitad de los archivos secuestrados en su canal de Telegram, porque la EPS no accedió a sus extorsiones económicas.

Este ataque llevó a que entidades de vigilancia y control en el país requirieran a la compañía y le pidieran planes de contingencia para garantizar la atención a los usuarios, -que llegaron a radicar más de 10.455 peticiones, quejas y reclamos-, e hicieran seguimiento a la vulneración de los datos de los afiliados a la entidad.

Audifarma sufrió un ataque a inicios de 2023

La red de farmacias Audifarma fue objeto de un ataque informático externo en su infraestructura tecnológica el domingo 22 de enero de 2023. La compañía informó en su momento que, tan pronto fue identificado el ataque, activaron los protocolos de seguridad informática dispuestos para este tipo de casos y se deshabilitaron los servidores físicos y virtuales para proteger la información de la organización y de sus usuarios.

Audifarma recibió el acompañamiento de empresas multinacionales expertas en ciberseguridad, con las cuales analizaron todos sus sistemas informáticos para lograr restablecer el servicio con normalidad para todos los usuarios.

Cafam presentó afectaciones en la prestación de servicios de salud

El 16 de junio de 2023, la Caja de Compensación Familiar Cafam informó en un comunicado oficial que, debido a un ataque cibernético a sus sistemas de información, se presentarían afectaciones en los servicios en los centros de atención en salud Cafam. Se informó que durante la contingencia no sería posible asignar nuevas citas médicas ni realizar tomas de muestras de laboratorio clínico. Asimismo, los servicios de imágenes de alta complejidad (TAC y resonancia magnética) se suspendieron temporalmente; además, confirmó que se presentaron algunas limitaciones que afectaban la entrega de algunos productos en los puntos de dispensación de Droguerías Cafam.

Ciberataque a IFX Networks afectó 64 páginas web en Colombia, 34 de instituciones públicas

La empresa proveedora de telecomunicaciones IFX Networks, que ofrece servicios en tecnología y transferencia de datos, fue víctima de un ataque cibernético que tuvo un impacto en varias operaciones digitales en Colombia, lo que explica las fallas en estas páginas web. Un total de 64 páginas web en Colombia, 34 de ellas de instituciones públicas del Estado, fueron objeto de un ataque cibernético en septiembre de 2023. Entre las entidades afectadas estuvieron el Ministerio de Salud, la Superintendencia de Industria y Comercio, la Superintendencia de Salud y el Consejo Superior de la Judicatura.

Desde las 6:00 de la mañana del 12 de septiembre de 2023, la Oficina de Tecnología de la Información y Comunicación (TIC) del Ministerio de Salud detectó fallas en los servicios tecnológicos alojados en el Datacenter institucional administrado por IFX Networks Colombia, proveedor de servicios tecnológicos de distintas entidades públicas del orden nacional.

El 13 de septiembre, el Ministerio de Salud informó que, debido al incidente de ciberseguridad en el Datacenter, donde están alojadas las aplicaciones misionales asociadas a la prestación de servicios derivados de la atención a nivel nacional, estas presentaban fallas y no era posible acceder a ellas. El 25 de septiembre, el Ministerio de Salud informó que ya estaban restablecidos en su totalidad todos los servicios y aplicativos tecnológicos y digitales a nivel interno y externo que resultaron afectados tras el ataque cibernético a la empresa IFX Networks.

Por su parte, la Superintendencia Nacional de Salud fue otra institución impactada por el ciberataque a IFX Networks, con afectaciones a

la plataforma donde se alojan los sistemas de gestión de auditorías, inventarios y de control de las EPS. El 13 de septiembre, la Supersalud informó a los usuarios que podían seguir radicando sus peticiones, quejas y reclamos cuando consideren vulnerado su derecho a la salud por negación o mala prestación de servicios, toda vez que el sistema que gestiona y garantiza la trazabilidad de las reclamaciones no sufrió afectación tras las fallas registradas en varios servicios tecnológicos que provee IFX Networks Colombia. El 22 de septiembre, se normalizaron los servicios tecnológicos, trámites jurisdiccionales y canales virtuales de la Supersalud, luego de que fueran restablecidos en su totalidad los servicios y aplicativos tecnológicos y digitales a nivel interno y externo que resultaron afectados tras el ataque cibernético a la empresa IFX Networks.

Afectaciones colaterales a entidades relacionadas con Minsalud

Desde la ADRES, se informó que la entidad no fue blanco directo de los ataques, pero al tener sus plataformas conectadas a las del Ministerio de Salud (que sí fueron vulneradas), hubo interrupción en la comunicación de algunos sistemas de información.

- El Instituto Nacional de Cancerología informó que sus sistemas de información y plataformas tecnológicas no fueron afectados en el incidente, pero que sí se presentaron problemas en el intercambio de información con entidades afectadas como el flujo de información con el operador de facturación electrónica y el Ministerio de Salud. La situación no comprometió la seguridad de la información institucional como historias clínicas ni los servicios a pacientes y proveedores.

Modelo actual de gobernanza en seguridad digital de Colombia

En 2009 se sancionó la Ley 1341 o Ley de Tecnologías de la Información y las Comunicaciones (TIC), que establece un marco jurídico acorde con la realidad mundial y el posicionamiento de las TIC en el ciberespacio. Ese mismo año, ante la necesidad de modificar el Código Penal para reconocer delitos informáticos, se expidió la Ley 1273 de 2009, en la cual se establece la protección de la información y los datos, y se "preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones". También en 2009 se crea la Unidad de Delitos Informáticos de la Fiscalía General de la Nación, encargada de investigar y perseguir los delitos informáticos.

En el 2011 Colombia formalizó sus esfuerzos en establecer un modelo de gobernanza para reconocer la ciberseguridad y la ciberdefensa como elementos fundamentales para garantizar la defensa nacional, pues el ciberespacio se considera el quinto dominio de la seguridad de un Estado (Douzet, 2014). Dada su importancia, el CONPES 3701 de 2011 estableció por primera vez los lineamientos de política para ciberseguridad y ciberdefensa del país, reconociendo la importancia de protegerlo de amenazas cibernéticas ante la importancia del ciberespacio para el desarrollo socioeconómico del país. Este CONPES tuvo como objetivo promover la cultura de la seguridad cibernética, concienciar a la población sobre los riesgos y buenas prácticas del uso de las TIC y establecer organismos de respuesta a los incidentes cibernéticos de la Nación.

El Conpes conformó varias instancias: ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), adscrito en su momento al Ministerio de Defensa Nacional; el Comando Conjunto Cibernético, encargado de la defensa del país en el ciberespacio; y el Centro Cibernético Policial, encargado de la seguridad ciudadana en el espacio. Dichas entidades fueron encargadas del diseño e implementación de políticas y estrategias de seguridad cibernética y del establecimiento de mecanismos de protección de la información y de respuesta a incidentes cibernéticos.

El Decreto 289 de 2011 establece el Comité Nacional de Ciberseguridad como órgano de consulta y asesoría para la formulación de políticas en materia de ciberseguridad y en 2012 se establece el Plan Nacional de Ciberseguridad desarrollando una serie de estrategias para proteger las infraestructuras críticas del país. En la Resolución 05839 de 2015, la Policía Nacional estableció las funciones del Centro Cibernético Policial como una dependencia de la Dirección de Investigación Criminal, "encargada de desarrollar estrategias, programas, y proyectos para la ciberseguridad, ciberdefensa y la protección de la información y los datos que circulan por el ciberespacio de los habitantes en el territorio nacional, a través de la investigación criminal" (art. 15).

En 2016 el Conpes 3855 estructura la Política Nacional de Seguridad Digital mediante la protección de la información crítica del país y se plantea la necesidad de mejorar las capacidades de respuesta ante incidentes cibernéticos por medio de la coordinación de diferentes entidades del Estado y la asignación de recursos económicos a las instancias creadas en el Conpes 3701 de 2011. "Colombia no cuenta con una instancia de coordinación nacional en seguridad digital que optimice la gestión de los recursos destinados a esta materia" (Conpes 3855, 2016, pág. 32).

En 2018 Colombia adoptó, mediante la Ley 1928, el "Convenio sobre la ciberdelincuencia",

firmado en Budapest en 2001, cuyo objetivo es promover la cooperación internacional en la lucha contra la ciberdelincuencia en delitos como acceso ilegal a sistemas informáticos, fraude informático, abuso de niños en línea, robo de identidad, entre otros.

En 2020 el Conpes 3995 estableció la *Política Nacional de Confianza y Seguridad Digital*, que busca ejecutar los lineamientos planteados en el Convenio de Budapest y establecer medidas para mejorar la seguridad digital del país por medio de una actualización del marco de gobernanza. En él se reitera la importancia de la coordinación entre las instancias del Estado, el sector privado y la academia para implementar de manera efectiva la política de confianza y seguridad digital, así como la necesidad de asignar recursos financieros para ejecutar las propuestas de dicha política.

La Resolución 500 de 2021 de MinTic establece los lineamientos para la implementación de la estrategia de seguridad digital y la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI). Asimismo, señala que todas las entidades públicas debían adoptar medidas técnicas, administrativas y de talento humano para garantizar la seguridad digital y prevenir incidentes.

En 2022 el Decreto 338 modificó el Título 21 de la parte 2 del libro 2 del Decreto 1078 de 2015, "con el fin de establecer lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de estructuras críticas, cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta incidentes de seguridad digital" (Decreto 339, 2022). De igual manera, el Ministerio de Tecnologías de la Información y las Comunicaciones expidió la Resolución 00473, actualizada en la Resolución 3066

del mismo año, en donde se establece que el Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) estaría adscrito a dicho ministerio bajo la dirección del Viceministerio de Transformación Digital y tendría como una de sus funciones "Actuar como punto único de contacto y coordinación para responder de manera rápida y eficiente a incidentes y vulnerabilidades de Seguridad Digital para la gestión de amenazas e incidentes de Seguridad Digital Nacional" (Resolución 03066, 2022, pág. 20).

De acuerdo con lo anterior, se evidencia que, en materia de Política Nacional de Seguridad Digital, Colombia se ha caracterizado por ser un país donde se han creado marcos normativos en materia de ciberseguridad. Sin embargo, la aplicación de los mismos se ha visto frenada ante la falta de coordinación de las instancias creadas, así como la falta de asignación presupuestal destinada al sector, lo que conlleva no contar con el personal necesario para aplicar la normativa.

Algunas obligaciones de entidades del sector salud en ciberseguridad

Los actores del sector salud (prestadores de servicios de salud públicos y privados, Entidades Promotoras de Salud, EPS; Entidades Adaptadas en Salud, EAS; entidades que administren planes voluntarios de salud, Administradoras de Riesgos Laborales, ARL; fondos de pensiones en sus actividades de salud, entidades pertenecientes a los

Se debe asegurar la infraestructura, sistemas de tecnología de la información y prácticas de negocios que interactúan o implican el uso de cualquier información o dato personal.

regímenes de excepción o regímenes especiales de salud, y las secretarías, institutos y unidades administrativas departamentales, distritales y municipales de salud), que accedan a la información de manera innominada, y las compañías de seguros que emitan pólizas de accidentes de tránsito deberán cumplir con las siguientes obligaciones en materia de seguridad de la información (de acuerdo con el artículo 19 de la Resolución 886 de 2021 de Minsalud y MinTic):

- Adoptar una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio, en la cual deberán desarrollar periódicamente una evaluación del riesgo de seguridad digital que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para el desarrollo de la estrategia deberán contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo. Deben adoptar los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la guía de gestión de riesgos de seguridad de la información, el procedimiento para la gestión de los incidentes de seguridad digital, y los lineamientos y estándares para la estrategia de seguridad digital emitidos por MinTic en el marco de la política de Gobierno Digital.

- Asegurar la infraestructura, sistemas de tecnología de la información y prácticas de negocios que interactúan o implican el uso de cualquier información o dato personal.

- Incorporar prácticas y procesos de desarrollos destinados a salvaguardar la información personal de los individuos a lo largo del ciclo de vida de un sistema, programa o servicio.

Obligaciones específicas para los prestadores de servicios de salud (IPS)

Las Instituciones Prestadoras de Servicios de Salud (IPS), tanto públicas como privadas, deberán tener en cuenta que les aplican las siguientes obligaciones específicas, de acuerdo con las disposiciones del artículo 24 de la Resolución 886 de 2021 de Minsalud y MinTic):

- Contar con estrategias de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio que permitan el uso de los mecanismos de comunicación y garantizar la

NOS SINCRONIZAMOS CON LOS LATIDOS

de nuestros pacientes para cuidar de lo

más importante: **Tu vida.**

Dr. Jhonattan Benavidez
Médico especialista en cardiología

Conoce nuestros servicios:

- Cardiopatías congénitas
- Cardiología Clínica
- Ayudas diagnósticas cardiovasculares
- Electrofisiología
- Hemodinamia e intervencionismo
- Cirugía cardiovascular
- Falla cardiaca
- Trasplante de corazón
- Rehabilitación cardiaca

Elige la mejor opción para tus **pacientes**
Remítelos en LaCardio

Fundación Cardioinfantil | laCardio

Nuestros aliados:

PHILIPS | Boston Scientific *Advancing science for life™* | J&J MedTech

confidencialidad, integridad, disponibilidad, autenticación y autorización en el intercambio de datos.

- Adoptar estándares alineados con la Política de Gobierno Digital, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, la cual en el Manual de Gobierno Digital establece las necesidades y problemáticas que determinan el uso de las TIC.

- Cumplir las obligaciones derivadas de la condición de responsable o encargado del tratamiento de datos y las derivadas de la Ley 1581 de 2012 y las normas que la modifiquen, sustituyan o desarrollen.

- En desarrollo de los principios de finalidad y libertad de los datos personales, la recolección, la transferencia y el uso de datos personales deberán limitarse a aquellos pertinentes y necesarios para la finalidad para la cual son recolectados o requeridos conforme a la normativa vigente.

Respecto a las obligaciones establecidas en la Resolución 866 de 2021 de Minsalud y MinTic, la inspección, vigilancia y control corre por cuenta de la Superintendencia Nacional de Salud, facultada por el artículo 131 de la Ley 1949 de 2019 para imponer sanciones. Entre dichas sanciones, se destacan multas entre 200 y 8.000 salarios mínimos legales mensuales vigentes (SMMLV) para personas jurídicas, y entre 50 y 2.000 SMMLV para las personas naturales, amonestaciones escritas y revocatoria total o parcial de la autorización de funcionamiento.

Buenas prácticas según normas HIPAA

El cumplimiento de las normas de seguridad de la regulación más relevante del sector salud y farmacéutico en Estados Unidos, como la Ley de Portabilidad y Responsabilidad de los Seguros Sanitarios de 1996 (HIPAA por sus siglas en inglés), se basa en varios principios clave que pueden constituir una guía de buenas prácticas que se deben considerar para los actores del sector salud en Colombia:

- Implementación de un proceso de gestión de la seguridad, que incluya un análisis de riesgos y medidas de seguridad para mitigar los riesgos potenciales.

- Adopción de los procedimientos ilustrados en su Título II, los cuales incluyen lineamientos de privacidad, reglas transaccionales y de seguridad, y pautas de aplicación para protegerse contra softwares maliciosos.

- Formación de los usuarios sobre los principios de protección contra el software malintencionado.

- Integración de limitaciones en los controles de acceso y concesión de acceso únicamente a personas que hayan recibido formación en materia de protección de datos.

Colombia tendría Agencia Nacional de Seguridad Digital

De aprobarse en el Congreso de la República el Proyecto de Ley N.º 010 de 2023-Senado, en Colombia se crearía la Agencia Nacional Digital como máxima autoridad para la formulación y aplicación de la estrategia nacional y políticas públicas en materia de seguridad digital y ciberdefensa nacional. Esta propuesta responde a la necesidad del país de fortalecer su marco institucional en seguridad digital, para prevenir y combatir ciberataques de manera coordinada, con tiempos acordes a las necesidades de reacción.

El proyecto, radicado el 24 de julio de 2023 por los senadores Ana María Castañeda y David Luna y la representante Ingrid Sogamoso, se justificó en el hecho de que Colombia es el segundo país de América Latina con más ciberataques presentados (IBM,2022), a nivel mundial ocupa el puesto 69 (NCIS, 2022) y solo en 2022 el país recibió 20.000 millones de intentos de ciberataques (con grandes entidades afectadas como la Fiscalía General de la Nación, el Invima, la EPS Colsanitas, Audifarma, Carvajal, Empresas Públicas de Medellín (EPM) y Cafam, entre otras).

"Actualmente Colombia enfrenta desafíos significativos en términos de preparación y respuesta a las amenazas cibernéticas. Para contrarrestarlas, la creación de un CSIRT (Equipo de Respuesta a Incidentes de Seguridad Cibernética) de Salud es fundamental[1]. Además, es necesario intensificar la concientización sobre ciberseguridad en todos los niveles, desde empleados hasta altos directivos para evitar poner en riesgo sus datos y los de la compañía, pues son ellos la primera puerta de acceso por donde ingresan los ciberdelincuentes".

Estas son las propuestas del senador y exministro de Tecnologías de la Información y Comunicaciones, David Luna, luego de señalar que "en Colombia hemos observado un marcado aumento de ciberataques a entidades tanto públicas como privadas, especialmente en el contexto post-COVID-19. Los ciberataques contra entidades prestadoras de servicios de salud o relacionadas con la salud como Keralty o el Invima han aumentado en 45 %, siendo el sector más afectado por los ciberataques".

Explica el exministro que "para los ciberdelincuentes se volvió un negocio muy rentable, incluso superior que el narcotráfico, extorsionar con los datos de salud de los ciudadanos, pues son una infraestructura crítica que puede poner en jaque al país y ellos lo saben. Es por ello que se pro-

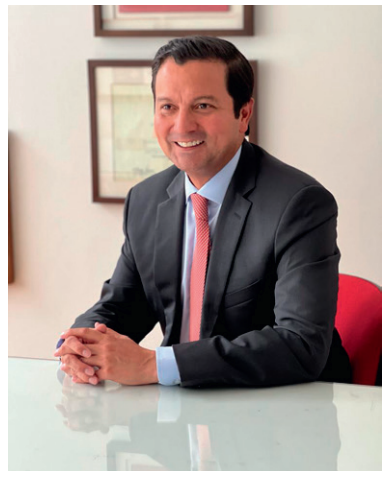


Foto: Cortesía Dr. David Luna

David Luna, Senador

[1] *Un Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés: Cyber Security Incident Response Team) es un grupo de expertos en ciberseguridad que se encarga de detectar, analizar y responder a los incidentes de seguridad informática en una organización. El objetivo principal de un CSIRT es minimizar el impacto de los incidentes de seguridad en la organización y reducir el tiempo de inactividad. Los CSIRT suelen estar formados por personal técnico especializado, como el responsable de seguridad de la información (CISO), el Centro de Seguridad de Operaciones (SOC) y el personal de Tecnología e Innovación (TI).*

Capacitar a los profesionales de la salud sobre las mejores prácticas de ciberseguridad y cómo reconocer posibles amenazas, puede reducir significativamente el riesgo de ataques

nostica que el mercado mundial de ciberseguridad en salud crecerá un 15 % al año, alcanzando 125.000 millones de dólares acumulados entre 2020 y 2025".

David Luna considera que la implementación de sistemas de detección temprana, que puedan identificar patrones de comportamiento sospechosos, también se vuelve esencial: "Las entidades prestadoras de servicios de salud y las entidades del Estado encargadas de la salud de los colombianos deben considerar la ciberseguridad como una de sus prioridades e invertir recursos de manera preventiva en su protección. También la colaboración entre el sector público y privado es clave, pues fortalece las defensas cibernéticas al compartir información sobre amenazas y adoptar mejores prácticas de seguridad".

El senador estima que, dada su alta vulnerabilidad, deben desarrollarse estrategias específicas para el sector: "Definitivamente el sector salud, al manejar información altamente sensible, requiere estrategias para protegerse contra ciberataques. Una de las principales medidas sería implementar, como lo dije anteriormente, el CSIRT de Salud. Asimismo, implementar sistemas de cifrado robustos para resguardar la confidencialidad de los datos del paciente, establecer protocolos de seguridad detallados y realizar auditorías periódicas para identificar y corregir posibles vulnerabilidades".

Agrega que la concientización del personal en el sector salud también juega un papel crucial: "Capacitar a los profesionales de la salud sobre las mejores prácticas de ciberseguridad y cómo reconocer posibles amenazas, puede reducir significativamente el riesgo de ataques".

También considera que la colaboración entre las entidades de salud, tanto públicas como privadas, es fundamental: "Compartir información sobre amenazas y vulnerabilidades puede fortalecer la postura de seguridad de todo el sector. Para esto hemos planteado la creación de una Agencia Nacional de Seguridad Digital, la cual esté encargada de la coordinación y la vocería a la hora de enfrentar un ciberataque".

David Luna recalca además que la inversión en tecnologías de prevención, detección y respuesta ante ciberataques, específicas para el ámbito de la salud, debe ser una prioridad, para mitigar los riesgos de manera efectiva. Asimismo, el exministro de Tecnologías de la Información y Comunicaciones formuló algunas recomendaciones de cara al futuro:

1. Pasar de la reacción a la prevención: implementar medidas de seguridad avanzadas, como firewalls actualizados y sistemas de detección de intrusiones, para fortalecer la infraestructura contra posibles amenazas.

2. Concientización: realizar programas regulares de formación en ciberseguridad para el personal del sector salud, enfocándose en la identificación de amenazas y prácticas seguras en línea.

3. Colaboración interinstitucional: fomentar una mayor colaboración entre las entidades de salud, tanto públicas como privadas, para compartir información sobre amenazas y adoptar estrategias comunes de ciberseguridad. Para esto será clave la creación de la Agencia Nacional de Seguridad Digital y el CSIRT Salud.

Pese a que Colombia ha establecido legislación para la investigación y reacción a ataques cibernéticos, se evidencia la falta de coordina-

ción entre las entidades ya creadas: Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), Comando Conjunto Cibernético y el Centro Cibernético Policial. Además, el poco presupuesto y la falta de personal capacitado para cumplir con las necesidades de seguridad digital del país son aspectos que deben corregirse.

La iniciativa legislativa establece acciones para garantizar la coordinación entre el Comando Conjunto Cibernético y el Centro Cibernético Policial, así como con el Ministerio de Tecnologías de la Información y las Comunicaciones y sus entidades adscritas, el Ministerio de Defensa Nacional, la Fiscalía General de la Nación y otros órganos del Estado necesarios para generar una política preventiva en seguridad digital.

El proyecto de ley crea la Agencia Nacional de Seguridad Digital como una entidad que garantice la articulación entre el Estado, el sector privado y los ciudadanos. La entidad no significa más gasto de recursos, pues se creará el Fondo Nacional para la Seguridad Digital y Ciberdefensa que distribuirá los recursos hoy destinados a la ciberdefensa y buscará la inversión del sector privado. Además, el proyecto determina las funciones de la Agencia, así como su estructura y presupuesto, creando institucionalidad en la materia y permitiendo que Colombia pase de una política reactiva a una preventiva en materia de seguridad digital. Asimismo, el país sería pionero en la región en crear una Agencia de dicha naturaleza.

Gestión de la ciberseguridad en entidades de salud

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, la telemedicina y los dispositivos médicos avanzados son sistemas críticos, y fueron víctimas de ataques en los últimos años. Los Datos Personales de Salud 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. En el 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. En ALC la tendencia de los ciberataques también es creciente.

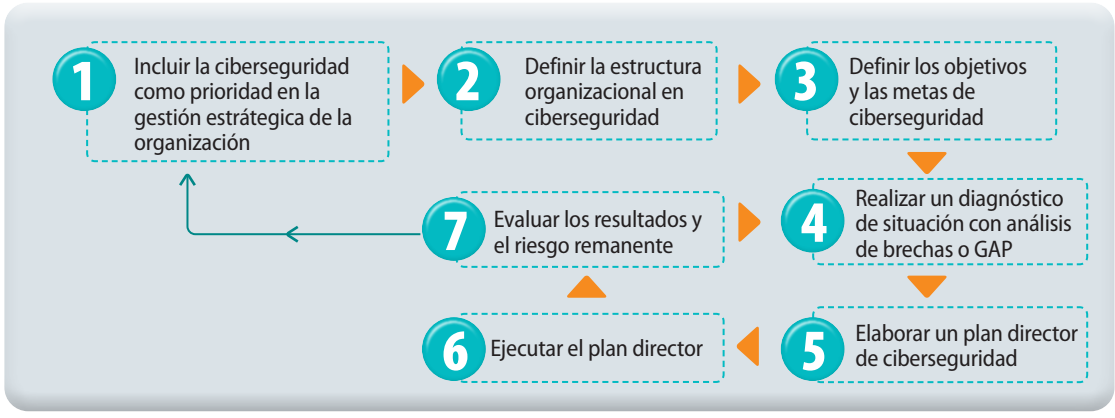
El sector salud no solo fue uno de los más atacados por *hackers* en 2019, sino que es la industria que sufrió los ataques más dañinos en los últimos años. El BID calcula que el costo promedio de un ciberataque en el sector salud en términos de pérdida de negocio, gastos de prevención, detección y recuperación equivale a 7,13 millones de dólares en comparación con los 3,86 millones de dólares que, en promedio, cuestan los ciberataques en cualquier otra industria. Además, el 80 % de la información comprometida por ciberataques son datos personales y, en el sector salud, se tarda más tiempo en detectar una posible vulneración de información: desde que tiene éxito un ataque hasta que la institución se da cuenta que vulneraron sus datos, pasa un promedio de 329 días. ALC tiene uno de los mayores tiempos de detección de ataques a nivel mundial.

BID propone siete pasos para implementación de ciberseguridad en organizaciones de salud

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. Para facilitar el acceso a conocimiento y herramientas de apoyo para diagnosticar y mejorar el estado

de la ciberseguridad en organizaciones de salud y para proteger a los ciudadanos de América Latina y el Caribe, el Banco Interamericano de Desarrollo (BID) elaboró la guía "Protegiendo la salud digital-Una guía de ciberseguridad en el sector de salud", en la cual propone una estrategia de siete pasos esenciales para iniciar o fortalecer la ciberseguridad en esas entidades, además de que recopila y clasifica el conocimiento existente a nivel global en cuanto a normas, marcos de trabajo, estándares, buenas prácticas y guías de implementación de ciberseguridad.

Figura 1. Siete pasos para la implementación de ciberseguridad



Tomado de "Protegiendo la salud digital-Una guía de ciberseguridad en el sector de salud", BID (2021).

El proceso de implementación debe realizarse de manera sistemática, estructurada y continua, ya que el cambio no se conseguirá de la noche a la mañana. El BID propone una metodología simple, un ciclo de mejora continúa compuesto por siete pasos, que se presentan a continuación:

1. *Incluir la ciberseguridad como prioridad en la gestión estratégica de la organización.* Dado que el fin de las organizaciones de salud es salvar vidas, para lograr este objetivo buscan garantizar la seguridad del paciente, lo que implica entre otras 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.

2. *Definir la estructura organizacional en ciberseguridad.* Para cumplir los objetivos, metas e hitos definidos en el paso anterior, así como para 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.

   Este Comité tendrá como objetivos definir lineamientos estratégicos, junto con sus objetivos, metas e hitos anuales; definir responsabilidades generales; definir, aprobar y hacer seguimiento de políticas de seguridad de la información; apoyar y hacer seguimiento a los proyectos definidos en el Plan Director (deberá conseguir los recursos para que dichos proyectos tengan éxito); y ser el interlocutor y facilitador en seguridad de la información para agentes externos a la organización.

   Se recomienda definir con dicho Comité toda la estructura de seguridad de la información. Por ejemplo, la gestión de la respuesta a incidentes que se puede abordar de múltiples maneras: con un equipo de respuesta a incidentes, un centro de res-

puesta a incidentes centralizado o descentralizado, entre otros. Para cada función de seguridad se debe definir la estructura que mejor se adapte a la organización y, para cada caso, las dependencias jerárquicas, responsabilidades y constitución del equipo con los perfiles asociados.

3. *Definir los objetivos y las metas de ciberseguridad.* Establecer claramente objetivos y metas de seguridad de la información y ciberseguridad, teniendo en cuenta objetivos organizacionales como necesidad de cumplimiento, normativa nacional e internacional aplicables, mejores prácticas de la industria y perfil de riesgo organizacional. Este perfil se puede definir por varios factores, como tamaño y recursos de la organización, sensibilidad de activos que maneja, nivel de madurez actual y umbrales aceptables de riesgo definidos. Es fundamental fijar métricas e indicadores para evaluar los objetivos y metas.

4. *Realizar un diagnóstico de situación con análisis de brechas o GAP.* Luego de definir objetivos y metas de seguridad de la información, se debe hacer un diagnóstico de la situación actual, considerando 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 hacer el diagnóstico; si se adoptó un marco, se debe elaborar un análisis de brechas con el mismo, lo cual puede efectuarse mediante consultorías especializadas o herramientas de evaluación (la mayoría de los marcos tienen herramientas de evaluación o autoevaluación).

   Para escenarios en los que no se adopta un marco, el BID desarrolló herramientas para facilitar el diagnóstico, como una de autoevaluación para el sector salud respecto a las mejores prácticas de la industria, basada en el marco de ciberseguridad del NIST; mediante un cuestionario simple, ayuda a calcular las brechas y brinda recomendaciones que sirven como base para elaborar el Plan Director. Y es importante incluir en el diagnóstico 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.

5. *Elaborar el Plan Director de Ciberseguridad.* El responsable de seguridad de la información, con apoyo y asesoría del Comité de Seguridad, debe elaborar un Plan Director. Este debe incluir los objetivos de seguridad de la información, las metas específicas y un portafolio de proyectos y/o servicios. Debe reflejar claramente el aporte de cada proyecto y/o servicio a

las metas, y cómo llegar al resultado mediante el logro de los hitos definidos, junto a los indicadores de gestión para los proyectos y 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. Y se recomienda que el plan contemple la gestión de riesgos asociados a los proyectos y/o servicios.

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.

6. *Ejecutar el Plan Director.* Es preciso hacer un monitoreo integral del Plan Director para asegurar su éxito. El responsable de seguridad de la información debe hacer seguimiento a 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.

7. *Evaluar los resultados y el riesgo remanente.* Los resultados obtenidos de la ejecución del plan deben evaluarse de forma periódica, analizando su impacto en la organización. En función de dicha evaluación, se debe hacer 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.

"Para evitar cuidados intensivos en ciberseguridad, la clave es la prevención": KPMG

Foto: Archivo personal

Felipe Silgado, director de servicios de consultoría en ciberseguridad de KPMG

Felipe Silgado, director de servicios de consultoría en ciberseguridad de KPMG Colombia, explica que es necesario entender qué es un ciberataque y su impacto en las organizaciones, para asumir la obligación de la protección de los datos y la información, "nunca antes las empresas habían sido tan dependientes de la tecnología digital, por tanto, la ciberseguridad y la resiliencia son claves para construir confianza digital".

De acuerdo con el informe *Insigths* de 2022 sobre ciberconfianza, esta la debe empezar a generar el equipo de seguridad dentro de las organizaciones mediante un debido manejo y gestión, para que colaboradores, clientes, la alta dirección, accionistas y demás personas que interactúan con la organización tengan más confianza en trabajar con ella y en utilizar sus servicios.

Según datos de varias encuestas a nivel mundial, el costo de una brecha de datos en una entidad del sector salud aumentó un 42 % entre 2020 y 2022. Esto significa que, cuando una entidad sufre un ataque efectivo, se llevan datos o afectan de alguna ma-

nera los datos, lo que implica costos para la organización por temas regulatorios, sanciones y reconstrucción de la información.

Según Silgado, el sector sanitario en 2022 registró un aumento del 45 % en ataques de *ransomware* respecto de 2021. De 381 empresas de salud encuestadas en 2022, el 66 % de estas fueron atacadas, el 61 % de ellas pagaron el rescate y el 64 % obtuvieron de vuelta los datos. Más de 59 millones de registros de pacientes fueron violados, se presentaron 956 incidentes y hubo un aumento del 30 % de violaciones de datos relacionados con empresas asociadas.

Los ataques de *ransomware* son los que más impactan las organizaciones y en empresas del sector salud impiden el acceso de los usuarios a los servicios. Vienen aumentando exponencialmente desde 2020, a raíz de la pandemia por COVID-19. Algunos de los más sonados en el mundo fueron los ataques a Allergy Partners, Apex Laboratory, Ireland HSE, CHwapi y al NHS (Servicio Nacional de Salud del Reino Unido), que afectó a hospitales británicos, cirugías en todo el país y rutas de ambulancias, así como canceló alrededor de 92 millones de citas y la atención en Urgencias (al final se pagó el rescate para recuperar los datos y, por lo tanto, los servicios).

Explica el experto que en ataques de *ransomware* secuestran datos, los cifran para que los usuarios de la organización no tengan acceso ni disponibilidad a ellos, y con la copia de los datos extorsionan a la empresa a cambio de recuperar la disponibilidad y la no divulgación pública. Ese rescate generalmente se exige en monedas digitales no rastreables como los bitcoins y, si la organización no paga, podría no recuperar el acceso a sus datos; cuando la organización decide no pagar, el atacante le muestra su información y empieza a divulgarla: si tiene una base de datos de un millón de

Los ataques de ransomware son los que más impactan las organizaciones y en empresas del sector salud impiden el acceso de los usuarios a los servicios. Vienen aumentando exponencialmente desde 2020, a raíz de la pandemia por COVID-19.

registros, divulga 100, 500 o 1.000 registros para demostrar que sí tiene una copia de esa base de datos. Pueden ser datos de personas, informes de la organización, resultados de exámenes de pacientes. Además, agrega Silgado: "En la medida en que la organización entra en el juego del atacante, se puede ver afectada no solo su operación, sino también su reputación y su imagen".

Por ejemplo, el grupo delictivo RansomHouse (Casa de Rescate) hace ataques como el de Keralty en Colombia, activa el *malware* llamado Mario (sale el muñequito de Mario Bross), secuestra los datos y saca una copia. Aclara Silgado: "Recomendamos que no se pague rescate; a nivel mundial hay instituciones que pagaron y no todas recuperaron la información; el atacante se cierra después de ese pago y no devuelve las llaves del cifrado de la información. En encuestas a nivel mundial, casi el 22 % decidió pagar el rescate y, del porcentaje que lo paga, solamente el 65 % recupera los datos (reporte de defensa digital de Microsoft). Cuando se pagan rescates, se fomenta que eso siga ocurriendo y que a la misma organización la vuelvan a atacar más adelante".

¿Por qué no pagar un rescate? No hay absolutamente garantías de nada, porque un cibercriminal no tiene ninguna obligación de devolver la información y probablemente está en otra jurisdicción o país. En algunas jurisdicciones es ilegal pagar por un rescate, así que debe asesorarse muy bien respecto a consecuencias legales, normativas y regulatorias que eso puede traer. Además, al pagar se envía una señal al mercado criminal de que hay un

En encuestas a nivel mundial, casi el 22 % decidió pagar el rescate y, del porcentaje que lo paga, solamente el 65 % recupera los datos (reporte de defensa digital de Microsoft).

negocio y crean métodos más sofisticados, hacen mejores campañas de ingeniería social, mejoran sus tácticas, técnicas y procesos, y todos podemos seguir siendo víctimas.

Otros cibercriminales utilizan herramientas de cifrado; instituciones de seguridad como la Interpol, el FBI y la Policía Nacional recuperan llaves de cifrado cuando capturan a estas personas y las usan para descifrar la información. Silgado explica que lo primero que uno puede hacer es utilizar las herramientas públicas para tratar de descifrar la información con llaves ya existentes, y si no funcionan procurar la recuperación a partir de copias de respaldo: "La reacción es activar sus planes de contingencia para darle continuidad al negocio, planes de recuperación de desastres, recuperar los datos a partir de copias de seguridad; si no hay acceso al servidor o donde se guarda la información, hacer reinstalar otra vez desde cero y recuperar a partir del *back-up*. Lo importante es tener mecanismos, que puedas decir: «yo tengo copias de respaldo, un plan de continuidad, un plan de recuperación, el día que pase algo podría recuperarme, aunque me tome algún tiempo»".

Principales conductores de cambio

Deben identificarse los riesgos llamados "conductores de cambio", que obligan a hacer una gestión de ciberseguridad en las organizaciones.

1. *Regulación.* La regulación del país en protección de datos en entes de vigilancia como la Superfinanciera o Superindustria y Comercio, regulación internacional aplicable a organizaciones en Colombia como el GDPR o el SEC, y la legislación de protección de datos personales.
2. *Amenazas de cyber.* Amenazas constantes y crecientes para la empresa y sus clientes; y ataques de *ransomware, pishing, malware,* DDoS, exfiltración de datos, entre otros.
3. *Cambios en la organización.* Llevan a extremar medidas de ciberseguridad de manera diferente, por ejemplo, proyectos de digitalización, incremento en el uso de aplicaciones, desarrollo de aplicaciones nuevas, fusiones y adquisiciones, objetivos de reducción de costos, entre otros.
4. *Cambios en el ambiente.* Cambios sociales, económicos y políticos del país y del mundo; crecimiento en la tasa de cambio del dólar; cambios en los clientes de la organización; cambios postpandemia; modas y seguidores. Por ejemplo: en pandemia la gente tuvo que trabajar de manera remota, se tuvieron que crear controles nuevos para que se conectaran con seguridad.

Riesgos para la organización

Silgado indica que los ciberataques generan riesgos en la operación, en la reputación y legales, o riesgo de litigios costosos. En términos de riesgos para la organización, el riesgo de ciberseguridad generalmente se enmarca en la operación, es un riesgo operacional en la continuidad, en el trabajo del día a día, que proyecta pérdidas de ingresos porque se detiene el negocio.

Pero cuando se materializan riesgos a partir de un incidente se activa también el riesgo reputacional, porque empieza a verse la empresa comprometida públicamente; empiezan sus usuarios a quejarse; las entidades de vigilancia y control aparecen a hacer revisiones y a cuestionar la gestión interna; es posiblemente el más difícil de reparar, porque cuando se afecta

#KidneyCare

Información comercial

Renal Care Services:

Transformamos la Nefrología Hospitalaria en Colombia:

- Innovando en modelos de atención integral y temprana.
- Garantizando oportunamente la tecnología adecuada para el paciente indicado.
- Potencializando mejores resultados clínicos, a través de la toma de decisiones clínicas conjuntas.

Nefrología hospitalaria

Baxter Renal Care Services ofrece un amplio portafolio de servicios una solución integral para toda la necesidad de renales durante la estancia hospitalaria/UCI:

Soporte Renal Primario
Hemodiálisis
Diálisis Peritoneal
Diálisis Expandida HDx

CRRT
Ultra filtración Continua Lenta
Hemofiltración Venovenosa Continua
Hemodiálisis Venovenosa Continua
Hemodiafiltración Venovenosa Continua

Soporte Renal Especializado
Remoción Extracorpórea de CO2 (ECCO2R)
Plasmaféresis
Plasmadsorción
Hemoperfusión
Hemoadsorción
Diálisis Hepática
Inmunoadsorción

Nefrología Clínica
Equipo de Respuesta Rápida
Interconsultas y Telemedicina
Implante, manejo y seguimiento de:
Catéteres vasculares y peritoneales

¿Deseas más información?

Humberto Moreno: 3153909696

Baxter Renal Care Services

la imagen de la organización es muy difícil recuperar la confianza de los usuarios.

Asimismo, un incidente también activa el riesgo legal por incumplimientos regulatorios y de contratos, por demandas de usuarios, por supervisión de la Superindustria y otros, donde incluso los representantes legales o de la alta dirección y la junta directiva pueden ser afectados directamente al tener que responder por la organización que administran cuando no hay una debida administración de la ciberseguridad. Se afecta el principio de seguridad demostrada cuando no se puede demostrar que hubo un debido trabajo, un debido cuidado y una debida gestión de seguridad. Toda la planeación de la organización debe darse hacia mitigar no solo el riesgo operacional, sino también el riesgo legal sobre todo desde el punto de vista del manejo de crisis, algo que debe tenerse en cuenta en un plan de continuidad del negocio.

¿Por qué el sector salud es un objetivo para los atacantes?

Silgado presentó varios aspectos que hacen atractivo el sector salud para los ciberataques:

- La información privada de los pacientes vale mucho dinero para los atacantes.
- Los dispositivos médicos son un punto de entrada fácil para los atacantes, pues no tienen un ambiente de seguridad suficientemente robusto.
- El personal necesita acceder a los datos a distancia, lo que abre más posibilidades de ataque.
- Los trabajadores no quieren interrumpir sus cómodas prácticas laborales con la introducción de nuevas tecnologías; estos servicios no necesariamente son prácticas seguras.
- El personal médico y de apoyo no está sensibilizado generalmente sobre los riesgos en línea; se necesita un plan de sensibilización, porque normalmente el trabajo del día a día no permite que haya mucha sensibilización en términos de ciberseguridad.
- El número de dispositivos utilizados en los hospitales dificulta el control de la seguridad, porque muchos que se conectan a la red requieren conexión a los datos y controlarlos es una tarea difícil.
- Las organizaciones de salud más pequeñas también están en peligro: mientras más pequeñas, hacen menos inversiones en temas de ciberseguridad.
- La tecnología obsoleta hace que el sector salud no esté preparado para los ataques, por lo que debe gestionar este tema, ya que las vulnerabilidades y debilidades empiezan a verse con el tiempo y permiten que ocurran ataques.

Debe anotarse que el *ransomware* se incrementó seis veces más desde la pandemia por COVID-19 y Colombia empezó a recibir muchos más ataques que antes (recibe el 30 % de ataques de *ransomware* de Latinoamérica). Por ello, hay que hacer un trabajo más formal y estructurado de ciberseguridad en las organizaciones. El costo de los negocios para recuperarse del *ransomware* cuesta en promedio USD $1,4 millones, y el tiempo de recuperación es de un mes.

Tipos de amenazas al sector salud

Además del *ransomware*, existen otros tipos de amenazas para el sector salud. Las *Insider Threats* o amenazas internas, por personas que trabajan en las instituciones y tienen acceso a la información, y que podrían por descuido u omisión compartir o afectar información, o porque quiere hacerle algún daño a la institución.

También hay riesgos de los proveedores externos de la cadena de suministro, que no cumplan buenos estándares de seguridad y que ponen en riesgo la organización. Los ataques de *phishing* permiten capturar datos de la or-

ganización: estos ataques también vienen creciendo; cada vez son más sofisticados y hacen que las personas no noten la diferencia entre un correo de una persona real y otra que sea ataque de *phishing*. Otro riesgo es la vulnerabilidad en los dispositivos médicos, aquellos de ambientes de IoT (Internet de las Cosas) o IoMT (Internet de las Cosas Médicas).

En el sector salud, este es uno de los riesgos emergentes en temas de tecnología, y hay dos interesados en atacar el sector: los cibercriminales que quieren dinero, hacen el ataque y solicitan un pago del rescate en bitcoins; y los llamados *Nation-State* que atacan Estados (cuando un gobierno quiere atacar a otro, afecta las infraestructuras críticas del país, dentro de las cuales están los servicios de salud, de transporte, servicios públicos como el agua, el gas, la electricidad).

Advierte Silgado que hay ataques relacionados con falta de protecciones de los datos que impactan las aplicaciones y repositorios en donde se trabaja la información, por lo que se deben implementar unas debidas protecciones en las organizaciones. Por ello, reitera que el tema se enfoca más en la prevención, en tratar de evitar que ocurra, planear para evitar que ocurra, pero que en el momento en el que ocurra, enterarse lo más rápido posible para tomar una acción: "En estas capacidades que tenga la organización de reaccionar más rápido, hace que este impacto del incidente se contenga y sea mucho menor y no se vea afectada de manera severa".

Recomendaciones de ciberseguridad inmediata

- *Revise su estrategia de continuidad del negocio.* Valide que tenga su plan actualizado, que las estrategias establecidas de recuperación de los servicios operen ante un incidente de ciberseguridad; asimismo, que tiene los protocolos de respuesta de incidentes y manejo de crisis implementados y probados. Es necesario revisar que la cobertura del plan va a servir para escenarios de nuevas afectaciones como una amenaza de ransomware, planear para las amenazas que pueden afectar a la organización y cómo se recupera de esas amenazas.

El *ransomware* se incrementó seis veces más desde la pandemia por COVID-19 y Colombia empezó a recibir muchos más ataques que antes (recibe el 30 % de ataques de ransomware de Latinoamérica).

- *Hacer una prueba de sus procedimientos de respuesta a incidentes.* No basta tener un plan, sino ponerlo a prueba. Valide que sus procedimientos contemplen los diferentes escenarios de ataques de ciberseguridad; diseñe y ejecute simulacros de prueba de estos escenarios en ejercicios de escritorio o tipo *Table Top*, incluyendo a la alta dirección como participantes, y que las personas los conozcan, porque a veces estos planes no se divulgan y el día que ocurre algo buscan el plan, lo que hay que hacer, las actividades, lo cual demora aún más la recuperación.

- *Revise los controles fundamentales de prevención y reacción.* Debe implementar estos controles fundamentales para prevenir la ocurrencia de ataques.

  – Doble factor de autenticación para conexiones remotas, para accesos de administradores y para acceso de cuentas privilegiadas.

  – Parches de seguridad al día, al menos para vulnerabilidades críticas y altas. Son actualizaciones que pide el sistema operativo de las aplicaciones y las bases de datos que mantienen el sistema protegido, cierra

posibles huecos en la infraestructura y en vulnerabilidades críticas y altas.

– *Antimalware* o antivirus, y XDR instalado y actualizado: el antimalware o antivirus evolucionó a una tecnología llamada XDR que tiene un sonido de respuesta, que no solo dice 'aquí viene un virus' sino que, a partir del comportamiento de las conexiones, del acceso a las aplicaciones, la internet y demás, permite ver si hay algún tipo de intento de ataque o no. Y cuando lo hay, la herramienta alerta, habla con otras herramientas y deciden prevenir y bloquear.

– Datos sensibles y confidenciales protegidos con DLP y cifrado: el DLP es una herramienta de prevención de fuga de información. Cuando se identifica la información más sensible y más confidencial de la organización, se ubica y clasifica, esta herramienta la protege.

– Protección anti-x para el correo electrónico: antivirus, *antispam, antiphishing*, antitipos de ataques.

– *Back-ups* de la información frecuentes y probados: entre más frecuentes es mejor, porque así se pierde menos información en un ataque. Esos *back-up* tienen que estar fuera de la red y de los sistemas de la organización, porque cuando están dentro del mismo servidor o en otro servidor que puede ser potencialmente atacado no sirven ni serán efectivos.

– Bloqueo de las USB: porque pasan por muchos sitios y resultan infectadas.

– Realizar monitoreos a los eventos de los controles de ciberseguridad, considerar el uso de servicios de SOC (internos o externos): el monitoreo permite saber que está pasando. Al hacer monitoreo de dos o tres herramientas mencionadas, al tener control del monitoreo se sabe si alguien está haciendo algo y si se debe tomar alguna acción.

- ***Cree una campaña de sensibilización especial de alerta a todos sus empleados y terceros.*** Incluya en la campaña mensajes frecuentes que ayuden a los usuarios a identificar los tipos de escenarios de incidentes (mensajes de correo o de intranet), capacitarlos en qué hacer en caso de identificar un incidente (autoestudio o sesiones virtuales o presenciales), y evalúe conocimientos de los usuarios (pruebas de phishing y de ingeniería social telefónica). Si en un ataque la persona está bien sensibilizada, no comete el error de abrir un correo sospechoso o un link. Este control se vuelve indispensable y muchas veces puede ser más fuerte que cualquiera de los otros, porque se enseña al usuario cómo prevenir, cómo identificar riesgos y advertencias.

Otro punto relevante, concluye Silgado, es darle la importancia desde la alta dirección a este tema en la organización, porque muchas veces se subestima y dicen "seguridad es una pequeña área de la tecnología, es una persona que ni siquiera trabaja tiempo completo para seguridad o el administrador de algo al que vuelven administrador de seguridad, y se cree que con eso es suficiente". Afirma el experto: "No necesariamente una organización tiene que invertir millones para tener una buena salud en seguridad, pero sí debe tener una buena identificación de sus puntos débiles y cómo asegurarlos, eso debe ser lo fundamental".

Diagnóstico y tratamiento de vulnerabilidades, y cultura de seguridad protectora, propone Expertos Seguridad

Foto: Cortesía Expertos Seguridad

Alberito Henao Zuluaga, Gerente
Expertos Seguridad Limitada

Albeiro Henao Zuluaga, gerente general de Expertos Seguridad Limitada, recomienda que, ante un ciberataque, lo primero que se debe hacer es un diagnóstico de la seguridad del ciberespacio y de la información para establecer el grado de vulnerabilidad de los sistemas de información y, luego, determinar estrategias de seguridad informática que permitan neutralizar ese ataque.

El diagnóstico se puede hacer mediante un "*hackeo* ético", una planificación de una intrusión mediante redes, correos electrónicos y la página web; así lo explica Henao Zuluaga: "Una vez determino qué vulnerabilidades tengo y las posibilidades de ser vulnerado por un ataque cibernético, procedo a establecer las estrategias. Nosotros tenemos herramientas como el Resecurity, un reseteo a los sistemas informáticos donde establecemos, mediante un hackeo ético, qué ventanas están abiertas y cómo pueden acceder no solo desde el punto de vista del hardware, sino del software, y desde la ingeniería social".

Explica el experto que la ingeniería social son aquellas actividades de inteligencia humana de *hackers* no éticos que pretenden vulnerar los sistemas de seguridad de la información de las empresas: "Ellos recurren al *malware*, al *phishing,* estratagemas que mediante el engaño hacen que la persona acceda a un sistema operativo y abra una ventana o descargue un sistema operativo que genere los mal llamados "gusanos informáticos", que acceden a la información, y ahí permiten vulnerar los sistemas de seguridad, sustrayendo información de manera continua o secuestrando, mediante el *ransonware,* información crítica de las compañías para posteriormente acudir a la extorsión o al chantaje como una medida de presión con fines lucrativos".

Indica Henao Zuluaga que, mediante ese diagnóstico, se establece la escala de vulnerabilidad en un rango medio, bajo o alto, para adoptar las medidas de tratamiento o protección de la seguridad en el ciberespacio: "Eso implica unos modelos o herramientas de monitoreo permanente frente a ataques continuos, en primer lugar, y en segundo lugar establecer los cortafuegos necesarios. Hay un aspecto muy importante que está ausente en las entidades en general, y es la cultura de la seguridad de la información: los líderes de las empresas debemos ser conscientes que tanto la seguridad física, en sus modos generales, como la seguridad informática hoy son susceptibles de ser vulneradas frente a las amenazas latentes de la asimetría del terrorismo en el ciberespacio".

Frente a este tema, agregó: "Anteriormente nos fijábamos solamente en que habían unos riesgos potenciales de cara a las medidas de seguridad física, eventualmente contra las locaciones, la infraestructura, las personas y demás, pero hoy después de la pandemia, la tecnología y las formas virtuales que se utilizan en el teletrabajo llegaron para quedarse; eso implica que la susceptibilidad de los sistemas de información tanto en el hogar como en la empresa, hace que exista la amenaza latente de manera permanente. Entonces ahí es donde vienen a implementarse

no solo los antivirus y los *firewall* como los sistemas básicos de las compañías en sus entornos o ecosistemas informáticos, sino otras medidas más sofisticadas y de otro nivel".

Por eso, Expertos Seguridad recomienda incorporar el trabajo de profesionales que tengan las capacidades y características en sus competencias acordes a la amenaza asimétrica a la que están expuestas las organizaciones y, adicionalmente, incorporar las herramientas de *software* o de monitoreo que permiten detectar de manera oportuna y neutralizar las amenazas de los ciberataques; es decir, básicamente hacer el diagnóstico para determinar el tratamiento.

Henao Zuluaga también recomienda unas medidas básicas como el nivel de accesibilidad de acuerdo con el rango y la confianza de los empleados, y clausurar completamente en el *hardware* o equipos de las empresas los puertos para sustraer información con *memory kits* que introducen *malwares* o gusanos informáticos dentro del sistema o ecosistema digital de la compañía. En suma, se proponen medidas físicas, medidas lógicas y medidas de carácter cultural o psicológico, en lo que consideran un verdadero y adecuado triángulo protector en temas de ciberespacio.

En este panorama, hospitales y clínicas son altamente sensibles a riesgos cibernéticos, y así lo aclara Henao Zuluaga: "La tecnificación y la digitalización de los procesos en las clínicas y hospitales hacen que de una u otra manera los ecosistemas sean vulnerables a bloqueos o al secuestro de la información; no solo es accesibilidad por la sensibilidad de la información sino por la sustracción y al bloqueo de la operatividad en los procesos médicos y clínicos; entonces este sector de la industria como las clínicas y hospitales son altísimamente sensibles a los ataques cibernéticos y a la vulnerabilidad que hoy genera esta economía global supeditada a la digitalización de la información y a los sistemas informáticos expuestos desde la misma internet".

Lecciones aprendidas y recomendaciones de ciberseguridad

Expertos Seguridad se ha dedicado al fortalecimiento de la cultura de seguridad en el sector salud. Esto señala el gerente: "En diversas entidades del sector hemos fortalecido la cultura de seguridad y protección de la información y de transmitir la alerta temprana en términos de esa escalabilidad que debe mantenerse en los accesos. Es decir, hemos integrado y automatizado procesos desde el carácter físico porque controlamos desde el ingreso a hospitales y clínicas, desde el ingreso tenemos plenamente identificadas a las personas y hacemos una traza con un *software* que diseñamos y patentamos en Expertos Seguridad, que nos permite identificar las personas que ingresan a las dependencias y servicios asistenciales de clínicas y hospitales. Esto permite que la persona se dirija a los lugares exactos donde se determinó la autorización o el permiso, que no esté en áreas restringidas, que no esté abordando los sistemas informáticos de manera subrepticia o no controlada, y esto de una u otra manera minimiza el riesgo potencial del acceso físico del antisocial dentro de estas organizaciones".

Henao Zuluaga hizo un llamado a los directivos: "Quiero llamar a los líderes de empresas que manejan información digital y en la nube a generar no solo planes de concienciación de la vulnerabilidad a la que estamos expuestos como una amenaza asimétrica global a las compañías de cualquier naturaleza, sino que también seamos previsivos en establecer desde nuestros presupuestos los rubros necesarios para intervenir estas áreas de gestión. La falta de conciencia de la existencia de un riesgo ya inmerso dentro de la gestión organizacional hace ver la necesidad de establecer los presupuestos necesarios para implementar las medidas de seguridad necesarias no solamente desde el *software*, desde la estructura y de la arquitectura de gestión que se requiere, sino también desde el *hardware* para efectos de tener esquemas robustos y tener los asesores necesarios en seguridad informática".

“Concientización del equipo interno, apoyo externo y planes de contingencia para prevenir y gestionar ataques”: Méderi

“De acuerdo a como hemos visto que se realizan los ciberataques en el sector salud, lo más importante es la concienciación o concientización al personal en las instituciones; es uno de los principales factores porque por ellos nos volvemos débiles o vulnerables, al no tener ellos una capacitación o formación permanente sobre los riesgos y amenazas que hay en el mercado. Ellos no validan y simplemente consultan lo que otros envían, sin darse cuenta que ahí, independiente del nivel que tengan dentro de las entidades, generan unos riesgos importantes como lo hemos visto en muchísimas instituciones”.

Así lo afirmó Constanza Rodríguez, jefe de TIC en Méderi, quien agrega que para enfrentar los ciberataques se debe hacer gestión sobre los recursos de tecnología en las instituciones, con apoyo de expertos en seguridad externos: “Al interior de las instituciones de salud no contamos con equipos de trabajo tan grandes ni con tanto conocimiento y experiencia para lograr la seguridad. En el mercado hay unos expertos muy buenos a nivel internacional y nacional que tienen que ser nuestros aliados, para que, con su experiencia y conocimiento, nosotros mitiguemos al máximo los riesgos que se presentan en las instituciones”.

Un tercer factor fundamental son los planes de contingencia, indicó Rodríguez: “Como nada de estas cosas es infalible, como lo acabamos de ver con este ataque tan monstruoso a nivel nacional e internacional (caso IFX), los planes de contingencia son la posibilidad de continuidad de nuestros servicios de salud. Y hay que estar evaluando esos planes, porque hoy tenemos un recurso humano diferente a unos años atrás; cuando no tenemos sistema de información, el usuario final en una contingencia ya no quiere escribir, porque está enseñado a que todo se volvió electrónico. Entonces, el plan de contingencia tiene que ir de la mano con soluciones digitales”.

Explica la jefe de TIC de Méderi que los planes de contingencia son los que permiten pensar metas en doble continuidad o continuidad de la operación, es decir, tener recursos disponibles alternos para seguir operando: “Ese plan de recuperación tiene que estar en nuestras instituciones; resulta obvio que tiene un tema económico importante, un tema de gestión importante, pero hoy por hoy —y nos lo demostró este último ataque— perdemos más no teniéndolo, perdemos más de nuestros ingresos, perdemos más en nuestra reputación, perdemos más en nues-

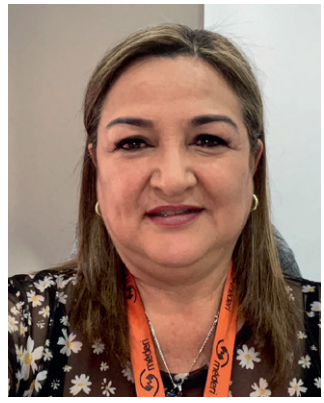


Foto: Archivo personal

Constanza Rodríguez, Jefe TIC en Méderi

tra confiabilidad del mercado de prestación de servicios de salud".

Agregó que en el plan de contingencia son importantes los sistemas de respaldo de la información, los procesos de *back-up*, las recuperaciones y las pruebas sobre el sistema de información, para que, cuando los ciberdelincuentes sustraigan la información, las instituciones tengan otro medio de recuperación de una información que previamente esté al día. Hacer estos procesos son los grandes retos para quienes manejan los procesos de tecnología en empresas del sector salud.

Para dar una idea del volumen de intentos de ataques que puede tener una institución de salud, señaló que Méderi registra más de 350.000 intenciones de ataques al mes, lo que califica de 'una cosa monstruosa'. Por ello, se han visto en la necesidad de alcanzar un grado de madurez en el tema y contar con aliados adecuados en estos procesos, para validar por ejemplo los intentos de *phishing,* que les envían a diario, y con los equipos biomédicos que constituyen hoy un riesgo altísimo para las instituciones.

Explica Rodríguez: "Antes pensábamos que una impresora o un escáner eran un riesgo, pero hoy que todos los equipos biomédicos son utilizados e intercomunicados a través de interoperabilidad con los sistemas de información, y ellos son un riesgo, entonces lo primero que debe hacerse es validar el proceso de vulnerabilidades que ellos nos generan y hacer todo el tema de remediación técnicamente para evitar que esas puertas abiertas que dejamos cuando instalamos esos equipos, se conviertan en una debilidad para nosotros y una oportunidad para el atacante".

La jefe de TIC de Méderi señala que indiscutiblemente hay que estar siempre alerta y que las alertas tienen que estar acompañadas de tecnología, de herramientas que de forma predictiva y anticipada puedan evitar lo que quieren intentar los atacantes dentro de las instituciones o por la vía que quieren ingresar. Y ya cuando se presenta el ataque, aplicar los planes de contingencia.

"Integrar personas, procesos y tecnología en la ciberseguridad": Fundación Santa Fe de Bogotá

Foto: Archivo personal

Jorge Mario Arango, Oficial de Seguridad de la Información y Protección de Datos Personales de la Fundación Santa fe de Bogotá

Jorge Mario Arango García, Oficial de Seguridad de la Información y Protección de Datos Personales de la Fundación Santa Fe de Bogotá, señala que, dentro de las lecciones y recomendaciones en materia de prevenir y resolver posibles ciberataques, lo principal es abordar la ciberseguridad con un enfoque que integre las personas, los procesos y la tecnología.

El experto explica que un punto muy importante es lograr que las personas tengan conciencia de los riesgos de ciberseguridad y comprendan de forma clara cómo protegerse. En este sentido, recomienda realizar ejercicios de apropiación de conceptos y medidas en los usuarios no técnicos, y contar con indicadores que midan el efecto de las acciones realizadas en los usuarios de la entidad, buscando mejorar el nivel de cultura de ciberseguridad.

Por otro lado, y como agrega Arango García, es muy importante contar con una estrategia, con una hoja de ruta definida que se adapte a todos los riesgos emergentes que van surgiendo.

En la Fundación Santa Fe de Bogotá, dicha estrategia se basa en cuatro pilares importantes que ha definido la organización:

- Gestión del Riesgo de la Operación.
- Datos, Privacidad y Cultura.
- Ciberseguridad Asistencial, Clínica e Infraestructura Hospitalaria.
- Gestión de la Cadena de Suministro.

Estas son algunas de las recomendaciones que se pueden replicar en otras organizaciones del sector salud, entendiendo que la dinámica de todas las instituciones puede ser diferente.

Finalmente, desde la experticia de la Fundación, se insiste en que, ante cualquier estrategia de prevención, es necesario comprender los riesgos propios del negocio: una vez se entienden estos riesgos, se pueden priorizar los controles de ciberseguridad correspondientes.

Controles de ciberseguridad: un reto de la era digital

La ciberseguridad es un tema que se ha convertido en un pilar fundamental para la integridad, sostenibilidad y seguridad en la era digital. Establecer controles efectivos y prepararse para recuperarse de un posible ataque cibernético es esencial para el bienestar de las empresas y sus activos. Es por esto que, desde un hospital afiliado a la Asociación Colombiana de Hospitales y Clínicas (ACHC), que pidió no ser identificado, se recomienda el siguiente enfoque estructurado para fortalecer la postura frente al control de la ciberseguridad:

1. *Marco de trabajo: definiendo estrategias.* El primer paso crucial es establecer un marco de trabajo que guíe las estrategias de ciberseguridad. Así, se deben adoptar estándares reconocidos como NIST, ISO 27001 o HIPAA que proporcionan un fundamento sólido. Estos marcos no solo establecen directrices claras, sino que también facilitan la adhesión a normas globalmente aceptadas.

2. *Estrategias y líneas base: mejorando la postura de ciberseguridad.* Para fortalecer la seguridad, es vital implementar estrategias específicas basadas en los marcos de trabajo seleccionados. Estas estrategias, también conocidas como líneas base, se centran en los controles de seguridad críticos de la siguiente manera:

- *Identificación: conociendo el terreno*
  - Activos: identificar los activos digitales esenciales para el negocio.
  - Ambiente del negocio: comprender el contexto operativo y las interdependencias.
  - Gobierno: establecer una estructura clara de gobierno para la ciberseguridad.
  - Riesgos: evaluar y categorizar los riesgos potenciales.
  - Estrategia de riesgos: desarrollar estrategias efectivas para gestionar los riesgos identificados.

- *Protección: salvaguardando la información*
  - Controles de acceso: implementar medidas robustas para restringir el acceso no autorizado.
  - Concientización del empleado: educar a los empleados sobre seguridad de datos.
  - Procesos y procedimientos: establecer protocolos para la protección de la información.
  - Tecnologías de protección: utilizar programas de protección para salvaguardar activamente contra amenazas.

- *Detección: anticipándose a las amenazas*
  - Anomalías y eventos: identificar comportamientos anómalos y eventos sospechosos.
  - Proceso de detección: implementar procedimientos efectivos para la detección temprana.

- Monitoreo continuo: mantener una vigilancia constante de la seguridad.

- *Respuesta: actuando con eficiencia*
  - Plan de respuesta a incidentes: desarrollar un plan detallado para responder a posibles incidentes.
  - Plan de comunicación: establecer un protocolo claro de comunicación durante situaciones críticas.
  - Análisis, mitigación y mejoras: evaluar, mitigar y aprender de cada incidente para mejorar continuamente.

- *Recuperación: volviendo a la normalidad*
  - Planes de recuperación: contar con planes detallados para restaurar operaciones tras un incidente.

Adoptar estos controles de ciberseguridad no solo protege los activos digitales de las empresas, sino que también contribuye a la confianza de los usuarios y la integridad de las entidades en un mundo digital cada vez más complejo.

Referencias

Banco Interamericano de Desarrollo [BID]. (2021). *Protegiendo la salud digital: Una guía de ciberseguridad en el sector salud.* Banco Interamericano de Desarrollo BID. https://publications.iadb.org/es/protegiendo-la-salud-digital-una-guia-de-ciberseguridad-en-el-sector-de-salud

Betancourt, Alejandra. (2023, 18 de noviembre). 5 millones de dólares en criptomonedas deberá pagar el INVIMA para recuperar su web. *Enter.co.* https://www.enter.co/colombia/5-millones-de-dolares-en-criptomonedas-debera-pagar-el-invima-para-recuperar-su-web/

City TV - El Tiempo. (2023). *Los ciberdelitos han registrado un aumento del 1,8% en el territorio nacional.* https://citytv.eltiempo.com/noticias/seguridad/los-ciberdelitos-han-registrado-un-aumento-del-18-en-el-territorio-nacional_65377

Critical Insight. (2023). *Healthcare breaches on the rise in 2022*. https://cybersecurity.criticalinsight.com/healthcare-breach-report-h1-2022

Dräger. (2017). *La ciberseguridad en los hospitales. Cómo contribuirá Dräger a que su hospital sea un lugar seguro.* Drägerwerk AG & Co. KGaA. https://www.draeger.com/Content/Documents/Content/how-draeger-will-help-keep-your-hospital-safe-br-pdf-10431-es.pdf

EMR. (2023). Análisis de la Industria de la Ciberseguridad en Colombia. https://www.informesdeexpertos.com/informes/mercado-de-la-ciberseguridad-en-colombia

Gómez-Pinzón. (2023). Guía de obligaciones en materia de ciberseguridad para el sector de la salud en Colombia. https://gomezpinzon.com/wp-content/uploads/2023/06/GUIA-LEGAL-CIBERSEGURIDAD-SALUD.pdf

González, Diana. (2023). *Ciberataques en Colombia siguen en aumento en el 2023*. Intexus. https://blog.intexus.la/ciberataques-en-colombia-en-el-2023#:~:text=Ciberataques%20en%20Colombia%20en%20el,su%20plataforma%20de%20correo%20corporativo

Infobae. (2023). *Las 34 empresas que fueron hackeadas en Colombia durante 2022*. https://www.infobae.com/america/tecno/2023/01/02/las-34-empresas-que-fueron-hackeadas-encolombia-durante-2022/

Itech SAS. (2023). *Listado de empresas afectadas por Ransomware en Colombia*. https://www.itechsas.com/blog/ciberseguridad/listado-de-empresas-afectadas-por-ransomware-en-colombia/

Kaspersky. (2022). ¿Qué es la ciberseguridad? https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Luna, David; Castañeda, Ana María y Sogamoso, Ingrid. (2023). *Informe de ponencia para primer debate Proyecto de Ley No. 010 de 2023 Senado "Por la cual se crea la Agencia Nacional de Seguridad Digital y se fijan algunas competencias específicas".* Gaceta del Congreso N.º 901 de 2023.

Morante, Andrea. (2017, 13 de mayo). Instituto Nacional de Salud entre víctimas de ciberataque mundial. *El Tiempo.* https://www.eltiempo.com/tecnosfera/novedades-tecnologia/alerta-por-cibertaque-que-golpeo-a-74-paises-87602

Resolución 866 de 2021 [Ministerio De Salud Y Protección Social y Ministerio de Tecnologías de la Información y Comunicaciones]. Por la cual se reglamenta el conjunto de elementos de datos clínicos relevantes para la interoperabilidad de la historia clínica y se dictan otras disposiciones. 25 de junio de 2021. Diario Oficial N.º 51.716 de 25 de junio de 2021.