Asociación Colombiana
de Hospitales y Clínicas

ISSN digital: 2745-0740
ISSN impreso: 0123-8760

Hospitalaria®

www.revistahospitalaria.org

LA REVISTA DEL SECTOR

25 AÑOS

SALUD COLOMBIANO

| Año 25 Nº 144 | noviembre 2023 - enero 2024 |

Asociación Colombiana de Hospitales y Clínicas

ISSN digital: 2745-0740
ISSN impreso: 0123-8760

Hospitalaria®

www.revistahospitalaria.org

Ciberseguridad en el sector salud

Calidad e innovación para mejorar TU SALUD

Oferta de servicios

Brindamos atención humanizada
y de calidad a nuestros usuarios.

- Consulta médica general y especializada
- Promoción y prevención
- Atención domiciliaria
- Odontología
- Imagenología
- Rehabilitación
- Procedimientos diagnósticos especializados
- Urgencias y hospitalización
- Cirugía ambulatoria
- Programas de cohortes especializadas

Más de **100 sedes integradas en red** en toda **Colombia**

Escanea éste código *y conoce más de nuestro portafolio de servicios*

www.virreysolisips.com

SaludTotal EPS-S / VIRREY SOLIS I.P.S.

| Año 25 Nº 144 | noviembre 2023 - enero 2024 |

Hospitalaria®

www.revistahospitalaria.org

ISSN digital 2745-0740 – ISSN impreso: 0123-8760

Para correspondencia por favor dirigirse a la Asociación Colombiana
de Hospitales y Clínicas. Cra. 4 Nº 73-15, Bogotá.
PBX: (1) 312 4411 - FAX: (1) 312 1005
E-mail: comunicaciones@achc.org.co
Internet: www.achc.org.co

DIRECCIÓN DE ARTE/DISEÑO GRÁFICO
Jesús Alberto Galindo Prada
almadigital2010@gmail.com

COMERCIALIZACIÓN PUBLICIDAD
Cila María Russi
publicidadhospitalaria@achc.org.co

ILUSTRACIÓN PORTADA
MIQUELOFF

Un cuarto de siglo

Hospitalaria completó sus primeros 25 años de circulación ininterrumpida, constituyéndose así en la publicación del sector hospitalario colombiano con mayor presencia en la historia y en la vida de los hospitales y clínicas de nuestro país.

Ni la pandemia por COVID-19, que tantos estragos causó en todos los frentes de la actividad humana, impidió que la Revista continuara su labor sin interrupción; únicamente obligó a acelerar la transición a un medio digital, que ya se venía analizando como una alternativa necesaria en un sector que, como el de la salud, depende cada día en mayor medida de la tecnología digital. Para nuestra sorpresa, además de la gran acogida de la versión digital, nuestros lectores han sido insistentes en la necesidad de tener también el medio impreso, pues lo consideran una fuente de consulta permanente, por lo que hemos tomado la decisión de mantener simultáneamente las dos versiones.

Reconocemos la importancia de tener un portal digital dinámico que responda a todas las necesidades del sector. Como ustedes habrán observado, el portal no solamente permite consultar el contenido de la Revista, sino también descargarlo, estando disponibles todos los números publicados en estos 25 años. Además, hemos querido que el portal tenga actividad permanente mostrando notas de actualidad y noticias del sector, en donde se destacan los hechos principales de la agenda gremial, así como temas relacionados con nuestros patrocinadores y cifras sectoriales que consideramos de interés. Para quienes no lo hayan visitado, los invitamos a hacerlo en la siguiente dirección: https://revistahospitalaria.org/

Del material publicado en estos años, se destacan documentos técnicos en los que se han presentado al sector la visión y propuestas del gremio para avanzar a un mejor sistema de salud como: Hospital 360°, Insight, Alternativas y Equilibrios, Salud Progresiva y Espacio en Blanco, el más reciente. Además, el estudio de salarios del sector, que realiza el equipo de investigación de la ACHC y que publicamos anualmente desde 2007. Este trabajo constituye una herramienta muy útil para quienes tienen que tomar decisiones salariales en sus organizaciones. Además, es un referente nacional y regional empleado en estudios e investigaciones sectoriales.

De las publicaciones recientes se destacan cuatro números que dedicamos a temas relacionados con la pandemia por COVID-19: en el primero de ellos, se presentan las experiencias de hospitales y clínicas colombianos en la preparación para la atención de la COVID-19 (octubre de 2020, Edición 130); luego, revisamos la vacunación contra la COVID-19 en Colombia (julio de 2021, Edición 133); también analizamos los impactos de la pandemia por COVID-19 en la salud mental en nuestro país (noviembre de 2021, Edición 134); finalmente, abordamos el tema de complicaciones y represa de atenciones en salud: el daño colateral de la pandemia (enero 2022, Edición 135). Estos números constituyen un testimonio histórico de la magnitud del desempeño sobresaliente de nuestro sistema de salud en temas críticos como la vacunación y la atención hospitalaria. Especialmente, se resalta la respuesta heroica de los hospitales y clínicas para lograr servir adecuada y oportunamente a la población colombiana en una situación tan crítica, como no había tenido que enfrentar la humanidad en tiempos recientes. Al revisar estas situaciones, resulta clara la razón para el reconocimiento y agradecimiento de la sociedad colombiana para con el cuerpo médico, los trabajadores de la salud y hospitales y clínicas del país.

Otros temas han sido constantes en estos años, como la cartera hospitalaria que sigue sin encontrar una solución definitiva, por lo que representa una de las principales fallas de nuestro actual sistema de salud y constituye una amenaza permanente para la operación adecuada de los prestadores. Si bien reconocemos los esfuerzos que se realizaron en el gobierno anterior con la estrategia de "punto final" que logró un alivio, desafortunadamente no constituyó la solución definitiva que todos anhelábamos.

También hemos abordado temas recurrentes como las liquidaciones de las EPS y el enorme impacto que han tenido sobre los hospitales y clínicas, que finalmente han resultado castigados con pasivos que debían asumir accionistas y dueños de las empresas que los generaron. Los intentos para reformar el sistema de salud han sido reiterados y han terminado naufragando en su trámite por el Congreso. Durante el último año, hemos presenciado el intenso debate que se ha suscitado en torno al proyecto de Ley 339, que ya surtió su trámite en la Cámara y próximamente hará lo propio en el Senado, sin que se vea por ahora con claridad con qué suerte correrá en la comisión séptima y, finalmente, en la plenaria.

Hemos resaltado temas que son cruciales para la actividad hospitalaria moderna y, en general, para el sector salud en este comienzo del siglo XXI, como son aquellos de la tecnología digital que incluyen la telemedicina y su gran desarrollo impulsado enormemente durante la pandemia, pero que continúa al haberse demostrado el papel que puede tener para beneficio de los pacientes. Analizamos también la actualidad en materia de Big Data y su desarrollo en el país. Asimismo, retomamos en otra edición el tema de la telemedicina en el contexto más amplio de telesalud.

Hemos resaltado temas que son cruciales para la actividad hospitalaria moderna y, en general, para el sector salud en este comienzo del siglo XXI, como son aquellos de la tecnología digital que incluyen la telemedicina y su gran desarrollo impulsado enormemente durante la pandemia

En esta misma edición, abordamos como eje central la ciberseguridad debido a que conlleva un compromiso moral, legal y de sostenibilidad del sector salud. El tema para muchos resulta extraño, pero como se muestra en el artículo central, durante 2022 y 2023 varias entidades del sector sufrieron ataques de diversa intensidad que trajeron en muchas ocasiones importantes consecuencias en la continuidad de sus servicios y un impacto financiero. Entidades gubernamentales como el INVIMA, varias EPS, gestores farmacéuticos y hospitales y clínicas han sido víctimas de ataques de diversa magnitud, además de innumerables intentos que han podido ser contenidos antes de que produjeran efectos gracias a buenos sistemas preventivos. Mantener las instituciones del sector protegidas contra posibles ataques cibernéticos se convierte en una cuestión prioritaria para el sector.

Culminamos así los primeros veinticinco años de *Hospitalaria*, que inicia este nuevo tramo de su historia, fiel al compromiso de constituirse en un medio de información veraz, que analiza la actualidad, promueve y difunde la investigación y la innovación, y propone soluciones, sin abandonar su compromiso gremial con el sector prestador, en su calidad de órgano oficial de la Asociación Colombiana de Hospitales y Clínicas, pero teniendo siempre como norte lo que más convenga a la salud de los colombianos. Son estas características las que la han llevado a ser considerada un medio de consulta confiable y respetado por todos los sectores.

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.

Retos y aprendizajes de un modelo de atención integral de hemofilia y otras patologías de la coagulación

Un modelo de atención integral que demostró resultados exitosos en los pacientes atendidos y que, no solo se centró en la parte clínica, sino también en los aspectos psicosociales de cada paciente para lograr una mejor calidad de vida.

La enfermedad de Von Willebrand (EWV), más conocida como hemofilia, y los trastornos de la coagulación son enfermedades huérfanas y hereditarias que se caracterizan por la deficiencia de factores de coagulación, que podrían conducir a sangrados peligrosos, e incluso, mortales. Para el tratamiento de estas enfermedades, es necesario el concurso interdisciplinario e integrado de especialistas e instituciones en red, debido al alto costo que el tratamiento implica y al tratamiento personalizado.

Cuando se habla de tratamiento integral, se hace referencia tanto a la aplicación del medicamento como a todas las estrategias de educación para su uso y el apoyo sicosocial que oriente hacia un proyecto de vida productivo, promoción de hábitos saludables para la prevención de daño articular y otras secuelas, manejo directo de su enfermedad de base y manejo indirecto de comorbilidades y, finalmente, rehabilitación y cuidados paliativos con relación al dolor, cuando lo requieran.

COHAN articulador de la Ruta de Integración de hemofilia

En 2019 COHAN firma un convenio con Savia Salud EPS para la dispensación del medicamento para su cohorte de hemofilia, y con Colombia Saludable para su aplicación. Ya para el segundo semestre del mismo año, se crea la Unión Temporal Gestión Integral de Hemofilia bajo el liderazgo de COHAN que articula esta atención en red.

Comenzó con la caracterización de la población, el mantenimiento de la profilaxis y las urgencias. Luego se evidenció una población muy poco adherente, con unos indicadores clínicos y administrativos desfavorables; las tasas de sangrado y hospitalizaciones anuales altas que aumentaban los costos y no se lograba impactar en los resultados de salud. Además, los pacientes tenían, aparte de su enfermedad, complejas dificultades socioeconómicas, familiares y sicosociales que obstaculizaban su manejo.

Retos y logros en el camino

En el primer año se impactaron las tasas de sangrado con inhibidores, pero con un costo alto para el programa y el sistema. Un estudio juicioso de costo-efectividad permitió, en conjunto con el asegurador, el ingreso de medicamentos para un tratamiento vanguardista con terapia de no reemplazo con anticuerpo monoclonal (Emicizumab), que redujo a cero las tasas de sangrado de los pacientes, y los costos por complicaciones.

En 2020, en diferentes reuniones con la Dirección Científica de COHAN, se empezó a construir la parte teórica de un programa ideal para tener el mejor programa de hemofilia centrado en el paciente, basado en los últimos protocolos y publicaciones, referenciándose con programas de trayectoria nacionales e internacionales y con la experiencia de los profesionales, ajustando todo a la realidad del país y la población.

Dado que, en ese momento se vivía la cuarentena por motivo del COVID-19, se habilitó el servicio de telemedicina y se creó un canal de YouTube para mantener la educación continua de los usuarios. De igual forma, se identificaron los factores de riesgo sicosociales que más afectaban la adherencia, y aumentaban sangrados y hospitalizaciones, haciendo estrategias de intervención con el asegurador. Se identificaron los factores de riesgo biológicos que incidían negativamente en las tasas de sangrado y, mediante la farmacocinética, se hicieron ajustes en la profilaxis de los pacientes, obteniendo una optimización del factor y mejores resultados clínicos y económicos.

En 2021, con el objetivo de hacer una adecuada clasificación clínica de los pacientes en términos de salud articular, se ajustó la modalidad de atención ambulatoria mediante las jornadas transdisciplinarias (juntas médicas en las que el paciente ingresa a valoración simultánea por hematología y equipo músculoesquelético para tomar decisiones conjuntas que involucran la profilaxis y actividad física o de rehabilitación).

La consolidación de este equipo multidisciplinario permitió mayor integración con todos los miembros de la Unión Temporal, mediante realización de mesas técnicas, capacitaciones y comunicación permanente para la atención integrada de la población, incluyendo también en el programa, un manejo integral de mujeres portadoras de hemofilia.

Para 2022 se evaluaron los resultados para ajustar los procesos. Tras dos años de gestión se empezaron a ver esos resultados en un menor número de hospitalizaciones, la optimización en el manejo de las urgencias y disminución de las recurrencias de sangrados en un mismo paciente, e impacto en salud articular. Gracias a los ajustes al modelo de atención inicial, se creó el "Modelo Medellín" con una atención conjunta, evaluando farmacocinética y ecografía en cada consulta para dar planes de manejo individualizados de cada especialidad.

Otros logros importantes han sido la generación del Protocolo de Fisioterapia individualizado por grupos de riesgo para daño articular, el entrenamiento y uso de ecografía articular como parte de la atención integral del paciente en cada consulta, el fortalecimiento en la plataforma de farmacocinética que viene permitiendo el ingreso de factores con nuevas tecnologías más costo-efectivas, la realización de nueva caracterización de la población integrando aspectos sicosociales y biológicos, y la incorporación al equipo de genetista y ginecólogo para el apoyo, principalmente, en el programa de portadoras.

INSTITUCIONES ALIADAS DE LA RUTA INTEGRAL DE HEMOFILIA

cohan Más vital	Responsable de articular a todas las instituciones que se unen para que la Ruta sea integral, dar todo el direccionamiento del programa (técnico y administrativo) y evaluar la gestión y resultados del mismo. Adicionalmente, cuenta con el Servicio Farmacéutico para la custodia y distribución de los medicamentos de la coagulación requeridos para las profilaxis y urgencias de los pacientes de la cohorte.
MEDICI	Para facilitar la gestión del riesgo, se ubicó al equipo multidisciplinario en una sola institución articuladora, se concentró la atención ambulatoria y la atención integral en MEDICI, la IPS especializada de COHAN y sus asociados en enfermedades huérfanas y de alto costo.
Colombia saludable	Responsable de la aplicación domiciliaria del medicamento ("Home Care") y de la atención de urgencias domiciliarias, es decir, aquellas en donde no está en riesgo la vida del paciente. Además, proporciona el equipo para la consulta de factores músculoesqueléticos.
Manuel Uribe Angel E.S.E. HOSPITAL Vinculados con la Vida!	IPS aliada para la atención ambulatoria de hematología y otros; emergencias, sangrados que ponen en riesgo la vida, hospitalización, cirugías y procedimientos.
Metrosalud	Entidad a cargo de la atención en salud oral tanto en actividades programadas de promoción, prevención y recuperación de la salud, como en tratamientos de urgencias.

APRENDIZAJES

- Los modelos de atención en hemofilia se deben adaptar a las necesidades de la población, porque el comportamiento clínico de la enfermedad es modificado por variables externas como las socioeconómicas, culturales, laborales y de hábitos saludables.
- Una población de régimen subsidiado tiene gran vulnerabilidad y debe recibir una intervención integral, de ahí que la estabilidad del equipo multidisciplinario es fundamental para lograr la adherencia del paciente al programa.
- Este tipo de programas se debe proyectar a, mínimo, diez años de gestión, si realmente se quiere evaluar el impacto de las intervenciones. Durante estos tres años se lograron los objetivos trazados, mas un periodo de seguimiento mayor posibilita evaluar resultados en salud articular que les permitan tener las mismas oportunidades que la población general y con buena calidad de vida.

En memoria

Ana María De Brigard

Ana María De Brigard no solo fue la mejor abogada de los médicos, de los hospitales y de las decisiones éticas del sector salud. Ana María ejerció la inteligencia, la amistad y la autonomía como consignas de vida, sin treguas ni ambivalencias. Defendía sus causas con una mezcla perfecta de razón y pasión; de lealtad con la verdad y de conocimiento decantado por una vida de estudio y de ejercicio profesional impecable y retador.

Ana María respetó siempre la palabra y las palabras precisas, y construyó sus argumentos sin lugar a grietas ni fisuras. Como buena lectora de lo académico y de novelas, de historia y biografías, construyó una cultura llena de humanismo y de batallas ganadas por la perseverancia. Trabajó desde su adolescencia con y por la comunidad, porque le apasionaba la justicia y tenía una especial sensibilidad por la capacidad de cada ser humano de tomar sus propias decisiones. Ana María enseñaba en las aulas y en los hospitales, enseñaba con lo que hacía, con lo que era, con lo que pensaba y sentía.

Amó y respetó a su familia y a sus amigos con intensidad, con solidaridad y devoción, y a todos los dejó ser, los dejó volar y vivir según los hilos que cada uno -cada una- había tejido en sus propios silencios y fortalezas, mejor dicho, en su propio espíritu.

Su vida y su muerte fueron coherentes con ella misma, con sus principios y con su irrenunciable defensa de la autonomía.

Ana María vivió la vida y no dejó pasar una sola oportunidad de ser feliz, de reírse a carcajadas, de abrazar con fuerza y mirar con luz propia los colores del mundo. Nada le pasaba desapercibido y nada en ella fue evasivo ni borroso. No ahorró emociones, no ahorró claridades ni contundencia… como si hubiera sabido que la vida sería breve, que casi todo es ahora o nunca.

Por 17 años Ana María de Brigard fue la asesora jurídica de la ACHC; durante 13 años nos acompañó en el comité editorial de esta revista y en 5 oportunidades fue la gerente de los congresos internacionales organizados por la Asociación.

Hoy no la despedimos, porque parte de Ana María seguirá viviendo en las páginas de *Hospitalaria* y en los escritorios de la casa, en los conceptos jurídicos, en el pulso y el impulso de quienes trabajamos por la salud de los colombianos. Hoy no la despedimos; solo le decimos otra vez, y como tantas veces, gracias por cada paso, por cada risa invencible, por la compañía y la sabiduría cuando nos caímos y cuando nos levantamos. Gracias, siempre, entrañable Ana María.

La ACHC pidió a Minsalud promover pacto de estabilidad con incremento de la UPC para 2024

La Asociación Colombiana de Hospitales y Clínicas (ACHC) pidió al Gobierno nacional promover un pacto de equilibrio o estabilidad económica entre los agentes del sector salud, que garantice trasladar el mismo porcentaje de incremento que se aprobó para la UPC del 2024 a los contratos y tarifas por prestación de servicios de salud acordados entre EPS e IPS. El siguiente es el texto completo de la comunicación enviada por el gremio:

ACHC-2023-091
Bogotá, D.C. 21 de diciembre de 2023

Doctor
GUILLERMO ALFONSO JARAMILLO MARTÍNEZ
Ministro de Salud y Protección social
MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL

ASUNTO: Pacto de estabilidad incremento tarifario a IPS conforme al incremento de la UPC

Estimado señor Ministro,

En momentos en que se discute y analiza el porcentaje de incremento de la UPC con la que se reconocen las coberturas del Plan de Beneficios de nuestro SGSSS, queremos insistir en el mecanismo que este gremio ha denominado *pacto por la estabilidad* entre las EPS y las IPS.

Según las disposiciones del Decreto 1464 de 2012, *"Por el cual se definen criterios para que el incremento de la UPC se vea reflejado en el valor de los servicios de salud"* —compilado en el Decreto 780 de 2016—, se definen los criterios para que los incrementos del valor de los servicios de salud acordados entre EPS e IPS, independiente de la modalidad pactada para la prestación de servicios de salud, se vean reflejados en lo que no corresponda a inclusiones o actualizaciones del Plan de Beneficios.

Conforme a esta disposición, se han venido expidiendo por parte del Ministerio de Salud y Protección Social las directrices para la materialización de esta medida, señalando en los actos administrativos que fijan la UPC para cada año, el porcentaje que debe trasladarse a las IPS, respetando la autonomía contractual de las partes y recordando que, si pasados 30 días desde la expedición de dichos actos no se realiza el ajuste, se tengan que hacer los incrementos en los porcentajes establecidos.

Comedidamente le solicitamos que para, el año 2024, se establezca en el acto administrativo correspondiente, con el fin de que el sector prestador de servicios de salud pueda tener las condiciones necesarias que le permitan reconocer y remunerar debidamente a su talento humano y a sus proveedores, y lograr así una atención oportuna y eficiente a todos los usuarios de nuestro Sistema de Salud.

De usted, atentamente,

JUAN CARLOS GIRALDO VALENCIA
Director General ACHC

En julio de 2024 se entregará el VII Galardón Nacional Hospital Seguro, ACHC

Desde el 15 de diciembre de 2023 y hasta el 20 de enero de 2024 se realizaron las inscripciones de los hospitales y clínicas al VII Galardón Nacional Hospital Seguro–ACHC, reconocimiento con el que la Asociación Colombiana de Hospitales y Clínicas busca exaltar a las Instituciones Prestadoras de Servicios de Salud que trabajan permanentemente para alcanzar de manera integral la excelencia en la atención en Salud, en beneficio de la población colombiana.

Además de la categorías tradicionales de postulación de entidades hospitalarias de baja, mediana y alta complejidad, así como de atención y de servicios ambulatorios, en este nueva edición del Galardón se iniciará el desarrollo de un piloto para premiar la categoría de entidades con atención extramural de carácter domiciliario.

Una vez formalizada la inscripción, las instituciones que se postularon tendrán hasta el 15 de febrero de 2024 para entregar los informes de autoevaluación, los cuales serán revisados por expertos que, de acuerdo con el cumplimiento de las condiciones técnicas de informes, definirán un grupo de instituciones preseleccionadas —los de mayores puntajes— que serán visitadas por los evaluadores para verificar los procesos.

Al concluir la etapa de visitas, con base en el informe presentado por los evaluadores, un jurado internacional evaluará los resultados alcanzados, a partir del informe de postulación y de lo encontrado en las visitas de campo. Una vez evaluadas estas variables, se otorgarán por consenso los puntajes finales a cada institución; todas las que superen 850 puntos sobre 1.000 serán reconocidas con el Galardón.

Los estándares de evaluación del premio están alineados con modelos de acreditación nacionales e internacionales, y basados en lineamientos de agencias técnicas expertas en el tema de seguridad, que les permite a las instituciones trabajar con base en las mejores prácticas disponibles.

Con la entrega de este Galardón, la ACHC busca destacar los procesos de mejoramiento de la seguridad en las instituciones hospitalarias del país, apoyar los esfuerzos que se vienen dando en este aspecto y fomentar la búsqueda de niveles de excelencia que puedan a futuro ser referentes de las mejores prácticas en seguridad del paciente.

Desde el 2010, cuando se entregó el Primer Galardón Nacional Hospital Seguro-ACHC, 21 reconocidas entidades del país han sido galardonadas. El VII Galardón Nacional Hospital Seguro-ACHC será entregado en julio de 2024, en el marco del *XV Congreso Internacional de Hospitales y Clínicas* y la *VIII Feria Internacional de la Salud, Meditech 2024*.

VII Foro de Soluciones Exitosas e Innovación en Salud, ACHC®, se consolidó como el escenario más grande de referenciación en salud en el país

La sesión de apertura estuvo presidida por la Secretaria de salud del Atlántico, Alma Solano; el Superintendente Nacional de Salud, Ulahí Beltrán; la presidente de la Junta Directiva de la ACHC, Doris Sarasty Rodríguez, y el Director General de la ACHC, Juan Carlos Giraldo Valencia

Los pasados 9 y 10 de noviembre, la Asociación Colombiana de Hospitales y Clínicas (ACHC) realizó en Barranquilla el *VII Foro de Soluciones Exitosas e Innovación en Salud, ACHC®*, un espacio académico en el que reconocidas entidades hospitalarias del país compartieron con el sector salud colombiano sus casos y procesos de éxito que los han llevado a ser referentes nacionales e internacionales por la innovación y resultados destacados en diferentes ejes de su gestión.

Durante dos días, más de 400 asistentes, a partir de la experiencia de reconocidas Instituciones Prestadoras de Servicios de naturaleza pública y privada, aprendieron nuevas maneras para desarrollar sus proyectos institucionales y conocieron herramientas efectivas y contenidos de valor para generar nuevas ideas y alcanzar mejores resultados en la gestión diaria de sus entidades.

La sesión de apertura estuvo presidida por la Secretaria de salud del Atlántico, Alma Solano; el Superintendente Nacional de Salud, Ulahí Beltrán; la presidente de la Junta Directiva de la ACHC, Doris Sarasty Rodríguez, y el Director General de la ACHC, Juan Carlos Giraldo Valencia.

En la apertura oficial, el director general de la ACHC, Juan Carlos Giraldo Valencia, expresó el agradecimiento del gremio a todos sus afiliados, especialmente a las entidades participantes en el Foro de Soluciones exitosas, tanto como expositores como asistentes, y recordó que este es un proceso de

En este séptima edición del foro se presentaron 57 soluciones exitosas de 34 entidades que prestan sus servicios en diferentes partes del país

construcción cultural que inició hace cerca de 15 años: "La obligación de la ACHC no es hacer el foro; es ser el foro; eso es lo que estamos haciendo: propiciando espacios como este donde se puede hacer una valoración colectiva de los esfuerzos individuales de las instituciones, donde se pueda hacer una exposición pública, que nos permita hacer comparaciones, generar enseñanzas y propiciar aprendizajes. Este evento es un acto de fe en el presente y el futuro del sistema de salud", enfatizó el director de la ACHC.

En esta edición del Foro, después de una rigurosa evaluación de tres jurados expertos, la agenda académica presentó 57 soluciones y casos de éxito de 34 Instituciones Prestadoras de Servicios de Salud, en ámbitos de gestión como liderazgo y relacionamiento con actores del sector; innovación en el modelo de atención; desarrollo innovador en infraestructura, tecnología, procesos administrativos y logística; generación de conocimientos en salud e información científica, y promoción del bienestar para el talento humano.

El evento contó con la innovación en desarrollo simultáneo de conferencias en una gran sala, a través de equipos de sonido multicanal, que les permitió a los asistentes atender las conferencias de su interés sin cambiarse de salón ni moverse de su silla, solo dirigiendo la mirada a la pantalla de la conferencia de su preferencia y sintonizando el canal de audio de esa pantalla.

El Foro de Soluciones Exitosas e Innovación en Salud es una iniciativa que la ACHC viene desarrollando desde el 2010

Al cierre del foro, la presidente de la Junta Directiva de la ACHC, Doris Sarasty Rodríguez, expresó sus agradecimiento a todas las entidades que compartieron de manera generosa sus mejores prácticas y a los profesionales que las representaron: "Con orgullo de patria y profunda satisfacción, exalto el resultado de un evento de alto nivel académico y de gran significado para el sector hospitalario colombiano". Y agregó: "Han sido dos días enriquecedores de excelente aprendizaje colectivo. Destaco que, bajo un entorno crítico, de incertidumbre y crisis del sistema, en estos dos días, lo relevante ha sido manifestar nuestra esencia, nuestro ejercicio profesional impecable, nuestro compromiso con la salud y la vida del pueblo colombiano; emociona verdaderamente esta disposición del sector prestador y la generosa entrega de su conocimiento".

Este Foro de Soluciones Exitosas e Innovación en Salud es una iniciativa que la ACHC viene desarrollando desde el 2010, y que se ha consolidado como un espacio de generación de conocimiento, referenciación comparativa entre entidades prestadoras de servicios de salud y relacionamiento entre los diferentes actores del sector.

isuite
Diseñe, Equipe y conecte

stryker

Experiencia
iSuite

Más de **10.000**
quirófanos en todo el mundo están equipados con las solubciones iSuite.

Este documento es sólo para uso de profesionales de la salud.

Los cirujanos siempre deben usar su juicio clínico profesional para decidir si usan o no un producto en particular en el tratamiento de un paciente. Stryker no ofrece ninguna asesoría médica y recomienda a los cirujanos estar enterados en el uso del producto antes de utilizarlo en cirugía.
La información presentada es para demostrar un producto de Stryker. Los cirujanos deben siempre consultar el folleto incluido en el producto, la etiqueta de producto y/o las instrucciones de uso incluyendo las instrucciones de limpieza y esterilización (si aplica) antes de usar cualquier producto Stryker. Es posible que algunos productos no estén disponibles en todos los mercados,
ya que la disponibilidad de productos está sujeta a las legislaciones y/o prácticas médicas vigentes en cada mercado.
Por favor contacte a su representante de Stryker Local si tiene preguntas sobre la disponibilidad de productos Stryker en su área. Todas las marcas registradas son marcas registradas de sus respectivos propietarios o poseedores.

Calle 116 No. 7-15 Piso 10. Oficina 1001
Bogotá, Colombia
P +571 743 8200
www.stryker.com

Reconocimiento del Instituto Colombiano del Sistema Nervioso-Clínica Montserrat como Hospital Universitario[1]

El Instituto Colombiano del Sistema Nervioso-Clínica Montserrat nació hace 72 años con el objetivo de brindar servicios de asistencia integral para pacientes, familias y comunidad, en el área de psiquiatría y salud mental. Durante los primeros años de su funcionamiento, se ha consolidado como una clínica innovadora y líder en el entendimiento de lo explícito e implícito de las problemáticas psiquiátricas, abanderando la atención alejada del estigma y del modelo manicomial imperante en su momento.

Se ha trabajado desde su fundación, con un enfoque académico y psicodinámico centrado en la autorreflexión constante sobre los procesos mentales y ambientales que determinan el funcionamiento humano. De esta manera, garantiza una comprensión integradora de los diferentes factores que impactan en el psiquismo con base en sólidos principios teóricos del funcionamiento mental, tanto en la atención del paciente y sus familias como en el proceso formativo de los estudiantes de diferentes niveles de formación.

Su modelo asistencial funciona tendiendo puentes a través del constante diálogo científico y humanizado entre los múltiples actores del sistema y sus visiones, por lo cual se ha consolidado como un sistema abierto, en el cual la perspectiva de cada miembro del equipo enriquece de manera sinérgica la comprensión y la atención.

Desde su fundación, la Clínica Montserrat se ha fortalecido como un centro de formación en varias áreas de la salud mental y la psiquiatría, resaltando su compromiso en

participar en la enseñanza a profesionales que sean capaces de dar respuesta a los desafíos en la atención de los pacientes y sus familias, así como en brindar solución a las diversas necesidades en este campo en nuestro país y en el mundo.

Fruto de esta esencia académica institucional, se crea uno de los primeros programas de Especialización en Psiquiatría en el país en 1974, con la aprobación académica de la Universidad El Bosque en 1982, para el cual se consolida como escenario de práctica base y se constituye en el primer convenio docencia-servicio de ambas instituciones, así como en la primera especialización médico-quirúrgica de dicha IES.

Dentro de los procesos misionales, se encuentra el académico y el investigativo, que ha permitido la gestión adelantada con la cual se ratifica el compromiso con la generación de conocimiento y la formación de profesionales como instrumento para el fortalecimiento de la atención en la salud mental en el país.

Esto ha llevado a consolidar el trabajo formativo con diez instituciones de educación superior,

[1] Diego Francisco Vargas Chávez, Coordinador Docente, Clínica Montserrat.

El Instituto Colombiano del Sistema Nervioso - Clínica Monserrat es el primer Hospital Universitario especializado en salud mental del país

por medio de convenios de docencia-servicio, con catorce programas de pregrado que se encuentran acreditados, programas de posgrado y siete programas de especialidades médico-quirúrgicas, entre las que se encuentra la Especialización en Psiquiatría en convenio con la Universidad El Bosque, del cual se consolida como un escenario de práctica base y que ha permitido formar 279 psiquiatras a la actualidad.

En lo investigativo, el compromiso se evidencia en el grupo de investigación PSIMONART, el cual recibió el reconocimiento como grupo de investigación en categoría B como resultado de la Convocatoria 894 de 2021 para el Reconocimiento y Medición de Grupos de Investigación de MinCiencias, vinculación a dos redes de investigación, un semillero de investigación en el que participan estudiantes y docentes de diferentes áreas y niveles de formación, con publicaciones en revistas indexadas y reconocimientos en eventos científicos.

Hace aproximadamente seis años que iniciamos con el camino que nos permitiera consolidar y ratificar el compromiso que tiene el Instituto con la formación de profesionales como un camino en la generación de conocimiento, una responsabilidad social con el país para fortalecer la adecuada atención a las necesidades en salud y enfermedad mental, así como para atender al llamado de la importancia de investigar en estas áreas.

Desde el año 2017, por medio de una planeación estratégica, se tomó la decisión de iniciar el camino hacia la acreditación en salud como un medio para lograr que nuestros procesos institucionales se presten con calidad superior, aunado a la intención de fortalecer el aspecto académico institucional y lograr así ser un Hospital Universitario.

El camino hacia el fortalecimiento de los procesos y la calidad en la atención, la formación y la investigación ha llevado al otorgamiento de la acreditación en salud por parte de ICONTEC, el 22 de agosto de 2022, y el reconocimiento como Hospital Universitario por medio del Acuerdo 245 de 2023, por la Comisión Intersectorial para el Talento Humano en Salud (CITHS) del Ministerio de Salud y Protección Social y el Ministerio de Educación Nacional.

Tener el reconocimiento como Hospital Universitario representa el desafío que nos hemos planteado de manera estratégica, la ratificación de la vocación académica en cada persona que tiene un contacto con la institución, la enseñanza de alta calidad, así como el compromiso en la generación y transferencia de conocimiento.

Por esta razón, nos llena de orgullo decir que somos el primer Hospital Universitario especializado en salud mental del país, por medio de lo cual confirmamos nuestro compromiso en seguir participando en la educación y la investigación. Estamos seguros de que una de las maneras para impactar la transformación de un país, con el fin de atender los requerimientos actuales en salud mental, es por medio de la educación.

Clínica del Occidente se transforma en el complejo hospitalario más moderno del suroccidente de Bogotá

La nueva torre tiene once pisos en los que la Clínica del Occidente pone al servicio de los pacientes nuevas especialidades y una moderna infraestructura para brindar atención integral

Con el propósito de ampliar la atención en servicios de salud de Bogotá y Colombia, agregar nuevas y necesarias especialidades médicas y brindar una mejor experiencia a los usuarios, la Clínica del Occidente abrió las puertas de una nueva torre de once pisos, que la convierte en el más moderno y único Complejo Hospitalario privado del suroccidente de la capital. En total, la institución tendrá 218 camas hospitalarias, 58 unidades de cuidados intensivos y 10 salas de cirugía.

"Un complejo médico significa integrar en un área física el mayor número de servicios de salud con respuestas inmediatas y completas para diferentes enfermedades. La ciudad y el país lo necesitaban y la Clínica del Occidente lo creó para atender crecientes y variadas necesidades, con nuevos servicios enfocados en fortalecer la integralidad y la alta complejidad", explica el doctor Iván Torres, director científico de la institución. El Complejo está conformado por tres torres: la primera es referente en atención a pacientes de mediana y alta complejidad, y recientemente cumplió 41 años; en la segunda se encuentra el Instituto de Oncología y Medicina Especializada del Occidente (IOMED), que atiende a personas con cáncer con servicios de diagnóstico y tratamientos de quimioterapia, radioterapia y cirugía; la tercera es la nueva torre.

Esta nueva torre la "consideramos una clínica del futuro, porque con esta transformación iniciamos una constante evolución que nos permitirá brindarle al paciente un servicio integral a partir de una infraestructura innovadora, avances tecnológicos e investigativos, nuevas especialidades y la integración de la telemedicina. Nos adelantaremos a las enfermedades que, en un futuro, se presenten para estar a la vanguardia médica y, por ejemplo, ofrecer tratamientos mínimamente invasivos, realizar complejas cirugías con menor tiempo de incapacidad y rápida recuperación, entre muchos otros avances. La clave será la anticipación", afirma el doctor Edgar Ruiz, Director General de la Clínica del Occidente.

Servicios

Con este proyecto, la Clínica del Occidente pone al servicio del país una de las más modernas infraestructuras hospitalarias, con la cual se planea beneficiar a 2.400.000 usuarios de Bogotá, el resto de Colombia y otros países. También se espera que al final de este año se generen 300 nuevos empleos directos y 100 indirectos. Un plan adicional es fortalecer las investigaciones científicas de diversas especialidades y subespecialidades, que hemos venido adelantando con la recolección de datos muy valiosos.

"Dentro de nuestros objetivos principales, está la ampliación de la atención médica con servicios como trasplante renal, neurocirugía, cirugía cardiovascular, cirugía plástica y reconstructiva, y

El Director General de la ACHC, Juan Carlos Giraldo Valencia acompañó en la inauguración de la nueva torre a los directivos y fundadores de la Clínica Dr. Edgar Alirio Ruiz y la Sra. Clara Lucia Lucena

oncología. También atenderemos nuevos mercados nacionales e internacionales, pólizas de salud, medicina prepagada y planes complementarios", revela el doctor Edgar Ruiz.

Tecnología para atención de enfermedades de alta complejidad

De acuerdo con el más reciente informe del Departamento Administrativo Nacional de Estadística (DANE), durante 2023 las principales causas de muerte en Colombia, tanto en hombres como en mujeres, han sido las enfermedades del corazón, las cerebrovasculares y las crónicas de las vías respiratorias. Teniendo en cuenta esta realidad y que esas enfermedades han venido aumentando en los últimos años, la Clínica del Occidente adquirió equipos como un innovador angiógrafo, que permitirá diagnosticar, de forma precisa y oportuna, a pacientes con afectaciones cardíacas y neurológicas graves.

El Complejo Hospitalario también fue dotado con un sistema de oxígeno único en el país y un mecanismo nuevo de succión de aire medicinal, más eficiente, para los pacientes que necesitan respiración artificial. Además, el laboratorio tendrá equipos de última generación que complementarán los que tiene la institución y optimizarán los procesos médicos de pacientes con enfermedades de alta complejidad.

El doctor Iván Torres expresó que también tendrán equipos para radiología de alta tecnología, que brindarán a los pacientes análisis más acertados. "Las innovaciones tecnológicas del Complejo Hospitalario ayudarán a dar atención óptima y completa a diversas enfermedades inclusive el cáncer, el cual se desatendió en los últimos años a raíz de la pandemia", concluyó.

Todas las habitaciones de la nueva torre del Complejo son amplias y están debidamente equipadas para garantizar una estancia cómoda. Adicionalmente, habrá un piso para usuarios de medicina prepagada con habitaciones individuales de lujo, tipo *suite*, con sala exclusiva para el paciente y su familia.

Con esta transformación, el Complejo Hospitalario espera posicionarse como la mejor y más importante clínica de Bogotá. Con ese propósito, brindará servicios humanos, seguros e integrales en la atención de enfermedades de alta complejidad, así como una excelente experiencia para el paciente y sus acompañantes.

La Clínica del Occidente es una institución privada con 41 años de trayectoria, líder en la prestación de servicios de salud en Colombia y referente en atención a pacientes de mediana y alta complejidad. Adicionalmente, ha sido reconocida como una de las mejores instituciones de Bogotá, Colombia y Latinoamérica, en prácticas y resultados hospitalarios, según América Economía; una de las IPS con mejor reputación en Colombia, según Merco Salud; y una de las 57 IPS acreditadas en salud, que brinda mejores servicios a todos los colombianos, según el Ministerio de Salud y el Ministerio de Comercio.

La Clínica del Occidente abrió el innovador Centro de Oncología y Medicina Especializada del Occidente, donde ofrece atención integral diagnóstica y terapéutica a personas con cáncer. El objetivo es convertirse en referente en el manejo de patologías oncológicas, que en los últimos años han cobrado la vida de miles de personas.

La OPS, el BID y el Banco Mundial se unieron para **fortalecer la Atención Primaria de Salud en las Américas**[1]

Foto: freepik.es

Con el objetivo de impulsar la inversión, la innovación y la implementación de políticas e iniciativas orientadas a transformar los sistemas de salud con un enfoque en la atención primaria en las Américas, la Organización Panamericana de la Salud (OPS), el Banco Interamericano de Desarrollo (BID) y el Banco Mundial (BM) decidieron unir esfuerzos y trabajar en conjunto para avanzar en el desarrollo de las políticas de APS.

Esta alianza llega a reforzar las iniciativas que se desarrollan actualmente en los diferentes países del continente para recuperarse de los impactos adversos de la pandemia por COVID-19, que provocó un retroceso en muchos indicadores de salud y puso de relieve las deficiencias estructurales de los sectores sanitario y de protección social para responder en forma eficaz a una emergencia de salud pública; así lo precisa el comunicado conjunto de estos organismos multilaterales.

"La atención primaria de salud es nuestro camino para recuperar el progreso perdido y una inversión esencial para abordar nuestros mayores desafíos en materia de salud y desarrollo", afirmó el doctor Jarbas Barbosa, Director de la OPS, y agregó: "La creación de esta nueva alianza es más necesaria que nunca para acelerar la acción en los países mediante una actuación colectiva y concertada".

Según la OMS, se estima que una tercera parte de la población de las Américas tiene necesidades de atención de salud insatisfechas, incluso desde antes de la pandemia, y ese porcentaje varía desde el 55 %, en países de ingresos medianos bajos, hasta el 12 %, en los de ingresos altos. Además, enfrentan graves desigualdades en la forma en que se presta la asistencia sanitaria, se distribuye y se pone a disposición de la población.

La atención primaria de salud puede contribuir a cerrar esa brecha al garantizar a las personas una atención integral de calidad para sus necesidades de salud a lo largo de toda la vida —no solo para una serie concreta de enfermedades—, y lo más cerca posible de sus lugares habituales.

Ana María Ibáñez, vicepresidenta de Sectores y Conocimiento del BID, explicó la alianza: "Para lograr una atención primaria de la salud efectiva y equitativa, es fundamental adoptar un enfoque intersectorial. Esto implica examinar no solo el ámbito de la salud, sino también otros sectores, coordinando es-

[1] Con información de nota de prensa de BID, OMS y BM.

AVEDIAN Processum

Más que información, mejores resultados

Gracias a nuestros a clientes, colaboradores y amigos por su confianza durante este 2023. Con su apoyo, hemos superado los retos de este año y logramos avanzar en nuestro compromiso con la calidad, eficiencia y el mejoramiento en los resultados de salud.

- Nos recertificaron en calidad y seguridad de la información.
- Procesamos más de **100 millones** de episodios de atención en salud.
- Fuimos elegidos en más de **5 países de Latinoamérica** como proveedor de GRD.
- Contribuimos en el cierre de las brechas de conocimiento para mejorar la calidad de la información en salud a través de la formación de talento humano.
- Impulsamos redes de conocimiento y colaboración con la puesta en marcha de **Innova GRD**.
- Promovimos la innovación mediante el uso de información en proyectos de investigación clínica y económica.

¡Estamos listos para el 2024!

Colocamos a su disposición todo nuestro ecosistema de herramientas de salud digital. Los esperamos.

www.avediangrd.com | www.processum.org | contacto@avediangrd.com

En la actualidad, existe un déficit de 6 millones de trabajadores de salud en las Américas, una brecha que debe cerrarse para que el sector salud pueda brindar la atención que las personas necesitan y sea más resistente ante futuras situaciones de crisis.

fuerzos entre distintos actores involucrados. La creación de esta alianza representa un paso crucial en este sentido, al ofrecer una plataforma colaborativa que respalda a nuestros países en esta tarea".

Asimismo, reforzar la APS implica realizar las inversiones necesarias en personal de salud, infraestructura, trabajo y educación. En la actualidad, existe un déficit de 6 millones de trabajadores de salud en las Américas, una brecha que debe cerrarse para que el sector salud pueda brindar la atención que las personas necesitan y sea más resistente ante futuras situaciones de crisis.

"Celebramos el lanzamiento de la Alianza por la Atención Primaria en Salud en las Américas, con el propósito de promover entornos saludables, prevenir enfermedades y salvar vidas. Tenemos el sentido de urgencia para fortalecer la atención primaria, expandiendo el acceso, la calidad, la equidad, la eficiencia y la resiliencia del sistema de salud. Es fundamental el compromiso político y la implementación de políticas de Estado para el impacto y beneficio de las personas, nuestro principal objetivo común", destacó Carlos Felipe Jaramillo, vicepresidente para América Latina y el Caribe del Banco Mundial.

Los países del mundo, incluidos los de la región de las Américas, se han comprometido a renovar y ampliar la atención primaria de salud como piedra angular de un sistema de salud sostenible que permita ampliar la cobertura y garantizar el acceso universal a la salud, así como alcanzar los Objetivos de Desarrollo Sostenible (ODS) relacionados con la salud y la seguridad sanitaria.

La nueva alianza entre la OPS, el BID y el Banco Mundial puede actuar como catalizador para impulsar los cambios necesarios. Esta asociación apoyará colectivamente el desarrollo de planes nacionales de inversión en APS, proporcionará orientación a los países para fortalecer la resiliencia y la capacidad de sus sistemas de salud, y cooperará para diseñar e implementar intervenciones basadas en evidencia, adaptadas a los contextos y retos específicos.

Los esfuerzos conjuntos de las tres organizaciones buscarán, además, fomentar la innovación para acelerar las acciones y garantizar el derecho a la salud, entre ellas, la transformación digital —como la telesalud, para llegar mejor a las zonas desatendidas—, y los nuevos medicamentos y vacunas.

¿En qué consiste la atención primaria de salud?[1]

El concepto de APS ha sido reinterpretado y redefinido en múltiples

[2] https://www.who.int/es/news-room/fact-sheets/detail/primary-health-care

ocasiones desde 1978, lo que ha generado confusión sobre su significado y en la práctica. Con miras a coordinar las labores futuras en materia de APS a nivel mundial, nacional y local, y a modo de orientación en su puesta en práctica, se ha elaborado una definición clara y sencilla:

«La APS es un enfoque de la salud que incluye a toda la sociedad y que tiene por objeto garantizar el mayor nivel posible de salud y bienestar y su distribución equitativa mediante la atención centrada en las necesidades de las personas tan pronto como sea posible a lo largo del proceso continuo que va desde la promoción de la salud y la prevención de enfermedades hasta el tratamiento, la rehabilitación y los cuidados paliativos, y tan próximo como sea posible del entorno cotidiano de las personas». OMS y UNICEF. A vision for primary health care in the 21st century: Towards UHC and the SDGs.

La APS tiene tres componentes que son interdependientes y sinérgicos, a saber: un conjunto de servicios de salud integrados e integrales que engloban la atención primaria y los bienes y funciones de salud pública como elementos centrales; distintas políticas y actuaciones multisectoriales encaminadas a abordar los determinantes generales de la salud más amplios; y la movilización y el empoderamiento de las personas, las familias y las comunidades para lograr una mayor participación social y mejorar la autoasistencia y la autosuficiencia en materia de salud.

¿Por qué es importante la atención primaria de salud?

Los Estados Miembros se han comprometido a renovar y aplicar la atención primaria de salud como piedra angular de un sistema de salud sostenible que permita lograr la CSU, los Objetivos de Desarrollo Sostenible relacionados con la salud (ODS) y la seguridad sanitaria. La APS es el «motor programático» para lograr la CSU, los ODS relacionados con la salud y la seguridad sanitaria. Este compromiso ha sido formulado y reiterado en la Declaración de Astaná, la resolución 72.2 conexa de la Asamblea Mundial de la Salud, los informes de monitoreo mundiales sobre la cobertura sanitaria universal y las declaraciones de alto nivel de la Asamblea General de las Naciones Unidas sobre la CSU. La CSU, los ODS relacionados con la salud y los objetivos de seguridad sanitaria son ambiciosos pero alcanzables. Es necesario lograr avances urgentemente, y la APS proporciona los medios para hacerlo.

La APS es el enfoque más inclusivo, equitativo, costoeficaz y efectivo para mejorar la salud física y mental de las personas, así como su bienestar social. Cada vez son más las pruebas en todo el mundo del amplio efecto que tiene invertir en la APS, particularmente en tiempos de crisis como los de la pandemia de COVID-19.

A nivel mundial, las inversiones en APS mejoran la equidad y el acceso en relación con los servicios de salud, el desempeño de la atención médica, la rendición de cuentas de los sistemas de salud y los resultados de salud. Aunque algunos de esos factores están directamente relacionados con el sistema de salud y el acceso a sus servicios, cada vez hay más pruebas que demuestran que una amplia gama de factores más allá de los servicios de salud tienen un papel fundamental en la configuración de la salud y el bienestar. Por ejemplo, la protección social, los sistemas alimentarios, la educación y los factores ambientales.

La APS también es fundamental para que los sistemas de salud sean más resilientes en situaciones de crisis, sean más dinámicos en la detección de los primeros signos de epidemias y estén más preparados para actuar de forma temprana en respuesta a los aumentos en la demanda de servicios. Aunque todavía faltan datos, existe un amplio consenso en que la APS es la «puerta principal» del sistema de salud y la base para el fortalecimiento de las funciones esenciales de salud pública ante crisis como la de la COVID-19. H

Principal reglamentación en materia de salud en el año 2023

Aunque en el 2023 ha tenido gran protagonismo la actividad legislativa debido a las propuestas de reforma al Sistema de Salud Colombiano, conformadas por un proyecto de Ley ordinaria que acumula la propuesta reformista del Gobierno y las propuestas de los partidos de oposición y propuestas de Ley Estatutaria, es importante recordar la normatividad destacada durante esta vigencia.

En materia de salud, se destaca la expedición de Leyes tramitadas en otras legislaturas: la Ley 2315, a través de la cual se incluyó a los odontólogos de especialización en cirugía oral y maxilofacial dentro del Sistema de Residencias Médicas; la Ley 2316, con la cual se creó el tipo penal de lesiones personales con sustancias modelantes invasivas e inyectables no permitidas (biopolímeros"); la Ley 2317, que creó la política pública de nutrición prenatal y seguridad alimentaria gestacional; la Ley 2315, de endometriosis, y la Ley 2291, que transformó la naturaleza jurídica del Instituto Nacional de Cancerología. Así mismo, se aprobó el Plan Nacional de Desarrollo 2022-2026 del actual Gobierno, denominado "Colombia, potencia mundial de la vida", mediante la expedición de la Ley 2294.

Desde el ejecutivo, se emitió normatividad relacionada con el estado de emergencia económica, social y ecológica en el departamento de La Guajira, pero que resultó inaplicable debido a la declaratoria de inexequibilidad hecha por la Corte Constitucional. Temas coyunturales fueron la reglamentación del procedimiento de cobro y pago de servicios del Seguro Obligatorio de Accidentes de Tránsito (SOAT) con rango diferencial y el Plan de contingencia Mipres y de reportes a la Supersalud, ante el ciberataque de los aplicativos web del Ministerio de Salud.

Como en los últimos tres años, se expidió la normatividad relacionada con la modificación de presupuestos máximos, servicios y tecnologías en salud con cargo y sin cargo a la UPC. Las líneas de crédito con tasa compensada Findeter, la actualización del portafolio de servicios de salud en el REPS y el sistema de facturación electrónica y soportes también tuvieron reglamentación. En materia de inspección, vigilancia y control, se dio continuidad a las medidas de intervención forzosa para administrar a diferentes EPS por parte de la Superintendencia y la modificación de los términos y condiciones de algunos reportes de información para sus vigilados. A manera de ilustración, relacionaremos en orden cronológico y según las temáticas más importantes la normatividad expedida.

Flujo de Recursos

- **Resolución 152 (3 de febrero). Incluye prima adicional para zona especial por dispersión al departamento de la Guainía.** Mediante la presente resolución, se incluye en la UPC una prima adicional por zona especial de dispersión geográfica en el Régimen Contributivo para los municipios y áreas no municipalizadas del departamento del Guainía y, en consecuencia, se modifica el artículo 2 de la Resolución 2809 de 2022. Lo anterior tiene lugar con base en que, en el artículo 15 de la referida Resolución, si bien se estableció la UPC específica para el departamento respecto del Régimen Subsidiado, no se contempló en el artículo 2 *ibidem* la prima adicional por dispersión geográfica que corresponde al Régimen Contributivo en los municipios y áreas no municipalizadas de dicha entidad territorial, cuando esta fue prevista con el fin de reconocer y pagar el recurso dispuesto para garantizar la financiación de la prestación de servicios de salud en las zonas que tienen estas características.

- **Resolución 052 de (12 de enero). Lineamientos para la distribución, asignación y giro de los recursos del esquema de solidaridad.** A través de esta Resolución, se definen los lineamientos para la distribución, asignación y giro de los recursos transferidos al esquema de solidaridad por parte de las cajas de compensación familiar en los términos del artículo 3 de la Ley 1929 de 2018, modificado por el Decreto Ley 800 de 2020. Adicionalmente, este acto administrativo determinará las especificaciones para el reporte de la información que se genere en el marco de la aplicación de estos recursos.

- **Resolución 326 (2 de marzo). Procedimiento de cobro y pago de servicios de salud de víctimas de accidentes de tránsito SOAT – Rango diferencial.** Con este Resolución, se establece que los servicios de salud prestados a víctimas de accidentes de tránsito, en el que el vehículo involucrado se encuentre amparado con la póliza del Seguro Obligatorio de Accidentes de Tránsito (SOAT) con rango diferencial por riesgo, serán reconocidos por la Administradora de los Recursos del Sistema General de Seguridad Social en Salud (ADRES), en los términos y condiciones establecidos en la Resolución 1645 de 2016 o aquella que la modifique o sustituya. La ADRES deberá definir ventanas de radicación de solicitudes de dicho reconocimiento, una vez cada dos (2) meses.

  Los prestadores de servicios de salud deberán anexar a la radicación de las reclamaciones de los servicios de salud prestados a víctimas de accidentes de tránsito, en el que el vehículo involucrado se encuentre amparado con la póliza del Seguro Obligatorio de Accidentes de Tránsito (SOAT) con rango diferencial por riesgo, de que trata el numeral 3 del artículo 2.6.1.4.2.3 del Decreto 780 de 2016, el certificado de reconocimiento de los servicios de salud prestados hasta 263,13 Unidades de Valor Tributario (UVT), emitido por la respectiva aseguradora autorizada para operar el ramo SOAT. Este documento deberá incluir el detalle de los servicios de salud reconocidos por la aseguradora y el valor en pesos y en Unidades de Valor Tributario (UVT), sin perjuicio del cumplimiento de los requisitos establecidos en el literal A del artículo 17 de la Resolución 1645 de 2016 o aquella que la modifique o sustituya.

- **Ley 2315 (17 de agosto). Incluye a los odontólogos de especialización en cirugía oral y maxilofacial dentro del Sistema de Residencias Médicas.** De esta manera, con la mencionada Ley se modifica la Ley 1917 de 2018 y se incluye a los odontólogos que se encuentren cursando programas de especialización médico-quirúrgica en cirugía oral y maxilofacial dentro del Sistema de Residencias Médicas, en aras de garantizar las condiciones adecuadas e igualitarias para su formación académica y práctica como especialistas.

- **Resolución 1653 (10 de octubre). Requisitos para solicitar concepto técnico de viabilidad de proyectos de inversión de adecuaciones en infraestructura física y en infraestructura móvil para prestación de servicios de salud.** Mediante esta Resolución, en el marco del Modelo de Atención Predictivo y Preventivo y Resolutivo y para el logro de mayor equidad en el acceso a los servicios de salud, con el propósito de eliminar barreras geográficas, económicas, sociales y culturales en zonas donde solo se llega por vía marítima, fluvial, aérea o caminos veredales, se requiere implementar alternativas de transporte que permita llegar a dichos lugares; para tal fin, se considera necesario incluir los requisitos para la presentación de proyectos de inversión para infraestructura móvil, por parte de las entidades territoriales y ESE.

- **Resolución 1621 (4 de octubre). Criterios de distribución y asignación de recursos a las entidades territoriales y a las ESE del Programa de Atención Psicosocial y Salud Integral a Víctimas del Conflicto Armado.** A través de este Resolución, se establece que se entenderán como recursos presupuestales para la operación

En la Resolución 1583 (03 de octubre), se fija un 70% el Porcentaje de los rendimientos financieros de la cuenta maestra de recaudo de cotizaciones en salud, para EPS y entidades adaptadas en salud 2023.

del PAPSIVI aquellos que la ADRES girará para financiar el programa establecido en el numeral 1 del artículo 2.6.4.4.4 del Decreto Único 780 de 2016, respecto del componente de Atención Psicosocial, así como aquellos provenientes de otras fuentes dispuestas por el Ministerio de Salud y Protección Social para tal fin.

Las entidades territoriales, para recibir dichos recursos y operar el PAPSIVI, deberán contar con mínimo una ESE con servicio habilitado de medicina general y psicología de acuerdo con la normatividad vigente. En caso de que la solicitante sea una ESE, deberá acreditar su habilitación como prestadora del servicio de medicina general y psicología, de conformidad con la normatividad vigente. La Oficina de Promoción Social del Ministerio de Salud y Protección Social, mediante documento técnico, realizará la evaluación de los criterios de ponderación para la asignación de los recursos presupuestales que se destinen a las entidades territoriales o sus ESE para la operación del programa.

- **Resolución 1583 (03 de octubre). Porcentaje de los rendimientos financieros de la cuenta maestra de recaudo de cotizaciones en salud, para EPS y entidades adaptadas en salud 2023.** Con esta Resolución, se fijó en un setenta por ciento (70 %) el porcentaje de los rendimientos financieros de las cuentas maestras de recaudo de cotizaciones en salud a apropiarse por las EPS y las entidades adaptadas en salud, durante la vigencia 2023, para financiar las actividades relacionadas con la gestión de cobro de cotizaciones, el manejo de la información sobre el pago de aportes y los servicios financieros asociados al recaudo. Las EPS y entidades adaptadas en salud que se encuentren en proceso de liquidación, y por el periodo que este se extienda, podrán apropiarse del veinte por ciento (20 %) de los rendimientos financieros de las cuentas maestras de recaudo de cotizaciones en salud.

- **Resolución 1491 (20 de septiembre). Condiciones de la operación, el acceso y el procedimiento para la ejecución de la línea de crédito FINDETER.** Se establecieron como recursos disponibles para ejecutar por concepto de la línea de crédito de redescuento con tasa "Compromiso Salud Liquidez" de FINDETER cuatrocientos cincuenta y cinco mil ciento siete millones cuatrocientos treinta y cinco mil sesenta y tres pesos m/cte. ($455.107.435.063), bajo las condiciones de operación establecidas en el presente acto administrativo.

  Las EPS e IPS públicas, privadas o mixtas, como entidades beneficiarias, con el objeto de continuar con la prestación del servicio de salud, deberán destinar los recursos de la línea exclusivamente en capital de trabajo y/o sustitución de deudas, con prelación a las entidades públicas.

Cobertura y atención a los usuarios

- **Resolución 051 (12 de enero). Atención integral frente a la interrupción voluntaria del embarazo (IVE) y se modifica la Ruta de Atención Integral en Salud Materno Perinatal.** Mediante esta Resolución, se adopta la regulación única para la atención integral en salud frente a la IVE, en las condiciones previstas por la Corte Constitucional en las Sentencias C-355 de 2006, SU-096 de 2018 y C-055 de 2022, y modifica el numeral 4.2 del Lineamiento Técnico y Operativo de la Ruta Integral de Atención en Salud Materno Perinatal.

- **Resolución 295 (27 de febrero). Gestión de la Salud Pública y responsabilidades de**

las entidades territoriales y ejecutores del Plan de Salud Pública de Intervenciones Colectivas. A través de esta Resolución, se fortalece el proceso de implementación de la estrategia de atención primaria en salud, reorientando la ejecución de acciones colectivas hacia las intervenciones continuas, sistemáticas territorializadas y por entornos, para lo cual se requiere modificar los artículos 3, 8, 11, 14, 16 y 18, de la Resolución 518 de 2015, en cuanto a los procesos de gestión de la salud pública, las responsabilidades de las entidades territoriales departamentales, distritales, municipales, y de los ejecutores del Plan de Salud Pública de Intervenciones Colectivas, así como las condiciones que se deben tener en cuenta para la ejecución de la intervenciones del Plan de Salud Pública de Intervenciones Colectivas.

- **Resolución 654 (28 de abril). Plan Provisional de Acción para materializar el Derecho fundamental a la Salud del pueblo Wayúu.** Con esta Resolución, se adopta el Plan Provisional de Acción contenido en el Anexo Técnico que hace parte integral del presente acto administrativo. Para lo anterior, la Gobernación del Departamento de La Guajira y los Municipios de Uribia, Manaure, Maicao y el Distrito de Riohacha, a través de las secretarías de salud o quien haga sus veces, en coordinación con las EPS y EPSI, con el apoyo técnico del Ministerio de Salud y Protección Social, organizará y conformará la red funcional de prestación de servicios de salud en los términos del artículo 62 y del Título VI de la Prestación de Servicios de Salud de la Ley 1438 de 2011, dentro de los 30 días calendario a partir de la expedición de la presente Resolución.

- **Ley 2317 (17 de agosto). Establecen los lineamientos para la formulación de la política pública de nutrición prenatal y seguridad alimentaria gestacional.** Con esta Ley, se dota al estado Colombiano de una estrategia integral que atienda y mejore el estado nutricional de las mujeres gestantes conforme al diagnóstico nutricional del médico tratante y de esta manera prevenir la desnutrición, malnutrición y enfermedades no "transmisibles tanto en las gestantes como en los recién nacidos".

- **Ley 2315 (12 de octubre). Lineamientos para la política pública de la endometriosis.** Se establecen los principios, contenidos y disposiciones de la Política Pública de prevención, acceso completo o lo detección, diagnóstico temprano, estudios, control, tratamiento y terapias necesarias para el abordaje integral de la endometriosis y garantizar el derecho a la salud de las personas con diagnóstico o presunción de endometriosis, así como la concientización de la población.

  En dicho marco, se reconoce la endometriosis como enfermedad crónica progresiva y debilitante; se crea el registro de pacientes para evaluar y garantizar la oportunidad en la atención a pacientes diagnosticados; se determina la ruta diagnóstica y de atención, al tiempo que se establece el Día Nacional de la concientización y prevención, entre otras medidas. El Ministerio de Salud y Protección Social en el término de un (1) año, contado a partir de dicha Ley, deberá formular, adoptar, dirigir, coordinar, ejecutar y evaluar la Política Pública para el abordaje integral de la endometriosis.

Medidas para mitigar el COVID-19

- **Resolución N.º 069 (16 de enero). Repone vacunas contra la COVID-19 del laboratorio Pfizer Inc. y BioNTech por fallas de fabricación o calidad.** A través de esta Resolución, se reponen por única vez seiscientas cuarenta y seis (646) dosis de vacunas del laboratorio Pfizer Inc. y BioNTech con seiscientas cincuenta y dos (652) dosis del biológico del laboratorio Sinovac Life Scienses Co. Ltda., teniendo en cuenta las cantidades por vial y empaques secundarios completos, a las entidades territoriales señaladas en el presente acto administrativo.

- **Resolución 986 (21 de junio). Lineamientos para la aplicación de las vacunas contra la COVID-19.** Se establen los lineamientos para la vacunación contra la COVID-19 contenidos en los siguientes anexos técnicos, los cuales hacen parte integral de esta Resolución: Anexo 1: Lineamientos técnicos y operativos para la vacunación contra la COVID-19; Anexo 2: Consentimiento informado para la aplicación de la vacuna contra el SARSCoV-2/COVID-19; Anexo 3: Anexo técnico para la aplicación de la vacuna BNT162b2 Pfizer-BioNTech contra la COVID-19; Anexo 4: Anexo técnico para la aplicación de la vacuna Sinovac Life Scienses Co. Ltd., denominada CoronaVac, contra la COVID-19; Anexo 5: Anexo técnico para la aplicación de la vacuna AD26. COV2.S JANSSEN contra la COVID-19; Anexo 6: Anexo técnico para la aplicación de la vacuna Moderna ARNm-1273, Switzerland GmbH contra la COVID-19.

- **Resolución 1862 (15 de noviembre). Lineamientos para la aplicación de las vacunas contra la COVID-19, y se dictan otras disposiciones.** Modifica el artículo 1.º de la Resolución 986 del 21 de junio de 2023, en virtud de la cual se establecieron los lineamientos para la aplicación de las vacunas contra la COVID-19, así como algunos de los lineamientos contenidos en sus anexos técnicos. Así mismo, se sustituye el Anexo técnico para la aplicación de la vacuna Moderna ARNm-1273, Switzerland GmbH contra la COVID-19, en aras de garantizar la protección del derecho a la salud y a la vida de los habitantes del territorio nacional.

Procedimientos, instrucciones y reportes de información

- **Resolución 163 (6 de febrero). Metodología para definir el ajuste del Presupuesto Máximo de la Vigencia 2021 para asignar a las EPS.** Se adopta la metodología para la definición del ajuste definitivo del presupuesto máximo de la vigencia 2021, contenida en el anexo técnico que hace parte integral del presente acto administrativo. El ajuste definitivo corresponde al resultante de la revisión de los grupos relevantes durante el periodo comprendido entre el 1.º de enero y el 31 de diciembre de 2021, en los términos del numeral 3.4 del Anexo técnico de la Resolución 1408 de 2022.

- **Resolución 087 (20 de enero). Corrige errores en la Resolución 2808 de 2022 que establecen los servicios y tecnologías de salud financiados con recursos de la UPC.** De esta manera, se corrige el Anexo 2 de la Resolución 2808 de 2022 *"Listado de procedimientos en salud financiados con recursos de la UPC"*, por un error involuntario en la transcripción de la categoría *99.5.2. OTRAS VACUNACIONES DEL PROGRAMA AMPLIADO DE INMUNIZACIONES*, ya que no se eliminó la salvedad de financiación del proc edimiento 99.5.2.02, Administración vacuna SARSCoV-2 (COVID-19), a pesar de que dicho procedimiento se encuentra financiado con cargo a los recursos de la UPC para la vigencia 2023. Así mismo, se corrige el parágrafo 2 del artículo 111 de la Resolución 2808 de 2022, ya que por un error de digitación se citó el artículo 115 del mismo acto administrativo, cuando la disposición correcta es el artículo 114 relacionado con el deber de la información.

- **Resolución 2023500020000093-6 (13 de enero). Modifica y adiciona la jurisdicción y las sedes de las Direcciones Regionales de la Superintendencia Nacional de Salud.** Mediante esta Resolución, se garantiza la ampliación de la cobertura de la Superintendencia Nacional de Salud en el territorio nacional, la debida ejecución de las nuevas funciones asignadas y la atención a los usuarios del Sistema, redefiniendo la jurisdicción y fijando las sedes de funcionamiento de las Direcciones Regionales que se organizan y determinan de acuerdo con las necesidades del servicio de la entidad.

- **Ley 2291 (17 de febrero). Transforma la naturaleza jurídica del Instituto Nacional de**

Asociación Colombiana de Hospitales y Clínicas

Agradece
el apoyo de sus miembros patrocinadores:

BD

B BRAUN SHARING EXPERTISE

BIOART TECNOLOGÍA PARA LA VIDA

bionexo

EXPERTOS SEGURIDAD

Johnson & Johnson MEDICAL DEVICES COMPANIES

PHILIPS

SIEMENS Healthineers

stryker

SYAC

VAMED health. care. vitality.

La Ley 2291 (17 de febrero), transforma la naturaleza jurídica del Instituto Nacional de Cancerología, empresa social del estado, se define su objeto, funciones, estructura y régimen legal.

Cancerología, empresa social del estado, se define su objeto, funciones, estructura y régimen legal. A través de esta Ley, se transforma la naturaleza jurídica del Instituto Nacional de Cancerología Empresa Social del Estado en una entidad pública de naturaleza especial, con personería jurídica, patrimonio propio y autonomía administrativa, técnica y financiera, la cual se denomina "Instituto Nacional de Cancerología", perteneciente al sector descentralizado de la rama ejecutiva del orden nacional, adscrita al Ministerio de Salud y Protección Social e integrante del Sistema General de Seguridad Social en Salud y el Sistema Nacional de Ciencia, Tecnología e Innovación.

- **Resolución 367 (13 de marzo). Proceso para el fortalecimiento de la gestión de la salud ambiental a nivel territorial.** Con esta Resolución, se modifican los artículos 6 y 8 de la Resolución 3496 de 2019, que establecen el proceso para el fortalecimiento de la gestión de la salud ambiental a nivel territorial, con el propósito de garantizar de manera oportuna y con calidad el reporte de la información del seguimiento a la gestión de la salud ambiental a nivel territorial y la elaboración de los planes de fortalecimiento de capacidades, para lo cual se modifican los tiempos definidos para el reporte de información establecidos en la Resolución 3496 de 2019.

- **Resolución 318 (1 de marzo). Procedimiento para determinar las tecnologías y servicios que no serán financiados con recursos públicos asignados a la salud.** Se actualiza el procedimiento técnico científico y participativo para la determinación de los servicios y tecnologías que no podrán ser financiados con recursos públicos asignados a la salud, con el propósito de optimizar su aplicación y explicitar la etapa de validación dentro de la primera fase del procedimiento, con el fin de identificar las nominaciones de servicios y tecnologías indicados para enfermedades huérfanas o raras, así como aquellos clasificados como cosméticos y no aprobados por autoridad competente.

- **Resolución 253 (21 de febrero). Excedentes conciliados para el saneamiento de aportes patronales de las vigencias 2012 a 2016.** Mediante esta Resolución, se modifica la Resolución 1545 de 2019, en cuanto al plazo para efectuar aplicaciones, traslados y devoluciones de excedentes conciliados en el procedimiento para el saneamiento de aportes patronales de las vigencias 2012 a 2016, financiados con recursos del Sistema General de Participaciones, de manera que se amplían los tiempos estableci-

dos para efectuar las aplicaciones, traslados y devoluciones de excedentes conciliados previstos en los artículos 13 y 14 de la precitada Resolución, en aras de lograr una mayor efectividad y cobertura en el desarrollo del proceso.

- **Resolución 861 (31 de mayo). Montos de mecanismo adicional para ajustar la desviación de la siniestralidad "Hemofilia A Severa".** Se definen los montos por aportar, reconocer y pagar a las EPS de los regímenes contributivos y subsidiados, así como a las entidades adaptadas de la vigencia 2022, que se encuentran relacionadas en el presente acto administrativo, en aplicación del mecanismo adicional para ajustar la desviación de la siniestralidad "Hemofilia A Severa". Los valores determinados en el artículo anterior deberán ser girados mensualmente por la ADRES, con cargo a los recursos correspondientes a la UPC de la vigencia 2023, durante el primer semestre, de manera concomitante con el proceso de compensación y liquidación mensual de afiliados.

- **Resolución 851 (30 de mayo). Categorización del riesgo de las Empresas Sociales del Estado del nivel territorial (ESE) para la vigencia 2023.** Se establece la categorización del riesgo de las Empresas Sociales del Estado del nivel territorial para la vigencia 2023, una vez aplicada la metodología prevista en la Resolución 2509 de 2012, modificada por la Resolución 2249 de 2018. Durante los años 2020, 2021 y 2022 no se realizó la categorización, debido a la emergencia sanitaria generada por la COVID-19 y sus efectos.

- **Resolución 748 (25 de mayo). Procedimiento de designación de los miembros elegibles del Consejo Directivo del Instituto Nacional de Cancerología (INC).** Se establece que la elaboración de las ternas que se postularán para la conformación del Consejo Directivo del INC se realizará democrática y meritocráticamente, garantizando tanto la amplia participación del sector al cual pertenecen como la equidad de género. En desarrollo de lo anterior, las asociaciones e instituciones deberán diseñar un proceso de elección público, participativo y transparente. Los mismos principios deberán atenderse para la elección del miembro designado por el ente o entes que se constituyan por iniciativa del INC para apoyar financieramente las labores de investigación, del representante del estamento médico o de investigaciones del Instituto Nacional de Cancerología y de los representantes de las asociaciones de usuarios del Instituto Nacional de Cancerología, en su calidad de pacientes.

- **Resolución 648 (27 de abril). Modifica el artículo 26 de la Resolución 3100 de 2019 en el sentido de ampliar un plazo a los prestadores de servicios de salud.** Mediante esta Resolución se amplía en dos (2) meses el plazo para que los prestadores de servicios de salud inscritos en el REPS actualicen el portafolio de servicios y realicen la autoevaluación de las condiciones de habilitación definidas en la Resolución 3100 de 2019, pasando de seis (6) a ocho (8) meses, y así garantizar la continuidad en la prestación del servicio de salud a la población del país bajo los estándares que hacen parte de los diversos componentes del Sistema Obligatorio de Garantía de Calidad de la Atención de Salud.

- **Circular 011 (15 septiembre). Plan de contingencia MIPRES.** A través de la presente Resolución, conforme a lo establecido en las Resoluciones 1885 y 2438 de 2018, ante el incidente de ciberseguridad en el Datacenter del proveedor de servicios tecnológicos, donde se encuentran alojadas las aplicaciones misionales asociadas a la prestación de servicios derivados de la atención a nivel nacional, específicamente en lo relacionado con la herramienta tecnológica MIPRES, y dada la imposibilidad de restablecer los servicios de manera inmediata, el Ministerio de Salud y Protección Social establece un plan de contingencia, mediante la adaptación temporal

de las responsabilidades de los agentes del SGSSS y la adopción de formatos de contingencia.

- **Ley 2333 (25 de septiembre). Requisitos de hospitales universitarios.** Con esta Ley, se modifica el artículo 100 de la Ley 1438 de 2011, de manera que establece mecanismos para otorgar la certificación de Hospitales Universitarios a las instituciones prestadoras de servicios de salud por medio de un proceso de acreditación cumplido en plazos específicos, buscando así garantizar la formación en servicios de salud con criterios de calidad. Conforme lo anterior, se modifican los requisitos y trámites que deben cumplir las IPS que ostenten el carácter de hospitales universitarios.

- **Resolución 1676 (12 de octubre). Manual de Normas Técnicas, Administrativas y de Procedimientos para Bancos de Sangre.** Mediante esta Resolución, se modifican los numerales 3.2.2 y 3.5 del Capítulo 3 y el numeral 9.1.8 del Manual de Normas Técnicas Administrativas y de Procedimientos para Bancos de Sangre, adoptado mediante la Resolución 901 de 1996, y deroga la Resolución 3212 de 2018, con el propósito de eliminar las referencias a las categorías de hombres que tienen sexo con hombres (HSH) y población trans como factores, grupos, poblaciones o conductas de riesgo. Así, se modifica el numeral 3.2.2. "PARA PROTEGER AL RECEPTOR" que hace parte del numeral 3.2 "REQUISITOS PARA SER DONANTE" del Capítulo 3 "DONANTES DE SANGRE" y el numeral 9.1.8 del numeral 9.1 "Plan de emergencia para el banco de sangre" del Capítulo 9 "El Banco de Sangre en casos de emergencia o calamidad pública" del Manual.

- **Resolución 165 (1 de noviembre). Sistema de facturación electrónica.** Atendiendo a que la DIAN requiere que los sujetos obligados a facturar que vienen expidiendo documento equivalente, expidan, generen y transmitan el documento equivalente electrónico tiquete de máquina registradora con sistema POS a la DIAN, a partir de la fecha que se establezca en el calendario de implementación que se prescribe en la presente Resolución; por lo tanto, se definen y establecen las condiciones, los términos y los mecanismos técnicos y tecnológicos para la interoperabilidad, interacción, generación, numeración, transmisión, validación, expedición y entrega de este documento electrónico, el cual se integrará a los demás que componen el sistema de facturación, y que de igual forma deberá tener la interacción con inventarios, sistemas de pago, impuestos y contabilidad e información tributaria legalmente exigida.

  Por lo anterior, es necesario desarrollar los aspectos técnicos y tecnológicos que se consideren necesarios para la adecuada implementación del sistema de facturación, adoptando la versión 1.9 del Anexo técnico de factura electrónica de venta, y el documento equivalente electrónico, expidiendo el Anexo técnico del documento equivalente electrónico versión 1.0, y expedir otras disposiciones en materia del sistema de facturación.

- **Resolución 1798 (1 de noviembre). SAT independientes.** Con esta Resolución, se fijan las condiciones generales para la operación del Sistema General de Riesgos Laborales en el Sistema de Afiliación Transaccional (SAT) y se definen los lineamientos para la incorporación de información y su interoperabilidad con las entidades Administradoras de Riesgos Laborales (ARL), en relación con la afiliación y reporte de novedades de los trabajadores independientes-afiliados obligatorios y voluntarios al referido sistema, según lo contenido en el Anexo Técnico N.º 1 "Incorporación de Información de la Afiliación y Novedades de los Trabajadores Independientes al Sistema General de Riesgos Laborales en el SAT" y en el Anexo Técnico N.º 2 "Operación del Sistema General de Riesgos Laborales en el Sistema de Afiliación Transaccional-Afiliación y novedades de los trabajadores

independientes en el SGRL" , que hacen parte integral de dicha Resolución.

- **Resolución 879 (2 de junio). Directrices para el trámite y emisión de conceptos institucionales a los proyectos de ley y de actos legislativos Minsalud.** De esta manera, se establecen directrices para el trámite y emisión de conceptos técnico-jurídicos por medio de los cuales se expresa la posición institucional del Ministerio de Salud y Protección Social, frente a los proyectos de ley y de actos legislativos que cursan en el Congreso de la República y de sus posibles objeciones presidenciales.

- **Ley 2294 (19 de mayo). Plan Nacional de Desarrollo 2022-2026 "Colombia, potencia mundial de la vida".** Mediante esta Ley, se sientan las bases para que el país se convierta en un líder de la protección de la vida a partir de la construcción de un nuevo contrato social que propicie la superación de injusticias y exclusiones históricas, la no repetición del conflicto, el cambio de nuestro relacionamiento con el ambiente y una transformación productiva sustentada en el conocimiento y en armonía con la naturaleza. Este proceso debe desembocar en la paz total, entendida como la búsqueda de una oportunidad para que todos podamos vivir una vida digna, basada en la justicia, es decir, en una cultura de la paz que reconoce el valor excelso de la vida en todas sus formas, y que garantiza el cuidado de la casa común.

Inspección vigilancia y control

- **Circular Externa 02 (3 de enero). Instrucciones para la intensificación y fortalecimiento de las acciones de prevención, atención integral, vigilancia y control del dengue en Colombia.** En el marco de esta disposición, le corresponde a las IPS, en el ámbito de sus funciones, implementar estrategias de capacitación y entrenamiento del talento humano en salud, conforme a los protocolos de vigilancia en salud pública, guía de manejo clínico o lineamientos de atención clínica integral vigentes, con el fin de realizar una adecuada evaluación del riesgo individual, así como de las medidas de aislamiento, diagnóstico, tratamiento y seguimiento; cumplir con los procesos de adopción, adaptación y cumplimiento de la guía de manejo clínico o lineamientos de atención clínica integral de dengue vigente, así como de las acciones de formación continua al talento humano a cargo de la prestación de servicios; remitir el número de muestras de los casos en fase aguda, esto es, dentro de los primeros cinco días de inicio de síntomas, que el Laboratorio de Salud Pública Departamental o Distrital le asigné según programación, en el marco del desarrollo de las acciones de la vigilancia por laboratorio, entre otras acciones.

La Resolución 879 (2 de junio), se establecen las directrices para el trámite y emisión de conceptos institucionales a los proyectos de ley y de actos legislativos Minsalud.

- **Circular Externa 2023310010007065–6 (29 de marzo).** Por medio de esta circular, se imparten instrucciones para garantizar el cumplimiento del flujo de recursos, y se modifican el archivo tipo ft025 de la circular externa 014 de 2020 y el archivo tipo st010 de la circular externa 008 de 2018.

  La Superintendencia Nacional de Salud, con el fin de generar las herramientas necesarias para la verificación del adecuado flujo de recursos entre los participantes del proceso de prestación de servicios de salud, el aumento de la UPC conforme a lo establecido en la Resolución 2809 de 2022 y el cumplimiento de la Circular Externa 0054 de 2022 expedidas por el Ministerio de Salud y Protección Social, imparte instrucciones a las

EPS, Regímenes exceptuados y especiales, las Entidades Territoriales, Empresas de Medicina Prepagada e IPS Públicas, Privadas y Mixtas, cuando celebren acuerdos de voluntades.

De esta manera, establece la obligatoriedad de publicar en la página Web de las EPS, a más tardar el 30 de abril de 2023, el registro del valor transferido a las IPS, e informar el enlace dispuesto para su consulta antes de la fecha límite de publicación. Vencido dicho plazo, los IPS dentro de los diez (10) días siguientes, debían informar a la Supersalud si dicha publicación correspondía a lo efectivamente pagado. El incumplimiento de estas instrucciones da lugar a las sanciones correspondientes.

- **Resolución 2023320030003984-6 (16 de junio). Ordena la toma de posesión inmediata de bienes, haberes y negocios y la intervención forzosa administrativa para administrar a SAVIA SALUD EPS.** De esta manera, se ordena la toma de posesión inmediata de los bienes, haberes y negocios, y la intervención forzosa administrativa para administrar por el término de un (1) año, es decir, desde el 16 de junio de 2023 hasta el 16 de junio de 2024, a SAVIA SALUD EPS, teniendo en cuenta que se evidencia el deterioro de la entidad vigilada en los componentes financiero, técnico-científico y jurídico, y las causales previstas en los literales d), e), h), i) del artículo 114 del Estatuto Orgánico del Sistema Financiero (EOSF).

- **Resolución 881 (2 de junio). Dolutegravir a licencia obligatoria.** Con esta Resolución, se ordena comunicar el inicio del procedimiento administrativo a los titulares de las patentes VIIV HEALTHCARE COMPANY y SHIONOGI & CO. LTD., y a los titulares del registro sanitario de los medicamentos contentivos del principio activo, dado el alto costo del Dolutegravir como medicamento base de los regímenes preferidos en personas con edad igual o mayor a 18 años con diagnóstico de infección por VIH; por lo tanto, limita la capacidad de respuesta del sistema de salud en términos de cobertura de la población afectada y compromete el uso eficiente de los recursos de este.

- **Resolución 2023320030002798-6 (11 de mayo). Intervención forzosa administrativa para administrar a ASMET SALUD EPS SAS.** Ordena la toma de posesión inmediata de los bienes, haberes y negocios, así como la intervención forzosa administrativa para administrar por el término de un (1) año, es decir, desde el 12 de mayo de 2023 hasta el 12 de mayo de 2024, por las razones expuestas en la parte motiva de esta Resolución, por presentarse las causales de los literales a, d, e, f, g, h y i del artículo 114 del EOSF.

- **Circular Externa 2023151000000 010-5 (22 de junio). Términos para resolver reclamos en salud.** La Superintendencia Nacional de Salud, atendiendo a la necesidad de resolver de fondo las peticiones y reclamos de los usuarios con la inmediatez que la situación requiera y conforme a las características de calidad, oportunidad, continuidad e integralidad inherentes al derecho fundamental a la salud, replantea los plazos máximos establecidos para dar respuesta a las PQR que reciben las EPS y las IPS.

  Adopta las definiciones de petición, queja, reclamo, reclamo de riesgo simple, reclamo de riesgo priorizado y reclamo de riesgo vital. Se establecen los mecanismos, procesos y procedimientos que deben adoptar las EAPB y las IPS para resolver de manera objetiva, oportuna y eficiente las PQR de los usuarios. Se conceden 72 horas, 48 horas y hasta 24 horas para resolver dichas quejas según la clasificación de las definiciones. Se establece el reporte de las línea de atención y se sustituye el anexo GT005 sobre inventario de peticiones, quejas, reclamos y denuncias radicadas.

- **Ley 2316 (17 de agosto). Resolución 1557 (27 de septiembre). Tipo penal de lesiones**

personales con sustancias modelantes invasivas e inyectables no permitidas (biopolímeros). A través de esta Ley, se crea el tipo penal de lesiones personales con sustancias modelantes no permitidas (biopolímeros), regula el uso, comercialización y aplicación de algunas sustancias modelantes, establece medidas a favor de las víctimas y promueve estrategias preventivas en la materia.

- **Resolución 2023320030005625-6 (15 de septiembre). Intervención forzosa administrativa para administrar a FAMISANAR EPS SAS.** Con esta Resolución, la Superintendencia Nacional de Salud ordenó la medida de toma de posesión e intervención forzosa administrativa para administrar por el término de un (1) año, es decir, desde el 15 de septiembre de 2023 hasta el 15 de septiembre de 2024, designando como INTERVENTORA a SANDRA MILENA JARAMILLO AYALA y a la firma NEXIA MONTES & ASOCIADOS SA como contralor.

  Esto tiene lugar como consecuencia del deterioro de la entidad en los componentes financiero, técnico-científico y jurídico que se evidencian en las causales previstas en los literales e), g) h), i) del artículo 114 del Estatuto Orgánico del Sistema Financiero, y ante la inminente afectación del aseguramiento en salud y de la garantía de la prestación de los servicios de salud, en cumplimiento de los preceptos establecidos en los artículos 48, 49 y 365 de la Constitución Política de Colombia, en concordancia con las normas del SGSSS.

- **Circular 2023150000000013-5 (15 septiembre). Modifica temporalmente los términos y condiciones para el reporte de información de algunos archivos tipo.** De esta manera, la Superintendencia Nacional de Salud modificó el plazo de reporte de los archivos tipo relacionados en la tabla "ARCHIVO TIPO" de esta circular, cuya fecha de corte corresponde al 31 de agosto de 2023, y las fechas de reportes que se encuentran establecidas entre los 10 días hábiles o los 20 primeros días calendario de septiembre de 2023.

La Superintendencia Nacional de Salud, atendiendo a la necesidad de resolver de fondo las peticiones y reclamos de los usuarios, replantea los plazos máximos establecidos para dar respuesta a las PQR que reciben las EPS y las IPS.

- **Circular 2023160000000012-5 (14 de septiembre). Modifica los términos y condiciones de algunos reportes de información.** A través de esta circular, la Superintendencia Nacional de Salud modifica el plazo de reporte de los archivos tipo relacionados en la presente Resolución, cuya fecha límite es el décimo día hábil de cada mes. Los demás reportes deberán seguir efectuándose con los cortes y periodicidad establecida en la Circular Única.

Resolución 2023310010007065–6 (10 de octubre). Cambio en la composición de la propiedad y de reforma estatutaria "SAVIA SALUD EPS". Con esta Resolución, se autoriza la solicitud de aprobación de la reforma de los artículos 46, 48 y 51 de los estatutos sociales de ALIANZA MEDELLÍN ANTIOQUIA EPS, aprobados por la Asamblea General de Accionistas, que implica la composición de la propiedad y la reforma de sus estatutos sociales, producto de la capitalización que pretende realizar, por la suma de sesenta y tres mil ciento setenta y dos millones novecientos ochenta y un mil quinientos doce pesos m/cte. ($63.172.981.512), de los cuales treinta y seis mil novecientos cincuenta y seis millones cuatrocientos cuarenta y cuatro mil setecientos setenta pesos m/cte. ($36.956.444.770) equivalen al capital suscrito y pagado.

Salpicón de la salud

Néstor Álvarez
Pacientes alto costo

La participación social en salud durante 2023 tuvo más de 339 razones para ejercerse desde todos los espacios legales y especialmente desde las redes sociales, como un escenario de opinión donde surgieron activistas de todas las corrientes.

Durante los 18 años de trabajo que llevo en defensa de los derechos de los usuarios, los diferentes agentes del sector nos habíamos acostumbrado a vernos en diferentes escenarios siempre los mismos y en las mismas, pero surgieron las 339 razones que despertaron esta reflexión. A continuación, intento relatar un poco los actos que se han dado en este proceso de validación de dichas razones:

Con la promesa de cumplir el mandato del pueblo, como lo argumentan todos los gobiernos: "me eligieron y debo cumplir"; entonces, surgió el primer acto donde se argumentaba que no se tuvieron en cuenta a los pacientes y sociedad civil para las 339 razones de la participación social, argumento que empezó a tomar fuerza dentro de la estrategia de gremios del sector económico del negocio de la salud. Es entonces cuando las imágenes religiosas enfrentan a la diosa creadora de las 339 razones de la participación social, y me preguntaba: "¿quién ganará? ¿La imagen de la religión o la creadora?". Pero fue pasando el tiempo y se diluyó este primer acto.

Luego viene el segundo acto donde muy estratégicamente un gremio da el apoyo a algunas asociaciones de usuarios de las EPS más importantes del sector, y ese acto es un poco largo, porque empiezan estas asociaciones a alejarse de sus funciones y a defender a ciegas la no eliminación del "florero". Todo esto se evidenció en espacios donde nunca antes se habían visto y fueron llegando muy empoderadas como representantes casi del gremio, pues éste siempre tenía a su equipo apoyándolas. A su vez, en la redes sociales nacían nuevos activistas en pro y contra de las 339 razones de la participación social, la mayoría de ellos dentro de marcos emocionales de la democracia y la política, y una casi nula defensa técnica o de apoyo de por qué 3×3 es 9: "339" razones de participación social.

Sigue el tercer acto, en el que los pacientes en redes sociales, con el apoyo y seguimiento de las ONG que han estado en el lobby del derecho a la salud de patologías que tienen productos de patente (porque no hay ONG para diarrea o acné), aparecen argumentando que el florero es importante y no se debe romper

porque quedaríamos sin dónde poner el agua y las flores, y eso sería muy grave. Pero sin ningún mensaje de por qué debe evolucionar el sistema, o explicación sobre por qué el florero quedó pequeño, que no le cabe toda el agua y mucho menos las flores, sino simplemente que debemos conservar el mismo florero y nada más.

En actos paralelos, gremios del sector con figuras públicas nos asustan con el coco y el infierno si ese florero se rompe y queda en 3 y 3 y 9 pedazos, y del otro lado nos dicen que es importante que se rompa en el florero en 3 y 3 y 9 pedazos, porque así podemos ir al cielo y ser felices, y las dos partes soportan sus argumentos en la defensa de los pobres: por lo pobres no se puede romper el florero y por los pobres se debe romper el florero.

Acto seguido, han venido diferentes intervenciones de defensores y opositores del rompimiento del florero en las calles, donde se ha evidenciado poca asistencia por aquello de que solo son 3 razones que multiplicadas por 3 dan 9 nada más.

Otro acto de nuevo corresponde a las organizaciones de pacientes con el PARE no rompa el florero y el acompañamiento de actores visibles en la opinión; obviamente, del otro lado se mantiene la insistencia de por qué se debe romper el florero, soportadas por los otros opinadores del sistema, con el sello del negocio de la educación "líderes académicos". Todos se encuentran en las plataformas de las redes sociales con una defensa política emocional y la oposición también con argumentos emocionales.

Todo esto ha estado acompañado de una mesa y un mantel donde se ha puesto el florero

La democracia avanza y sale el florero medio roto de un cuarto a esperar si se acaba de romper en el otro o si se pega o si nace otro grito de independencia.

así: tres EPS salieron a decir que no alcanzaba la plata sino hasta noviembre, y que les debían plata y los que organizan la mesa diciendo que no deben. Luego, aparece una granada para jugar con el tema de las reservas técnicas, y esa granada pareciera que se estalla en la manos, debido a que la EPS mixta es la líder del incumplimiento; sale un gremio de las EPS a pedir al que arregla la mesa que se sienten a hablar del tema de reservas, pero este guarda silencio y nada pasa. Se rompe el silencio con otra granada de mano, como fue el velo para el mantel o algo parecido, pero en últimas otros actores dicen que no opinarán si el mantel es de velo o algo más, y entonces se pregunta uno: ¿será que se agotaron las 339 razones o hay más? Pero claro que hay más. La democracia avanza y sale el florero medio roto de un cuarto a esperar si se acaba de romper en el otro o si se pega o si nace otro grito de independencia.

Faltaba que alguien abriera la cortina para que la luz alumbrara el florero y un tercero dice que no puede dar más flores para el florero, porque le deben plata, y de nuevo 339 razones para pensar qué sigue. Todo esto se acompañó al final de una activa protesta por las UCI en COVID con espejo retrovisor en la plata y en las vacunas; pero las redes siguen sumando actores y temas a las 339 razones y el estigma por apoyar o no la ruptura del florero.

Creo que este salpicón ha tenido mucha fructosa y nos puede llevar a una prediabetes o diabetes de cualquier tipo; por eso, le pedí al niño Dios que nos ayude a entender las 339 razones de mantener o romper el florero.

50.° Informe de **seguimiento de cartera hospitalaria***

La Asociación Colombiana de Hospitales y Clínicas (ACHC) presentó su tradicional estudio de cartera hospitalaria, *correspondiente a la situación de cuentas por cobrar de 207 Clínicas y Hospitales reportantes* o Instituciones Prestadoras de Servicios de Salud-IPS- *con corte a junio 30 de 2023*. Dichas instituciones representan *cerca del 30 % de las camas hospitalarias habilitadas en todo el país*.

De las 207 IPS que reportaron información en el actual corte, 109 son de naturaleza privada, 96 de naturaleza pública y 2 de carácter mixto. A su vez, el 43,0 % de las instituciones son de alta complejidad, el 22,2 % de mediana y el 34,8 % de baja.

Metodología

Desde hace tres cortes, se decidió fusionar o agrupar algunas categorías que representan, en su conjunto, menos del 20 % de todo el volumen de la deuda reportada por las instituciones hospitalarias, a lo largo de todos los estudios anteriormente elaborados por la ACHC, dejando abierta únicamente las categorías principales de mayor peso y representatividad dentro de la deuda total.

El análisis que sustenta el presente estudio se hizo tomando como fuente de información primaria, los registros de deuda depurados de 207 IPS, a partir de la expedición de la Circular Externa N.º 016 de noviembre de 2016 (inclusión del formato FT003 cuentas por cobrar-deudores), mediante la cual la Superintendencia Nacional de Salud derogó en su totalidad la información que debían reportar obligatoriamente las IPS en el marco de la Circular Externa N.º 047 de 2007, por efecto de la implementación de las Normas Internacionales de Información Financiera (NIIF).

Es importante aclarar que, para los estudios anteriores al año 2017, se tuvieron en cuenta los formatos contemplados en la Circular Externa Única 047 de 2007 (archivo tipo de cuentas por cobrar) y la Circular Externa 049 de 2008, emanadas de la Supersalud; dichos formatos fueron identificados como archivo de deudores tipo 059 para las IPS de naturaleza privada y tipo 064 y 114 para las públicas. Igualmente, se tuvieron en cuenta la Resolución 4362 de 2011 y su respectivo ajuste con la Resolución 1121 de 2013 por las cuales se emite y se ajusta el nuevo Plan Único de Cuentas (PUC) para IPS de naturaleza privada, expedidas ambas por la Supersalud. De igual forma, se incluyó la Resolución 421 de 2011 de la Contaduría General de la Nación que tiene en cuenta estas mismas

* Dirigido por Juan Carlos Giraldo Valencia, director de la ACHC. Elaborado por Juan Guillermo Cuadros Ruiz, miembro del grupo de Investigación y Proyectos de la ACHC. Con el apoyo de Ana Sofía Zea Ruiz, miembro del grupo de Investigación y Proyectos de la ACHC.

modificaciones del PUC para las IPS de naturaleza pública, denominado Catálogo General de Cuentas del Manual de Procedimientos del Régimen de Contabilidad Pública. Se tuvo en cuenta, igualmente, el Decreto 1095 de 2013, por el cual se reglamentó el inciso 2 del Artículo 3 de la Ley 1608 de 2013, donde se estipula el procedimiento de aplicación de los giros directos[1] entre los agentes del Sistema. Para el efecto, se presenta la clasificación ajustada de los siete (7) tipos de deudores establecida por la ACHC a partir del periodo anterior y los cuales se describen brevemente a continuación:

1. Régimen contributivo: comprende el registro de la deuda de las EPS en operación que administran dicho régimen, así como la de aquellas que entraron en liquidación.
2. Estado: categoría bajo la cual se consolida la deuda de las entidades territoriales de salud (ETS), representadas en las secretarías departamentales y locales de salud, las direcciones o departamentos seccionales de salud, alcaldías, gobernaciones, municipios o departamentos, en lo que se refiere a la atención de la población pobre no afiliada y la atención de servicios No POS[2], más la deuda de las antiguas cajas de previsión social del orden territorial, que no se transformaron en entidades adaptadas de salud (EAS), del extinto operador fiduciario del FOSYGA[3], de la ADRES[4] y de otras entidades del Estado[5].
3. Régimen subsidiado: comprende el registro de la deuda de las entidades promotoras de salud (EPS-S) en operación que administran este régimen, así como la de aquellas que entraron en liquidación, ya sean estas EPS, cajas de compensación familiar, empresas solidarias, mutuales o indígenas; e igualmente incluye la cartera identificada por código del tipo de negocio, incluso de administradoras que anteriormente se fusionaron y aún registran deuda.
4. Entidades de medicina prepagada y planes complementarios.
5. Aseguradoras por reclamaciones del Seguro Obligatorio de Accidentes de Tránsito (SOAT) y por cubrimiento de pólizas de salud y accidentes, y empresas donde se registra el nombre, sin identificar el tipo de cubrimiento.
6. Administradoras de riesgos profesionales o laborales.

[1] Artículo 10 de la Ley 1608 de 2013; Resoluciones 0654 de 2014, 3503 de 2015, 3110 y 2916 de 2018 (contributivo); Resoluciones 2320 de 2011 y 1587, 4621 de 2016 y 3110 de 2018 (subsidiado).

[2] De acuerdo con lo establecido en el Decreto 804 de 1998 y la Resolución 5334 de diciembre de 2008, que reglamenta lo ordenado por la Sentencia T -760 de 2008.

[3] En muchos reportes, se registra deuda de FOSGA, FISALUD y FIDUFOSYGA, las primeras fiducias que operaron los recursos del FOSYGA. Hasta 2017, el consorcio que manejaba estos recursos era el operador SAYP, integrado por FIDUPREVISORA y FIDUCOLDEX (estas entidades operaban desde del día 29 de septiembre de 2011) y fueron reemplazadas por la ADRES.

[4] Artículo 27 del Decreto 1429 de 2016. Transferencia de derechos y obligaciones: Todos los derechos y obligaciones que hayan sido adquiridos por la Dirección de Administración de Fondos de la Protección Social del Ministerio de Salud y Protección Social, con ocasión de la administración de los recursos del Fondo de Solidaridad y Garantía (FOSYGA) y del Fondo de Salvamento y Garantías para el Sector Salud (FONSAET), se entienden transferidos a la Administradora de los Recursos del Sistema General de Seguridad Social en Salud (ADRES). Todos los derechos y obligaciones a cargo del FOSYGA pasarán a la Administradora de los Recursos del SGSSS-ADRES, una vez sean entregados por el Administrador Fiduciario de conformidad con lo establecido en el contrato de encargo fiduciario con éste celebrado.

[5] Fuerzas militares (Ejército, Armada y Fuerza Aérea) y Policía Nacional, INPEC, SENA, ICBF, Fiscalía General de la Nación, Ministerios y demás entidades públicas que dependen de aportes del presupuesto general de la nación.

7. Otras, las cuales incluyen:
   - Instituciones Prestadoras de Servicios de Salud: deuda de otras instituciones que se clasifican en IPS públicas y privadas en general, las que conforman Uniones Temporales y capitadoras, cuando el reporte permite identificar esta modalidad de contratación y pago.
   - Empresas: en aquellos casos que cuentan con planes de salud para sus empleados y familiares, o deudas de compañías o empresas propiamente dichas sean nacionales o extranjeras.
   - Particulares: corresponde al registro de la deuda de personas naturales.
   - Magisterio: corresponde a la cartera que se registra para este grupo de trabajadores, anteriormente a través del Fondo Educativo Regional (FER) o de la Fiduciaria La Previsora, que administra los recursos de este régimen de excepción, u otras entidades que prestan servicios de atención al magisterio.
   - Cartera sin clasificar y otros conceptos: categoría en la cual se registra la deuda de otras entidades e, incluso, de organismos internacionales, y que no corresponden a las categorías antes enunciadas, más anticipos, avances, entre otros.

Principales resultados

Los estudios de cartera hospitalaria se vienen realizando desde el año 1998, *lo que corresponde a un periodo de 25 años consecutivos de seguimiento*. El estudio de cartera Número 50, elaborado por la ACHC, presenta los siguientes resultados:

- Para el conjunto de las 207 instituciones que reportaron información en el presente corte, la cifra adeuda asciende a más de *$16,0 billones de pesos*; variación positiva del 14,7 % con respecto a la deuda reportada en el semestre a diciembre de 2022. De esta cifra, el 47,7 % corresponde a cartera corriente (menor a 60 días) y el *52,3 % a cartera vencida*[6] o de difícil cobro *(mayor a 60 días por valor de $8,4 billones de pesos aproximados)*.
- De manera global, y según las categorías de deuda presentadas en el estudio, la mayor participación en la deuda total de los más de $16 billones de pesos corresponde una vez más a *las Entidades Promotoras de Salud (EPS) del Régimen Contributivo ($7,9 billones de pesos, equivalente al 49,4 %)*, seguida por las *EPS-S del Régimen Subsidiado ($3,5 billones de pesos, equivalente al 21,9 %)*, y en tercer lugar la *categoría Estado ($1,5 billones de pesos, equivalente al 9,5 %)*, la cual incluye la deuda de las Entidades Territoriales de Salud, el extinto operador fiduciario del FOSYGA, la deuda de la Entidad Administradora de los Recursos del Sistema General de Seguridad Social en Salud (ADRES) y otras entidades del estado como fuerzas militares, policía nacional, ministerios, entre otros. Las otras categorías de deudores donde se incluyen planes complementarios

[6] El literal d) del artículo 13 de la Ley 1122 sobre el flujo y la protección de los recursos, donde se precisó que los servicios de salud deben cancelarse dentro de los 60 días posteriores a la presentación de la factura.

y medicina prepagada, aseguradoras, administradoras de riesgos laborales, IPS, empresas, particulares, el magisterio y la categoría sin clasificar *suman únicamente el 19,2 % del total de la deuda reportada.*

- En síntesis, las EPS del Régimen "Contributivo" y "Subsidiado", más la categoría "Estado", *representan el 80,8 % del total de la deuda a junio de 2023 (más de $ 13,0 billones de pesos).*
- La morosidad, expresada como la concentración de cartera de 60 días y más, es *del 65,6 % para la categoría Estado* (compuesta del 100,0 % de cartera morosa del desaparecido operador fiduciario del FOSYGA y del 77,0 % de cartera morosa de los Entes), *seguida del 60,8 % para las EPS del Régimen Subsidiado y, finalmente, del 51,9 % para las EPS del Régimen Contributivo.*
- Es preciso anotar que la deuda referida a la ADRES a junio 30 de 2023 (más de $ 298.000 millones) corresponde al proceso relacionado con el reconocimiento y pago de Reclamaciones por Accidentes de Tránsito y Eventos Catastróficos y Terroristas, es decir, *no* se tienen en cuenta los demás procesos de reconocimiento, pago y giro de recursos a favor de los actores del SGSSS[7] y que, según sus informes, equivalen *al 99,4% del uso total de los recursos apropiados para la vigencia 2023, estimados en $82,8 billones de pesos.*[8] Dicho lo anterior, se desataca la labor de esta entidad como pagadora en lo referente a los giros ordinarios del sistema (UPC, licencias, presupuestos máximos, reconocimientos servicios NO PBS, giro directo a prestadores).

[7] Artículo 67 de la Ley 1753 de 2015, recaudo de los recursos del SGSSS.

[8] Presentación ADRES año 2023. Debates control político e informe de rendición de cuentas.

Cuadro 1. Composición de cartera por tipo de deudor (cifras en miles de pesos) a junio 30 de 2023.

Tipo de deudora	A 30 días mas cte	Part % edad	De 31 a 60 días	Part % edad	De 61 a 90 días	Part % edad	Más de 91 días	Part % edad	TOTAL	Part % TOTAL Junio 2023	Part % TOTAL Diciembre 2022
1. REG. CONTRIBUTIVO	3.250.573.138	40,9%	579.475.093	7,3%	439.641.423	5,5%	3.684.816.351	46,3%	7.954.506.005	49,4%	50,6%
2. ESTADO	467.258.032	30,7%	56.888.895	3,7%	50.294.499	3,3%	949.572.678	62,3%	1.524.014.104	9,5%	9,1%
ADRES	78.261.286	26,2%	14.105.287	4,7%	11.717.720	3,9%	194.541.426	65,1%	298.625.718	1,9%	1,8%
ENTE TERRITORIAL	141.768.030	19,4%	26.051.945	3,6%	18.023.149	2,5%	543.687.506	74,5%	729.530.629	4,5%	5,1%
OPERADOR FIDUCIARIO (EXTINTO FOSYGA)		0,0%		0,0%		0,0%	99.472.161	100,0%	99.472.161	0,6%	0,6%
OTRAS	247.228.717	62,4%	16.731.664	4,2%	20.553.630	5,2%	111.871.586	28,2%	396.385.596	2,5%	1,6%
3. REG. SUBSIDIADO	1.139.216.360	32,3%	242.022.794	6,9%	187.835.818	5,3%	1.953.711.752	55,5%	3.522.786.724	21,9%	22,8%
4. PC Y MP	267.656.075	77,8%	15.713.081	4,6%	10.435.392	3,0%	50.201.541	14,6%	344.006.089	2,1%	2,2%
5. ASEGURADORAS	246.673.504	44,8%	23.960.622	4,4%	22.579.118	4,1%	256.839.834	46,7%	550.053.078	3,4%	3,2%
6. ARL (RIESGOS LABORALES)	23.449.997	53,3%	2.063.814	4,7%	1.186.100	2,7%	17.275.779	39,3%	43.975.690	0,3%	0,3%
7. OTROS CONCEPTOS (IPS, EMPRESAS, PARTICULARES, MAGISTERIO, SIN CLASIFICAR)	1.266.171.828	58,7%	93.741.184	4,3%	91.935.340	4,3%	706.174.050	32,7%	2.158.022.403	13,4%	11,8%
Total general	6.660.998.935	41,4%	1.013.865.483	6,3%	803.907.689	5,0%	7.618.591.985	47,3%	16.097.364.093	100,0%	100,0%

Fuente: ACHC, información que reportaron 207 instituciones hospitalarias.

- Al detallar la deuda por EPS, tenemos que esta representa $11,5 billones de pesos aproximados, con una concentración morosa del 54,6 %, en donde la de las EPS Activas es por un valor de $8,5 billones de pesos y la de las EPS Liquidadas por valor de $2,9 billones de pesos.

Por su parte, la deuda de las EPS Activas en Medidas Especiales (vigilancia especial, programa de recuperación o toma de posesión e intervención para administrar) por parte de la Supersalud es por valor de $1,5 billones de pesos.

Cuadro 2. Deuda por grupos de EPS (cifras en miles de pesos) a junio 30 de 2023.

CARTERA ADEUDADA GRUPOS DE EPS		Cartera en Mora (mayor a 60 días)	Cartera TOTAL	% MORA (mayor a 60 días)
TOTAL EPS	*TOTAL EPS CONTRIBUTIVO + SUBSIDIADO*	$ 6.266.005.343	$ 11.477.292.729	54,6%
EPS CONTRIBUTIVO	*TOTAL EPS CONTRIBUTIVO*	$ 4.124.457.774	$ 7.954.506.005	51,9%
	EPS CONTRIBUTIVO "ACTIVAS"	$ 2.357.911.052	$ 6.187.959.283	38,1%
	EPS CONTRIBUTIVO "LIQUIDADAS"	$ 1.766.546.722	$ 1.766.546.722	100,0%
EPS SUBSIDIADO	*TOTAL EPS SUBSIDIADO*	$ 2.141.547.570	$ 3.522.786.724	60,8%
	EPS SUBSIDIADO "ACTIVAS"	$ 954.997.269	$ 2.336.234.428	40,9%
	EPS SUBSIDIADO "LIQUIDADAS"	$ 1.186.550.300	$ 1.186.552.296	100,0%

Fuente: ACHC, información que reportaron 207 instituciones hospitalarias.

- Frente a las cinco principales entidades por tipo de deudor, tenemos casos destacados de EPS Activas como la Nueva EPS y Sanitas (en el contributivo) y Emssanar, Savia Salud y Asmet Salud (en el subsidiado). En la categoría ESTADO resaltan Norte de Santander, el Distrito Capital y Valle del Cauca. Dentro de los entes territoriales y frente a las Aseguradoras SOAT, destaca la deuda de la Compañía Mundial de Seguros S.A., La Previsora S.A. Compañía de Seguros de carácter público, Seguros de Vida del Estado, Seguros de Vida Suramericana S.A. y AXA Colpatria Seguros S.A., como se muestra en el cuadro 3.

Cuadro 3. Deuda de las cinco principales deudoras por tipo (cifras en miles de pesos) a junio 30 de 2023.

CATEGORÍA	NOMBRE DEL DEUDOR	NATURALEZA JURIDICA	60 días y más (mora)	Total	Concentración morosa a Junio 2023	Concentración morosa a Diciembre 2022	DIFERENCIA % CARTERA MOROSA
REG. CONTRIBUTIVO	NUEVA EPS	MIXTA	1.045.672.943	2.415.771.512	43,3%	42,6%	0,6%
	MEDIMAS EPS SAS	PRIVADO	618.237.786	618.237.786	100,0%	100,0%	0,0%
	COOMEVA EPS	PRIVADO	500.703.161	500.703.161	100,0%	100,0%	0,0%
	EPS SANITAS	PRIVADO	409.161.041	899.233.093	45,5%	40,4%	5,1%
	CAFESALUD EPS	PRIVADO	320.998.250	320.998.250	100,0%	100,0%	0,0%
REG. SUBSIDIADO	EMSSANAR ESS	PRIVADO	243.911.463	453.820.746	53,7%	43,5%	10,3%
	ECOOPSOS ESS	PRIVADO	190.963.920	190.963.920	100,0%	68,3%	31,7%
	CONVIDA	PUBLICO	176.935.393	176.935.393	100,0%	100,0%	0,0%
	SAVIA SALUD EPS	MIXTA	159.647.522	486.591.052	32,8%	30,9%	1,9%
	ASMET SALUD ESS	PRIVADO	153.665.863	347.209.814	44,3%	49,8%	-5,6%
ESTADO	ADRES	PUBLICO	206.259.146	298.625.718	69,1%	75,5%	-6,4%
	NORTE DE SANTANDER	PUBLICO	133.511.332	166.098.320	80,4%	83,0%	-2,6%
	EXTINTO OPERADOR FIDUCIARIO (FOSYGA)	PUBLICO	99.472.161	99.472.161	100,0%	100,0%	0,0%
	BOGOTA D.C.	PUBLICO	81.594.314	124.567.091	65,5%	77,6%	-12,1%
	VALLE DEL CAUCA	PUBLICO	54.430.194	66.157.350	82,3%	83,9%	-1,6%

Continua en la siguiente página

CATEGORÍA	NOMBRE DEL DEUDOR	NATURALEZA JURIDICA	60 días y más (mora)	Total	Concentración morosa a Junio 2023	Concentración morosa a Diciembre 2022	DIFERENCIA % CARTERA MOROSA
ASEGURADORAS SOAT	COMPAÑIA MUNDIAL DE SEGUROS S.A. (SEGUROS MUNDIAL)	PRIVADO	48.849.250	70.832.334	69,0%	68,6%	0,4%
	LA PREVISORA S.A. COMPAÑIA DE SEGUROS	PUBLICO	43.750.244	69.166.599	63,3%	73,4%	-10,1%
	SEGUROS DE VIDA DEL ESTADO S.A.	PRIVADO	29.042.107	46.675.129	62,2%	59,9%	2,3%
	SEGUROS DE VIDA SURAMERICANA S.A.	PRIVADO	16.280.174	53.452.919	30,5%	41,6%	-11,2%
	AXA COLPATRIA SEGUROS S.A.	PRIVADO	15.859.103	22.122.763	71,7%	62,9%	8,8%

Fuente: ACHC a partir de la información reportada por instituciones reportantes (207 en el último corte).

- Las principales entidades deudoras por participación relativa de la cartera mayor a 60 días presentaron un incremento de 1,9 puntos porcentuales. El monto de cartera morosa de las primeras diez entidades del *ranking,* por valor de 4,3 billones, es superior en más de $495.000 millones con respecto a diciembre de 2022. Se agrega adicionalmente, que la totalidad de la cartera de estas entidades a junio 30 de 2023 suma un total de más de $7,3 billones aproximados (45,1 % del total de los más de $16,0 billones presentados en el siguiente informe), lo cual es bastante representativo para referenciar a los mayores poseedores de deuda actual.

Cuadro 4. Concentración de cartera de 60 días y más por los 10 principales deudores agrupados (cifras en miles de pesos) a junio 30 de 2023.

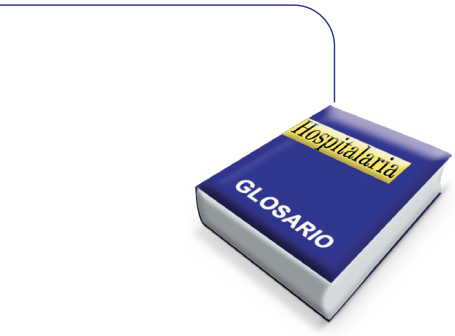
Entidad deudora	60 días y más (mora)	Total	Part % TOTAL Junio 2023	Part % TOTAL Diciembre 2022	DIFERENCIA % CARTERA MOROSA (JUN VS DIC)
1. NUEVA EPS (ambos regímenes)	1.124.977.375	2.614.897.177	43,0%	42,5%	0,5%
2. MEDIMAS EPS SAS (liquidada ambos regímenes)	717.812.407	717.812.407	100,0%	100,0%	0,0%
3. COOMEVA EPS (liquidada)	500.703.161	500.703.161	100,0%	100,0%	0,0%
4. EPS SANITAS	409.161.041	899.233.093	45,5%	40,4%	5,1%
5. CAFESALUD EPS (liquidada ambos regímenes)	356.884.266	356.884.266	100,0%	100,0%	0,0%
6. OPERADOR FIDUCIARIO (extinto) Y ADRES	305.731.307	398.097.879	76,8%	81,5%	-4,7%
7. COOSALUD (ambos regímenes)	292.152.474	643.659.730	45,4%	45,3%	0,1%
8. EMSSANAR ESS (intervención para administrar)	243.911.463	453.820.746	53,7%	43,5%	10,3%
9. ECOOPSOS ESS (liquidada)	190.963.920	190.963.920	100,0%	68,3%	31,7%
10. FAMISANAR EPS	182.530.422	488.359.316	37,4%	42,5%	-5,1%
Total general	4.324.827.835	7.264.431.696	59,5%	57,6%	1,9%

Fuente: ACHC, información que reportaron 207 instituciones hospitalarias.

- En cuanto a los principales deudores del actual estudio de cartera hospitalaria, según el monto absoluto de la cartera mayor a 60 días a junio 30 de 2023, se destacan la *Nueva EPS (ambos regímenes),* la intervenida para liquidar *Medimás EPS SAS* (ambos regímenes), la intervenida para liquidar Coomeva EPS, la activa en operación *EPS Sanitas* y, en quinto lugar, la intervenida para liquidar *Cafesalud EPS (ambos regímenes),* como aquellas entidades que encabezan el *ranking* de las entidades que adeudan mayor valor absoluto de cartera considerada en mora (concentraciones de cartera morosa por encima del 43,0 % y deudas superiores a los dos billones de pesos en el caso de la *Nueva EPS*).

GLOSARIO NORMATIVO ACHC

*** Trascendente **Importante *Informativa



1. CONGRESO DE LA REPÚBLICA

*****Ley 2315 (12 de octubre).**

Por medio de la cual se establecen los lineamientos para la Política Pública en Prevención, Diagnóstico Temprano y Tratamiento Integral de la Endometriosis, para la promoción y sensibilización ante la enfermedad, y se dictan otras disposiciones.

Esta Ley tiene por objeto establecer los principios, contenidos y disposiciones de la Política Pública de prevención, acceso completo o detección, diagnóstico temprano, estudios, control, tratamiento y terapias necesarios, para el abordaje integral de lo endometriosis, y garantizar el derecho a la salud de las personas con diagnóstico o presunción de endometriosis, así como la concientización de la población.

En dicho marco, se reconoce la endometriosis como enfermedad crónica progresiva y debilitante; se crea el registro de pacientes paro evaluar y garantizar lo oportunidad en la atención a pacientes diagnosticados; se determina la ruta diagnóstica y de atención, al tiempo que se establece el Día Nacional de la Concientización y Prevención, entre otras medidas. El Ministerio de Salud y Protección Social, en el término de un (1) año contado a partir de la presente Ley, deberá formular, adoptar, dirigir, coordinar, ejecutar y evaluar la Política Pública para el abordaje integral de la endometriosis.

2. MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL

*****Resolución 2073 (11 de diciembre).**

Por la cual se adoptan los lineamientos técnicos y operativos del Programa Nacional de Prevención, Control y Eliminación de la Malaria, y se dictan otras disposiciones.

Mediante esta Resolución, se adoptan los lineamientos técnicos y operativos del Programa Nacional de Prevención, Control y Eliminación de la Malaria, la Guía de Práctica Clínica Diagnóstico y tratamiento de la malaria; además, modifica parcialmente la Resolución 2257 de 2011 y dicta otras disposiciones.

Dentro de las responsabilidades y participación de los agentes del Sistema de Salud les corresponde a los Prestadores de Servicios de Salud las siguientes acciones: garantizar la atención integral de todo paciente

diagnosticado con malaria, en el marco de su alcance y capacidades; cumplir con lo indicado en la guía de práctica clínica y/o en sus futuros ajustes para la atención integral, acorde con la evolución de la evidencia científica, para los pacientes con malaria; garantizar el diagnóstico de malaria en los pacientes febriles durante las primeras 48 horas posteriores al inicio de los síntomas y el inicio del tratamiento antimalárico de primera línea de acuerdo con la política nacional dentro de las primeras 24 horas después del diagnóstico positivo; garantizar la recolección y el procesamiento de muestras a aquellos pacientes donde se sospeche un caso de malaria, en el sitio de atención de servicios, conforme lo establece la Guía para la atención clínica integral del paciente con malaria, entre otras acciones.

****Resolución 1884 (21 de noviembre).**

Por la cual se determinan los criterios para la distribución y asignación de recursos a las entidades territoriales para la implementación y prestación de las medidas de atención dirigidas a mujeres víctimas de violencia, sus hijos e hijas y personas dependientes.

Para efectos de esta Resolución, se entenderán como recursos presupuestales para la implementación y prestación de las medidas de atención aquellos referidos en el numeral 4 del artículo 2.6.4.4.4 del Decreto 780 de 2016.

La Oficina de Promoción Social del Ministerio de Salud, como responsable de la administración técnica de los recursos para la implementación y prestación de las medidas de atención, verificará el cumplimiento de los criterios establecidos en esta Resolución para la asignación de los recursos presupuestales que se destinen a las entidades territoriales.

*****Resolución 1862 (15 de noviembre).**

Por la cual se modifica el artículo 1.° de la Resolución 986 de 2023, en virtud de la cual se establecieron los lineamientos para la aplicación de las vacunas contra la COVID-19, y se dictan otras disposiciones.

A través de esta Resolución, se establecen los lineamientos para la vacunación contra la COVID-19 contenidos en los siguientes anexos técnicos. Anexo 1: Lineamientos técnicos y operativos para la vacunación contra la COVID-19; Anexo 2: Consentimiento informado para la aplicación de la vacuna contra el SARSCoV-2/COVID-19; Anexo 3: Anexo técnico para la aplicación de la vacuna BNT162b2 Pfizer-BioNTech contra la COVID-19; Anexo 4: Anexo técnico para la aplicación de la vacuna Sinovac Life Scienses Co., denominada CoronaVac contra la COVID-19; Anexo 5: Anexo técnico para la aplicación de la vacuna Moderna ARNM, contra la COVID-19.

****Resolución 1798 (1 de noviembre).**

Por la cual se definen las condiciones generales para la operación del Sistema General de Riesgos Laborales en el Sistema de Afiliación Transaccional (SAT) para la afiliación obligatoria y voluntaria de trabajadores independientes.

Esta Resolución tiene por objeto fijar las condiciones generales para la operación del Sistema General de Riesgos Laborales en el Sistema de Afiliación Transaccional (SAT) y definir los lineamientos para la incorporación de información y su interoperabilidad con las entidades Administradoras de Riesgos Laborales (ARL), en relación con la afiliación y reporte de novedades de los trabajadores independientes-afiliados obligatorios y voluntarios al referido sistema, según lo contenido en el Anexo Técnico N.º 1 "Incorporación de Información de la Afiliación y Novedades de los Trabajadores Independientes al Sistema General de Riesgos Laborales en el SAT", y en el Anexo Técnico N.º 2 "Operación del Sistema General de Riesgos Laborales en el Sistema de Afiliación Transaccional-Afiliación y novedades de los trabajadores

independientes en el SGRL" , que hacen parte integral de dicha Resolución.

*****Resolución 1676 (12 de octubre).**

Por medio de la cual se modifican los numerales 3.2.2, 3.5 y 9.1.8 del Manual de Normas Técnicas, Administrativas y de Procedimientos para Bancos de Sangre adoptado mediante la Resolución 901 de 1996.

Con esta Resolución se modifican los numerales 3.2.2 y 3.5 del Capítulo 3 y el numeral 9.1.8 del *Manual de Normas Técnicas Administrativas y de Procedimientos para Bancos de Sangre*, adoptado mediante la Resolución 901 de 1996, y deroga la Resolución 3212 de 2018, con el propósito de eliminar las referencias a las categorías de hombres que tienen sexo con hombres (HSH) y población trans como factores, grupos, poblaciones o conductas de riesgo.

Así, se modifica el numeral 3.2.2. "Para proteger al receptor", que hace parte del numeral 3.2 "Requisitos para ser donante" del Capítulo 3 "Donantes de sangre" y el numeral 9.1.8 del numeral 9.1 "Plan de emergencia para el banco de sangre" del Capítulo 9 "El Banco de Sangre en casos de emergencia o calamidad pública" de dicho Manual.

****Resolución 1653 (10 de octubre).**

Por la cual se modifica el artículo 7 de la Resolución 2053 de 2019 en el sentido de incluir requisitos para solicitar concepto técnico de viabilidad de proyectos de inversión de adecuaciones en infraestructura física y en infraestructura móvil para prestación de servicios de salud.

En el marco del Modelo de Atención Predictivo, Preventivo y Resolutivo, y para el logro de mayor equidad en el acceso a los servicios de salud, el Ministerio de Salud busca eliminar barreras geográficas, económicas, sociales y culturales, en zonas donde solo se llega por vía marítima, fluvial, aérea o caminos veredales, para lo cual se requiere implementar alternativas de transporte que permitan llegar a dichos lugares; para tal fin, considera necesario incluir los requisitos para la presentación de proyectos de inversión para infraestructura móvil, por parte de las entidades territoriales y ESE.

****Resolución 1621 (4 de octubre).**

Por la cual se determinan los criterios de distribución y asignación de recursos a las entidades territoriales y a las Empresas Sociales del Estado (ESE), para la operación del Programa de Atención Psicosocial y Salud Integral a Víctimas del Conflicto Armado (PAPSIVI) en su componente de atención psicosocial.

Se entenderán como recursos presupuestales para la operación del PAPSIVI aquellos que la ADRES girará para financiar el programa establecido en el numeral 1 del artículo 2.6.4.4.4 del Decreto Único 780 de 2016, respecto del componente de Atención Psicosocial, así como aquellos provenientes de otras fuentes dispuestas por el Ministerio de Salud y Protección Social para tal fin.

Las Entidades Territoriales, para recibir recursos y operar el PAPSIVI en su componente de atención psicosocial, deberán contar con mínimo una ESE con servicio habilitado de medicina general y psicología, de acuerdo con la normatividad vigente. En caso de que la solicitante sea una ESE, deberá acreditar su habilitación como prestadora del servicio de medicina general y psicología, de conformidad con la normatividad vigente.

La Oficina de Promoción Social del Ministerio de Salud y Protección Social, como responsable del direccionamiento del PAPSIVI en el territorio nacional, mediante documento técnico realizará la evaluación de los criterios de ponderación para la asignación de los recursos presupuestales que se destinen a las entidades territoriales o sus ESE para la operación del programa.

****Resolución 1583 (03 de octubre).**

Por la cual se define el porcentaje de los rendimientos financieros de la cuenta maestra de recaudo de cotizaciones en salud, para entidades promotoras de salud y entidades adaptadas en salud para la vigencia 2023.

Esta Resolución fija en un setenta por ciento (70 %) el porcentaje de los rendimientos financieros de las cuentas maestras de recaudo de cotizaciones en salud, a apropiarse por las EPS y las entidades adaptadas en salud, durante la vigencia 2023, para financiar las actividades relacionadas con la gestión de cobro de cotizaciones, el manejo de la información sobre el pago de aportes y los servicios financieros asociados al recaudo.

Las EPS y entidades adaptadas en salud que se encuentren en proceso de liquidación y por el periodo que este se extienda, podrán apropiarse del veinte por ciento (20 %) de los rendimientos financieros de las cuentas maestras de recaudo de cotizaciones en salud.

3. SUPERINTENDENCIA NACIONAL DE SALUD

****Circular Externa 023151000000010-5 – 6 (22 de junio).**

Por la cual se modifican los términos para resolver los reclamos en salud establecidos en la circular externa 047 de 2007, modificada entre otras por la circular externa 008 de 2018, así como los anexos técnicos relacionados con reclamos en salud dispuestos en la circular externa 017 de 2020.

La Superintendencia Nacional de Salud, atendiendo a la necesidad de resolver de fondo las peticiones y reclamos de los usuarios con la inmediatez que la situación requiera y conforme a las características de calidad, oportunidad, continuidad e integralidad inherentes al derecho fundamental a la salud, replantea los plazos máximos establecidos para dar respuesta a las PQR que reciben las EPS y las IPS.

De esta manera, adopta las definiciones de *petición, queja, reclamo, reclamo de riesgo simple, de riesgo priorizado y reclamo de riesgo vital*. Se establecen los mecanismos, procesos y procedimientos que deben adoptar las EAPB y las IPS para resolver de manera objetiva, oportuna y eficiente las PQR de los usuarios. Se conceden 72 horas, 48 horas y hasta 24 horas para resolver dichas quejas según la clasificación de las definiciones. Se establece el reporte de las línea de atención y se sustituye el anexo GT005 sobre inventario de peticiones, quejas, reclamos y denuncias radicadas.

****Circular Externa 2023310010007065 – 6 (29 de marzo).**

Por la cual se imparten instrucciones para garantizar el cumplimiento del flujo de recursos, y se modifican el archivo tipo ft025 de la circular externa 014 de 2020 y el archivo tipo st010 de la circular externa 008 de 2018.

La Superintendencia Nacional de Salud, con el fin de generar las herramientas necesarias para la verificación del adecuado flujo de recursos entre los participantes del proceso de prestación de servicios de salud, el aumento de la UPC conforme a lo establecido en la Resolución 2809 de 2022 y el cumplimiento de la Circular Externa 0054 de 2022 expedidas por el Ministerio de Salud y Protección Social, imparte instrucciones a las EPS, regímenes exceptuados y especiales, las entidades territoriales, empresas de medicina prepagada e IPS públicas, privadas y mixtas, cuando celebren acuerdos de voluntades.

Así establece la obligatoriedad de publicar en la página Web de las EPS, a más tardar el 30 de abril de 2023, el registro del valor transferido a las IPS e informar el enlace dispuesto para su consulta antes de la fecha límite de publicación. Vencido dicho plazo, los IPS dentro de los 10 días siguientes, debían informar a la Supersalud si dicha

publicación correspondía a lo efectivamente pagado. El incumplimiento de estas instrucciones da lugar a las sanciones correspondientes.

****Resolución 2023310010007065 – 6 (10 de octubre).**

Por la cual se resuelve una solicitud de autorización previa de cambio en la composición de la propiedad y de reforma estatutaria presentada por ALIANZA MEDELLÍN ANTIOQUIA EPS S.A.S. "SAVIA SALUD EPS", identificada con NIT 900.604.350-0.

A través de esta Resolución, la Superintendencia Nacional de Salud autoriza la solicitud de aprobación de la reforma de los artículos 46, 48 y 51 de los estatutos sociales de Alianza Medellín Antioquia EPS, aprobados por la Asamblea General de Accionistas, que implica la composición de la propiedad y la reforma de sus estatutos sociales, producto de la capitalización que pretende realizar, por la suma de sesenta y tres mil ciento setenta y dos millones novecientos ochenta y un mil quinientos doce pesos m/cte. ($63.172.981.512), de los cuales treinta y seis mil novecientos cincuenta y seis millones cuatrocientos cuarenta y cuatro mil setecientos setenta pesos m/cte. ($36.956.444.770) equivalen al capital suscrito y pagado.

4. DIRECCIÓN DE IMPUESTO Y ADUANAS NACIONALES (DIAN)

*****Resolución 165 (1 de noviembre).**

Por la cual se desarrolla el sistema de facturación, los proveedores tecnológicos, se adopta la versión 1.9 del anexo técnico de factura electrónica de venta, se expide el anexo técnico 1.0 del documento equivalente electrónico, y se dictan otras disposiciones en materia del sistema de facturación.

Mediante esta Resolución, la DIAN requiere que los sujetos obligados a facturar, que vienen expidiendo documento equivalente, expidan, generen y transmitan el documento equivalente electrónico tiquete de máquina registradora con sistema POS a la DIAN, a partir de la fecha que se establezca en el calendario de implementación que se prescribe en dicha Resolución; por lo tanto, se definen y establecen las condiciones, los términos y los mecanismos técnicos y tecnológicos para la interoperabilidad, interacción, generación, numeración, transmisión, validación, expedición y entrega de este documento electrónico, el cual se integrará a los demás que componen el sistema de facturación, y que de igual forma deberá tener la interacción con inventarios, sistemas de pago, impuestos y contabilidad e información tributaria legalmente exigida.

Por lo anterior, es necesario desarrollar los aspectos técnicos y tecnológicos que se consideren necesarios para la adecuada implementación del sistema de facturación, adoptando la versión 1.9 del Anexo técnico de factura electrónica de venta, y el documento equivalente electrónico expidiendo el Anexo técnico del documento equivalente electrónico versión 1.0, y expedir otras disposiciones en materia del sistema de facturación.

Los Nogales Clínica | 10 años | efr

Atención Integral en Oncología

Pensando siempre en tus necesidades y las de tu familia

Servicios diagnósticos

- Laboratorio Clínico Especializado
- Patología
- Imágenes Diagnósticas

Tratamiento, Rehabilitación y Complementarios

- Quimioterapia
- Radioterapia
- Medicina Nuclear
- Trasplante de Progenitores Hematopoyéticos
- Servicio Farmacéutico
- Nutrición
- Psicología
- Trabajo Social

Consulta, Cirugía y Especialidades Oncológicas

- Oncología Clínica
- Hemato Oncología
- Dermato Oncología
- Ginecología Oncológica
- Ortopedia Oncológica
- Urología Oncológica
- Mastología
- Coloproctología
- Dolor y Cuidados Paliativos
- Hematología
- Neurocirugía
- Cirugía Gastrointestinal
- Cirugía Hepatobiliar
- Cirugía Cabeza y Cuello
- Cirugía Tórax
- Cirugía Plástica Oncológica
- Cirugía de Mama y Tumores Tejidos Blandos
- Entre otras.

PET - CT
(Tomógrafo por Emisión de Positrones)

Próximamente

¡Síguenos en nuestras redes!
@losnogalesclinica

www.clinicanogales.com

Salud Total EPS-S

CAMBIO DEL LENGUAJE AUTORIZADOR – IPS

A partir del 24 de octubre del 2023, cambiarán los estados autorizado y preautorizado en el sistema autorizador, pasamos a un proceso que nos permite medir eficazmente la demanda y la prestación efectiva de servicios, de esta manera nuestro proceso será así:

Términos:

1. ORDENAMIENTO MÉDICO:

Orden o fórmula médica que el tratante le prescribe a su paciente.

2. DIRECCIONAMIENTO:

Posterior a un ordenamiento médico la EPS procede a direccionar al protegido a una institución prestadora de servicios para que le sea entregada la tecnología en salud o prestado efectivamente el servicio ordenado por el tratante.

3. ENTREGADO:

Prestado el servicio por parte de la IPS, esta procede a ingresar a la Oficina Virtual de la EPS y realiza la actividad de marcar el direccionamiento como entregado, de esta manera la transacción cambia de estado a entregado y la EPS puede garantizar que se le prestó a su afiliado el servicio que ha demandado, la plataforma le devuelve como respuesta un número el cual será el que la IPS utiliza para realizar la facturación a la EPS.

4. N° DP:

Número asignado por la Oficina Virtual cuando la IPS cambia el estado de direccionado a entregado, este número es el que se deberá adjuntar a la facturación para la EPS.

» **Tener presente:** La implementación de este cambio se llevará a cabo de manera escalonada, si un protegido tiene vouchers con el lenguaje actual (Autorizaciones) debe ser atendido y no solicitar el cambio. Estos serán válidos tanto para la atención, como para facturación de la cuenta.