REPÚBLICA DE COLOMBIA

MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL

RESOLUCIÓN NÚMERO DE 2025

( )

Por medio de la cual se crea, implementa y adopta el Equipo de Respuesta a Incidentes de Seguridad Informática del Sector Salud y Protección Social CSIRT Salud - y se dictan otras disposiciones.

EL MINISTRO DE SALUD Y PROTECCIÓN SOCIAL

En ejercicio de sus facultades legales, en especial las conferidas por los artículos 112 de la Ley 1438 de 2011, 19 de la Ley 1751 de 2015, 246 de la Ley 1955 de 2019, 3 y 4 de la Ley 2015 de 2020, y

CONSIDERANDO

Que, mediante los artículos 1.1.1.1 del Decreto 780 de 2016, "*Por medio del cual se expide el Decreto Único Reglamentario del Sector Salud y Protección Social",* se establece al Ministerio de Salud y Protección Social como entidad cabeza del sector Administrativo de Salud y Protección Social y seguidamente, el artículo 1.2.1.1 de la misma disposición normativa define las Entidades Adscritas a dicho Ministerio.

Que, el Decreto 338 de 2022 *"Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"*, nombra en su numeral 7 del artículo 2.2.21.1.3.5. "Conformación del Comité Nacional de Seguridad Digital" al Ministerio de salud y Protección Social como miembro del Comité Nacional de Seguridad Digital y establece como funciones el articular el desarrollo de políticas y capacidades de seguridad digital para reducir el cibercrimen y el ciberdelito.

Que, la Resolución 500 de 2021, *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"* en su artículo 2°, obliga a las Entidades que hacen parte de la Integración de la Administración Pública a implementar el Modelo de Seguridad y Privacidad de la Información, y el artículo 9° establece que los sujetos obligados, deben establecer procedimientos de gestión de incidentes de seguridad de la información comunicándolos al CSIRT Gobierno para determinar planes de mejoramiento y cumplimiento.

Que, el Decreto 1078 de 2015, establece la estructura del sector de Tecnologías de la Información, incluyendo al Ministerio de Salud y Protección Social como integrante del Comité Nacional de Seguridad Digital, entidad responsable de vigilancia y control y garante de las redes de comunicaciones del Sistema Nacional de Telecomunicaciones de Emergencia.

Que, mediante los CONPES 3701 DE 2011 y 3854 de 2016, se constituyeron los primeros esfuerzos estratégicos de Colombia en materia de ciberseguridad y ciberdefensa.

El CONPES 3701 estableció los lineamientos iniciales para la creación de capacidades nacionales frente a amenazas en el ciberespacio, priorizando la conformación del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) y la articulación institucional básica. Posteriormente, el CONPES 3854 profundizó en estos lineamientos y definió una Política Nacional de Seguridad Digital más estructurada, orientada a fortalecer la confianza en el entorno digital, proteger infraestructuras críticas y promover una cultura de gestión del riesgo cibernético, integrando al sector privado, la academia y la ciudadanía en una estrategia nacional más amplia y coordinada.

Que, mediante el CONPES 3995 de 2020, se estableció la Política Nacional de Confianza y Seguridad Digital en Colombia, con el objetivo de fortalecer la confianza en el entorno digital mediante la mejora de la seguridad digital. Esta política busca que ciudadanos, entidades gubernamentales y empresas comprendan y gestionen los riesgos digitales, promoviendo una cultura de responsabilidad compartida. Sus pilares incluyen la promoción de una cultura de seguridad digital, la actualización del marco de gobernanza, la gestión integral de riesgos, la protección de infraestructuras críticas y la mejora de la capacidad de respuesta ante incidentes cibernéticos. Además, se enfatiza la adopción de tecnologías emergentes y la colaboración entre sectores público y privado para enfrentar los desafíos de la Cuarta Revolución Industrial

Que, en virtud del objetivo específico OE 1 del CONPES 3995 de 2020, titulado "*Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país"*, se asignó al Ministerio de Salud y Protección Social, como entidad cabeza del sector, al Departamento Nacional de Planeación a través de la Dirección de Estudios Económicos con apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones, al Archivo General de la Nación, y las demás autoridades rectoras del Sistema de la Seguridad Social Integral – SSSI, una acción con el objeto de diseñar, estructurar y presentar el proyecto de implementación del Equipo de Respuesta ante Incidentes de Seguridad en inglés Computer Security Incident Response Team del Sector de la Seguridad Social Integral.

Que, por medio de la Resolución 2486 de 2024, del Ministerio de salud y Protección Social, se crea el Grupo de Seguridad de la Información e Innovación, asignándole funciones para la generación y apropiación de conocimientos basados en la cooperación intersectorial, mejores prácticas y lecciones aprendidas en materia del Sistema de Gestión de Seguridad y Privacidad de la Información, y apoyar las estrategias de ciberseguridad nacional de acuerdo con los lineamientos impartidos por la Coordinación Nacional de Seguridad Digital.

Que, mediante licitación pública MSPS-LP-004-2024, adelantada, se tramitó el proceso de contratación cuyo objeto fue "PRESTAR LOS SERVICIOS DE DISEÑO Y OPERACIÓN DE UN EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DIGITAL - CSIRT SECTORIAL, SUSCRIPCIÓN A SERVICIOS ESPECIALIZADOS, HERRAMIENTAS Y OTROS SERVICIOS CONEXOS PARA EL SECTOR SALUD Y PROTECCIÓN SOCIAL".

Que, mediante Resolución No. 2173 del 7 de noviembre de 2024, fue adjudicado dicho proceso contractual, a la empresa COMPAÑÍA DE INGENIEROS DE SISTEMAS ASOCIADOS – COINSA S.A.S.

Que, el día 28 de noviembre de 2024, se perfeccionó el Contrato 1734 de 2024, cuya acta de inicio es de misma fecha, contrato que se encuentra actualmente en ejecución, hasta el 30 de junio de 2026.

Que, conforme al contrato suscrito, el contratista ejecuta las actividades necesarias para habilitar un Equipo de Respuesta a Incidentes de Seguridad Informática del Sector Salud y Protección Social - CSIRT Salud.

Que, para efecto de conseguir el reconocimiento institucional, tanto interno como externo (v.gr. otros equipos de respuesta nacionales e internacionales y redes de intercambio de información, como la red CSIRT Américas), se precisa la formalización de la instancia "CSIRT Salud", como Equipo de Respuesta a Incidentes de Seguridad Informática del Sector Salud y Protección Social - CSIRT Salud, encargado de identificar, analizar, contener y dar respuesta a incidentes de seguridad de la información que puedan llegar a presentarse sobre las Entidades del Sector Salud.

Que, de conformidad con lo expuesto, resulta pertinente y necesario crear, implementar y adoptar un Equipo de Respuesta a Incidentes de Seguridad Informática del Sector Salud y Protección Social – CSIRT Salud.

En mérito de lo anteriormente expuesto,

RESUELVE

Artículo 1. Objeto. Crear, implementar y adoptar el Equipo de Respuesta a Incidentes de Seguridad Informática del Sector Salud y Protección Social – CSIRT, correspondiente al sector Salud.

Parágrafo primero: La operación actual del CSIRT Salud, está soportada en los recursos asignados por este Ministerio en el marco de la ejecución del contrato vigente.

Parágrafo segundo: La continuidad de la operación del CSIRT Salud en fases posteriores, se ejecutará mediante la contratación de un operador o de manera directa por parte del Ministerio de Salud y Protección Social, siempre y cuando pueda contar con los recursos financieros, técnicos y humanos requeridos para el efecto.

Artículo 2. *Ámbito de aplicación*. Las disposiciones contenidas en la presente Resolución serán aplicables a:

1. Ministerio de Salud y Protección Social
2. Instituto Nacional de Salud
3. Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima)
4. Fondo de Pasivo Social Ferrocarriles Nacionales de Colombia
5. Fondo de Previsión Social del Congreso de la República
6. Centro Dermatológico Federico Lleras Acosta
7. Instituto Nacional de Cancerología
8. Sanatorio de Agua de Dios
9. Sanatorio de Contratación
10. Superintendencia Nacional de Salud
11. Administradora de los Recursos del Sistema General de Seguridad Social en Salud
12. Instituto de Evaluación Tecnológica en Salud

El Equipo de Respuesta a Incidentes de Seguridad Informática – CSIRT Salud, cobijará los incidentes de seguridad de la información que puedan llegar a presentarse sobre los activos de información que cada una de las Entidades mencionadas en el presente artículo, determinen como críticos y priorizados.

Artículo 3. *Definiciones:* Para el entendimiento sobre la creación, implementación y adopción del Equipo de Respuesta a Incidentes de Seguridad Informática – CSIRT Salud, se presentan el siguiente glosario normativo:

- **Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Ciberdefensa:** Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

- **Cibernética:** Ciencia de los sistemas de control y comunicación basados en retroalimentación, soportados o impulsados por la computación, particularmente en su relación con los seres vivos y el ser humano.

- **Ciberdelito / Delito Cibernético:** Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito.

- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.

- **CSIRT:** Equipo de Respuesta ante incidentes de seguridad (en inglés, *Computer Security Incident Response Team*).

- **Impacto:** El costo para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros p.ej., pérdida de reputación, implicaciones legales.

- **Incidente de Seguridad:** Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

- **Sector Salud:** Para la presente resolución, hace referencia a las entidades que hacen parte del ámbito de aplicación del presente documento.

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Artículo 4. *Objetivo del CSIRT Salud*: El propósito del CSIRT Salud es fortalecer la postura de seguridad digital del ecosistema del sector salud y protección social en Colombia, mediante la prevención, detección, análisis y respuesta efectiva a incidentes de ciberseguridad, bajo el ámbito descrito en el artículo 2° del presente artículo.

Artículo 5. *Funciones del CSIRT Salud:* El marco operativo del CSIRT Salud se basará en las relaciones de áreas de servicios de ciberseguridad como lo son el monitoreo y detección de eventos, la gestión de incidentes de seguridad de la información y la articulación con otras instancias de seguridad digital en lo pertinente, la gestión de vulnerabilidades técnicas y la transferencia de conocimiento a las Entidades del sector salud, entre otros.

Adicional a las funciones principales, el CSIRT Salud deberá realizar seguimiento a los planes de mejoramiento y recomendaciones de seguridad digital a las Entidades del sector salud y asistirlas técnicamente para que sean llevadas a cabo las implementaciones recomendadas.

Como servicio de generación de valor, el CSIRT Salud dispondrá bajo modalidad de consumo bolsa de horas, provisión de servicios especializado tales como análisis forense en ciberseguridad, los cuales deberán ser solicitados por las entidades al Ministerio de Salud y Protección Social, como coordinador y supervisor del tercero contratado para la operación del CSIRT Salud.

La solicitud de servicios con cargo a la bolsa de horas, deberá elevarse por escrito y debidamente justificada por parte del contacto líder de seguridad de la información de la entidad adscrita que así lo requiera, a los correos electrónicos seguridadyprotecciondedatos@minsalud.gov.co y csirtsalud@minsalud.gov.co, la cual será objeto de estimación por parte del operador, y, posteriormente, sometida a revisión y aprobación -en caso de ser pertinente- por parte del Ministerio de Salud y Protección Social a través del supervisor contractual.

Artículo 6. *Estructura de roles y responsabilidades:* El operador contratado bajo la coordinación y supervisión del Ministerio de Salud y Protección Social, se apoyará en una estructura de roles, responsabilidades y autoridades del CSIRT Salud, identificando los roles pertinentes para la adecuada operación del Equipo de Respuesta a Incidentes de Seguridad Informática y el personal de apoyo que sea requerido en lo referente a gestión administrativa, gestión de comunicaciones y conceptos jurídicos, entre otros.

El tercero contratado operará bajo los lineamientos y canales de comunicación -acordados con el Supervisor- para interactuar con las Entidades del sector salud. Igualmente, será responsabilidad de cada una de las Entidades del sector salud, designar el(los) profesional(es) de enlace responsable(s), de la gestión, comunicación e interacción entre el CSIRT Salud y la entidad.

Artículo 7. *Intercambio de información:* No obstante, no se prevé que el operador tenga acceso directo alguno a bases de datos, repositorios digitales u otras fuentes directas de información, en todo caso, se adoptará un protocolo para el intercambio de información de tipo sensible, privada, publica confidencial y publica reservada, de forma que se cumpla con las disposiciones legales vigentes. Para el efecto, el operador y cada entidad del sector salud, suscribirán acuerdos de confidencialidad y no divulgación de la información, por medio del cual se establecerán los lineamientos que garanticen el adecuado tratamiento de la información, asegurando la confidencialidad, disponibilidad y la integridad de la información.

Artículo 8. *Coordinación Interinstitucional y colaboración:* Las Entidades Adscritas y Vinculadas, relacionadas en el artículo 2° de la presente resolución, deberán suministrar la información requerida para facilitar la prevención, análisis y respuesta de incidentes de seguridad de la información, garantizando que desde el CSIRT Salud se pueda llevar a cabo monitoreo y detección de eventos de seguridad sobre los activos críticos determinados por las entidades.

Es responsabilidad del operador, bajo supervisión del Ministerio de Salud y Protección Social, establecer el protocolo de comunicación e intercambio de información entre el CSIRT Salud y otros CSIRT sectoriales afines, CSIRT Gobierno y demás instancias que se considere pertinentes para facilitar la centralización de la información proveniente de otras instancias y facilitar así el desarrollo de capacidades tales como, inteligencia de amenazas. Bajo este mismo protocolo se establecerán los detalles operativos para facilitar el intercambio de información desde el CSIRT Salud hacia otras instancias. Este protocolo deberá adoptar los estándares y mejores prácticas aplicables.

Los protocolos mencionados anteriormente, deberán ser publicados mediante el portal web del CSIRT del sector salud y dados a conocer a las Entidades Adscritas y Vinculadas al Ministerio de Salud y Protección Social, bajo responsabilidad del operador contratado.

Artículo 9. *Responsabilidades de las Entidades Adscritas y Vinculadas:* Para la adecuada implementación y adopción del CSIRT Salud, son responsabilidades de las Entidades Adscritas y Vinculadas, las siguientes:

- Facilitar la implementación y puesta en operación del CSIRT Salud, mediante la designación de puntos de contacto, la provisión de espacios físicos y lógicos, y la disponibilidad de medios tecnológicos e información requerida. Asimismo, asegurar el cumplimiento de los requisitos técnicos necesarios para el despliegue de la infraestructura, incluyendo conectividad, servidores, software y demás elementos que serán dispuestos por el CSIRT Salud.

- Efectuar la gestión de incidentes de seguridad en articulación con el CSIRT Salud, de conformidad con el artículo 11 de la presente resolución.

- Participar en las actividades de fortalecimiento de capacidades en seguridad digital que se programen por parte del CSIRT Salud, incluidas capacitaciones, ejercicios de simulación y planes de mejoramiento que se programen.

- Adoptar las recomendaciones, ejecutar los planes de acción / remediación derivados de los análisis de vulnerabilidades y compartir retroalimentación con el CSIRT Salud sobre su progreso.

- Colaborar y apoyar activamente el desarrollo de las demás actividades y acciones propias de la implementación y adopción del CSIRT Salud, en lo referente a su entidad.

Artículo 10. *Responsabilidades en cuanto a la Gestión de Incidentes de Seguridad:* El CSIRT Salud determinará y dará a conocer -a través de los canales formalizados a los profesionales de enlace de las entidades- el procedimiento de gestión de incidentes de seguridad, para poder realizar tratamiento, investigación y gestión de incidentes de seguridad de la información que se presenten frente a los activos críticos de las entidades del sector.

Para efecto de la Gestión de Incidentes de Seguridad, el CSIRT Salud será responsable de:

- Gestionar los incidentes de seguridad de la información, de acuerdo con el procedimiento establecido, detallando las actividades desarrolladas en la gestión de cada uno de estos.

- Analizar e investigar los incidentes de seguridad de la información determinando causa raíz y planes de mejoramiento, incluyendo su seguimiento y cumplimiento.

- Reportar la identificación, el análisis, la respuesta y los planes de mejora sobre los incidentes de seguridad de la información catalogados como críticos, ante el Ministerio de Salud y Protección Social y CSIRT Gobierno, y otras instancias según corresponda.

Por su parte, las Entidades Adscritas y Vinculadas serán responsables de:

- Designar un responsable para la gestión de incidentes de seguridad de la información a nivel de la entidad.

- Reportar los incidentes de seguridad de la información ante el CSIRT Salud y colaborar con la gestión y respuesta ante el incidente materializado conforme al protocolo operativo que se establezca.

Artículo 11. Informes de Actividades*:* En desarrollo de su operación, el CSIRT Salud generará y emitirá comunicados, informes y reportes de la siguiente manera:

- Informes de gestión administración de las plataformas de ciberseguridad implementadas para el cumplimiento de las funciones descritas en el artículo 6° de la presente resolución, ante el Ministerio de Salud y Protección Social, de manera mensual.

- Informes de análisis de vulnerabilidades técnicas sobre los activos críticos de las entidades del sector salud, a cada una de estas y al Ministerio de Salud y Protección Social, de manera mensual.

- Informes de estadísticas y métricas de desempeño del CSIRT Salud y nivel de madurez de la ciberseguridad del sector, ante el Ministerio de Salud y Protección Social, de manera mensual.

- Boletines de ciberseguridad, comunicados a las entidades del sector salud, de acuerdo con la necesidad del servicio.

- Alertas de ciberseguridad, comunicadas a las entidades del sector salud, una vez se cuente con el conocimiento sobre la vulnerabilidad y amenazas relacionadas.

Artículo 12. *Vigencia:* La presente resolución rige a partir de la fecha de su publicación y surte efectos a partir de la fecha de expedición.

COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá D.C. a los

GUILLERMO ALFONSO JARAMILLO MARTÍNEZ
Ministro de Salud y Protección Social

Continuación de la resolución *“Por medio de la cual se crea, implementa y adopta el Equipo de Respuesta a Incidentes de Seguridad Informática – CSIRT Salud en Colombia y se dictan sus disposiciones”*

AprobóOficina de Tecnología de la Información y la Comunicación

Vo. Bo.: Rodolfo Enrique Salas Figueroa- Director Jurìdico (E).