Instituto Nacional de Servicios Sociales para Jubilados y Pensionados
AÑO DE LA RECONSTRUCCIÓN DE LA NACIÓN ARGENTINA

Resolución

Número: RESOL-2025-936-INSSJP-DE#INSSJP

CIUDAD DE BUENOS AIRES
Martes 6 de Mayo de 2025

Referencia: EX-2025-44346289- -INSSJP-GSIYAD#INSSJP - RESOLUCIÒN - ANALISIS E INTERCAMBIO DE SEGURIDAD DE LA INFORMACIÓN

VISTO el EX-2025-44346289- -INSSJP-GSIYAD#INSSJP, la Ley 19.032 y sus modificatorias, la Ley 25.615, el Decreto N° 02/04, la Resolución N° RESOL-2024-3194-INSSJP-DE#INSSJP, la Disposición N° DI-2024-1-INSSJP-JGA#INSSJP, la Resolución N° RESOL-2024-810-INSSJP-DE#INSSJP, la Resolución N° RESOL-2025-191-INSSJP-DE#INSSJP y

CONSIDERANDO:

Que el Artículo 1° de la Ley N° 19.032, de conformidad con las modificaciones introducidas por su similar N° 25.615, asigno al INSTITUTO NACIONAL DE SERVICIOS SOCIALES para JUBILADOS y PENSIONADOS (INSSJP), el carácter de persona jurídica de derecho público no estatal, con individualidad financiera y administrativa.

Que en virtud de las competencias atribuidas al Directorio Ejecutivo Nacional del INSTITUTO NACIONAL DE SERVICIOS SOCIALES para JUBILADOS y PENSIONADOS (INSSJP), en especial lo dispuesto por el Artículo 6° de la Ley N° 19.032 y modificaciones introducidas por su similar N° 25.615, y el Artículo 3° del Decreto N° 02/04-PEN, el Órgano Ejecutivo posee plenas facultades para dictar las normas necesarias para la adecuada administración y funcionamiento del organismo.

Que, de acuerdo a las mencionadas leyes, el Instituto tiene como objeto otorgar - por sí o por terceros - a las personas jubiladas y pensionadas del régimen nacional de previsión y del Sistema Integrado de Jubilaciones y Pensiones y a su grupo familiar primario, las prestaciones sanitarias y sociales, integrales, integradas y equitativas, tendientes a la promoción, prevención, protección, recuperación y rehabilitación de la salud.

Que, a fin de cumplir dichos objetivos, la Ley Nº 25.615 asignó al Directorio Ejecutivo Nacional del INSTITUTO NACIONAL DE SERVICIOS SOCIALES para JUBILADOS y PENSIONADOS (INSSJP) las competencias para dictar las normas necesarias para la adecuada administración y funcionamiento del organismo.

Que, el artículo 3° del Decreto N° 02/04, asigna al Director Ejecutivo del Órgano Ejecutivo de Gobierno las facultades de gobierno y administración previstas por la Ley N° 19.032 y sus modificatorias en favor del Directorio Ejecutivo Nacional.

Que, en la actualidad, la seguridad de la información, y por inclusión la ciberseguridad, en el sector sanitario y previsional son desafíos constantes para cualquier organización, observándose que durante los años 2023, 2024 y los primeros meses del año 2025, las amenazas son cada vez más sofisticadas y la tecnología avanza rápidamente hacia ataques más fortalecidos por la falta de elementos claves como la prevención, el análisis de amenazas y la concientización así como por la inteligencia artificial (IA) utilizada para ayudar a los atacantes, por el incremento de actividad de los grupos de ransomware, por las filtraciones y la llegada del desafío post-cuántico tanto para cifrado de comunicaciones como de datos, por lo que es crucial implementar estrategias efectivas para proteger los activos digitales tanto de usuarios, afiliados, pacientes, prestadores y todo otro dato personal y sensible que pueda impactar en las prestaciones, su población objeto y su cadena de suministro.

Que, como referencia, es necesario considerar que se prevé que los daños causados por los delitos cibernéticos a nivel mundial se estimen en aproximadamente 10,5 billones de dólares anuales para el año 2025 (acorde Cybersecurity Ventures). Dentro de ese número podemos destacar que en el año 2023 se detectaron 30 millones de nuevas muestras de malware (acorde AV-Test) y que en USA más de 141 hospitales, 108 distritos escolares y 95 entidades gubernamentales se vieron afectados por ransomware en 2023 (acorde Emsisoft). Asimismo, el Global Threat Report 2025 (CrowdStrike) identifica a más de 27 actores de amenazas identificados y el reporte Annual Threat Report (Health-ISAC) informa que durante 2024 registraron 458 incidentes de ransomware con foco en el sector sanitario donde los grupos más activos fueron Lockbit, INC Ransomware, Ransum Hub, BianLian y Qilin, adicionando que la Cybersecurity and Infrastructure Security Agency (CISA) emitió 11 avisos sobre dispositivos médicos detallando que las vulnerabilidades más comunes identificadas en estos Industrial Control Systems Medical Advisories (ICSMA) fueron debilidades de software CWE-502 y CWE-125, con CVE asignados con puntuaciones CVSS de entre 4,8 y 10.

El informe "*Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care 2024*" (acorde Proofpoint y el Instituto Ponemon, resultados de su tercera encuesta anual sobre ciberseguridad en la atención médica en Estados Unidos de América) indican que el 88% de las organizaciones encuestadas experimentó al menos un ciberataque en el último año, en la cual un 69% reporóo interrupciones en la atención al paciente, el 100% de las organizaciones (de los 653 profesionales del sector salud consultados) han sufrido al menos un incidente donde información sensible de salud ha sido perdida o robada, y adicionalmente, el 68% de los encuestados contaron que sus organizaciones sufrieron un ataque contra sus cadenas de suministro (laboratorios, proveedores, etc.), de los cuales un 82% dijo que interrumpió la atención al paciente, siendo un 77% más que en el año 2023.

Que durante el año 2024 el U.S. Department of Health & Human Services (Estados Unidos de América), publicó una lista de las brechas de información médica protegida (brechas que afecten a 500 o más personas), cuyo resultado arroja que más de 584 organizaciones de salud reportaron haber sufrido algún tipo de ataque informático que totaliza la exposición de datos personales, sensibles y otros, de más de 180 millones de personas, que considerando los datos publicados por el Population Clock del U.S. Census Bureau's, representa aproximadamente al 52.7% de la población de ese país .

Que a esta problemática podemos añadir la existencia de un panorama en el que se observa que el 86,6 % de las organizaciones se enfrentan a una escasez de recursos humanos con habilidades en seguridad informática, frente al 84,1 % en 2022 mostrando el crecimiento de la demanda (acorde Imperva 2023).

Que, el sector sanitario se encuentra ante el desafío de lograr disminuir la cantidad de incidentes de seguridad de la información por medios digitales pero que hace falta fortalecer las acciones, teniendo en cuenta la información de dominio público donde surge que en el último semestre ya se cuentan con más de 9 incidentes de seguridad cibernética que afectan a más de 20 hospitales, obras sociales y laboratorios, marcando una tendencia ascendiente a los años anteriores.

Que la importancia de abordar la problemática sectorial, incluyendo todos los aspectos de la seguridad de la información en su entorno digital, radica en aumentar el conocimiento de las amenazas para incrementar la capacidad de proteger los datos sensibles de manera coordinada, mantener la confianza del ecosistema de salud, implementar detecciones tempranas, recabar información para prevenir amenazas, crear resiliencia y fortalecer el cumplimiento de las normativas legales.

Que en este plano cada vez más digitalizado, una brecha de seguridad puede tener consecuencias devastadoras, desde la sustracción de datos sensibles, pérdidas financieras, riesgo en prescripciones y análisis de laboratorio, cese de actividades y daño a la reputación de las organizaciones, entre otros aspectos. Por ello es esencial que se adopte un enfoque proactivo para detectar y mitigar amenazas antes de que se conviertan en incidentes graves.

Que, por los grandes y variados volúmenes de información a proteger, la cantidad, velocidad y complejidad de los intentos de vulneración así como ataques de ransomware y exfiltraciones exitosas como las producidas en los últimos meses, a hospitales, laboratorios y obras sociales a nivel internacional, que totalizan cientos de millones de datos expuestos y daños financieros a las organizaciones, debe tomarse una acción proactiva para prevenir, analizar e intercambiar información e amenazas cibernéticas en el sector sanitario donde los datos personales y datos sensibles de nuestros afiliados y afiliadas circulan y son utilizados para los fines de su atención, así como de toda la cadena de suministro que pudiera afectar el normal desenvolvimiento del INSSJP hacia sus afiliados y afiliadas.

Que para lograr un análisis de amenazas de seguridad de la información de manera integral y proponer acciones para el abordaje de la problemática es también importante analizar nuevos escenarios de cifrado de comunicaciones y datos con las tecnologías más avanzadas, así como, utilizar la IA como parte integrante de las herramientas que ayude a responder frente a escenarios conocidos al automatizar tareas repetitivas, al mejorar el análisis de datos, al ayudar a monitorear grandes volúmenes de datos en tiempo real detectando patrones sospechosos que podrían indicar una amenaza, personalizar el abordaje de la seguridad de la información en formato digital basándose en el comportamiento y los patrones específicos de cada organización y permitiendo que el recurso humano (el más escaso) se centre en las tareas que ameriten su intervención.

Que, ya en el año 1998 a través Directiva de Decisión Presidencial-63 (PDD-63) de los Estados Unidos de América, se fomentó la creación de los centros de intercambio y análisis de información (Information Sharing and Analysis Center, ISAC por su sigla en inglés) de los diferentes sectores y en la actualidad cuentan con más de veinte (20) ISAC sectoriales donde están incluidos los sectores de salud, transporte, financiero, entre otros.

Que los ISAC sectoriales de EE.UU., como en diferentes naciones, son creados para fortalecer la resiliencia cibernética y sirviendo como ejemplo el Health-ISAC (Health Information Sharing and Analysis Center), siendo su objetivo principal el facilitar el intercambio de información sobre ciberamenazas, vulnerabilidades y mejores prácticas entre sus miembros, que incluyen hospitales, proveedores de servicios de salud, empresas de tecnología médica y otras organizaciones relacionadas con la salud.

Que el FIRST (*Forum of Incident Response and Security Teams*) organización mundial líder que tiene como objetivo fomentar la cooperación y la coordinación en la prevención de incidentes, estimular la reacción rápida ante

incidentes y promover el intercambio de información entre sus miembros y la comunidad en general, quien cuenta con más de 700 miembros, distribuidos en África, América, Asia, Europa y Oceanía, describe entre los diferentes tipos de equipos que desempeñan diversas funciones en el ámbito de la seguridad de la información para prevenir, detectar, analizar y mitigar incidentes, amenazas o vulnerabilidades, a los Centros de Análisis e Intercambio de Información (ISAC).

Que también se han adoptado medidas en la Unión Europea (UE) y puede verse reflejada la importancia de los ISAC en la Directiva NIS2, sumado a la propuesta del 15 de enero de 2024, donde la Comisión Europea puso en marcha el "Plan de acción europeo para reforzar la ciberseguridad de los hospitales y los prestadores de asistencia sanitaria" como parte de las orientaciones políticas del mandato de la Comisión para 2024-2029, centrado en la mejora de la detección de amenazas, la preparación, el intercambio de información y la respuesta a las crisis de ciberseguridad en el sector sanitario, apoyando y fortaleciendo el European Health ISAC, e incentiva a los países miembros a crear sus propios ISAC del sector Salud. Asimismo, señala que se debe alentar a los ISAC a reunir a los profesionales sanitarios con los fabricantes para fomentar una comprensión conjunta de las amenazas a la ciberseguridad, incluso en la cadena de suministro, y facilitar un diálogo sobre el diseño seguro de productos que realmente tengan en cuenta las realidades de implementación sobre el terreno.

Que debemos mencionar que, en el cuarto trimestre de 2023, el INSSJP fue objeto de un ataque de ransomware del grupo criminal autodenominado RHYSIDA causando exposición de datos un cese de operaciones con altos costos de recupero de vuelta a la operación.

Que, en el contexto previamente mencionado, el INSSJP sumó a su estructura la GERENCIA DE SEGURIDAD DE LA INFORMACIÓN Y ACTIVOS DIGITALES (GSIYAD) con los departamentos específicos de datos personales y de procesos (RESOL-2025-191-INSSJP), que posibilitan el desarrollo, continuidad y mejora de las políticas en la materia, y resultado de esto se diseñó y puso en ejecución el PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (DI-2024-1-INSSJP-JGA#INSSJP), el COMITÉ DE SEGUIMIENTO Y SEGURIDAD DE LA INFORMACIÓN-CSSI (RESOL-2024-810-INSSJP-DE#INSSJP), la POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (RESOL-2024-3194-INSSJP-DE#INSSJP) basada en el estándar internacional ISO 27001, así como los más de 28 procedimientos aprobados, acompañando esta estrategia de fortalecimiento de la seguridad de la información con cinco (5) cursos en línea en su plataforma virtual, más de quince (15) talleres prácticos presenciales y un (1) simulacro para la formación y comprensión necesaria de cada acción y medida tendiente a hacer proactiva y resiliente a la organización.

Que, a nivel de infraestructura tecnológica se vienen realizando inversiones en cambios en plataformas y sistemas para proteger las sedes centrales del INSSJP y en todo el territorio, pero que ninguna acción por si sola va a garantizar el cese de los ataques e incidentes de seguridad y que es necesario contar con toda la información posible para prevenirlos.

Que, ante el contexto planteado, el INSSJP toma la iniciativa de fortalecer sus acciones de protección de los datos y la seguridad de la información en el ámbito del ciberespacio, integrando la mayor cantidad de fuentes de información de amenazas y vulnerabilidades, permitiendo analizar los patrones de los ataques, reconocer los intentos de vulneración, detectar posibles nuevas amenazas y filtraciones permitiendo intercambiar los hallazgos con las organizaciones parte de la cadena de suministro y donde se procesen, almacenen o transiten datos de los afiliados y afiliadas.

Que deviene necesario en este marco crear el CENTRO DE ANALISIS E INTERCAMBIO DE INFORMACION DEL INSTITUTO NACIONAL DE SERVICIOS SOCIALES para JUBILADOS y PENSIONADOS (INSSJP), con

la finalidad de fortalecer la seguridad de la información de los activos digitales del Instituto en el ciberespacio y compartir la información con demás miembros de la cadena de suministro.

Que, la JEFATURA DE GABINETE DE ASESORES, GERENCIA ECONOMICO FINANCIERA, GERENCIA DE ASUNTOS JURÍDICOS, COORDINACIONES TECNICA LEGAL Y TECNICA ECONOMICA dependiente de la Sindicatura General del Instituto y la UNIDAD DE LEGAL Y TECNICA han intervenido en el marco de sus funciones.

Por ello, y en uso de las facultades conferidas por el Artículo Nº 6 de la Ley 19.032 y sus modificatorias y los Artículos 2° y 3° del Decreto N° 2/04, el artículo 1° del Decreto PEN N° DECTO-2023-63-APN-PTE,

EL DIRECTOR EJECUTIVO

DEL INSTITUTO NACIONAL DE SERVICIOS SOCIALES

PARA JUBILADOS Y PENSIONADOS

RESUELVE:

ARTICULO 1°. – Crease el CENTRO DE ANALISIS E INTERCAMBIO DE INFORMACION DEL INSTITUTO NACIONAL DE SERVICIOS SOCIALES para JUBILADOS y PENSIONADOS (INSSJP), denominado “ISAC-PAMI” con el objeto de fortalecer la seguridad de la información de los activos digitales del Instituto en el ciberespacio

ARTÍCULO 2°. - El CENTRO DE ANALISIS E INTERCAMBIO DE INFORMACION DEL INSTITUTO NACIONAL DE SERVICIOS SOCIALES para JUBILADOS y PENSIONADOS (INSSJP) “ISAC-PAMI” deberá:

1. Recopilar, analizar, compartir y coordinar información sobre ciberamenazas e incidentes en su ámbito de acción,
2. Detectar vulnerabilidades y filtraciones de información que pudieren comprometer al INSSJP, a sus afiliados, a las organizaciones parte de la cadena de suministro y donde se procesen, almacenen o transiten datos de los afiliados y afiliadas,
3. Compartir información con organizaciones parte de la cadena de suministro y donde se procesen, almacenen o transiten datos de los afiliados y afiliadas,
4. Proponer mejoras para fortalecer la postura de seguridad de la información en medios digitales expuestos a internet del INSSJP y de la comunidad objeto,
5. Facilitar el intercambio de datos entre grupos de los sectores público y privado, de acuerdo con las políticas gubernamentales o las leyes nacionales,
6. Elaborar reuniones de intercambio de mejores prácticas con miembros de la cadena de suministro,
7. Proponer y dictar cursos, talleres y simulacros, en un todo de acuerdo con el Plan Estratégico de Seguridad de la Información del INSSJP.
8. Proponer convenios que propendan a la creación, operación y eficaz funcionamiento del ISAC-PAMI.

ARTICULO 3”. - El CENTRO DE ANALISIS E INTERCAMBIO DE INFORMACION DEL INSTITUTO

NACIONAL DE SERVICIOS SOCIALES para JUBILADOS y PENSIONADOS (INSSJP) “ISAC-PAMI” desarrollará sus tareas en el ámbito de la GERENCIA DE SEGURIDAD DE LA INFORMACION Y ACTIVOS DIGITALES dependiente de la JEFATURA DE GABINETE DE ASESORES, no adicionado estructuras funcionales a las ya existentes en el área.

ARTÍCULO 4°. – El CENTRO DE ANALISIS E INTERCAMBIO DE INFORMACION DEL INSTITUTO NACIONAL DE SERVICIOS SOCIALES para JUBILADOS y PENSIONADOS (INSSJP) “ISAC-PAMI” no se involucrará en la operación diaria de los sistemas internos, lo cual dependerá de cada área informática de las organizaciones parte de la cadena de suministro y donde se procesen, almacenen o transiten datos de los afiliados y afiliadas, fortaleciendo la postura de seguridad de los miembros de su comunidad sin comprometer la soberanía de sus infraestructuras.

ARTICULO 5°.- Regístrese, comuníquese y publíquese en el Boletín del Instituto. Cumplido, archívese.

Digitally signed by LEGUIZAMO Esteban Ernesto
Date: 2025.05.06 09:47:08 ART
Location: Ciudad Autónoma de Buenos Aires

Esteban Ernesto Leguizamo
Director Ejecutivo
Dirección Ejecutiva
Instituto Nacional de Servicios Sociales para Jubilados y Pensionados

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2025.05.06 09:47:12 -03:00