Instituto Nacional de Servicios Sociales para Jubilados y Pensionados
AÑO DE LA DEFENSA DE LA VIDA, LA LIBERTAD Y LA PROPIEDAD

Disposición

Número: DI-2024-1-INSSJP-JGA#INSSJP

CIUDAD DE BUENOS AIRES
Viernes 12 de Abril de 2024

Referencia: EX-2024-36547616-INSSJP-JGA#INSSJP Plan Estratégico de Seguridad de la Información 2024

VISTO: la Ley 19032 y sus modificatorias, la Decisión Administrativa N° 641/2021, la Disposición de la Dirección Nacional de Ciberseguridad N° 7/ 2021, la RESOL-2024-810-INSSJP-DE#INSSJP; el EX-2024-36547616- -INSSJP-JGA#INSSJP, y

CONSIDERANDO:

Que el Artículo 1° de la Ley N° 19032, de conformidad con las modificaciones introducidas por su similar N° 25615, asignó 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 INSSJP, en especial lo dispuesto por el Artículo 6° de la Ley N° 19032 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 la Decisión Administrativa Nº 641 de fecha 25 de junio de 2021 actualizó y aprobó los “REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL” que son aplicables a todas las entidades y jurisdicciones comprendidas en el inciso a) del Artículo 8° de la Ley N° 24.156.

Que, conforme lo establece el Artículo 3° de la Decisión mencionada, las referidas entidades y jurisdicciones del Sector Público Nacional deben aprobar sus Planes de Seguridad, estableciendo los plazos en que se dará cumplimiento con los lineamientos básicos en materia de seguridad de la información.

Que la DIRECCIÓN NACIONAL DE CIBERSEGURIDAD emitió la Disposición N° 7 del 12 de agosto de 2021, añadiendo en el Artículo 3° una serie de contenidos mínimos a contemplar en la elaboración de los Planes de Seguridad Informática.

Que mediante la RESOL-2024-810-INSSJP-DE#INSSJP, se crea el COMITÉ DE SEGUIMIENTO Y SEGURIDAD DE LA INFORMACIÓN con naturaleza interdisciplinaria, con asignación específica de funciones para asesorar a las autoridades en cuanto a la seguridad e integridad de la información, su disposición, su preservación y custodia, tendiente a facilitar la coordinación y participación de todas las GERENCIAS tanto en el resguardo de la información como en su disponibilidad, velando por el cumplimiento de las obligaciones legales. Que, asimismo, por la norma antes mencionada se procedió a la derogación de la Disposición N° 0002/GITyC/2015 relativa al MANUAL DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Que el mentado COMITÉ DE SEGUIMIENTO Y SEGURIDAD DE LA INFORMACIÓN se encuentra en la órbita de la JEFATURA DE GABINETE DE ASESORES dependiente de la Dirección Ejecutiva, en el marco de sus misiones y funciones como nexo con las distintas instancias de este Instituto.

Que el JEFE DE GABINETE DE ASESORES del INSSJP o quién este designe en forma expresa, es el COORDINADOR del funcionamiento del mismo en el marco del REGLAMENTO que se aprobara por el mentado acto resolutivo, delineando su integración, funciones, facultades y acciones operativas a su cargo.

Que conforme a las misiones y funciones de la JEFATURA DE GABINETE DE ASESORES de la DIRECCIÓN EJECUTIVA, se delinean las políticas integrales y transversales del INSSJP en lo que respecta al PLAN ESTRATÉGICO DE GESTIÓN 2024/2027; resultando uno de sus hitos la SEGURIDAD DE LA INFORMACIÓN.

Que en tal sentido, se considera necesario aprobar un plan a fin de establecer una estrategia para el abordaje de seguridad de la información del INSSJP tendiente a desarrollar los lineamientos necesarios para propender a aumentar la confidencialidad, integridad y disponibilidad de la información, mitigando riesgos para asegurar el cumplimiento de regulaciones y estándares relevantes, buscando fomentar una cultura de seguridad dentro de la organización para promover la conciencia y responsabilidad de todos los empleados en la protección de la información sensible.

Que entonces, desde la JEFATURA DE GABINETE DE ASESORES conforme las normas que sustentan la materia, signadas en el VISTO, se ha desarrollado un documento conteniendo los lineamientos sobre los cuales reposará la nueva “POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL INSSJP”.

Que por lo expuesto, se considera oportuno proceder a la aprobación del PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2024, conforme constancias glosadas en el IF-2024-37198717-INSSJP-JGA#INSSJP, documento que se incorpora para su aprobación a la presente como ANEXO I.

Por ello en uso de las facultades conferidas en el marco de la RESOL-2023-2042-INSSJP-DE#INSSJP,

EL JEFE DE GABINETE DE ASESORES DE LA DIRECCION EJECUTIVA

DEL INSTITUTO NACIONAL DE SERVICIOS SOCIALES PARA

JUBILADOS Y PENSIONADOS

DISPONE:

ARTICULO 1°. – Aprobar el PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2024, que como ANEXO I (IF-2024-37198717-INSSJP-JGA#INSSJP) se incorpora como parte integrante, embebida a la presente.

ARTICULO 2°. – Registrar, comunicar a la SECRETARÍA GENERAL DE ADMINISTRACIÓN y las GERENCIAS del INSSJP, publicar en el Boletín del Instituto. Cumplido, proceder a su archivo. -

Digitally signed by Damian Rodrigo Gonzalez
Date: 2024.04.12 12:24:56 ART
Location: Ciudad Autónoma de Buenos Aires

Damian Rodrigo Gonzalez
Jefe de Gabinete de Asesores
Jefatura de Gabinete de Asesores
Instituto Nacional de Servicios Sociales para Jubilados y Pensionados

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.04.12 12:26:24 -03:00

Instituto Nacional de Servicios Sociales para Jubilados y Pensionados
AÑO DE LA DEFENSA DE LA VIDA, LA LIBERTAD Y LA PROPIEDAD

Informe

Número: IF-2024-37198717-INSSJP-JGA#INSSJP

CIUDAD DE BUENOS AIRES
Viernes 12 de Abril de 2024

Referencia: EX-2024-36547616-INSSJP-JGA#INSSJP Plan Estratégico de Seguridad de la Información 2024

ANEXO I

Plan Estratégico de Seguridad de la Información 2024

1.Propósito del Documento

El presente documento tiene como objetivo establecer la Estrategia de Seguridad de la Información del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP), desarrollando y estableciendo los lineamientos necesarios para propender a aumentar la confidencialidad, integridad y disponibilidad de la información, mitigando riesgos y asegurando el cumplimiento de regulaciones y estándares relevantes. Asimismo, esta estrategia busca fomentar una cultura de seguridad dentro de la organización, promoviendo la conciencia y responsabilidad de todos los empleados en la protección de la información sensible.

2.Análisis de Contexto:

2.1.Contexto de amenazas en el sector

El desarrollo y el crecimiento exponencial del uso de las tecnologías de la información y las comunicaciones (TIC) en los últimos años han encauzado la transformación digital y los procesos mediante el cual una organización integra tecnología digital a todas las áreas organizacionales. Desde el año 2020, con la irrupción de la pandemia por COVID-19, se aceleró la digitalización de nuestras sociedades en la vida diaria, especialmente en el sector de salud.

A modo de ejemplo, durante el año 2017 la aparición del ransomware *WannaCry* tuvo un impacto mundial, afectando entre otros al Servicio Nacional de Salud de Reino Unido, provocando la cancelación de 19.000 citas y operaciones con un coste económico estimado en 111 millones de libras en concepto de horas extras de TI y pérdida de productividad.

El Banco Interamericano de Desarrollo (BID) en su informe del año 2021 *"Protegiendo la salud digital - Una guía de ciberseguridad en el sector de salud"**[1]*, señala que el sector de salud en varios países de América Latina y el

Caribe (LAC) comenzó a ofrecer, a partir del COVID-19, una mejor calidad de servicio a los ciudadanos a través de proyectos de acceso a servicios digitales de salud por medio de teleconsultas o telemedicina, brindando así acceso a los ciudadanos a historias clínicas electrónicas, entre otros. A la par de ello, se generó un crecimiento exponencial de los ataques e incidentes cibernéticos llevados adelante por ciberdelincuentes, siendo el sector de salud a nivel mundial una de las áreas que se ha visto constantemente comprometida.

Por otra parte, la empresa de tecnología Sophos, publicó el informe *"Estado del Ransomware en el Sector de Salud-2022"* ***[2]***, el cual indica que en 2021 se produjo un incremento de 94% en los ataques de ransomware hacia las organizaciones en este sector.

En la misma línea, y según el informe elaborado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA)[3] con datos del año 2022 y 2023, se observa que el sector sanitario europeo se enfrentó a un número importante de incidentes, afectando en el sector a proveedores de atención sanitaria (53% del total de incidentes). Los actores afectados fueron principalmente hospitales (42%) y autoridades, organismos y agencias sanitarias (14%) y la industria farmacéutica (9%).

Asimismo, en relación con los tipos de activos objetivo de los ataques, se destacan los datos médicos del paciente, incluyendo historias clínicas electrónicas, resultados de laboratorio, así como datos demográficos y administrativos (30% de los incidentes) los cuales permiten a los ciberdelincuentes realizar suplantación, fraude o extorsión al centro de salud o al paciente. Los datos de infraestructura TIC representan un 28% y los datos corporativos un 15% de los incidentes registrados.

Acorde al informe de IBM, del año 2023 sobre el costo de las brechas de datos en salud revela estadísticas impactantes, más de 500 entidades sufrieron brechas entre 2022 y 2023, con un aumento del 15,3% en costos desde 2020, alcanzando un promedio de 4,45 millones de dólares por incidente.

Complementariamente, la empresa Fortinet informa que, en el sector de la industria de la salud a nivel global, detectó más de 12 millones de distribuciones de malware, más de 71 millones de actividades de botnets, más de 38 mil ransomware y más de 233 millones de ataques de DoS, entre otros durante el 2023.

Según menciona el Instituto de Ciberseguridad de España (INCIBE)[4], el crecimiento constante y sostenido de ataques al sector de salud a nivel mundial, durante 2023, estaría sostenido en 4 particularidades fundamentales del sector en los cual ha hecho foco la ciberdelincuencia centrados principalmente en el beneficio económico:

- Alta criticidad de los servicios, principalmente los asistenciales: cualquier interrupción de servicio, aunque sea temporal o momentánea, puede suponer un fuerte prejuicio en la asistencia a pacientes, incluso con consecuencias vitales, lo cual crea una fuerte alarma social y daño reputacional.
- Alto valor de los datos que gestionan: los datos de salud tienen un alto valor en el mercado negro. El precio de una historia clínica puede variar de 30 u$s hasta los 1.000 u$s en casos específicos, mientras que comparativamente el valor de una tarjeta de crédito ronda entre 1 u$s y 6 u$s de media, acorde lo indica la empresa Kaspersky[5].
- Heterogeneidad e hiperconectividad de sistemas y dispositivos: la incorporación de gran cantidad de tecnología en infraestructuras asistenciales. Estos avances tecnológicos y de sistemas, a su vez, conviven con sistemas más antiguos, incluso legados, aumentando así la gestión de su operación y mantenimiento.
- Aumento del volumen y flujos de datos entre sistemas: se ha incrementado el volumen y la heterogeneidad de datos que se generan, interconectándose entre sí, tanto dentro y fuera de la propia organización. Se amplia de este modo, el perímetro de ataque para los cibercriminales.

2.2.Antecedente en la Organización

En los últimos años han existido múltiples incidentes en la región, por ejemplo, exposición de datos sensibles tanto en México, Chile, Brasil y la República Argentina, entre otros.

En el ámbito local, durante el mes de agosto de 2023, el INSSJP fue víctima de un incidente de seguridad que afectó sus oficinas y servicios. La afectación temporal de los servicios que se prestan puso en evidencia la importancia de fortalecer las capacidades de seguridad de la información y la necesidad de implementar medidas sólidas y actualizadas para proteger la privacidad de los afiliados, así como también la integridad, confidencialidad y disponibilidad de la información del organismo y su infraestructura tecnológica.

Dentro de la red de servicios de salud en la República Argentina, el INSSJP emerge como una institución de vital importancia, dedicada al cuidado integral de nuestros ciudadanos. Como la obra social más grande del país y de Latinoamérica, el Programa de Atención Médica Integral (PAMI) despliega una extensa gama de programas y servicios diseñados para atender las necesidades médicas, sociales y emocionales de nuestros afiliados a lo largo y ancho de todo el país.

Algunos de los aspectos principales de su misión residen en el compromiso de brindar atención médica integral de calidad y promover el bienestar de más de 5.000.000 afiliados (entre jubilados y sus familiares a cargo, discapacitados, pensionados y veteranos de Malvinas) que forman parte del instituto. Con una red a nivel federal de más de 600 Agencias de Atención y 38 Unidades de Gestión Local, más de 8.000 médicos de cabecera y 17.000 prestadores médicos, el organismo se erige como un pilar fundamental en el ecosistema de la salud argentina.

Frente al panorama nacional e internacional mencionado, los retos de asegurar la información y tender al aseguramiento de la prestación de servicios esenciales se torna vital contar con una Estrategia de Seguridad de la Información que desarrolle objetivos centrales en materia de protección de los activos de la organización, contando con planificación estratégica y compromiso organizacional en un contexto seguro tanto para el personal, prestadores y afilados a lo largo de todo nuestro país

3.Ejes Estratégicos de Seguridad de la Información

El INSSJP define los siguientes ejes estratégicos a fin promover la Seguridad de la Información en el organismo:

3.1. Liderazgo y compromiso

La Dirección del INSSJP se compromete con el fortalecimiento de la Gobernanza de la Seguridad de la Información, siendo el mismo primordial para establecer una base sólida en la protección de los activos de la organización. Este compromiso se refleja en la voluntad de proporcionar la estructura y el liderazgo necesarios para abordar de manera efectiva los riesgos relacionados con la seguridad de la información, así como para efectivizar el cumplimiento con los requisitos normativos pertinentes.

Al mismo tiempo, este enfoque se orienta hacia el fomento de una cultura arraigada en todos los ámbitos de la organización, donde la conciencia y la responsabilidad en cuanto a la protección de la información sean valores fundamentales compartidos por todos los miembros del equipo.

Alineado con esto, se define un Comité de Seguridad de la Información a fin de proporcionar orientación estratégica y supervisión sobre los aspectos relacionados con la seguridad de la información.

3.2.Políticas de Seguridad de la Información

El INSSJP establecerá una Política de Seguridad de la Información con el propósito de proporcionar un marco claro y formal que defina los principios, objetivos y directrices para proteger sus activos de información. Esta política no solo establece normas y procedimientos para salvaguardar la información sensible, sino que también es la base para la comunicación y promoción de una cultura de seguridad en toda la organización, por lo que será de revisión y actualización periódica permitiendo adaptarse a los cambios que, por las lecciones aprendidas, por la evolución de las tecnologías o servicios, sean necesarios realizar en búsqueda de la mejora continua.

3.3.Roles, Responsabilidades y Autoridades

El INSSJP define, establece y comunica roles, responsabilidades y autoridades relacionados con la gestión de la seguridad de la información. Se asignarán recursos adecuados en función de la estrategia, los roles, las responsabilidades y las políticas.

3.4.Gestión de Riesgos de Seguridad de la Información

El INSSJP establecerá una gestión de riesgos de seguridad de la información, elaborada con la participación y compromiso de todas las áreas incumbentes, con el objetivo de identificar, evaluar y mitigar las amenazas y vulnerabilidades que puedan comprometer la confidencialidad, integridad y disponibilidad de sus activos de información. Esta gestión se orientará hacia la protección de datos sensibles y estratégicos, así como hacia el cumplimiento de regulaciones y normativas aplicables

La gestión de riesgos considera a todas las partes interesadas, así como las prioridades, limitaciones, y los niveles aceptables de riesgo de la organización, así como los análisis que respaldan las decisiones operativas relacionadas con el riesgo.

3.5.Gestión de los Activos

El INSSJP identificará, actualizará y mantendrá un inventario de los activos de la información gestionándolos consistentemente de acuerdo con su importancia para los objetivos de la organización y los riesgos identificados a través de todo su ciclo de vida.

El Instituto analizará adoptar la implementación de políticas para dispositivos traídos por los usuarios (BYOD, “Bring you own device”) a fin de establecer protocolos de seguridad claros y robustos que aborden los riesgos asociados con la conexión de dispositivos personales a la red del organismo.

Se establecerán procedimientos para las copias de seguridad de datos con una frecuencia adecuada según la criticidad de estos. Se definirá la realización de pruebas periódicas de restauración para garantizar la integridad y la disponibilidad de los datos en caso de una eventualidad.

3.6.Seguridad de los datos

El INSSJP adoptará una clasificación de la información con el objetivo de identificar y categorizar los diferentes tipos de datos según su sensibilidad y su impacto en la organización. Esta clasificación permitirá aplicar medidas de protección proporcionales a la importancia de la información, garantizando así su nivel adecuado de confidencialidad, integridad y disponibilidad. Además, se establecerán criterios definidos y directivas sobre el

tratamiento y protección de cada tipo de datos en todas las etapas de su ciclo de vida.

Se implementarán medidas de control de acceso con el fin de que solo las personas autorizadas puedan acceder a la información. Asimismo, se aplicarán controles de integridad para prevenir la manipulación no autorizada de los datos.

Por último, se implementarán controles de redundancia y medidas de recuperación ante desastres para que la información esté disponible cuando sea necesario, minimizando el tiempo de inactividad en caso de incidentes. Además, se implementarán medidas específicas de seguridad para proteger los datos en cada una de sus fases (en uso, en tránsito o en reposo). En el caso de los datos en uso, se establecerán controles de acceso basados en roles y políticas de uso aceptable. Durante el tránsito, se emplearán herramientas de cifrado robustas, mientras que, para los datos en reposo, se utilizarán mecanismos de encriptación y políticas de gestión de claves para protegerlos contra accesos no autorizados y manipulaciones indebidas. Por su parte, para datos en formato físico, se establecen buenas prácticas para su protección durante todo su ciclo de vida en sintonía con cada nivel de confidencialidad asignado.

3.7.Gestión de Identificación, Autenticaciones y Control de Accesos

El acceso a los activos físicos y lógicos se limitarán a usuarios, servicios y hardware autorizados, y se gestionarán de acuerdo con el riesgo evaluado de acceso no autorizado. Las identidades y credenciales de los usuarios, servicios y hardware autorizados son gestionadas por el Instituto, y las identidades son verificadas y vinculadas a las credenciales según el contexto de las interacciones.

Se definen políticas para la gestión de los permisos de acceso, los derechos y las autorizaciones incorporándose los principios de privilegio mínimo y separación de funciones. La gestión del acceso físico a los activos se realiza, supervisa y aplica de manera proporcionada al riesgo.

3.8.Concientización y capacitación

El Instituto establece programas de concientización y capacitación para el personal para llevar adelante sus responsabilidades. Se proporciona tanto capacitación general como específica para roles especializados, con el objetivo de fortalecer la postura de seguridad de la organización y mitigar los riesgos asociados con las amenazas cibernéticas.

El Instituto considera también otras partes interesadas tales como los afiliados y prestadores para la promoción de la concientización sobre la responsabilidad y los riesgos existentes para la seguridad de la información.

3.9.Seguridad de los activos de información

El INSSJP realizará una gestión segura de hardware, software y servicios para proteger la información de la organización. Se establecerán prácticas para gestionar las configuraciones, así como para mantener y actualizar software y hardware de manera proporcional al riesgo.

Se generarán registros para el monitoreo continuo del estado de los activos en uso y se prevendrá el acceso no autorizado y la utilización de software no autorizado.

Se promueve también el desarrollo seguro de software a través del uso de las mejores prácticas vigentes y se monitoriza su desempeño durante todo el ciclo de vida del desarrollo, tanto internamente como con desarrollos externos.

3.10.Mejora continua

El INSSJP realiza auditorías internas periódicas a fin de evaluar los procesos de seguridad de la información establecidos e identificar sus oportunidades de mejora. Se establecerán también métricas con el objetivo de monitorear el desempeño de los procesos definidos.

La Alta Gerencia mantiene su compromiso con la seguridad de la información realizando revisiones gerenciales e incorporando a su plan estratégico general los lineamientos y acciones surgidas del análisis de los resultados.

3.11.Gestión de Incidentes

A fin de identificar y analizar posibles ataques y compromisos a la Seguridad de la Información del Instituto, se establecerá el monitoreo de activos para detectar anomalías, indicadores de compromiso y otros eventos potencialmente adversos, tanto en redes y servicios de red, como en el entorno físico, actividades del personal y uso de tecnología, así como en actividades y servicios de proveedores externos y hardware y software informático.

Se definirán procedimientos para la detección de incidentes de seguridad de la información a partir de anomalías, indicadores de compromiso u otros eventos potencialmente adversos. Los incidentes serán gestionados considerando la realización de análisis para apoyar actividades de respuesta, así como la coordinación de actividades de restauración con partes internas y externas.

Se implementarán los controles de detección de amenazas y de posibles vulnerabilidades presentes en los activos de información, a fin de actuar preventiva y proactivamente para la mitigación de riesgos.

3.12.Resiliencia

El INSSJP establece como requisito la planificación de la continuidad del negocio y la recuperación ante desastres a fin de mantener la disponibilidad y la integridad de los sistemas y datos, ante la ocurrencia de situaciones adversas. Se definen procesos sólidos de BCP (Plan de Continuidad de Negocios) y DRP (Plan de Recupero ante Desastre). Asimismo, se definirán claramente los roles y responsabilidades del personal en caso de emergencia, y se realizarán simulacros periódicos para probar la eficacia del plan y mejorar la preparación de nuestro equipo.

3.13.Cooperación

Para contribuir al fortalecimiento de la Seguridad de la Información del Instituto, se promueve el desarrollo de acuerdos y alianzas estratégicas a nivel nacional, bilateral, regional e internacional, con organismos público, privados y académicos, que contribuyan a fortalecer la seguridad de la información y la protección de los datos personales.

4.Conclusiones:

El contexto y los antecedentes expuestos hacen que la implementación de un plan estratégico de seguridad de la información sea fundamental para el Instituto. Se hace necesario enfoque integral basado en riesgos y el reconocimiento de la importancia de una cultura de seguridad sólida dentro de la organización, promoviendo la conciencia y la responsabilidad en todos los niveles. La formación y sensibilización del personal son elementos clave para fortalecer esta cultura y reducir la probabilidad de incidentes relacionados con errores humanos. Es crucial también la necesidad de implementar medidas técnicas robustas para proteger los activos de información de la organización.

Por último, se remarca la importancia de establecer un marco de gobernanza claro y eficiente para la gestión de la seguridad de la información. Esto implica la asignación de roles y responsabilidades, la definición e implementación de políticas y procedimientos, y la realización periódica de evaluaciones de riesgos para garantizar la efectividad de las medidas implementadas.

---

[1] Protegiendo la salud digital - Una guía de ciberseguridad en el sector de salud | Publicaciones (iadb.org)

[2] The State of Ransomware in Healthcare 2022 – Sophos News

[3] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullRe port

[4] Ciberseguridad en el sector salud: características, amenazas y recomendaciones | INCIBE-CERT | INCIBE

[5] ¿Por cuánto se venden mis datos personales en la Dark Web? | Blog oficial de Kaspersky

Damian Rodrigo Gonzalez
Jefe de Gabinete de Asesores
Jefatura de Gabinete de Asesores
Instituto Nacional de Servicios Sociales para Jubilados y Pensionados