Auditoría General de la Nación

INFORME DE AUDITORÍA

Sistema Interactivo de Información (SII)
Instituto Nacional de Servicios Sociales para Jubilados y Pensionados
- PAMI (INSSJP)

Auditoría General de la Nación
Gerencia de Planificación y Proyectos Especiales
Departamento de Auditoría Informática

INFORME DE AUDITORÍA

Índice

INFORME DE AUDITORÍA

Glosario

AGN: Auditoría General de la Nación.

ANSES: Administración Nacional de la Seguridad Social.

CobIT: Objetivos de Control para Información y Tecnologías Relacionadas, versión 4.1, por sus siglas en inglés. Se utiliza como marco de referencia de buenas prácticas en TI.

CPD: Centro de Procesamiento de Datos, también referido como Data Center.

DC: Ver CPD.

DRP: Plan de Recuperación de Desastres, por sus siglas en inglés.

Incidente: De acuerdo con ITIL, cualquier evento que no forma parte del desarrollo habitual del servicio y que causa o puede causar su interrupción o una reducción de su calidad. Ver también "problema".

INSSJP: Instituto Nacional de Servicios Sociales para Jubilados y Pensionados. Ver PAMI.

ISO 27000/1/2: conjunto de estándares desarrollados por la Organización Internacional de Normalización - ISO y por la Comisión Electrotécnica Internacional - IEC, que proporcionan un marco de gestión de la seguridad de la información y que en este informe se utilizan como referencia de buenas prácticas.

ITIL: Biblioteca de Infraestructura de Tecnologías de Información, por sus siglas en inglés. Se utiliza como marco de referencia de buenas prácticas en TI.

PAMI: Programa de Asistencia Médica Integral. Es la función para la que fue creado el INSSJP. Actualmente las siglas "PAMI" son la denominación común del organismo.

Problema: Fallo producido en un sistema por un mal funcionamiento del software o hardware, que puede generar desde una disminución en su rendimiento hasta la salida de servicio de todo el sistema afectado.

QA: Aseguramiento de la Calidad (*Quality Assurance*).

RENAPER: Registro Nacional de las Personas.

RPO: Punto de recuperación objetivo (*Recovery Point Objetive*). Volumen de datos en riesgo de pérdida que la organización considera tolerable, en caso de que se produzca un fallo del sistema.

RTO: Tiempo de recuperación Objetivo (*Recovery Time Objetive*). Tiempo que una organización puede tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad de sus tareas.

RUB: Registro Único de Beneficiarios. Sistema de la ANSES que almacena los datos de todos sus beneficiarios.

Sala cofre: espacio físico cerrado, sin ventanas, que responde a una serie de normativas internacionales de protección y seguridad física (resistencia al impacto, ambiente de atmósfera controlada, protección ignifuga, accesos restringidos, etc.) donde se alojan los servidores corporativos de una organización. Sus instalaciones deben preservar el equipamiento informático, la información almacenada y, en el caso de siniestro, permitir una rápida puesta en marcha de los equipos y sistemas.

SII: Sistema Interactivo de información. Plataforma de software utilizada por el PAMI a través de la cual se realizan gestiones para afiliados y prestadores.

SIPA: Sistema Integrado Previsional Argentino.

SQL: Lenguaje de Consulta Estructurada, por sus siglas en inglés. Permite administrar y recuperar información de sistemas de gestión de bases de datos relacionales.

TI: Tecnologías de la Información.

UGL: Unidad de Gestión Local.

UPS: Sistema de Alimentación Ininterrumpida, por sus siglas en inglés.

INFORME DE AUDITORÍA

Al Sra. Directora Ejecutiva del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados
Lic. Luana VOLNOVICH
S. / D.

En uso de las facultades conferidas por el artículo 118 de la Ley 24.156, la Auditoría General de la Nación (AGN) efectuó un examen en el ámbito del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP o PAMI), con el objeto que se detalla en el apartado 1.

1. OBJETO DE AUDITORÍA

Sistema Interactivo de Información (SII) y Sistemas Relacionados.

2. ALCANCE

2.1. Ejecución del Trabajo de Auditoría

El examen fue realizado de conformidad con las Normas de Control Externo Gubernamental y las Normas de Control Externo de la Gestión Gubernamental, aprobadas por Resoluciones AGN 26/15 y 186/16, respectivamente, dictadas en virtud de las facultades conferidas por el artículo 119 inciso "d" de la Ley 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional, aplicándose los procedimientos detallados en el punto 2.3.

El inicio de las tareas de auditoría se notificó al organismo el 24/04/2018 mediante Nota AGN 269/18-P, recibida el 26/04/2018.

El período auditado comprende del 1/01/2017 al 31/03/2018.
Las tareas de campo se desarrollaron de mayo de 2018 a abril de 2019.

2.2. Enfoque del Trabajo de Auditoría

La auditoría se desarrolló bajo un enfoque orientado a procesos. La tarea abarcó la verificación de la gestión informática del Sistema Interactivo de Información (SII) a cargo de la Gerencia de Sistemas y la Gerencia de Infraestructura Tecnológica, los servicios de implementación, soporte y mantenimiento continuo de la aplicación, la gestión de la infraestructura tecnológica y la disponibilidad del sistema para los usuarios, con especial énfasis en la evaluación del módulo que administra el padrón de afiliados del organismo por ser un elemento transversal a todas las actividades que realiza el PAMI.

Producto del relevamiento preliminar realizado y del análisis de riesgo resultante, se identificaron las siguientes cuestiones de auditoría como las más relevantes del SII:

- Seguridad de la información.
- Integridad de los datos.
- Disponibilidad de los datos.
- Estabilidad.

La auditoría tuvo en cuenta estándares internacionales establecidos como marco de referencia de buenas prácticas de TI, tales como CobIT versión 4.1, normas ISO de la serie 27000 e ITIL versión 4, así como normativa aplicable a la gestión de TI (Resolución 48/2005 SIGEN, Norma de Control Interno para Tecnología de la Información del Sector Público Nacional), entre otras. Estas describen los procedimientos que una organización debe implementar para obtener resultados óptimos en la gestión de la información.

2.3. Procedimientos de Auditoría

En la etapa de ejecución se realizaron los procedimientos de auditoría que se exponen a continuación, desagregados por cuestión de auditoría:

Seguridad del SII:

- Verificación de la existencia de una política de seguridad informática, de su aprobación formal aprobada y de su conocimiento por los agentes del organismo;

- verificación de la existencia de un área dedicada exclusivamente a los temas de seguridad informática y de su adecuada ubicación dentro de la organización;
- verificación de la determinación de los perfiles de usuarios y sus roles para asegurar una adecuada cadena de responsabilidad en la confidencialidad de la información;
- determinación del grado de cumplimiento de las pautas de seguridad de la información en los procedimientos de requerimientos de nuevas aplicaciones y cambios a las existentes;
- verificación de la adecuación de los controles ambientales del Data Center;
- determinación de la posibilidad de que un solo individuo afecte un proceso crítico;
- evaluación de la asignación de propiedad de datos y sistemas;
- verificación del cumplimiento de los procedimientos de administración de cuentas de acceso con el fin de asegurar la confidencialidad de la información almacenada.

Integridad de los datos almacenados en el SII:

- Verificación de la presentación de la información del SII con integridad, precisión y exactitud;
- verificación de la adecuación del modelo de arquitectura de la información del SII al modelo requerido por las distintas áreas del PAMI;
- verificación de la posibilidad de realizar seguimiento y control sobre los procesos que se ejecutan a través de pistas de auditoría del SII;
- verificación de la existencia, actualización y utilización de un Diccionario de Datos que impida la duplicación de datos y que mitigue la posibilidad de incurrir en inconsistencias en el SII.

Disponibilidad de los datos almacenados en el SII:

- Verificación del aseguramiento por el DRP de la continuidad del Sistema ante un posible desastre, y de la suficiencia y adecuación de las pruebas regulares que se hacen sobre ese plan;
- evaluación de la eficacia y eficiencia de los procedimientos de ejecución del DRP;
- verificación de las políticas de back-up, su formalización, la suficiencia de los procesos que garanticen el resguardo de la información del SII, y de la ejecución regular de las pruebas de restauración para

asegurar la disponibilidad de la información;
- verificación de la adecuación de los CPD para garantizar servicios estables a la infraestructura tecnológica del SII;
- verificación de la realización de pruebas regulares al Plan de Continuidad;
- verificación de la suficiencia de la información que ofrecen las herramientas de exploración y explotación estadística con las que cuenta el SII a las áreas operativas y ejecutivas del PAMI.

Estabilidad del SII:
- Evaluación de la existencia de procedimientos que permitan el aseguramiento de la calidad y su monitoreo;
- determinación de la existencia de un adecuado control de versiones de la aplicación ante la realización de cambios;
- determinación de la existencia y uso de los distintos ambientes o entornos;
- determinación de la adecuación de los procedimientos de administración de los entornos de prueba, control de calidad y pase a producción para garantizar la disponibilidad del SII;
- evaluación de la realización de los requerimientos funcionales y técnicos mediante un proceso formalizado de Ciclo de Vida de Desarrollo de Sistemas;
- verificación de la suficiencia y de la ejecución en tiempo y forma de los procedimientos establecidos para acciones correctivas;
- verificación de la consideración de las modificaciones en el Plan de Mantenimiento de la Infraestructura en el procedimiento de control de cambios.

2.4. Limitaciones

2.4.1. *No se proveyeron los registros de auditoría de los módulos del SII, lo que impide conocer las actividades realizadas sobre las tablas de las bases de datos.*

Como parte del procedimiento para verificar si el SII permite realizar el seguimiento y control de los procesos que se ejecutan, por Nota N° 1092/18–P recibida por el organismo el 25 de octubre de 2018, se solicitaron los registros de auditoría de los módulos del SII (*logs* de auditoría). Ante la falta de respuesta al vencimiento, el requerimiento fue reiterado por Nota N° 1192/18–P, recibida por el organismo el 15 de

noviembre de 2018. La información no fue suministrada al vencimiento. La carencia de esta información impide verificar si eventualmente se realizaron modificaciones en forma directa sobre las tablas de la base de datos asociada al SII, y su naturaleza.

2.4.2. *Esta auditoría no tuvo acceso al modelo de arquitectura de la información, las Políticas de Buenas Prácticas de Desarrollo, y los procedimientos de calidad del desarrollo, lo que limitó la posibilidad de emitir opinión sobre la adecuación y suficiencia de los procedimientos de control de calidad de desarrollo de software.*

Por Nota N° 1092/18–P, recibida por el organismo el 25 de octubre de 2018, se solicitaron los documentos detallados en el acápite. Ante la ausencia de respuesta al vencimiento, el requerimiento se reiteró por Nota N° 1192/18–P, recibida por el organismo el 15 de noviembre de 2018. La información no fue suministrada al vencimiento. La carencia de esta información limita la posibilidad de emitir opinión sobre los procedimientos internos de la Gerencia de Sistemas y la metodología utilizada para medir la calidad de los desarrollos informáticos vinculados al SII.

2.4.3. *No fue posible presenciar la ejecución de las consultas solicitadas a la base de datos productiva, lo que impide asegurar la integridad de los datos suministrados.*

Durante la etapa de ejecución se coordinó con el auditado un procedimiento orientado a recabar evidencia sobre inconsistencias en los datos almacenados mediante la ejecución de consultas a la base de datos del SII. Las consultas fueron ejecutadas por el área de operaciones del organismo, que suministró los resultados en archivos en formato de texto y tablas de Excel. El equipo de auditoría no pudo presenciar el procesamiento de las consultas dado que su ejecución, en algunos casos, requería más de un día de procesamiento, mientras que en el resto de los casos se realizaron durante intervalos de baja demanda de procesamiento del sistema. En virtud de ello no fue posible asegurar la integridad de los datos obtenidos.

2.5. Hechos posteriores al período auditado

A partir de los trabajos de verificación de inconsistencias de las bases de datos, ejecutados entre febrero y marzo del 2019 sobre datos provistos en diciembre del 2018, se pudo constatar que durante enero de 2019 la Subgerencia de Afiliaciones subsanó algunos casos de doble afiliación y de afiliados fallecidos activos identificados por esta auditoría.

Durante las tareas de campo también se pudo comprobar la implementación de procedimientos que mejoraron el proceso de bajas de afiliados, en particular, la disminución del tiempo entre actualizaciones.

3. ACLARACIONES PREVIAS

3.1. Marco conceptual

El Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP), más conocido como PAMI, es un organismo que brinda Prestaciones Médicas y un amplio abanico de servicios a sus afiliados, como descuentos en medicamentos y subsidios económicos.

El PAMI no solo cubre las necesidades asistenciales de la mayoría de los jubilados y pensionados de todo el país y sus familiares a cargo, sino también a excombatientes de la Guerra de Malvinas, personas mayores de 70 años que no tengan ningún tipo de cobertura de obra social, personas sujetas a curatela, entre otros.

El Instituto tiene 4.951.001 afiliados distribuidos en todo el país[1]. Para cubrir las necesidades de atención médica en sus distintas especialidades, el organismo cuenta con 37.503 prestadores, de los cuales 8.852 son médicos de cabecera que se ocupan de la atención médica primaria de los afiliados[2].

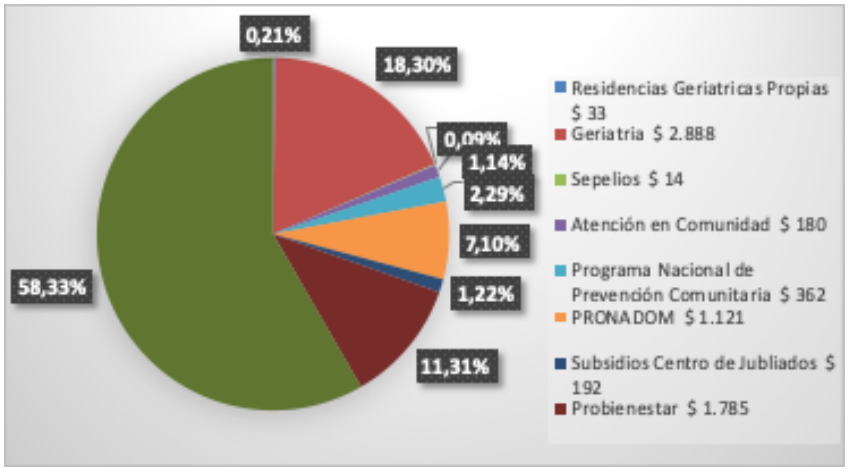
[1] Datos obtenidos de http://datos.pami.org.ar:5000/dataset/padron-de-afiliados/archivo/37d4de3b-062c-4c2f-afbb-d5c53f980f04 el 3 de julio de 2018.
[2] Datos obtenidos de http://datos.pami.org.ar:5000/dataset/prestadores-medicos el 3 de julio de 2018.

INFORME DE AUDITORÍA

A efectos de graficar la importancia del organismo, en 2016 aplicó 1.007.688 vacunas antigripales, mientras que se emitieron 87.327.321 órdenes de medicamentos, de las cuales 66.396.138 (76%) fueron emitidas electrónicamente[3].

De los datos suministrados por el organismo se obtiene que el total del presupuesto para 2016[4] ascendió a $54.215 millones que corresponden a salud (65,82%), $15.786 millones corresponden a Promoción y Asistencia Social (19,17%) y $12.363 millones a otras Actividades (15,01%).
Cada uno de estos conceptos se subdividen en:

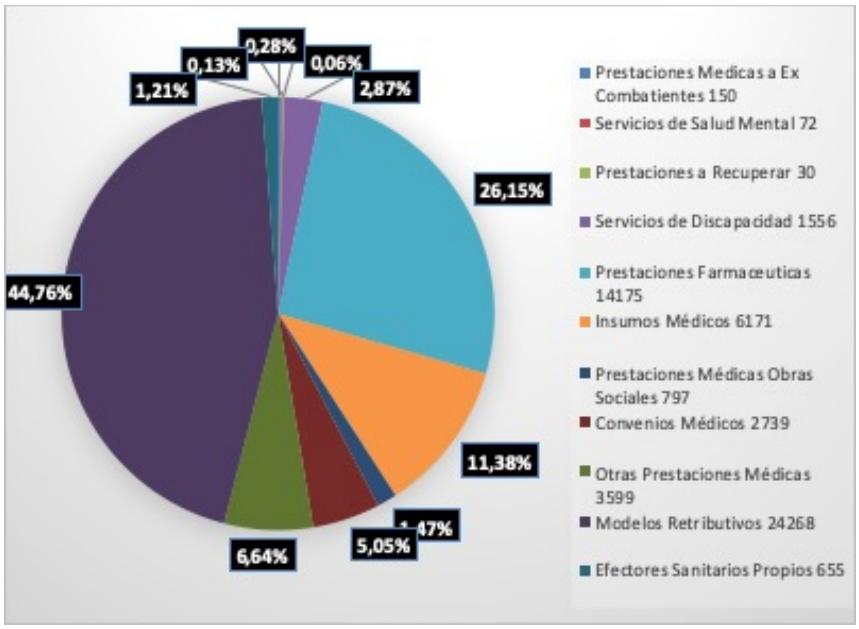
Ilustración N° 1 - Presupuesto de Promoción y Asistencia Social en millones de pesos



Fuente: Elaboración propia a partir de datos del INSSJP.

Ilustración N° 2 - Presupuesto de Salud en millones de pesos

[3] Datos obtenidos de http://datos.pami.org.ar:5000/dataset/receta-electronica/archivo/65ca83f2-5833-45bd-b0eb-a0934602a863 el 12 de julio de 2018.
[4] Últimos datos disponibles al momento del relevamiento.



Fuente: Elaboración propia a partir de datos del INSSJP.

En cuanto al Presupuesto de Actividades, $11.264 millones están destinados a la Coordinación y Administración Central (91,11%), $550 millones a Coordinación y Administración de UGL (4.45%), $544 millones a Efectores Sanitarios Propios (4,40%) y $5 millones a Servicios de la Deuda (0,04%).

3.2. Marco normativo e institucional

El Instituto Nacional de Servicios Sociales para Jubilados y Pensionados es una persona jurídica de derecho público no estatal, con individualidad financiera y administrativa (Ley 19.032 y modificatorias, Art. 1).

El PAMI tiene por objeto otorgar, por sí o por terceros, a los jubilados y pensionados 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, organizadas en un modelo prestacional que se base en criterios de solidaridad, eficacia y eficiencia, que respondan al mayor nivel de calidad disponible para todos los beneficiarios del Instituto, atendiendo a las particularidades e idiosincrasia propias de las diversas jurisdicciones provinciales y de las regiones del país. Estas

prestaciones son consideradas servicios de interés público y los recursos destinados a su financiamiento son intangibles (Ley 19.032 y modificatorias, Art. 2).

Además, el PAMI puede prestar otros servicios destinados a la promoción y asistencia social de los afiliados, tales como subsidios, préstamos, vivienda en comodato, promoción cultural, recreación, turismo, etc. (Ley 19.032 y modificatorias, Art. 3).

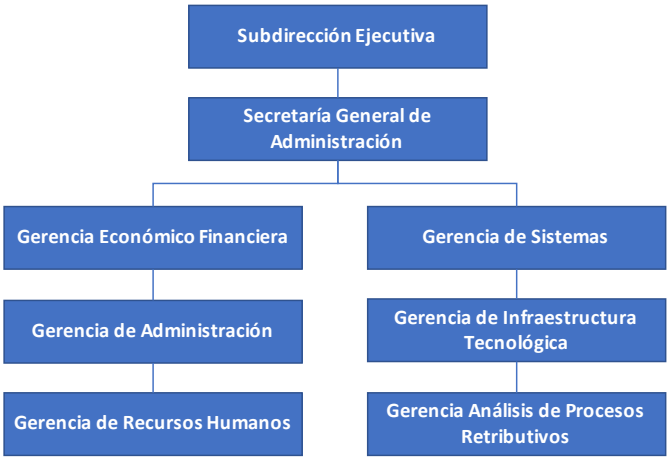
El gobierno y la administración del PAMI están a cargo de un Órgano Ejecutivo de Gobierno y de Unidades de Gestión Local (UGL).

El Órgano Ejecutivo de Gobierno está integrado por un Director Ejecutivo y un Subdirector Ejecutivo, designados por el Poder Ejecutivo (DNU 2/2004, Art. 2 y 3).

Las UGL están a cargo de un Director Ejecutivo local y actúan como unidad de ejecución de los programas implementados por el PAMI, elaborando propuestas y programas prestacionales para la jurisdicción, basados en los factores sociodemográficos, epidemiológicos, tasas de uso estimativas y costos de cada jurisdicción, para lo cual son responsables de mantener actualizado el padrón de afiliados de su área de cobertura (Ley 19.032 y modificatorias, Arts. 5 y 6 bis).

El organigrama del PAMI incluye dos áreas con competencias vinculadas al objeto de auditoría: la Gerencia de Sistemas y la Gerencia de Infraestructura Tecnológica, ambas dependientes de la Secretaría General de Administración, a su vez dependiente de la Subdirección y la Dirección Ejecutiva.

Ilustración 3 - Organigrama del PAMI (solo áreas significativas para este informe)



Fuente: elaboración propia en base a https://www.pami.org.ar/pdf/personigrama190124.pdf.

Entre las responsabilidades de la Gerencia de Sistemas se encuentra velar por el mantenimiento y correcto funcionamiento de los sistemas del PAMI, y planificar e instrumentar el desarrollo de soluciones tecnológicas con una visión centralizada en el usuario siguiendo las últimas tendencias y estándares globales de la industria de las TICs. Por su parte, es responsabilidad de la Gerencia de Infraestructura Tecnológica asegurar el mantenimiento del hardware, el software base, el almacenamiento de datos y las redes que conforman la infraestructura tecnológica del PAMI, garantizando la calidad en la prestación de servicios informáticos y tecnológicos (Resolución 678/DE/17, Anexo XI, apartado IV, puntos 20 y 21[5]).

Respecto a las prestaciones que brinda el PAMI a sus beneficiarios, se encuentran previstas -en un importante número- en el denominado Modelo Prestacional Sociocomunitario de Atención Médica y otras Prestaciones Asistenciales, que debe adecuarse a las particularidades regionales y la realidad prestacional local de cada UGL. Este modelo fue previsto con el objetivo de ser un programa médico asistencial de carácter integral, por lo que se puede ampliar e incorporar otras prestaciones al sistema (Resolución 284/DE/05[6]).

En sus grandes líneas, el modelo de atención médica es la forma de organización de los recursos prestacionales para cubrir la demanda específica con prioridad en las acciones de atención primaria, y en

[5] Disponible en: http://institucional.pami.org.ar/files/boletines_inssjp/12-07-17.pdf
[6] Disponible en: http://institucional.pami.org.ar/files/boletines_inssjp/01-04-05.pdf

los programas de promoción y prevención de la salud, fundamentado en criterios epidemiológicos y de regionalización geográfica. Define niveles de atención de complejidad creciente integrados funcionalmente, estructurados de la siguiente manera: un primer nivel constituido por médicos de cabecera y los demás recursos para la atención primaria (I Nivel[7]); un segundo nivel ambulatorio, para la atención vertical del beneficiario, conformado por los especialistas y demás recursos correspondientes a ese nivel y de internación general de agudos (II Nivel[8]); y un tercer nivel de alta complejidad diagnóstica y terapéutica, ambulatoria y en internación (III Nivel[9]).

El modelo prevé la existencia de sistemas de información que permitan un seguimiento continuo y efectivo de las prestaciones brindadas.

El ingreso al sistema se realiza a través del Médico de Cabecera, que es el principal referente y nexo para la articulación de todos los procesos de atención de los afiliados asignados a su padrón. Es el responsable de la realización de la historia clínica y debe establecer el orden de prioridad de las distintas terapéuticas que recibe el paciente en forma conjunta con los especialistas (Resolución 284/DE/05, Anexo).

Respecto del pago de las prestaciones por el PAMI, inicialmente el modelo analizado establecía una modalidad de retribución capitada[10] que luego fue substituida por la modalidad contractual de pago por prestación con cartera asignada (Resolución 687/DE/13 y su modificatoria 911/DE/2013 y Resolución 846/DE/13), para los tres niveles de atención.

[7] Comprende médicos de cabecera, laboratorios para determinaciones ambulatorias de baja y media complejidad, centros de diagnóstico por imágenes de baja y media complejidad, fisiokinesioterapia, traslados a cargo del Instituto (área metropolitana bonaerense) o de quien sea prestador en otras localidades.

[8] Comprende consulta médica de especialistas, prácticas especializadas de diagnóstico y tratamiento, internación, internación domiciliaria para agudos, atención de urgencias, etc.

[9] Incluye medicina nuclear, análisis clínicos de alta complejidad, laboratorio, tomografía axial computada, densitometría ósea, terapia radiante, resonancia nuclear magnética, procedimientos hemodinámicos, cirugía vascular, angioplastías, cirugía cardiovascular, neurocirugía, estudios electrofisiológicos, entre otros.

[10] Consiste en un sistema por el cual los prestadores cobran una suma fija por una determinada cantidad de afiliados, sea que los atiendan o no.

En 2017 se decidió volver al sistema de cápita previsto inicialmente para los Niveles I y II, y establecer un nuevo sistema por prestación para el Nivel III, para lo cual se ordenó la rescisión unilateral de los contratos vigentes y la suscripción de nuevos contratos con los prestadores. Se dispuso el pago capitado de las prestaciones socio-sanitarias a los afiliados, con excepción de los Médicos de Cabecera y los Prestadores de las Provincias de Jujuy, La Pampa, Neuquén, Río Negro, Santa Cruz, Chubut y Tierra del Fuego (Resolución 395/DE/17[11]).

A fin de implementar la modalidad del sistema de cápita reestablecido se aprobó el Modelo Capitado para el I y II Nivel de Atención que establece que el prestador se obliga a brindar los servicios asistenciales, percibiendo en concepto de honorarios/contraprestación la suma equivalente a la resultante de multiplicar el monto de la cápita mensual fijada en pesos por el PAMI por la cantidad de beneficiarios asignados por módulo, en función de la categoría definida por el PAMI a la cual pertenezca el prestador. Por su parte, se dispuso que el modelo de contrato relativo al III Nivel de Atención incluya como contraprestación de los servicios brindados, el pago por prestación modulada a los valores que serán establecidos en el denominado Nomenclador Común del PAMI (Resolución 408/DE/2017[12]).

El PAMI brinda atención a sus afiliados a través de tres modalidades: Prestadores que contrata en el marco del modelo de retribución capitada (I y II Nivel) o pago por prestación modulada (III Nivel); prestadores alternativos y efectores propios. Para las prácticas excluidas de los modelos retributivos mencionados (principalmente referidas a prestaciones de alta complejidad), el PAMI contrata a prestadores alternativos. Los efectores propios del PAMI participan en la resolución de la atención de los afiliados, especialmente en los servicios de Guardia Médica e Internación de II Nivel y en los servicios de atención primaria de II Nivel para pacientes ambulatorios.

3.3. Contexto de TI del objeto de control

El PAMI dispone de una amplia plataforma tecnológica orientada a gestionar los diversos servicios que brinda a sus afiliados, que incluye a los sistemas de gestión necesarios para la administración del

[11] Disponible en: https://www.boletinoficial.gob.ar/#!DetalleNormaBusquedaAvanzada/161590/20170405
[12] Disponible en: https://institucional.pami.org.ar/files/boletines_inssjp/25-04-17.pdf

organismo. Para la atención de sus afiliados el Instituto cuenta con 2 grandes sistemas o plataformas, denominados Clave Única PAMI (CUP)[13] y Sistema Interactivo de Información (SII), el último de los cuales fue objeto de esta auditoría.

El SII es la principal plataforma del organismo para la gestión de sus diversas actividades. Fue desarrollado externamente entre 2006 y 2009, y se entregó al Instituto en 2010, para que inicialmente fuera administrado por la Unidad de Análisis, Estadística y Planeamiento dependiente de la Dirección Ejecutiva, y actualmente se encuentra bajo la órbita de la Dirección de Sistemas.

Este sistema es utilizado a nivel nacional por aproximadamente 13.000 usuarios internos de PAMI además de prestadores externos y para consulta por los afiliados. Dentro de los distintos módulos se destacan el de padrón de afiliados que administra los datos de los casi cinco millones de afiliados y el de prestaciones médicas, por el cual se gestionan aproximadamente 12 millones de prestaciones mensuales que se realizan a través del PAMI.

El sistema está diseñado para acceder en forma WEB tanto desde la intranet del organismo, como desde su página WEB. Es utilizado por todas las UGL y Agencias distribuidas en todo el país.

Los beneficiarios pueden realizar ciertas consultas al sistema accediendo desde la página www.pami.org.ar a través de Mi PAMI, que es un portal de autogestión *online* para realizar las siguientes gestiones sin concurrir a la agencia: consultar la cartilla médica, consultar la información del afiliado en poder de PAMI e imprimir una credencial provisoria.

Algunos de los principales módulos del SII son los siguientes: Padrón de Beneficiarios; Registro Informático Único Nacional de Prestadores y Proveedores; Configuración Prestacional; Sistema de

[13] A través del CUP se gestionan: i) medicamentos sin cargo; ii) padrón de diabéticos; iii) receta electrónica; iv) audífonos; v) oxigenoterapia; vi) ópticas; vii) viviendas en comodato; entre otros servicios.

Recuperos; Gestión de Afiliados Derivados por Razones de Salud; Orden de Prestación; Insumos Médicos; Sociales; Diálisis; Fisiatría; Contratos de Prestadores; además de un módulo específico para la configuración general de seguridad del SII.

4. HALLAZGOS

4.1. Seguridad de la información

4.1.1. *La Política de Seguridad de la Información no es aplicada correctamente ni fue eficazmente comunicada a los agentes del organismo, lo que pone en riesgo la integridad de la información almacenada en las bases de datos del SII.*

De las reuniones mantenidas con los responsables de distintas áreas de la Gerencia de Sistemas y de la Gerencia de Infraestructura Tecnológica surge que en algunos casos se desconoce la existencia del documento que formaliza las Políticas de Seguridad de la Información MGSI-02 aprobado por la Disposición N° 2/2015/GITC emitida por la Gerencia de Infraestructura Tecnológica, y que en otros casos no se aplica. A modo de ejemplo, el Comité de Seguridad de la Información previsto en el manual respectivo, no se encuentra en funcionamiento. Adicionalmente, ni la Resolución 48/05 SIGEN ni las Resoluciones N°0566 - 03 INSSJP y 1406 - 05 INSSJP son aplicadas.

Se deben definir y comunicar todas las políticas, planes y procedimientos que dirigen los procesos de TI. Éstos deben estar documentados, revisados, mantenidos, aprobados, almacenados, comunicados y deben ser utilizados para el entrenamiento. También deben estar asignadas las responsabilidades para cada una de estas actividades y oportunamente, revisar si se ejecutan correctamente. Se debe asegurar que las políticas, planes y procedimientos son accesibles, correctos, entendidos y actualizados (CobIT v4.1 - PC5: Políticas, planes y procedimientos). El plan de seguridad de TI debe contemplar los requerimientos de negocio, los riesgos y el control del cumplimiento de las reglas establecidas en él (CobIT v4.1 - DS5.2 - Plan de Seguridad de TI).

INFORME DE AUDITORÍA

El incumplimiento de la Política de Seguridad de la Información o su incorrecta aplicación expone al organismo a un incremento en el riesgo de afectar los datos almacenados en la base de datos del SII por errores o acciones mal intencionadas.

4.1.2. *El Departamento de Seguridad Informática depende de la Gerencia de Infraestructura Tecnológica, lo que no asegura su independencia ni la adecuada separación de funciones respecto del resto de las áreas a las que debe controlar. Esta situación debilita el control de la aplicación de los procedimientos de seguridad informática.*

Por Resolución 0678/17 de la Dirección Ejecutiva, PAMI aprueba un nuevo organigrama donde asigna a Seguridad Informática el rango de Departamento, dependiente de la Gerencia de Infraestructura y Tecnología, área a la que debe controlar en los aspectos relativos al cumplimiento de los procedimientos de seguridad informática.

Las buenas prácticas indican que se debe administrar la seguridad de TI al nivel más alto apropiado dentro de la organización (CobIT v4.1 – DS 5.1: Administración de la seguridad de TI).

No contar con un control estándar independiente y con funciones segregadas aumenta el riesgo de modificación, mal uso o uso no autorizado o involuntario de un activo de TI.

4.1.3. *La gestión de roles y perfiles de usuarios del SII no es adecuada, ni se lleva adelante una metodología de seguimiento y control permanente sobre la actividad de los usuarios, con riesgo para la integridad, confidencialidad y disponibilidad de la información.*

RESERVADO COLEGIO DE AUDITORES GENERALES

INFORME DE AUDITORÍA

RESERVADO COLEGIO DE AUDITORES GENERALES

INFORME DE AUDITORÍA

RESERVADO COLEGIO DE AUDITORES GENERALES

Según las mejores prácticas en gestión de usuarios, se debe garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y sus privilegios relacionados, sean previstos en un conjunto de procedimientos del área responsable del tema. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema los privilegios de acceso para cada uno de los roles. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, y para casos normales o de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la organización deben acordarse contractualmente para todos los tipos de usuarios. Periódicamente se deben realizar revisiones de la gestión de las cuentas de usuario y los privilegios asociados (CobIT v4.1 - DS5.4: Administración de cuentas del usuario).

Conforme surge de la evidencia obtenida, la gestión de usuarios y segregación de funciones de los roles asignados en el sistema es inadecuada por falta de un procedimiento de control y seguimiento, lo que compromete la confidencialidad, integridad y disponibilidad de la información.

[17] Según surge del listado provisto por el área de Recursos Humanos del PAMI.

4.1.4. *No se realiza un adecuado Control por Oposición de roles y perfiles de usuarios del SII. Esta situación aumenta el riesgo de que se produzcan errores o manipulación indebida de los datos, entre otros factores que pueden comprometer la integridad de la información.*

De los procedimientos realizados surge que existen dos agentes del PAMI que cuentan con rol "solicitante" y "autorizante" simultáneamente, para el módulo "Orden de Prestaciones v2" del SII. Ello pone en evidencia la ausencia de controles en la asignación de roles conforme al principio de control por oposición de intereses.

Mediante el denominado "control por oposición de intereses" se distribuye la responsabilidad de un proceso total en tramos, de forma tal que al culminar un tramo cesa la responsabilidad del que entrega y comienza la del que recibe el insumo. Para el caso de una solicitud y autorización de una determinada prestación, no debería haber un sólo usuario que controle la totalidad de un determinado proceso o transacción, sino el menos dos, pertenecientes a distintas áreas y con distintos intereses.

Se debe implementar una adecuada división de roles y responsabilidades que disminuya el riesgo de que un proceso crítico sea afectado por la acción de un único individuo y las tareas deben ser realizadas únicamente por el personal autorizado (CobIT v4.1 – PO4.11: Segregación de funciones).

La ausencia de una distribución de roles de usuarios basada en una adecuada segregación de funciones, incrementa el riesgo de que se produzcan errores o manipulación indebida que afecten la integridad de los datos almacenados en el sistema.

4.1.5. *No se realiza un adecuado análisis de seguridad informática de los requerimientos técnicos y funcionales para desarrollos o cambios en las aplicaciones existentes. De este modo se incrementa el riesgo de permitir el acceso no autorizado a los sistemas, a las redes de datos y a los equipos conectados a ella, comprometiendo la integridad, disponibilidad y confidencialidad de la información.*

INFORME DE AUDITORÍA

Si bien existe una política de seguridad de la información, dependiendo del sector, no se aplica o se aplica parcialmente, situación que fue observada en los procedimientos de solicitudes de cambio, requerimientos de nuevas aplicaciones o mejoras de las existentes.

Las buenas prácticas indican que los responsables deben garantizar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad para alcanzar el cumplimiento de las políticas y normas de seguridad (ISO 27001, Anexo A, A.15.1.2).

No aplicar o aplicar parcialmente la política de seguridad de la información vigente en los análisis de los requerimientos técnicos y funcionales, compromete la integridad, disponibilidad y confidencialidad de la información.

4.1.6. *El sistema de control ambiental instalado en el centro de procesamiento de datos no cuenta con redundancia, lo que aumenta el riesgo de que, ante una falla en el sistema, el CPD quede sin controles que puedan alertar sobre incidentes. Esta situación se agrava por no disponer el PAMI de un sitio alternativo de procesamiento.*

Es necesario diseñar e implementar medidas de protección contra factores ambientales, mediante la instalación de dispositivos y equipo especializado para monitorear y controlar el ambiente (CobIT v4.1 - DS12.4: Protección contra factores ambientales). Los sistemas de control ambiental de un CPD permiten controlar las condiciones de temperatura, flujo de aire, humedad, presencia de líquidos, entre otros, a través de sensores.

Si bien los dispositivos de control ambiental instalados en el CPD son adecuados, se torna necesario disponer de un sistema redundante para efectuar los controles, dado que el Instituto carece de un sitio alternativo de procesamiento (véase 4.3.2.). Un sistema redundante para el control de los parámetros

ambientales disminuye el riesgo de que el CPD o los equipos que almacena queden inutilizables total o parcialmente ante un evento, lo que dificultaría o impediría brindar atención a los beneficiarios.

4.1.7. *El PAMI no aplica adecuadamente los controles establecidos en la política de administración de cuentas de usuarios del SII, con riesgo para la integridad y confidencialidad de los datos almacenados*.

Las mejores prácticas orientadas a la gestión de TI establecen la necesidad de que todos los usuarios sean identificables de manera unívoca (CobIT v4.1 - DS5.3: Administración de identidad; y DS5.4: Administración de cuentas del usuario).

El PAMI cuenta además con normativa interna que incluye buenas prácticas en gestión de usuarios: la Disposición 0002-15-GITC (Manual de Política de Seguridad de la Información del INSSJP) y la Resolución 0566-03 (Política de Uso Aceptable de los Recursos Informáticos). De ellas se extrae que: los usuarios deben ser personalizados, deben identificarse y autenticarse unívocamente; todos los usuarios -incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos- deben tener un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable, a fin de garantizar la trazabilidad de las transacciones; y que los identificadores de usuario no deben dar ningún indicio del nivel de privilegio otorgado; entre otras relativas al control, monitoreo y reporte de actividades de usuarios.

[18] Permite a un usuario realizar consultas a una tabla o tablas de una base de datos en forma directa.

Estos hallazgos permiten asegurar que la normativa interna no se cumple en lo relativo a la gestión de usuarios, mientras que los controles, monitoreos y reportes no se cumplen.

La presencia de usuarios genéricos activos dificulta el control e imposibilita la identificación unívoca de las acciones que realizó cada individuo, con riesgos para la integridad y confidencialidad de los datos obrantes en el SII.

4.2. Integridad de los datos

4.2.1. *El PAMI no posee un Diccionario de Datos, lo que aumenta el riesgo que exista duplicación y/o inconsistencias en los datos almacenados*

Las mejores prácticas orientadas a la gestión de TI establecen la necesidad de contar con un Diccionario de Datos único y actualizado, que permita indicar cómo están organizados y estructurados, cuál es su significado, la relación, el origen, el formato y su uso. Entre otras funcionalidades, el Diccionario de Datos es una herramienta clave para ser utilizada durante los distintos procesos del ciclo de vida del desarrollo y mantenimiento de un sistema de información, brindando soporte al equipo de analistas que participan, como así también a los usuarios de la organización involucrados en los requerimientos funcionales del sistema (CobIT v4.1 - PO2.2: Diccionario de datos empresarial y reglas de sintaxis de datos).

Se verifica la inexistencia de un Diccionario de Datos del PAMI. Su ausencia conlleva el riesgo de producir información duplicada, interpretaciones erróneas, e inconsistencias en los flujos de datos, en sus relacionamientos y en su estructura.

4.2.2. *Los usuarios del SII no cuentan con información íntegra y exacta al momento de ejecutar los diferentes procesos del sistema, lo que aumenta el riesgo de que se produzcan perjuicios económicos al PAMI por el pago de cápitas indebidas y afecta la calidad de atención de los beneficiarios.*

INFORME DE AUDITORÍA

De las pruebas realizadas sobre el sistema y de análisis realizados sobre extracciones de datos de la base, se desprende que el SII no brinda información consistente y exacta al realizar operaciones sobre él[19]. El resultado de esta tarea se sintetiza en la siguiente tabla.

Tabla 1 - Resumen de errores encontrados en el Padrón de Beneficiarios

Grupo	Casos	Detalle
Fallecidos	6	Beneficiarios con doble afiliación, fallecidos y activos (4 casos subsanados al 12/2018)[20]
	6	Beneficiarios fallecidos y activos (5 casos subsanados al 12/2018)
Afiliación	57	Beneficiarios con doble afiliación (24 casos subsanados al 12/2018)
Hijos	14	Hijo no estudiante con vencimiento previsto a edades superiores a los 21 años
	9	Hijo no estudiante con vencimiento de afiliación mal aplicado
	12	Hijo no estudiante mayor de 21 años habilitado
	13	Hijo estudiante mayor de 25 años habilitado[21]
	13	Hijo estudiante con vencimiento de afiliación mal aplicado
Registración	6	Beneficiarios con número de documento o de CUIT/CUIL que difiere del asentado en la ANSES
	3	Beneficiarios con error en la fecha de nacimiento registrada
	1	Beneficiario con datos personales en el SII que difieren de los que posee el ANSES
	14	Beneficiarios con el CUIT/CUIL en ceros
	6	Beneficiarios oportunamente registrados como recién nacidos, pero sin documentos registrados a la fecha de los procedimientos
	4	Beneficiario mayor de 50 años registrado como recién nacido
	3	Beneficiarios registrados con error en el tipo y nro. de documento
	11	Beneficiarios con número de documento no coincidente con la parte central de su número de CUIT/CUIL
	4	Beneficiarios registrados con un número de CUIT/CUIL inexistente
	29	Beneficiarios diferentes con idéntico número de documento (17 casos verificados visualmente)
	7	Beneficiarios cuyo nombre difiere del asentado en la ANSES
	12	Beneficiarios registrados con error en el número de CUIT/CUIL

Fuente: Elaboración propia a partir de datos suministrados por el INSSJP.

[19] El procedimiento estuvo dirigido a identificar la existencia de inconsistencias y no el quantum de posibles pagos indebidos resultado de los errores encontrados.

[20] A modo de ejemplo, la afiliada *A.M.*, con CUIT 27-XXXXXXX-5, figura en el Padrón de Beneficiarios con doble afiliación activa. Consultado el Sistema Integrado Previsional Argentino de la ANSES, la persona se encuentra con estado fallecido.

[21] A modo de ejemplo, el afiliado *J.M.E.*, con CUIT 20-XXXXXXXX-9, figura en el Padrón de Beneficiarios afiliado como "hijo estudiante" siendo mayor de 25 años.

INFORME DE AUDITORÍA

Los resultados expuestos en la tabla precedente corresponden a extracciones de datos realizadas a las tablas del Padrón de Afiliados tomando solamente los afiliados activos en ese momento y se encuentran alcanzados por los efectos de la limitación detallada en el punto 2.4.3. De lo que surge que la cantidad de errores expuestos no expresan su total.

Los análisis realizados verificaron deficiencias en la información contenida en las bases de datos del SII que reflejan fallas en los procedimientos de carga y validación de datos ingresados al SII.

De los procedimientos de auditoría ejecutados sobre el sistema y del análisis de consultas realizadas a la base de datos del SII surge que:[22]

- no existen manuales de procedimientos ni procedimientos formalizados para la afiliación de beneficiarios;
- no se realizan cruces de datos con las Cajas Provinciales, lo que admite la afiliación de personas que disponen de cobertura como beneficiarios de aquellas[23];
- el SII no cuenta con vínculos automáticos de consulta con la ANSES o el RENAPER que permita procesar las altas o bajas en forma rápida y eficiente;
- no existen controles para evitar la afiliación de un familiar a cargo que posea una pensión no contributiva[24];
- no existen controles de ingreso sobre campos importantes, como número de documento o número de teléfono;
- si bien existe un campo para indicar el ejemplar del DNI presentado, no se controla y es optativo;
- no existe un adecuado proceso de baja de beneficiarios, que impida que personas fallecidas sigan figurando en el padrón como beneficiarios activos;

[22] En el Anexo III se exponen ejemplos de casos.
[23] Causa de exclusión conforme a Resolución N° 1100/06 INSSJP.
[24] Idem nota al pie Nº 19.

- el campo que verifica el domicilio del beneficiario se administra mediante una aplicación externa que produce errores en la carga de los datos de los afiliados y que carece de contrato de mantenimiento;
- no existe un control automático del vencimiento de la afiliación por razones de edad y estudios de los hijos de beneficiarios.

La solución de los problemas arriba mencionados no asegura la integridad de los datos del Instituto, pero permitirían disminuir el riesgo que se produzcan errores en los mismos.

El INSSJP trata las bajas de los afiliados a partir de la notificación que le realiza la ANSES. Este procedimiento consistió inicialmente en procesar las novedades de acuerdo a archivos que suministraba la ANSES a solicitud de PAMI. Posteriormente se estableció que este proceso tuviera una frecuencia mensual y durante las tareas de campo se estableció que las actualizaciones debían realizarse semanalmente. Cabe destacar que para la ANSES puede ocurrir que no tenga información fehaciente sobre el fallecimiento de un afiliado (solamente toma conocimiento que el jubilado no retiró los haberes de su cuenta bancaria o no completó el trámite de supervivencia) motivo por el cual puede informar su baja meses después de haberse producido.

Salvo casos específicos en los que la Subgerencia de Afiliaciones de PAMI lo considere necesario, se realizan consultas al RENAPER para establecer si un afiliado se encuentra fallecido.

Conforme a las mejores prácticas, es necesario definir e implementar procedimientos que garanticen la integridad y consistencia de los datos almacenados en formato electrónico, como bases de datos y archivos (CobIT v4.1 – PO2: Definir la arquitectura de la información).

Los casos señalados generan el pago de cápitas a prestadores médicos por beneficiarios fallecidos. Además, esta situación puede producir que el sistema informe erróneamente que un determinado prestador tiene todas sus cápitas cubiertas y, ante una nueva afiliación, se asigne esta cápita a otro prestador más alejado del domicilio del beneficiario, obligándolos a desplazamientos innecesariamente más extensos para conseguir atención médica.

INFORME DE AUDITORÍA

4.3. Disponibilidad de los datos

4.3.1. *El PAMI no cuenta con un Plan de Continuidad de Servicios de TI ni un Plan de Recuperación de Desastres (DRP) aprobados y vigentes. Tampoco cuenta con procedimientos de análisis y gestión de riesgos que permitan su diseño e implementación, lo que pone en riesgo la atención de sus beneficiarios ante salidas de servicio no planificadas de sus sistemas.*

El PAMI redactó e implementó un Plan de Continuidad de Negocios para cumplir con la certificación de la norma ISO 27001. Esta certificación se limitaba al sistema que registra la trazabilidad de medicamentos, y venció en 2017. Desde ese entonces el Instituto avanza en una actualización completa de las políticas de seguridad de la información y en la revisión de los procesos correspondientes, sin que el trabajo se encontrara finalizado a la fecha de cierre de tareas de campo.

Tampoco posee el PAMI un plan que asegure la continuidad del servicio ante incidentes o desastres ocurridos en el centro de procesamiento de datos. Esta auditoría no pudo constatar la existencia de un análisis de riesgo ni un catálogo formal de servicios del SII, que permita priorizar aquellos que deberían ser atendidos en forma inmediata ante un desastre.

Frente a la posibilidad de que ocurran eventos que puedan dejar fuera de servicio a los sistemas, las organizaciones deben contar con un plan de recuperación de desastres (DRP), que especifique los pasos a seguir para asegurar la continuidad del servicio frente a dichos eventos. Los planes deben ponerse a prueba con cierta regularidad para que, ocurrido el desastre, las funciones estén automatizadas y aprendidas por los responsables y las áreas interesadas. Conforme a las mejores prácticas, se debe desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar al personal de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio (CobIT v4.1 - DS4: Garantizar la continuidad del servicio).

Contar con un Plan de Continuidad del Servicio permite, entre otras: mejorar la capacitación del personal y su capacidad de respuesta; identificar las situaciones que pueden afectar la continuidad del servicio; predecir el tiempo necesario de recuperación de los sistemas; proteger los activos de acuerdo a su prioridad; identificar los puntos más vulnerables de la infraestructura; reducir pérdidas económicas y gastos por recuperación; identificar los recursos mínimos para garantizar su disponibilidad (Norma ISO 27001).

4.3.2. *El PAMI no cuenta con un Centro de Procesamiento de Datos alternativo y se verificaron fallas en la gestión del sistema de extinción de incendios de la Sala Cofre y el Data Center, con riesgo para la disponibilidad y continuidad del servicio.*

La infraestructura informática se encuentra adecuadamente dimensionada y se verifica redundancia de *hardware* dentro del propio *Data Center*. Sin embargo, no existe redundancia geográfica (*Data Center* alternativo situado en otro edificio o localidad) que asegure la continuidad del servicio en caso de ocurrir un evento que impida la operación del *Data Center* principal. Ante la posibilidad de que ocurran salidas de servicio del *Data Center* principal (cualquiera sea la causa), las organizaciones deben contar con redundancia de infraestructura lógica y física.

Respecto de las medidas de protección del DC, la inspección de las instalaciones permitió advertir la ausencia de los tubos contenedores del agente extintor de incendios de la Sala Cofre. De acuerdo con la información suministrada por el auditado, se produjeron disparos manuales del sistema de extinción de incendios en las dos salas en las que se encuentra divida la Sala Cofre, y se encontraron sin tubos de extinción por aproximadamente 80 días. Una nueva inspección ejecutada durante la ejecución de la auditoría permitió verificar que los tubos faltantes habían sido instalados.

El contrato vigente entre el PAMI y el proveedor que brinda servicio de mantenimiento a su CPD, no contempla la provisión de cilindros provisorios al momento de retirar los instalados para realizar pruebas, recargar o efectuar tareas de mantenimiento. Tampoco contempla la recarga de cilindros como tarea de mantenimiento preventivo.

INFORME DE AUDITORÍA

Conforme a las buenas prácticas, el organismo debe proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivo) o fallas humanas, lo que resulta posible mediante la instalación de controles físicos y ambientales adecuados. Estos deben ser revisados regularmente y se deben definir los procedimientos respectivos (CobIT v4.1 - DS12: Administración de las instalaciones).

La falta de controles adecuados en los sistemas de protección aumenta el riesgo de que fallen y dejen al CPD fuera de servicio, consecuentemente imposibilitando al organismo para prestar servicios en un contexto en el que se carece de redundancia geográfica.

4.3.3. *No se encuentra debidamente comunicada ni se aplica adecuadamente la normativa que rige la realización de copias de respaldo de la información (backups). Esta circunstancia y la falta de insumos para la realización de las copias de respaldo, aumentan el riesgo de que las copias no se realicen o que se generen archivos defectuosos.*

El procedimiento para la realización de las copias de respaldo en cintas se encuentra definido en la Resolución 566/03 INSSJP y formó parte de la documentación necesaria para que el organismo oportunamente obtuviera la certificación ISO 27001 (actualmente vencida). En las entrevistas realizadas con distintos responsables de las áreas involucradas se tomó conocimiento de que la normativa no está adecuadamente comunicada al personal, incluidos los responsables de generar o resguardar las copias.

El organismo carece de insumos suficientes, principalmente cintas, para realizar las copias. Las existentes se utilizan hasta el final de su vida útil, sin que se haya establecido la cantidad máxima de veces que pueden ser reescritas. Además, no se encuentran establecidos en el PAMI parámetros de RPO[25] ni RTO[26].

[25] Volumen de datos en riesgo de pérdida que la organización considera tolerable.
[26] Tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad de sus tareas.

Por su parte, la obsolescencia de los discos donde se procesan las copias de respaldo ocasionalmente impide que las tareas se realicen adecuadamente.

Una vez hechas las copias de respaldo, las cintas se almacenan en cajas ignífugas que se ubican en el edificio de Nivel Central. Dado que el espacio resulta insuficiente para almacenarlas en su totalidad, las restantes se alojan en el edificio donde se encuentra el Data Center del Instituto.

Se constató que la infraestructura en general acusa cierto grado de obsolescencia y se verifican fallas de *hardware*, tanto de los dispositivos de *storage pool* primarios de discos, como de las librerías de cintas. El *software* y el *hardware* se encuentran sin contrato de mantenimiento externo.

La infraestructura actual no cuenta con la capacidad de almacenamiento para respaldar bases de datos de grandes dimensiones (superiores a los 2TB). A modo de ejemplo, la base de Trazabilidad de Medicamentos tiene un tamaño aproximado de 7 Tb, mientras que el tamaño aproximado del Padrón de Afiliados es de 4 Tb.

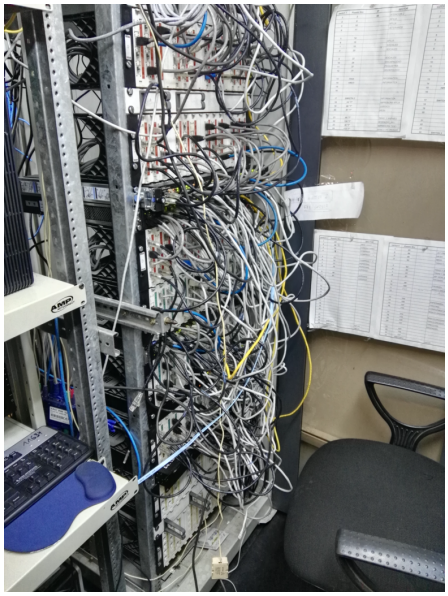
Las mejores prácticas para la seguridad de la información indican que la falta de difusión y aplicación de una política clara de resguardo de datos acarrea el riesgo de depender de personal clave para la realización de las tareas y el no cumplimiento estricto del procedimiento, de forma tal que ante cualquier incidente no se disponga de las copias de respaldo necesarias para asegurar la continuidad de las tareas (CobIT v4.1 – DS4.9: Almacenamiento de respaldos fuera de las instalaciones; ISO/IEC 27001).

4.3.4. *Se observó equipamiento obsoleto e instalaciones no adecuadas y en mal estado en distintas UGL ubicadas en el Área Metropolitana de Buenos Aires. Esta situación aumenta el riesgo de sufrir indisponibilidades en el sistema y perjudicar la atención de los beneficiarios.*

El equipamiento informático utilizado por los agentes del PAMI en las UGL de Quilmes, San Justo y Morón, es obsoleto. A modo de ejemplo, en la UGL de Morón se opera con PCs algunas de las cuales tienen doce años de antigüedad. Como por su antigüedad ya no existen repuestos, se utilizan partes de equipos fuera de servicio. También pudo verificarse la ausencia de UPS que suministren energía para los

momentos en que el suministro de red eléctrica domiciliaria se encuentre interrumpido y el mal estado general de las instalaciones de red de datos (véase imágenes a continuación):

Ilustración Nº 4 - Rack de Comunicaciones UGL San Justo

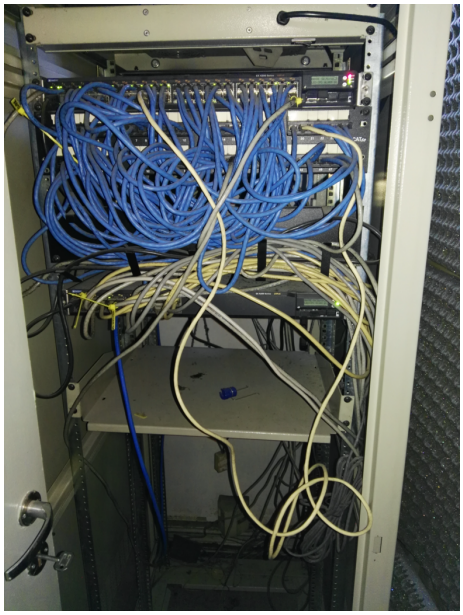


Fuente: imágenes obtenidas por la AGN

Ilustración N° 5 - Rack de Comunicaciones UGL Morón

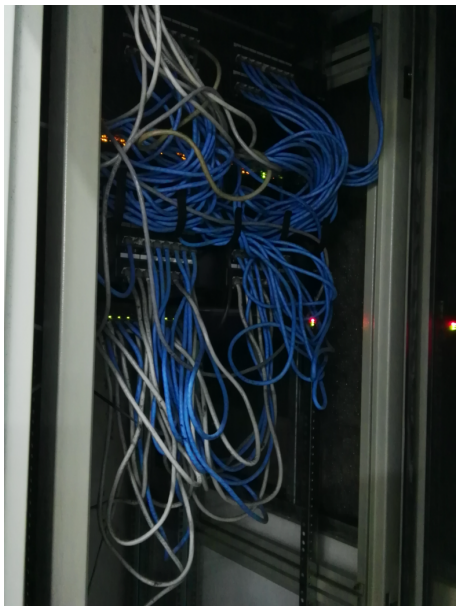
Fuente: imágenes obtenidas por la AGN

Ilustración N° 6 - Rack de comunicaciones UGL Morón



Fuente: imágenes obtenidas por la AGN

Ilustración N° 7 - Rack de comunicaciones UGL Morón



Fuente: imágenes obtenidas por la AGN

INFORME DE AUDITORÍA

Las organizaciones deben contar con instalaciones bien diseñadas y administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del CPD, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico (CobIT v4.1 - DS12.2-5: Administración del ambiente físico). Además, se debe desarrollar y ejecutar un plan de mantenimiento preventivo del hardware con el fin de reducir la frecuencia y el impacto de las fallas que pongan en riesgo la continuidad del servicio (CobIT v4.1 - DS13.5: Mantenimiento Preventivo del Hardware, y Resolución 48/05-SIGEN: 8.3).

El estado actual del equipamiento y las instalaciones de las redes de datos no permiten asegurar la disponibilidad de los sistemas informáticos del PAMI en las oficinas de las UGL o en las agencias, lo que aumenta el riesgo de fallas o salidas de servicio imprevistas que perjudiquen la normal atención de los beneficiarios.

4.4. Estabilidad

4.4.1. No *existe un procedimiento que defina el criterio de aceptación de requerimientos de nuevos desarrollos de software o cambios en las aplicaciones existentes. Esta situación aumenta el riesgo de que se detecten errores o se produzcan fallos que retrasen su puesta en producción y afecten la estabilidad del SII.*

Ante la necesidad de las áreas usuarias de realizar cambios en las aplicaciones existentes o nuevos desarrollos de software, la solicitud se registra mediante una herramienta de gestión de desarrollo de proyectos denominada JIRA. La Subgerencia de Control de la Demanda, dependiente de la Gerencia de Sistemas, toma el requerimiento y de acuerdo a su envergadura se reúne con un interlocutor del área usuaria con el fin de definir las especificaciones funcionales del pedido. Si la tarea es de menor envergadura directamente se comienza con la etapa de análisis. No existe una definición que delimite cuándo se utiliza uno u otro procedimiento, ni un documento donde quede formalizada la aceptación del

diseño por el usuario en todos los casos. Sólo en algunos desarrollos la aprobación queda registrada en el JIRA.

Las buenas prácticas señalan la necesidad de definir el criterio de aceptación y aprobación de los requerimientos para garantizar que el diseño de alto nivel[27] responde a los requerimientos (CobIT v4.1 - AI2: Adquirir y mantener software aplicativo).

La situación actual no asegura que los requerimientos realizados por las áreas usuarias se conviertan en desarrollos adecuados para la función para la que fueron solicitados, aumentando el riesgo de tener que realizar modificaciones en el software y retrasando su puesta en producción.

4.4.2. *No existen procedimientos para la administración de los entornos de desarrollo, prueba, control de calidad y pase a producción con controles adecuados, lo que aumenta la probabilidad de que se produzcan fallas o no se detecten errores en la etapa de pase a producción. Estos fallos afectan principalmente a la estabilidad del sistema, mientras que las salidas de servicio no planificadas pueden afectar la atención de los beneficiarios.*

De los análisis realizados y la documentación suministrada por el auditado se observa que no existen procedimientos formales que definan la utilización de distintos entornos dentro del proceso de diseño y desarrollo de sistemas. Al respecto, con posterioridad a la etapa de análisis funcional, los proyectos se derivan al área de desarrollo donde los programadores trabajan sobre un entorno que administran ellos mismos hasta que finalizan la etapa. Las pruebas a las que son sometidos los desarrollos son realizadas por los mismos programadores y solo en algunos casos de mayor envergadura se realizan consultas al área que realizó la solicitud para que preste conformidad a la tarea realizada. A través de la herramienta JIRA, el Departamento de Diseño y Desarrollo de Sistemas Prestacionales de la Gerencia de Sistemas le informa al Departamento de Operaciones de la Gerencia de Infraestructura Tecnológica que el desarrollo está listo para ser puesto en producción.

[27] En el diseño de alto nivel se describen los componentes principales del sistema y el modo en que interactúan entre sí para lograr los objetivos del requerimiento.

INFORME DE AUDITORÍA

Todos los cambios en los sistemas -incluido el mantenimiento de emergencia- deben ser administrados formal y controladamente. Además, se debe definir y establecer un entorno seguro de pruebas que sea representativo del entorno de operaciones (CobIT v4.1 - AI6: Administrar cambios; y AI7: Instalar y acreditar soluciones y cambios).

La falta de una administración adecuada de los distintos entornos aumenta el riesgo de no detectar errores y fallas en la implementación de aplicaciones o cambios cuando son puestas en producción.

4.4.3. *El Procedimiento de Gestión de Cambios no es aplicado por las distintas áreas de análisis y desarrollo. Ello incrementa el riesgo de que se produzcan fallas en la implementación de cambios o modificaciones no autorizadas en los sistemas que pueden, en casos extremos, producir la salida de servicio del sistema.*

Del análisis realizado y la documentación suministrada por el organismo se verifica la existencia de un procedimiento formalmente aprobado de gestión de cambios que no se aplica: PGSI-10 Procedimiento de Gestión de Cambios.

El Departamento de Seguridad Informática, dependiente de la Gerencia de Infraestructura Tecnológica, no realiza análisis de seguridad de las modificaciones a incluir en una aplicación, dado que por razones de urgencia generalmente el desarrollo debe estar operativo a la mayor brevedad. El auditado informó que, ocasionalmente, los desarrollos fueron pasados al entorno de producción sin un adecuado plan de análisis previo a su implementación.

Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formal y controladamente (CobIT v4.1 - AI6: Administrar cambios).

La situación descripta, sumada a la falta de controles eficaces en las etapas de desarrollo, genera el riesgo de que un sistema quede fuera de servicio. El riesgo se incrementa si el desarrollo es implementado un viernes por la tarde, dado que las áreas de desarrollo no prevén guardias y recién podrán resolver un eventual problema a partir del lunes siguiente.

El apartamiento de las buenas prácticas indicadas apareja un aumento en el riesgo de implementar modificaciones sin pruebas necesarias, lo que tiene como consecuencia que se produzcan fallas o salidas de servicio no planificadas.

4.4.4. *El PAMI no cuenta con un área específica a cargo del monitoreo y aseguramiento de la calidad, lo que incrementa el riesgo de existencia de errores no detectados y fallas, y, en casos extremos, puede ocasionar la salida de servicio no prevista de los sistemas.*

De las entrevistas realizadas surge que no existe un área de control de calidad separada de las áreas de desarrollo que tenga como función el control y aseguramiento de la calidad de los desarrollos de *software* realizados.

El proceso de control de calidad no está definido dentro del ciclo de vida de desarrollo de *software*. Durante la etapa de desarrollo, el programador realiza de manera informal las pruebas que considera adecuadas, teniendo en cuenta un grupo de pruebas publicadas en una herramienta de colaboración denominada *Confluence*. Del análisis de la documentación almacenada surge que los procedimientos descriptos no son suficientes para garantizar un adecuado nivel de calidad en el *software* desarrollado (no contemplan una instancia de pruebas independientes). Una vez terminado el desarrollo, se implementa en un entorno de Aseguramiento de la Calidad (QA por sus siglas en inglés) en el que se realizan las pruebas de integración, donde en algunas ocasiones son los propios desarrolladores los que verifican el funcionamiento del *software* realizado.

Por su parte, el Departamento de Gestión de la Demanda, dependiente de Gerencia de Sistemas, aunque cuenta con personal capacitado, no integran un sector formal para realizar pruebas de calidad de los desarrollos.

Las buenas prácticas indican que se debe establecer y mantener un sistema de administración de la calidad que proporcione un enfoque estándar, formal y continuo, con respecto a la administración de la calidad. Éste debe identificar los requerimientos y los criterios de calidad, los procesos claves de TI, y su secuencia e interacción, así como las políticas, criterios y métodos para definir, detectar, corregir y prever las no conformidades. También debe definir la estructura organizacional para la administración de la calidad, cubriendo los roles, las tareas y las responsabilidades. Las áreas clave deben desarrollar sus planes de calidad de acuerdo con los criterios y las políticas, y registrar los datos de calidad (CobIT v4.1 - PO8: Administrar la calidad).

La falta de un área específica dedicada al monitoreo y aseguramiento de la calidad, aumenta el riesgo de fallos o salidas de servicio no previstas que afecten la atención de los beneficiarios del PAMI.

5. RECOMENDACIONES

Las recomendaciones aquí expuestas siguen la secuencia de las observaciones.

5.1. Seguridad de la información

5.1.1. Revisar, actualizar y aplicar una política de Seguridad de la Información acorde a la envergadura del organismo y los riesgos inherentes a su negocio. Realizar las tareas necesarias para que sea conocida y utilizada por todos los agentes del organismo.

5.1.2. Asignar a la función Seguridad de la Información una posición acorde a su importancia e independiente de las áreas informáticas a las cuales debe controlar.

5.1.3. *RESERVADO COLEGIO DE AUDITORES GENERALES*

5.1.4. Implementar una metodología que permita una ingeniería de roles y perfiles de todo el organismo, a fin de garantizar la seguridad de la información y minimizar los riesgos de fraude informático.

5.1.5. Diseñar, aprobar e implementar un procedimiento que garantice la realización de análisis de seguridad de los requerimientos técnicos y funcionales, de forma tal de asegurar la integridad, confidencialidad y disponibilidad de la información de acuerdo con lo establecido en la Política de Seguridad del PAMI.

5.1.6. Implementar un sistema alternativo de control de los parámetros ambientales de tal manera que se minimicen los riesgos de no detección de anomalías ambientales.

5.1.7. *RESERVADO COLEGIO DE AUDITORES GENERALES*

5.2. Integridad de los datos

5.2.1. Generar un Diccionario de Datos único y completo del PAMI, que sea periódicamente actualizado y que incluya las reglas de sintaxis de los datos de la organización.

5.2.2. Implementar controles y validaciones en los sistemas que impidan la carga de datos erróneos. Asimismo, iniciar las acciones que corresponda tendientes a evaluar la eventual existencia de responsabilidades de funcionarios o agentes vinculados al registro y permanencia de datos inconsistentes en el Padrón de Afiliados, sus derivaciones en términos de perjuicio fiscal y las medidas conducentes a su recupero.

INFORME DE AUDITORÍA

5.3. Disponibilidad de los datos

5.3.1. Desarrollar, aprobar, e implementar un Plan de Continuidad de Servicios de TI y un Plan de Recuperación de Desastres (DRP) que aseguren la continuidad de los servicios asociados a la atención de los beneficiarios ante salidas de servicios no planificadas o catástrofes que puedan presentarse.

5.3.2. Implementar redundancia geográfica del CPD del PAMI. Adecuar los contratos de mantenimiento de forma tal de cubrir todos los eventos que puedan producirse, como la recarga de los cilindros de extinción y la instalación de cilindros provisorios para estos casos. Establecer indicadores adecuados con el fin de monitorear y evaluar la gestión de la administración de las instalaciones.

5.3.3. Establecer procedimientos que protejan al PAMI contra la pérdida de información, de forma de asegurar su disponibilidad ante cualquier incidente que se produzca. Para ello se deben realizar y probar regularmente copias de respaldo que incluyan toda la información necesaria (datos y *software*) para restablecer el servicio ante su pérdida.

5.3.4. Definir e implementar un procedimiento para que se evalué cada cierto tiempo la obsolescencia y tendencias tecnológicas sobre la infraestructura informática, tal que permita asegurar que la totalidad del parque de PC se renueve periódicamente conforme a los estándares del sector. Adecuar las instalaciones de red de forma tal que se cumpla con las buenas prácticas.

5.4. Estabilidad

5.4.1. Implementar un procedimiento formal para la aceptación de los requerimientos de cambios a aplicaciones existentes o de desarrollos nuevos, de forma tal que se asegure que el diseño de alto nivel cumpla con las necesidades del área que lo solicitó.

5.4.2. Implementar procedimientos para la administración de los entornos de desarrollo, prueba, control de calidad y pase a producción con controles adecuados.

5.4.3. Implementar un procedimiento formal de control de cambios que contemple elementos tales como cambios de emergencias**,** la asignación de prioridades y autorización de cambios, entre otros. Los cambios se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación.

5.4.4. Establecer y mantener un procedimiento para la administración de la calidad que proporcione un enfoque estándar, formal y continuo en el desarrollo e implementación de los sistemas.

6. CONCLUSIONES

El Sistema Interactivo de Información (SII) forma parte de la plataforma tecnológica de PAMI destinada a gestionar diversos servicios que presta a sus afiliados. El SII es utilizado por alrededor de 13.000 usuarios internos, y por prestadores externos y afiliados para realizar consultas. Entre sus módulos se destacan el Padrón de Afiliados, que administra los datos de casi cinco millones de afiliados, y el de Prestaciones Médicas, por el que se gestionan aproximadamente 12 millones de prestaciones mensuales. La auditoría se centró en cuatro ejes principales: 1) seguridad de la información, 2) integridad de los datos, 3) disponibilidad de los datos, y 4) estabilidad del sistema; aspectos que impactan sobre la confiabilidad de la información y la eficiencia de la atención de los beneficiarios.

Los principales hallazgos en materia de seguridad refieren fallas en el cumplimiento de las Políticas de Seguridad de la Información, una inadecuada ubicación del Departamento de Seguridad Informática en la estructura orgánica de PAMI para las tareas de control que debe realizar, y una inadecuada gestión de roles y perfiles de usuarios. *[RESERVADO COLEGIO DE AUDITORES GENERALES]* Se suma a ello que no se realizan análisis de seguridad informática de los requerimientos de nuevos desarrollos o para realizar cambios en las aplicaciones existentes.

INFORME DE AUDITORÍA

En cuanto a la integridad de los datos, de las pruebas realizadas sobre el sistema y de análisis realizados sobre extracciones de datos de la base, se desprende que el SII no brinda información consistente y exacta. Entre las inconsistencias detectadas puede mencionarse la existencia de beneficiarios con doble afiliación, beneficiarios fallecidos que figuran como activos, beneficiarios con el CUIT/CUIL en ceros, beneficiarios con datos incompletos o incorrectos, familiares de beneficiarios que no cumplen las condiciones para recibir beneficios del PAMI, entre otras.

En otro orden, la disponibilidad de los datos se encuentra comprometida por la falta de un Plan de Continuidad de Servicios de TI y de un Plan de Recuperación de Desastres (DRP). También se incrementa el riesgo para la disponibilidad y continuidad del servicio por la inexistencia de un Centro de Procesamiento de Datos alternativo, además de fallas en la gestión del sistema de extinción de incendios de la Sala Cofre y del Data Center. Se destaca en este sentido que en visitas realizadas a distintas UGL del Gran Buenos Aires se observó equipamiento obsoleto e instalaciones en mal estado. Este conjunto de factores pone en riesgo la atención de los beneficiarios ante salidas de servicio no planificadas de los sistemas.

De los procedimientos realizados para verificar la estabilidad del SII surgió que no existe un criterio definido para la aceptación de requerimientos de nuevos desarrollos de software o de cambios en las aplicaciones existentes. Se observó también que PAMI no cuenta con un área específica a cargo del monitoreo y aseguramiento de la calidad, lo que incrementa el riesgo de errores no detectados y de fallas que en casos extremos pueden ocasionar la salida de servicio no prevista de los sistemas.

El conjunto de vulnerabilidades detectadas sobre el SII en su calidad de sistema central para la atención de la salud de un sector vulnerable de la población, pone en evidencia que resulta indispensable que el Instituto de Servicios Sociales para Jubilados y Pensionados implemente en forma urgente un plan de mejoras que enfatice el aseguramiento de la disponibilidad de la información, sin desatender la mejora de

los restantes aspectos señalados que hacen a la confiabilidad de la información que el PAMI administra, en pos de garantizar una eficiente atención de los beneficiarios.

7. COMUNICACIÓN AL ENTE

Por Nota N° 973/19-P del 29 de octubre de 2019 la AGN remite el proyecto de informe al Instituto de Servicios Sociales para Jubilados y Pensionados recibida el 30 de octubre de 2019. El 22 de noviembre de 2019 el Instituto de Servicios Sociales para Jubilados y Pensionados envía sus comentarios, recibidos el mismo día.

Producto del análisis de los comentarios recibidos, en el hallazgo 4.3.4. se modifica el pasaje que dice: "*A modo de ejemplo, el parque de PCs de la UGL Morón tiene una antigüedad promedio de 12 años*", por el siguiente: "*A modo de ejemplo, en la UGL de Morón se opera con PCs algunas de las cuales tienen doce años de antigüedad"*.

Adicionalmente, se complementa el texto original de la recomendación 5.2.2 con la siguiente frase: "Asimismo, iniciar las acciones que corresponda tendientes a evaluar la eventual existencia de responsabilidades de funcionarios o agentes vinculados al registro y permanencia de datos inconsistentes en el Padrón de Afiliados, sus derivaciones en términos de perjuicio fiscal y las medidas conducentes a su recupero".

En el ANEXO II al presente informe, en orden simultáneo, se presentan tanto la respuesta del organismo auditado como los comentarios de la AGN.

INFORME DE AUDITORÍA

8. LUGAR Y FECHA

BUENOS AIRES, abril de 2020

9. FIRMA

Firmado digitalmente por RUBIONE Martín Pablo
Fecha: 2020.04.21 '16:39:16 -03'00

Lic. Martín Rubione
Jefe de Departamento de Auditoría Informática
AUDITORÍA GENERAL DE LA NACIÓN

Firmado digitalmente por PRATAVIERA Gerarado Gabriel
Fecha: 2020.05.07 '10:54:01 -03'00

Cdor. Gerardo Prataviera
Gerente de Planificación y Proyectos Especiales
AUDITORÍA GENERAL DE LA NACIÓN

10. ANEXOS

Anexo I – Comentario del auditado

ADMGS-389

FOLIO

PAMI

Instituto Nacional de Servicios Sociales para Jubilados y Pensionados
2019 - Año de la Exportación

Providencia de Sala

Número: IF-2019-103332394-INSSJP-GS#INSSJP

CIUDAD DE BUENOS AIRES
Miércoles 20 de Noviembre de 2019

Referencia: Respuesta a Prov. N° 555/SDE/2019 (PV-2019-99256022-INSSJP-SE#INSSJP –Fs. 4) - SOBRE CERRADO N° 142/2019-00352A - PROV 2082/USA/2019 (PV-2019-9833696-INSSJP-DE#INSSJP) - Auditoria SII - Nota 973/19 AGN (ADMGS-389)

A: SUBDIRECCIÓN EJECUTIVA

En el marco del Proyecto de Informe de Auditoria emitido por la Auditoria General de la Nacion (AGN), el cual versa sobre el "Sistema Interactivo de Informacion (SII) y Sistemas relacionados, la Gerencia de Sistemas efectúa las siguientes observaciones y/o consideraciones:

Punto 2.4.3 – (Página 5) ***"… No fue posible presenciar la ejecución de las consultas solicitadas a la base de datos productiva, lo que impide asegurar la integridad de los datos suministrados…"***

Al respecto se informa que el INSSJP designó agentes destinados a la ejecución de los queries, los cuales estuvieron en contacto con los auditores de la AGN y ejecutaron los mismos ante su presencia siempre que ello resultara posible en virtud de la dimensión del procesamiento.

En aquellos casos en que resultó necesario el procesamiento de las consultas por el área de Operaciones (en función de las causales descriptas por la AGN en el Proyecto), se documentó el modo en que se llevó a cabo la ejecución.

Página 22 – ***"… No existe un adecuado proceso de bajas de beneficiarios que impida que personas fallecidas sigan figurando en el padrón como beneficiarios activos …"***

Esta Gerencia no comparte tal criterio, ya que en función de las medidas adoptadas por el INSSJP para evitar la citada situación (las cuales fueron puestas en conocimiento de las instancias de contralor cuando lo han requerido), se ha logrado un avance significativo en el proceso tendiente a impedir que personas fallecidas continuen figurando en el padrón como beneficiarios activos.

A su vez, respecto a las recomendaciones realizadas por la AGN a lo largo del informe, se pone en conocimiento que toda medida a adoptar para dar solución a lo que se estime corresponder deberá ser solicitado a esta instancia

JUAN MARTÍN DE ESTRADA
JEFE DE DEPARTAMENTO
SEGUIMIENTO DE GESTION
DIRECCIÓN EJECUTIVA
ES COPIA FIEL

Auditoría General de la Nación

INFORME DE AUDITORÍA

por el área dueña del dato a través del proceso interno de Gestión de la demanda destinado a ello, lo cual deberá ser oportunamente priorizado debido a que las mismas representan tareas de largo plazo.

Atentamente,

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2019.11.19 16:23:25 -03:00

ALEJANDRO JAVIER REGUEIRO
Subgerente
Gerencia de Sistemas
Instituto Nacional de Servicios Sociales para Jubilados y Pensionados

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2019.11.20 12:08:29 -03:00

Fernando Carlos Spena
Gerente
Gerencia de Sistemas
Instituto Nacional de Servicios Sociales para Jubilados y Pensionados

Nota Nº 189/GS/19 - 3001A

INSTITUTO NACIONAL DE SERVICIOS SOC. PARA JUBILADOS Y PENSIONADOS
SALIÓ
20 NOV 2019
GERENCIA DE SISTEMAS

INSTITUTO NACIONAL DE SERVICIOS SOC. PARA JUBILADOS Y PENSIONADOS
ENTRÓ
21 NOV 2019
SUBDIRECCIÓN EJECUTIVA

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2019.11.20 12:08:31 -03:00

INFORME DE AUDITORÍA

Instituto Nacional de Servicios Sociales para Jubilados y Pensionados
2019 - Año de la Exportación

Informe firma conjunta

Número: IF-2019-103677487-INSSJP-GIT#INSSJP

CIUDAD DE BUENOS AIRES
Jueves 21 de Noviembre de 2019

Referencia: Respuesta a REGISTRO 40/SDE/2019 (PV-2019-99256022-INSSJP-SE#INSSJP) - Prov. N° 555/SDE/2019 (PV-2019-99256022-INSSJP-SE#INSSJP) - PROV 2082/USA/2019 (PV-2019-9833696-INSSJP-DE#INSSJP) - Auditoria Sistemas interactivos de Información (SII) - Nota 973

A: SUBDIRECCION EJECUTIVA

En el marco del Proyecto de Informe de Auditoria emitido por la Auditoria General de la Nacion (AGN), el cual versa sobre el "Sistema Interactivo de Informacion (SII) y Sistemas relacionados, la Gerencia de Infraestructura Tecnológica efectúa las siguientes observaciones y/o consideraciones:

- **Subgerencia de Gestión de la Demanda Distribuida**

Punto 4.3.4 - ***"... El parque de PCs de la UGL Morón tiene una antigüedad promedio de 12 años..."***

El promedio de antigüedad del parque de PCs es inferior a 12 (doce) años.

- **Departamento de Seguridad Informática**

Punto 4.1.1 - ***"... La Política de Seguridad de la Información, no es aplicada correctamente ni fue eficazmente comunicada a los agentes del organismo, lo que pone en riesgo la integridad de la información almacenada en las bases de datos del SII..."***

En lo que respecta al SII, la política de seguridad es aplicada en todos los circuitos de ABM de usuarios, roles y perfiles, implementando segregación de funciones entre el usuario, el dueño de datos autorizante y el Departamento de Seguridad Informática como autorizante en el alta.

Asimismo, la política recomienda aplicar controles y mecanismos tendientes a garantizar la confidencialidad, disponibilidad e integridad de la información, los cuales están disponibles para todas las áreas que quieran implementarlos dentro de su marco.

JUAN MARTIN DE ESTRADA
JEFE DE DEPARTAMENTO
SEGUIMIENTO DE GESTION
DIRECCIÓN EJECUTIVA
I.N.S.S.J.P.

ES COPIA FIEL

INFORME DE AUDITORÍA

Desde su aprobación inicial, la Política de Seguridad de la Información se encuentra publicada en la intranet del Instituto. Su difusión se brinda en forma periódica, de acuerdo al plan de concientización de usuarios, a través de noticias vía correo electrónico, gacetillas emitidas en Intranet y resúmenes enviados junto al recibo de cobro.

A su vez, en la plataforma de e-learning se encuentra disponible el curso de Seguridad Informática, el cual está basado en las políticas de seguridad para el conocimiento de todo el personal. Este fue el primer curso en la plataforma de e-learning del Instituto.

Corresponde indicar que tanto la Resolución 48/05 de la SIGEN como las resoluciones 566/03 y 1406/05 del INSSJP, son parte de los considerandos del Manual de Políticas, vigentes por la disposición 2/GITC/2015, que da soporte y vigencia a la misma, y por lo tanto, son aplicadas.

La División Normas y Políticas de Seguridad Informática, tiene entre sus responsabilidades la revisión, actualización e implementación de las políticas y procedimientos. Cada uno de los procedimientos tienen un responsable, los cuales deben informar los cambios realizados en los circuitos para poder así realizar el mantenimiento y actualización de la política y sus procesos, dentro del plan de revisión permanente.

Asimismo, y dado el limitado número de recursos con los que cuenta el Departamento de Seguridad Informática, se encuentra en análisis promover una contratación de servicios de consultoría a los fines de posibilitar la implementación del plan de actualización y ampliación de la Política actual.

Punto 4.1.3 – "...*La gestión de roles y perfiles de usuarios del SII no es adecuada, ni se lleva adelante una metodología de seguimiento y control permanente sobre la actividad de los usuarios, con riesgo para la integridad, confidencialidad y disponibilidad de la información...*".

De acuerdo a lo establecido en el Manual de Políticas de Seguridad de la Información (Aprobadas por Disposición 002/GITC/2015), en el "Punto 7 - Gestión de Activos" se establece que los Propietarios de los Activos de la información, que en la generalidad de los casos es la máxima autoridad de la gerencia de la cual depende cada activo, son los encargados y/o responsables de:

- Clasificarlos de acuerdo con su grado de sensibilidad y criticidad.
- Documentar y mantener actualizada la clasificación efectuada.
- Definir las funciones que deben tener permisos de acceso a los activos.
- Mantener los controles adecuados para garantizar su seguridad.

Es decir, los Propietarios de los Activos de la información son la máxima autoridad del sistema y los encargados de designar a la persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.

A su vez, el dueño de Datos es el personal del Instituto responsable de administrar los datos de una Aplicación, Sistema y/o Plataforma, constando ello en:

- Clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma.
- Documentar y mantener actualizada la clasificación efectuada.
- Definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

Cada sistema tiene un único dueño de datos (clasificado como Nivel 1), el cual puede designar dueños de datos de Nivel 2 como colaboradores en la tarea.

Punto 4.1.5 – *"... No se realiza un adecuado análisis de Seguridad Informática de los requerimientos técnicos y funcionales para desarrollos o cambios en las aplicaciones existentes. De este modo se incrementa el riesgo de permitir el acceso no autorizado a los sistemas, a las redes de los datos y a los equipos conectados a ella, comprometiendo la integridad, disponibilidad y confidencialidad de la información...".*

Actualmente el Departamento de Seguridad Informática se encuentra participando desde el inicio en los nuevos proyectos y se ha puesto énfasis en realizar un análisis de seguridad en forma previa a la salida a producción de los sistemas, como así también el participar en la confección de pliegos técnicos.

Punto 4.1.7 – *"... El PAMI no aplica adecuadamente los controles establecidos en la política de administración de cuentas de usuarios del SII, con riesgo para la integridad y confidencialidad de los datos almacenados... ".*

Actualmente se está llevando a cabo un proyecto de reingeniería de accesos a las bases de datos.

- **Subgerencia de Planificación de Infraestructura**

Punto 4.3.3

Respecto a lo manifestado a lo largo del presente punto por la AGN, se informa que el INSSJP ha migrado la plataforma de backup corporativos a IBM Spectrum Protect a partir de Agosto 2019.

De esta manera se logró recuperar y mejorar la capacidad de procesamiento y ventanas necesarias para resguardo y recuperación del volumen de información corporativa, sobre nuevas tecnologías, con 2 nuevos servidores físicos en Cluster, logrando HA sobre la plataforma, con un nuevo Storage IBM Storwize V5030 dedicado para la gestión de copias de resguardo y recuperación.

Asimismo, se realizó el upgrade de la librería High End IBM TS3584 con 8 Drives LTO7 de mayor capacidad y vida útil a lo largo del tiempo, además de la gestión completa de la doble copia de resguardo en cintas almacenadas en un armario ignífugo con capacidad suficiente para contener la doble copia off-site.

Toda la nueva plataforma cuenta con soporte y mantenimiento por los próximos 3 años, tanto de software como del hardware.

La infraestructura actual cuenta con licenciamiento y capacidad para almacenar 200 TeraByte de Front End, sin importar cuantas copias sean tomadas de una misma BD, para todos los clientes requeridos, tanto en el ambiente de BD, entorno virtual, de correo, SharePoint, etc.

A partir de esta nueva implementación se está trabajando para difundir todas las políticas de resguardo actualmente vigentes. Las mismas serán publicadas en los próximos meses, en la Intranet del Instituto, previa validación y ratificación por los dueños de datos.

JUAN MARTIN DE ESTRADA
JEFE DE DEPARTAMENTO
SEGUIMIENTO DE GESTIÓN
DIRECCIÓN EJECUTIVA
I.N.S.S.J.P.

ES COPIA FIEL

INFORME DE AUDITORÍA

Atentamente,

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2019.11.20 18:19:54 -03:00

CLAUDIO VILLAMONTE
Subgerente
Gerencia de Infraestructura Tecnológica
Instituto Nacional de Servicios Sociales para Jubilados y Pensionados

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2019.11.20 18:50:27 -03:00

GERMAN ARIEL PASOS
Subgerente
Gerencia de Infraestructura Tecnológica
Instituto Nacional de Servicios Sociales para Jubilados y Pensionados

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2019.11.21 11:02:02 -03:00

FERNANDO PABLO RAYA
Jefe de Departamento
Gerencia de Infraestructura Tecnológica
Instituto Nacional de Servicios Sociales para Jubilados y Pensionados

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2019.11.21 11:05:37 -03:00

DIEGO CARLOS AIETA
Gerente
Gerencia de Infraestructura Tecnológica
Instituto Nacional de Servicios Sociales para Jubilados y Pensionados

NOTA: 849/2019/3501A

INSTITUTO NACIONAL DE SERVICIOS SOC PARA JUBILADOS Y PENSIONADOS
SALIÓ
21 NOV 2019
GERENCIA DE INFRAESTRUCTURA TECNOLÓGICA

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2019.11.21 11:05:39 -03:00

Anexo II – Análisis de los comentarios del auditado

Sección del Informe	Comentario del Auditado	Análisis del Comentario
2.4.3. *No fue posible presenciar la ejecución de las consultas solicitadas a la base de datos productiva, lo que impide asegurar la integridad de los datos suministrados.* Durante la etapa de ejecución se coordinó con el auditado un procedimiento orientado a recabar evidencia sobre inconsistencias en los datos almacenados mediante la ejecución de consultas a la base de datos del SII. Las consultas fueron ejecutadas por el área de operaciones del organismo, que suministró los resultados en archivos en formato de texto y tablas de Excel. El equipo de auditoría no pudo presenciar el procesamiento de las consultas dado que su ejecución, en algunos casos, requería más de un día de procesamiento, mientras que en el resto de los casos se realizaron durante intervalos de baja demanda de procesamiento del sistema. En virtud de ello no fue posible asegurar la integridad de los datos obtenidos.	Punto 2.4.3 — (Página 5) *"... No fue posible presenciar la ejecución de las consultas solicitadas a la base de datos productiva, lo que impide asegurar la integridad de los datos suministrados..."* Al respecto se informa que el INSSJP designó agentes destinados a la ejecución de los queries, los cuales estuvieron en contacto con los auditores de la AGN y ejecutaron los mismos ante su presencia siempre que ello resultara posible en virtud de la dimensión del procesamiento. En aquellos casos en que resultó necesario el procesamiento de las consultas por el área de Operaciones (en función de las causales descriptas por la AGN en el Proyecto), se documentó el modo en que se levé a cabo la ejecución.	La respuesta del auditado no contradice lo expuesto. Se mantiene la limitación.
4.1.1. *La Política de Seguridad de la Información no es aplicada correctamente ni fue eficazmente comunicada a los agentes del organismo, lo que pone en riesgo la integridad de la información almacenada en las bases de datos del SII.* De las reuniones mantenidas con los responsables de distintas áreas de la Gerencia de Sistemas y de la Gerencia de Infraestructura Tecnológica surge que en algunos casos se desconoce la existencia del documento que formaliza las Políticas de Seguridad de la Información MGSI-02 aprobado por la Disposición N° 2/2015/GITC emitida por la Gerencia de Infraestructura Tecnológica, y que en otros casos no se aplica. A modo de ejemplo, el Comité de Seguridad de la Información previsto en el manual respectivo, no se encuentra en funcionamiento. Adicionalmente, ni la	**Punto 4.1.1 - "… La Política de Seguridad de la Información, no es aplicada, correctamente ni fue eficazmente comunicada a los agentes del organismo, lo que pone en riesgo la integridad de la información almacenada en las bases de datos del SII ..."** En lo que respecta al SII, la política de seguridad es aplicada en todos los circuitos de ABM de usuarios, roles y perfiles, implementando segregación de funciones entre el usuario, el dueño de datos autorizante y el Departamento de Seguridad informática como autorizante en el alta.	Si bien el auditado cuenta con mecanismos de difusión de la Política de Seguridad del Información, la comunicación no fue eficaz, puesto que en algunos casos se desconoce la existencia del documento que formaliza las Políticas de Seguridad de la Información, tal como se expone en el cuerpo del hallazgo. Por su parte, y, de acuerdo con entrevistas mantenidas con responsables del área de seguridad

INFORME DE AUDITORÍA

Sección del Informe	Comentario del Auditado	Análisis del Comentario
Resolución 48/05 SIGEN ni las Resoluciones N°0566 - 03 INSSJP y 1406 - 05 INSSJP son aplicadas. Se deben definir y comunicar todas las políticas, planes y procedimientos que dirigen los procesos de TI. Éstos deben estar documentados, revisados, mantenidos, aprobados, almacenados, comunicados y deben ser utilizados para el entrenamiento. También deben estar asignadas las responsabilidades para cada una de estas actividades y oportunamente, revisar si se ejecutan correctamente. Se debe asegurar que las políticas, planes y procedimientos son accesibles, correctos, entendidos y actualizados (CobIT v4.1 - PC5: Políticas, planes y procedimientos). El plan de seguridad de TI debe contemplar los requerimientos de negocio, los riesgos y el control del cumplimiento de las reglas establecidas en él (CobIT v4.1 - DS5.2 - Plan de Seguridad de TI). El incumplimiento de la Política de Seguridad de la Información o su incorrecta aplicación expone al organismo a un incremento en el riesgo de afectar los datos almacenados en la base de datos del SII por errores o acciones mal intencionadas.	Asimismo, la política recomienda aplicar controles y mecanismos tendientes a garantizar la confidencialidad, disponibilidad e integridad de la información, los cuales están disponibles para todas las áreas que quieran implementarlos dentro de su marco. Desde su aprobación inicial, la Política de Segundad de la Información se encuentra publicada en la intranet del Instituto. Su difusión se brinda en forma periódica, de acuerdo al plan de concientización de usuarios, a través de noticias vía correo electrónico, gacetillas emitidas en intranet y resúmenes enviados junto al recibo de cobro. A su vez, en la plataforma de e-learning se encuentra disponible el curso de Seguridad Informática, el cual está basado en las políticas de seguridad para el conocimiento de todo el personal. Este fue el primer curso en la plataforma de e-learning del Instituto. Corresponde indicar que tanto la Resolución 48/05 de la SIGEN como las resoluciones 566/03 o 1406/05 del INSSJP, son parte de los considerandos del Manual de Políticas, vigentes por la disposición 2/GITC/2015,	informática se tomó conocimiento entre otros puntos de: • La Comisión Revisora de Políticas de Uso, Manual de Seguridad Informática, Normas y Procedimientos, quedó sin efecto una vez finalizado el proceso de certificación de la Norma ISO27001. • El libro de actas, donde se volcaban las reuniones y novedades se dejó de utilizar una vez finalizado el proceso de certificación. • La División de Normas y Políticas de Seguridad, existe en la estructura de la Gerencia como parte del Departamento de Seguridad Informática, pero aún no tiene designado formalmente un responsable. • En el Manual de Políticas, existe un proceso llamado Gestión del Comité de Seguridad, que no se encuentra en funcionamiento, ya que la mayoría de sus miembros, no pertenecen actualmente a la planta del Instituto.

Sección del Informe	Comentario del Auditado	Análisis del Comentario
	que da soporte y vigencia a la misma y por lo tanto, son aplicadas. La División Normas y Políticas de Seguridad Informática, tiene entre sus responsabilidades la revisión, actualización e implementación de políticas y procedimientos. Cada uno de los procedimientos tienen un responsable, los cuales deben informar los cambios realizados en los circuitos para poder así realizar el mantenimiento y actualización de la política y sus procesos, dentro del plan de revisión permanente. Asimismo y dado el limitado número de recursos con los que cuenta el Departamento de Seguridad Informática, se encuentra en análisis promover una contratación de servicios de consultoría a los fines de posibilitar la implementación del plan de actualización y ampliación de la Política actual.	De acuerdo a lo expresado en este punto, y en el resto de los hallazgos se concluye que la aplicación de lo establecido en la Resolución 48/05 de la SIGEN no se cumple en su totalidad. Tomando en cuenta lo expresado y el análisis de roles y perfiles de usuarios del SII se mantiene el hallazgo.
4.1.3. *La gestión de roles y perfiles de usuarios del SII no es adecuada, ni se lleva adelante una metodología de seguimiento y control permanente sobre la actividad de los usuarios, con riesgo para la integridad, confidencialidad y disponibilidad de la información.* *RESERVADO COLEGIO DE AUDITORES GENERALES*	**Punto 4.1.3 - "… La gestión de roles y perfiles de usuarios del SII no es adecuada, ni se lleva adelante una metodología de seguimiento y control permanente sobre la actividad de los usuarios, con riesgo para la integridad, confidencialidad y disponibilidad de la información..."** De acuerdo a lo establecido en el Manual de Políticas de Seguridad de la Información (Aprobadas por Disposición 002/GITC/2015), en el "Punto 7 - Gestión de Activos" se establece que los Propietarios de los Activos de la información, que en la generalidad de los casos es la máxima autoridad de la gerencia de la	*RESERVADO COLEGIO DE AUDITORES GENERALES*

INFORME DE AUDITORÍA

Sección del Informe	Comentario del Auditado	Análisis del Comentario
[RESERVADO COLEGIO DE AUDITORES GENERALES *]* Según las mejores prácticas en gestión de usuarios, se debe garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de	cual depende cada activo, son los encargados y/o responsables de: • Clasificarlos de acuerdo con su grado de sensibilidad y criticidad. • Documentar y mantener actualizada la clasificación efectuada. • Definir las funciones que deben tener permisos de acceso a los activos. • Mantener los controles adecuados para garantizar su seguridad. A su vez, el dueño de Datos es el personal del Instituto responsable de administrar los datos de una Aplicación, Sistema y/o Plataforma, constando ello en: • Clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma. • Documentar y mantener actualizada la clasificación efectuada. • Definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia. Cada sistema tiene un único dueño de datos (clasificado como Nivel I), el cual puede designar dueños de datos de Nivel 2 como colaboradores de la tarea.	*RESERVADO COLEGIO DE AUDITORES GENERALES* Las insuficiencias y los riesgos detectados en el hallazgo no han sido controvertidos por el Auditado, por lo que no contradice lo expuesto por esta auditoría. Se mantiene el hallazgo

Sección del Informe	Comentario del Auditado	Análisis del Comentario
cuentas de usuario y sus privilegios relacionados, sean previstos en un conjunto de procedimientos del área responsable del tema. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema los privilegios de acceso para cada uno de los roles. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, y para casos normales o de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la organización deben acordarse contractualmente para todos los tipos de usuarios. Periódicamente se deben realizar revisiones de la gestión de las cuentas de usuario y los privilegios asociados (CobIT v4.1 - DS5.4: Administración de cuentas del usuario). Conforme surge de la evidencia obtenida, la gestión de usuarios y segregación de funciones de los roles asignados en el sistema es inadecuada por falta de un procedimiento de control y seguimiento, lo que compromete la confidencialidad, integridad y disponibilidad de la información.		
4.1.5. *No se realiza un adecuado análisis de seguridad informática de los requerimientos técnicos y funcionales para desarrollos o cambios en las aplicaciones existentes. De este modo se incrementa el riesgo de permitir el acceso no autorizado a los sistemas, a las redes de datos y a los equipos conectados a ella, comprometiendo la integridad, disponibilidad y confidencialidad de la información.* Si bien existe una política de seguridad de la información, dependiendo del sector, no se aplica o se aplica parcialmente, situación que fue observada en los procedimientos de solicitudes de cambio, requerimientos de nuevas aplicaciones o mejoras de las existentes. Las buenas prácticas indican que los responsables deben garantizar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad para alcanzar el cumplimiento de las políticas y normas de seguridad (ISO 27001, Anexo A, A.15.1.2).	**Punto 4.1.5 – "… No se realiza un adecuado análisis de Seguridad Informática de 1os requerimientos técnicos y funcionales para desarrollos o cambios en las aplicaciones existentes. De este modo se incrementa el riesgo de permitir el acceso no autorizado a los sistemas, a las redes de los datos y a los equipos conectados a ella, comprometiendo la integridad, disponibilidad y confidencialidad de la información..."** Actualmente el Departamento de Seguridad Informática se encuentra participando desde el inicio en los nuevos proyectos y se ha puesto énfasis en realizar un análisis de seguridad en forma previa a la salida a producción de los sistemas, como así también el participar en la confección de pliegos técnicos.	La respuesta del auditado no contradice lo expuesto en el hallazgo. Respecto de las acciones emprendidas, por tratarse de hechos posteriores al período auditado, eventualmente serán objeto de análisis en futuras labores de auditoría. Se mantiene el hallazgo.

INFORME DE AUDITORÍA

Sección del Informe	Comentario del Auditado	Análisis del Comentario
No aplicar o aplicar parcialmente la política de seguridad de la información vigente en los análisis de los requerimientos técnicos y funcionales, compromete la integridad, disponibilidad y confidencialidad de la información.		
4.1.7. *El PAMI no aplica adecuadamente los controles establecidos en la política de administración de cuentas de usuarios del SII, con riesgo para la integridad y confidencialidad de los datos almacenados*. Las mejores prácticas orientadas a la gestión de TI establecen la necesidad de que todos los usuarios sean identificables de manera unívoca (CobIT v4.1 - DS5.3: Administración de identidad; y DS5.4: Administración de cuentas del usuario). El PAMI cuenta además con normativa interna que incluye buenas prácticas en gestión de usuarios: la Disposición 0002-15-GITC (Manual de Política de Seguridad de la Información del INSSJP) y la Resolución 0566-03 (Política de Uso Aceptable de los Recursos Informáticos). De ellas se extrae que: los usuarios deben ser personalizados, deben identificarse y autenticarse unívocamente; todos los usuarios -incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos- deben tener un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable, a fin de garantizar la trazabilidad de las transacciones; y que los identificadores de usuario no deben dar ningún indicio del nivel de privilegio	**Punto 4.1.7 – "… El PAMI no aplica adecuadamente los controles establecidos en la política de administración de cuentas de usuarios del SII, con riesgo para la integridad y confidencialidad de los datos almacenados..."** Actualmente se está llevando a cabo un proyecto de reingeniería de accesos a las bases de datos.	La respuesta del auditado no contradice lo expuesto en el hallazgo. Respecto de las acciones emprendidas, por tratarse de hechos posteriores al período auditado, eventualmente serán objeto de análisis en futuras labores de auditoría. Se mantiene el hallazgo.

Sección del Informe	Comentario del Auditado	Análisis del Comentario
otorgado; entre otras relativas al control, monitoreo y reporte de actividades de usuarios. *[RESERVADO COLEGIO DE AUDITORES GENERALES* *]* La presencia de usuarios genéricos activos dificulta el control e imposibilita la identificación unívoca de las acciones que realizó cada individuo, con riesgos para la integridad y confidencialidad de los datos obrantes en el SII.		
4.2.2. *Los usuarios del SII no cuentan con información íntegra y exacta al momento de ejecutar los diferentes procesos del sistema, lo que aumenta el riesgo de que se produzcan perjuicios económicos al PAMI por el pago de cápitas indebidas y afecta la calidad de atención de los beneficiarios.* De las pruebas realizadas sobre el sistema y de análisis realizados sobre extracciones de datos de la base, se desprende que el SII no brinda información consistente y exacta al realizar operaciones sobre él. De los procedimientos de auditoría ejecutados sobre el sistema y del análisis de consultas realizadas a la base de datos del SII surge que: • no existen manuales de procedimientos ni procedimientos formalizados para la afiliación de beneficiarios;	Página 22 – "*...No existe un adecuado proceso de bajas de beneficiarios que impida que personas fallecidas sigan figurando en el padrón como beneficiarios activos...*' Esta Gerencia no comparte tal criterio, ya que en función de las medidas adoptadas por el INSSJP para evitar la citada situación (las cuales fueron puestas en conocimiento de las instancias de control cuando lo han requerido) se ha logrado un avance significativo en el proceso tendiente a impedir que personas fallecidas continúen figurando en el padrón como beneficiarios activos. A su vez, respecto a las recomendaciones realizadas por la AGN a lo largo del informe. se pone en conocimiento	Tal como se observa en los casos mostrados como ejemplo en el ANEXO I del informe de auditoría, a pesar de lo manifestado por el auditado, existen dentro del padrón de afiliados casos de fallecidos que figuran como beneficiarios activos, casos de doble afiliación con árboles prestacionales distintos, hijos de beneficiarios que no cumplen con lo establecido por las normas para continuar afiliados como familiares del titular, entre otros hallazgos que surgen del análisis de la base de datos del Padrón de Afiliados.

INFORME DE AUDITORÍA

Sección del Informe	Comentario del Auditado	Análisis del Comentario
• no se realizan cruces de datos con las Cajas Provinciales, lo que admite la afiliación de personas que disponen de cobertura como beneficiarios de aquellas; • el SII no cuenta con vínculos automáticos de consulta con la ANSES o el RENAPER que permita procesar las altas o bajas en forma rápida y eficiente; • no existen controles para evitar la afiliación de un familiar a cargo que posea una pensión no contributiva; • no existen controles de ingreso sobre campos importantes, como número de documento o número de teléfono; • si bien existe un campo para indicar el ejemplar del DNI presentado, no se controla y es optativo; • no existe un adecuado proceso de baja de beneficiarios, que impida que personas fallecidas sigan figurando en el padrón como beneficiarios activos; • el campo que verifica el domicilio del beneficiario se administra mediante una aplicación externa que produce errores en la carga de los datos de los afiliados y que carece de contrato de mantenimiento; • no existe un control automático del vencimiento de la afiliación por razones de edad y estudios de los hijos de beneficiarios. La solución de los problemas arriba mencionados no asegura la integridad de los datos del Instituto, pero permitirían disminuir el riesgo que se produzcan errores en los mismos. El INSSJP trata las bajas de los afiliados a partir de la notificación que le realiza la ANSES. Este procedimiento consistió inicialmente en procesar las	que toda medida a adoptar para dar solución a lo que se estime corresponder deberá ser solicitada a esta instancia por el área dueña del dato a través del proceso interno de Gestión de la demanda destinado a ello, lo cual deberá ser oportunamente priorizado debido a que las mismas representan tareas a largo plazo.	De la respuesta del auditado surge que a la fecha de la contestación quedaban tareas pendientes tendientes a resolver las inconsistencias, por lo que subsistían situaciones como las señaladas en el hallazgo. Por otra parte, el auditado no aporta elementos de juicio sobre eventuales: i) responsabilidades de los funcionarios competentes; ii) perjuicios fiscales, iii) acciones tendientes a su recupero y iv) gestiones que procuren revertir las debilidades de control interno señaladas en este informe, entre otras que pudieran abonar a la situación expuesta en el hallazgo y que podrían redundar en la repetición sistemática de la situación descripta. Puesto que el auditado no brinda documentación que permita revisar lo expuesto por esta auditoría, se mantiene el hallazgo y se agrega a la recomendación 5.2.2 el siguiente texto: "*Asimismo, iniciar las acciones que corresponda tendientes a evaluar la eventual existencia de responsabilidades de funcionarios o*

Sección del Informe	Comentario del Auditado	Análisis del Comentario
novedades de acuerdo a archivos que suministraba la ANSES a solicitud de PAMI. Posteriormente se estableció que este proceso tuviera una frecuencia mensual y durante las tareas de campo se estableció que las actualizaciones debían realizarse semanalmente. Cabe destacar que para la ANSES puede ocurrir que no tenga información fehaciente sobre el fallecimiento de un afiliado (solamente toma conocimiento que el jubilado no retiró los haberes de su cuenta bancaria o no completó el trámite de supervivencia) motivo por el cual puede informar su baja meses después de haberse producido. Salvo casos específicos en los que la Subgerencia de Afiliaciones de PAMI lo considere necesario, se realizan consultas al RENAPER para establecer si un afiliado se encuentra fallecido. Conforme a las mejores prácticas, es necesario definir e implementar procedimientos que garanticen la integridad y consistencia de los datos almacenados en formato electrónico, como bases de datos y archivos (CobIT v4.1 – PO2: Definir la arquitectura de la información). Los casos señalados generan el pago de cápitas a prestadores médicos por beneficiarios fallecidos. Además, esta situación puede producir que el sistema informe erróneamente que un determinado prestador tiene todas sus cápitas cubiertas y, ante una nueva afiliación, se asigne esta cápita a otro prestador más alejado del domicilio del beneficiario, obligándolos a desplazamientos innecesariamente más extensos para conseguir atención médica.		*agentes vinculados al registro y permanencia de datos inconsistentes en el Padrón de Afiliados, sus derivaciones en términos de perjuicio fiscal y las medidas conducentes a su recupero*".
4.3.3. *No se encuentra debidamente comunicada ni se aplica adecuadamente la normativa que rige la realización de copias de respaldo de la información (backups). Esta circunstancia y la falta de insumos para la realización de las copias de respaldo, aumentan el riesgo de que las copias no se realicen o que se generen archivos defectuosos.* El procedimiento para la realización de las copias de respaldo en cintas se encuentra definido en la Resolución 566/03 INSSJP y formó parte de la	Respecto a lo manifestado a lo largo del presente punto por la AGN, se informa que el INSSJP ha migrado la plataforma de backup corporativos a IBM Spectrurn Protect a partir de Agosto 2019. De esta manera se logró recuperar y mejorar la capacidad de procesamiento y ventanas necesarias para resguardo y recuperación del volumen de información	La respuesta del auditado no contradice lo expuesto en el hallazgo. Respecto de las acciones emprendidas, por tratarse de hechos posteriores al período auditado, eventualmente serán objeto de análisis en futuras labores de auditoría. Se mantiene el hallazgo.

INFORME DE AUDITORÍA

Sección del Informe	Comentario del Auditado	Análisis del Comentario
documentación necesaria para que el organismo oportunamente obtuviera la certificación ISO 27001 (actualmente vencida). En las entrevistas realizadas con distintos responsables de las áreas involucradas se tomó conocimiento de que la normativa no está adecuadamente comunicada al personal, incluidos los responsables de generar o resguardar las copias. El organismo carece de insumos suficientes, principalmente cintas, para realizar las copias. Las existentes se utilizan hasta el final de su vida útil, sin que se haya establecido la cantidad máxima de veces que pueden ser reescritas. Además, no se encuentran establecidos en el PAMI parámetros de RPO ni RTO. Por su parte, la obsolescencia de los discos donde se procesan las copias de respaldo ocasionalmente impide que las tareas se realicen adecuadamente. Una vez hechas las copias de respaldo, las cintas se almacenan en cajas ignífugas que se ubican en el edificio de Nivel Central. Dado que el espacio resulta insuficiente para almacenarlas en su totalidad, las restantes se alojan en el edificio donde se encuentra el Data Center del Instituto. Se constató que la infraestructura en general acusa cierto grado de obsolescencia y se verifican fallas de *hardware*, tanto de los dispositivos de *storage pool* primarios de discos, como de las librerías de cintas. El *software* y el *hardware* se encuentran sin contrato de mantenimiento externo. La infraestructura actual no cuenta con la capacidad de almacenamiento para respaldar bases de datos de grandes dimensiones (superiores a los 2TB). A modo de ejemplo, la base de Trazabilidad de Medicamentos tiene un tamaño	corporativa, sobre nuevas tecnologías, con 2 nuevos servidores físicos en Cluster, logrando HA sobre la plataforma, con un nuevo Storage IBM Storwize V503 dedicado para la gestión de copias de resguardo y recuperación. Asimismo, se realizó el upgrade de la librería High End IBM TS3584 con 8 Drives LTO7 de mayor capacidad y vida útil a lo largo del tiempo, además de la gestión completa de la doble copia de resguardo en cintas almacenadas en un armario ignífugo con capacidad suficiente para contener la doble copia off-site. Toda la nueva plataforma cuenta con soporte y mantenimiento por los próximos 3 años, tanto de software como del hardware. La infraestructura actual cuenta con licenciamiento y capacidad para almacenar 200 TeraByte de Fornt End, sin importar cuantas copias sean tomadas de una misma BD, para todos los clientes requeridos, tanto en el ambiente de BD, entorno virtual, de correo, Sharepoint, etc A partir de esta nueva implementación se está trabajando para difundir todas las políticas de resguardo actualmente vigentes. Las mismas serán publicadas en	

Sección del Informe	Comentario del Auditado	Análisis del Comentario
aproximado de 7 Tb, mientras que el tamaño aproximado del Padrón de Afiliados es de 4 Tb. Las mejores prácticas para la seguridad de la información indican que la falta de difusión y aplicación de una política clara de resguardo de datos acarrea el riesgo de depender de personal clave para la realización de las tareas y el no cumplimiento estricto del procedimiento, de forma tal que ante cualquier incidente no se disponga de las copias de respaldo necesarias para asegurar la continuidad de las tareas (CobIT v4.1 – DS4.9: Almacenamiento de respaldos fuera de las instalaciones; ISO/IEC 27001).	los próximos meses, en la Intranet del Instituto, previa validación y ratificación por los dueños de datos.	
4.3.4. *Se observó equipamiento obsoleto e instalaciones no adecuadas y en mal estado en distintas UGL ubicadas en el Área Metropolitana de Buenos Aires. Esta situación aumenta el riesgo de sufrir indisponibilidades en el sistema y perjudicar la atención de los beneficiarios.* El equipamiento informático utilizado por los agentes del PAMI en las UGL de Quilmes, San Justo y Morón, es obsoleto. A modo de ejemplo, el parque de PCs de la UGL Morón tiene una antigüedad promedio de 12 años. Como por su antigüedad ya no existen repuestos, se utilizan partes de equipos fuera de servicio. También pudo verificarse la ausencia de UPS que suministren energía para los momentos en que el suministro de red eléctrica domiciliaria se encuentre interrumpido y el mal estado general de las instalaciones de red de datos. Las organizaciones deben contar con instalaciones bien diseñadas y administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del CPD, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico (CobIT v4.1 - DS12.2-5: Administración del ambiente físico). Además, se debe desarrollar y ejecutar un plan de mantenimiento preventivo del hardware con el fin de reducir la frecuencia y el impacto de las fallas que pongan en riesgo la continuidad del	Punto 4.3.4 - "... El parque de PCs de la UGL Morón tiene una antigüedad promedio de 12 años..." El promedio de antigüedad del parque de PCs es inferior a 12 (doce) años.	Durante las inspecciones realizadas a las distintas UGL pudo observarse que el parque de computadoras en los puestos de trabajo es obsoleto (por ejemplo, PCs con Windows XP, a la fecha discontinuado), entre otro equipamiento que por su antigüedad no admite la instalación de versiones más recientes. También se observó el estado de las instalaciones de red y la falta de UPS (que permitan seguir operando los sistemas ante una caída de suministro eléctrico). Se cuenta con evidencia de PCs con doce años de antigüedad pero que no necesariamente, tal como indica el auditado en su descargo, dan cuenta de esa antigüedad como promedio. En virtud de ello, se reemplaza el pasaje que dice: "*A modo de ejemplo, el parque de PCs de la UGL Morón tiene una antigüedad promedio de 12 años*", por "*A modo de ejemplo, en la UGL de*

INFORME DE AUDITORÍA

Sección del Informe	Comentario del Auditado	Análisis del Comentario
servicio (CobIT v4.1 - DS13.5: Mantenimiento Preventivo del Hardware, y Resolución 48/05-SIGEN: 8.3). El estado actual del equipamiento y las instalaciones de las redes de datos no permiten asegurar la disponibilidad de los sistemas informáticos del PAMI en las oficinas de las UGL o en las agencias, lo que aumenta el riesgo de fallas o salidas de servicio imprevistas que perjudiquen la normal atención de los beneficiarios.		*Morón se opera con PCs algunas de las cuales tienen doce años de antigüedad.*

Anexo III – Casos ilustrativos de inconsistencias

RESERVADO COLEGIO DE AUDITORES GENERALES