Auditoría General de la Nación

INFORME DE AUDITORÍA

INSTITUTO NACIONAL DE SERVICIOS SOCIALES PARA JUBILADOS Y PENSIONADOS (INSSJP)

Clave Única PAMI (CUP) y sistemas relacionados.

Act. Nº 127/21-AGN

Proyecto Nº 050600994

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

Tabla de contenido

Glosario

ABM: Altas, Bajas y Modificaciones.

AFMSRA: Asociación de Farmacias Mutuales y Sindicales de la República Argentina.

CAMOyTE: Centro de Autorización de Medicamentos Oncológicos y Tratamientos Especiales.

CIT: Circuito de Identificación de Talonarios.

COBIT: Objetivos de Control para Tecnología de la Información y relacionadas, por sus siglas en inglés *Control Objectives for Information and Related Technology.*

COFA: Confederación Farmacéutica Argentina.

CUP: Clave Única PAMI.

DC: Departamento de Contabilidad.

DE: Dirección Ejecutiva.

DEN: Directorio Ejecutivo Nacional.

DIF: Departamento de Ingreso de Facturación.

DNI: Documento Nacional de Identidad.

DURF: Departamento Único de Recepción de Facturas.

EN: Entidades Nacionales.

FACAF: Federación Argentina de Cámaras de Farmacias.

FARMASUR: Asociación Mutual Farmasur.

FEFARA: Federación Farmacéutica.

FFAA: Fuerzas Armadas Argentinas.

GD: Gestión de la Demanda.

GDE: Sistema de Gestión de Documentación Electrónica.

GIT: Gerencia de Infraestructura.

GM: Gerencia de Medicamentos.

GS: Gerencia de Sistemas.

IEC: Comisión Electrónica Internacional, por sus siglas en inglés *International Electrotechnical Commission*.

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

ISO: Organización Internacional de Estandarización Internacional, por sus siglas en inglés *International Organization for Standardization*.

ITIL: Biblioteca de Infraestructura de Tecnologías de Información, por sus siglas en inglés *Information Technology Infrastructure Library*.

JIRA: Sistema de consultas y gestión de proyectos.

MSC: Sistema de Medicamentos Sin Cargo.

ONCO: Sistema de Protocolos Oncológicos.

PAMI: Programa de Asistencia Médica Integral.

PMBok: Cuerpo de Conocimientos de la Gestión de Proyectos, por sus siglas en inglés *Project Management Body of Knowledge.*

RE: Receta Electrónica.

RRHH: Recursos Humanos.

RTF: Registro de Tratamiento Farmacológico.

SADES: Sistema de Administración de Seguridad.

SAP: Sistemas, Aplicaciones y Productos (Software de gestión de procesos de negocios), por sus siglas en inglés *Systems, Applications, Products in Data Processing*.

SARHA: Sistema de Administración de Recursos Humanos Automatizados.

SDE: Subdirección Ejecutiva.

SGSI: Sistemas de Gestión de la Seguridad de la Información.

SICA: Sistema Integrado de Control de Auditorías.

SII: Sistema Interactivo de Información.

SV: Subgerencia de Validación y Control de Medicamentos.

TI: Tecnología de la Información.

TIC: Tecnología de la Información y las Comunicaciones.

UAI: Unidad de Auditoria Interna.

UFI-PAMI: Unidad Fiscal para la Investigación de Delitos Cometidos en el ámbito de actuación del INSSJP y su Programa de Atención Médica Integral.

UGL: Unidad de Gestión Local.

VIH: Virus de la Inmunodeficiencia Humana.

INFORME DE AUDITORIA

Al Sr. Director
Dr. Esteban Leguízamo.
S. / D.

En virtud de las funciones conferidas por el artículo 85 de la Constitución Nacional y en uso de las facultades establecidas por el artículo 118 de la Ley Nº 24.156, de Administración Financiera y de los Sistemas de Control del Sector Público Nacional, la AUDITORÍA GENERAL DE LA NACIÓN efectuó un examen en el ámbito del INSTITUTO NACIONAL DE SERVICIOS SOCIALES PARA JUBILADOS Y PENSIONADOS (INSSJP), con el objeto que se detalla en el apartado 1.

1. OBJETO DE AUDITORÍA

Gestión de TI. Sistemas de información – Clave Única PAMI y sistemas relacionados, en el Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP).

2. ALCANCE

2.1. Ejecución del Trabajo de Auditoría

El Informe fue realizado de conformidad con las Normas de Control Externo Gubernamental y las Normas de Control Externo de 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, teniendo en cuenta el marco metodológico establecido en el "Manual de la IDI y del WGITA sobre auditorías de TI para las Entidades Fiscalizadoras Superiores"[1], y aplicándose los procedimientos detallados en el punto 2.3.

[1] https://www.intosaicommunity.net/wgita/wp-content/uploads/2018/04/it-audit-handbook-spanish-version.pdf

El inicio de las tareas de auditoría se notificó al Instituto Nacional de Servicios Sociales para Jubilados y Pensionados mediante Nota de la Auditoria General de la Nación, recibida el 10/05/2021.

El período auditado se extiende del 01/02/2018 al 31/03/2021.
Las tareas de campo se desarrollaron entre los meses de mayo de 2021 y agosto de 2023.

2.2. Enfoque del Trabajo de Auditoría

La auditoría se desarrolló bajo un enfoque orientado a procesos y basado en riesgos, consistiendo en una revisión independiente y objetiva, para evaluar la eficacia, eficiencia, economía y aspectos de confidencialidad y seguridad de la información en la gestión integral de las Tecnologías de la Información y Comunicaciones (TICs) y los Sistemas de Información críticos del negocio (aplicaciones transaccionales/operacionales y de toma de decisiones de la organización) con el objetivo de detectar los riesgos potenciales (inherentes) que puedan causar el mayor impacto negativo en las operaciones de la organización auditada. Esta auditoría también verifica la operación y administración de los controles, la seguridad en los servicios de TI de la organización y el cumplimiento con las normas legales vigentes relacionadas con la información, los datos, el software y las redes de comunicaciones de datos. Para ello, el equipo de auditoría de TI se apoya en criterios, estándares y buenas prácticas de reconocimiento internacional que permiten identificar los riesgos, ponderar su probabilidad de ocurrencia y el nivel de impacto que estos riesgos tienen para la organización, como así también, se aplican estos criterios y estándares para establecer los desvíos existentes entre las prácticas aplicadas por el auditado y el "deber ser" según lo que estas buenas prácticas indican.[2]

La tarea abarcó el estudio y verificación de: i) la gestión informática aplicada en el organismo; ii) los procesos técnicos y administrativos practicados por las Gerencias de Sistemas,

[2] Fuente: ISACA (Information Systems Audit and Control Association - Asociación de Auditoría y Control de Sistemas de Información), asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.

Tecnología y Medicamentos y las áreas dependientes de estas gerencias en lo que respecta a la prescripción, dispensa y liquidación de medicamentos con cobertura del INSSJP; iii) el soporte y mantenimiento continuo de las aplicaciones y herramientas informáticas utilizadas para el punto ii); y iv) la gestión de la infraestructura tecnológica y la gestión de la seguridad de la información a nivel organizacional.

Producto del relevamiento preliminar realizado y del análisis de riesgo resultante, se identificaron las siguientes cuestiones de auditoría[3] como las más importantes relativas al objeto de auditoría:

- Gobierno de TI;
- Seguridad de la Información;
- Continuidad de las operaciones organizacionales;
- Operaciones de TI;
- Adquisiciones y contrataciones de TI;
- Desarrollo de software aplicativo;
- Sistemas de información.

Adicionalmente, por Disposición 62/22-AGN, de manera trasversal a la Institución, se incorporó un objetivo específico sobre el cumplimiento de la Ley 27.499, LEY MICAELA, de *Capacitación obligatoria en la temática de género y violencia contra las mujeres*.

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 27.000, Norma ISO 24.762 (Tecnologías de la información – Técnicas de seguridad - Directrices para los servicios de recuperación de desastres de las tecnologías de la información y comunicaciones) e ITIL versión 4, entre otras. Éstas buenas prácticas describen los procedimientos que una organización debe implementar para obtener resultados óptimos en la gestión de la información.

[3] Las cuestiones de auditoría son aquellas que, en función del objeto de auditoria, revisten la mayor significatividad en base a los riesgos más relevantes que fueron ponderados por el equipo de auditoria.

Los procedimientos de auditoría ejecutados se exponen a continuación, desagregados por las cuestiones de auditoría previamente identificadas.

2.3. Procedimientos de Auditoría

Gobierno de TI:

- evaluación de que el Plan Estratégico Institucional esté alineado con el Plan Estratégico, Planes Operativos y Plan de Infraestructura de TI, y que su nivel de desagregación permita su seguimiento y monitoreo;
- verificación de que las políticas, normas y procedimientos estén formalizados, actualizados y sean difundidos de manera adecuada;
- constatación de que la estructura organizacional aprobada promueva un eficaz desempeño del área de TI y que las misiones y funciones estén adecuadamente definidas;
- análisis y evaluación de la capacidad de control interno sobre el ambiente de TI.

Seguridad de la información:

- verificación de la existencia de una orientación estratégica adecuada hacia la seguridad de la información por parte del organismo, con la existencia de una política de seguridad de la información formalizada, su cobertura, la concientización del personal y su cumplimiento por parte de toda la organización;
- constatación de la existencia, formalidad, cobertura, concientización y cumplimiento por parte de toda la organización de un Plan de Seguridad de la Información;
- estudio de la gestión de usuarios, evaluando si es adecuada en términos de ABM, política de claves y permisos otorgados;
- análisis de la seguridad de la red implementada en el organismo mediante la identificación de vulnerabilidades, verificando la realización por parte del organismo de tests de penetración no intrusivos[4].

[4] *Los* **test** *o pruebas de* **penetración** *son un proceso sistemático para comprobar las vulnerabilidades de las aplicaciones y redes informáticas.*

Continuidad de las operaciones organizacionales:

- diagnosis del plan de recuperación ante desastres, verificando que se prueba y se actualiza con regularidad, y que cumple con la cobertura operacional requerida por la organización;
- análisis de las políticas y procedimientos de respaldo de la información (*backup),* verificando las pruebas de restauración implementadas, a fin de comprobar la integridad de las copias.

Operaciones de TI:

- evaluación de la capacidad y el proceso de respuesta ante problemas e incidentes tecnológicos;
- constatación de que se lleva a cabo un eficaz control de nivel de los servicios de TI con las áreas usuarias del INSSJP.

Adquisiciones y contratación de TI:

- verificación y análisis de los acuerdos de niveles de servicio pactados con los proveedores, en especial con aquellos que brindan servicios de TI en los procesos de dispensa y liquidación de medicamentos con cobertura del INSSJP.

Desarrollo de sistemas aplicativos:

- análisis de la eficiencia de la gestión de proyectos, mediante el contraste entre las metas ejecutadas y las planificadas;
- evaluación de la documentación de planificación y seguimiento de proyectos.

Sistemas de información:

- evaluación de la integración de los procesos relacionados con la prescripción, dispensa y liquidación de medicamentos con cobertura del INSSJP.

Procedimientos transversales:

- inspección a la Sala de Servidores del INSSJP;

- sobre la Ley 27.499- Ley MICAELA, *de capacitación obligatoria en género y violencia de género para todas las personas que se desempeñan en la función pública, en los poderes Ejecutivo, Legislativo y Judicial de la Nación*:

    - verificación de que el organismo haya desarrollado un programa o plan de capacitación en género y violencia contra las mujeres;
    - evaluación de que el organismo cuente con la certificación de calidad del Órgano Rector;
    - análisis del listado del personal capacitado con el programa o plan en la temática de género y violencia contra las mujeres, comparado con la totalidad del personal del organismo.

2.4. Hechos Posteriores

El pasado 2 de agosto de 2023, el INSSJP sufrió un ciberataque perpetrado con un ransomware[5]. Ante esta situación, se vieron afectados todos los sistemas informáticos y se bloqueó el acceso a las computadoras utilizadas en el Instituto, iniciando un período de contingencia, en donde la dirección a cargo debió adoptar una serie de medidas excepcionales y urgentes a fin de mantener su funcionamiento esencial, aunque sin el soporte de sus sistemas críticos, para todo lo cual declaró haber culminado el 31 de agosto de ese año[6].

[5] https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/informes-de-la-direccion-6.

[6] Esto último se convalida en la Resolución 2025/2023-INSSJP-DE#INSSJP[6], del 06/12/2023, en referencia a la Resolución - EX-2023-90100207- -INSSJP-SGA#INSSJP -Resolución- *Convalidación Circuito extraordinario de pago del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados* (INSSJP)

3. ACLARACIONES PREVIAS

3.1. Marco conceptual

Clave Única PAMI (CUP) es un sistema de inicio de sesión unificada (*Single Sign On*[7]) que cuenta con un proceso de acceso seguro a través del cual los usuarios solicitan autorización para acceder al uso de sus más de 60 aplicaciones. No obstante, obtener acceso a CUP no implica contar con el permiso de acceso a todas estas aplicaciones, y esto debido a que la mencionada Plataforma cuenta con su propio Sistema de Administración de Seguridad (SADES), el cual permite la autogestión de aplicaciones, funciones y perfiles, mediante la aprobación del dueño de datos de la aplicación solicitada (las áreas usuarias del INSSJP).

CUP es un portal de acceso a diversas aplicaciones o sistemas del INSSJP, cuenta con un portal interno y otro externo en la Internet para el acceso de usuarios por fuera de la red del Instituto. El sistema CUP es utilizado por todo el personal del INSSJP, por los prestadores y por los proveedores habilitados por el Instituto.

A nivel módulos, CUP solo se encarga de la autenticación de usuarios y realiza la validación, según el tipo de usuario de la siguiente manera:

- ✓ Usuarios Planta: *Active Directory*[8] - valida en sistema Sarha[9] de RRHH.
- ✓ Usuarios Contratados: *Active Directory - Login* y Alta de usuario - valida en el Sistema SAP[10].
- ✓ Usuarios Pasantes: Active *Directory - Login* y Alta de usuario.
- ✓ Usuarios Prestadores: valida en el Sistema Interactivo de Información (SII) - *Login* y Alta de usuario.

[7] **Single Sign On** conocido también como **SSO** por sus siglas en inglés, permite a los usuarios tener acceso a múltiples aplicaciones ingresando solo con una cuenta a los diferentes sistemas y recursos.
[8] ***Active Directory*** *(AD),* es una base de datos y un conjunto de servicios informáticos que conectan a los usuarios con los recursos de red que necesitan para realizar su trabajo.
[9] Es un sistema integrado de liquidación de haberes y de Administración del personal.
[10] El nombre del sistema SAP representa las siglas en alemán *Systeme Anwendungen und Produkte* que significa en español 'sistemas, aplicaciones y productos'. El sistema SAP es un sistema ERP, por las siglas en inglés *Enterprise Resource Planning* o planificación de los recursos empresariales. Todos los sistemas ERP son sistemas integrales compuestos por diferentes módulos para la administración de los recursos de cada área de la empresa como las áreas de administración y finanzas, compras, ventas, producción, recursos humanos, mantenimiento y más dependiendo del tamaño de la organización.

- ✓ Usuarios Proveedores: valida en sistema de Proveedores - *Login* y Alta de usuario.

- **Sistema SADES:**

  El sistema CUP tiene asociado internamente el Sistema de Administración de Seguridad (SADES), que administra el ABM (Altas, Bajas y Modificaciones) de los usuarios, los sistemas que lo componen y los permisos de acceso que se les habilitan a los usuarios en esas aplicaciones. El SADES es un sistema de seguridad de control de accesos.

  Los módulos que componen el SADES son:

- ✓ ***ADMINISTRACIÓN DE USUARIO:*** módulo de Seguridad Informática. Administra Usuarios, permisos a los sistemas y perfiles asignados dentro de los sistemas.
- ✓ ***AUDITORIA DE USUARIOS:*** módulo de Seguridad Informática. Auditoría de usuarios, permisos, accesos y bloqueos.
- ✓ ***MÓDULO DE NOTICIAS Y NOVEDADES:*** carga de noticias para usuarios de sistemas internos y externos.
- ✓ ***MÓDULO DE DESARROLLO:*** administración de códigos de perfiles de sistemas.
- ✓ ***MÓDULO DE SISTEMAS:*** administración de sistemas y perfiles.
- ✓ ***MÓDULO DE ADMINISTRACIÓN DE CUENTA:*** sección del usuario donde puede pedir corrección de datos y permisos sobre sistemas y roles.

  A continuación, se describe el alcance funcional y operativo de las principales aplicaciones relacionadas a la prescripción, valorización y dispensa de medicamentos que se encuentran incluidas dentro de la Plataforma CUP:

- **El Sistema de Gestión de Medicamentos Sin Cargo (MSC):**

  Se trata de una aplicación web alojada en la Plataforma CUP y creada con la finalidad de sistematizar la solicitud, evaluación, autorización y renovación de los medicamentos con cobertura al 100% para los afiliados al INSSJP, a través de las distintas vías administrativas disponibles, también conocidas como Registros de Tratamientos Farmacológicos (RTF): Subsidio Social, Vía de Excepción, Discapacidad, Urgencias Locales y Amparo Judicial.

Todos los medicamentos cuentan con un nivel de autorización, algunos pueden ser autorizados por el personal administrativo de las Unidades de Gestión Local (UGL/Agencia), otros por profesionales médicos de UGL/Agencia, y finalmente existen medicamentos que sólo pueden ser autorizados por auditores médicos de la Gerencia de Medicamentos a nivel central.

Los módulos que componen el MSC son:

- ✓ ***ALTA DE REGISTRO TRATAMIENTO FARMACOLÓGICO (RTF):*** carga de las solicitudes de medicación que cada afiliado requiere con las cantidades, presentaciones y documentación que respalda dicho pedido.
- ✓ ***VISUALIZACIÓN DE BANDEJAS DE NIVEL CENTRAL Y UGL:*** este módulo es para los casos que requieren un nivel de autorización mayor y son enviados digitalmente desde las dependencias del INSSJP para la evaluación por parte del equipo de la Gerencia de Medicamentos en la central. Permite la consulta de las diferentes autorizaciones para cada afiliado, accediendo al detalle de la medicación, presentaciones, cantidades, fechas de autorización y *log*[11] de los agentes que intervinieron en el proceso.

- **Sistema de Recetas Electrónicas (RE):**

  La transición de las Recetas Manuales a la Recetas Electrónicas marcan, de acuerdo a los fundamentos en su Ley de creación[12], un avance en el sistema de salud como una herramienta que facilita y agiliza el circuito de dispensa de medicamentos a través de un procedimiento que otorga más seguridad al acto médico de la prescripción. En su art. 4º, la Ley 27.553 de Recetas Electrónicas o digitales, remarcaba para el año 2020, la necesidad de *"... Para la implementación de la presente ley se deben desarrollar y/o adecuar los sistemas electrónicos existentes y regular su implementación para utilizar recetas electrónicas o digitales, y plataformas de teleasistencia en salud, todo lo cual debe regular el organismo que el Poder*

[11] En informática, se usa el término *log*, historial de log o registro, para referirse a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.). De esta forma constituye una evidencia del comportamiento del sistema.

[12] https://www.hcdn.gob.ar/proyectos/proyectoTP.jsp?exp=3979-D-2019

Ejecutivo nacional oportunamente establezca y los organismos que cada jurisdicción determine" ...

Asimismo, dichos organismos son los responsables de la fiscalización de los sistemas de recetas electrónicas o digitales, y de los sistemas de plataformas de teleasistencia en salud, quienes deben garantizar la custodia de las bases de datos de asistencia profesional virtual, prescripción, dispensación y archivo. También son responsables de establecer los criterios de autorización y control de acceso a dichas bases de datos y garantizar el normal funcionamiento y estricto cumplimiento de la ley 25.326 de Protección de los Datos Personales, la ley 26.529 de Derechos del Paciente y demás normativas vigentes en la materia.

El sistema cuenta con un *vademecum*[13] de medicamentos online, mediante el cual el usuario (profesional médico habilitado) selecciona los medicamentos a prescribir y los mismos son informados en forma automática a las farmacias, para que el afiliado pueda obtener el medicamento en forma más ágil.

Los módulos que componen el sistema de recetas electrónicas son:

- ✓ ***ALTA RECETA:*** módulo en el cual se realiza la prescripción de la receta electrónica. En ella, el usuario (profesional médico habilitado) podrá hacer uso de 2 renglones (para prescribir en ella dos especialidades medicinales diferentes en la cantidad que sea necesaria). También deberá indicar el diagnóstico por cada especialidad prescrita.
- ✓ ***BÚSQUEDA DE RECETA:*** panel que le permite al usuario buscar las recetas que hayan sido prescriptas para un afiliado, ya sea por él mismo o por otro profesional médico habilitado. En este panel se pueden buscar recetas de medicamentos, de actividades terapéuticas no medicamentosas y de pañales.
- ✓ ***DATOS DEL MÉDICO:*** en esta sección el usuario puede ver sus datos personales y cargar los datos de su matrícula nacional y provincial según corresponda.

[13] *Vademecum*, significado: libro o manual de poco volumen y fácil de consultar que contiene las nociones elementales de una ciencia o técnica. En este caso específico se trata un manual sintético que registra todos los medicamentos disponibles en un determinado país, sus dosajes y principios activos.

- ✓ ***RECETA PAÑALES:*** módulo para la prescripción de recetas electrónicas de pañales y otros higiénicos absorbentes descartables.
- ✓ ***ADMINISTRACIÓN UNIDADES OPERATIVAS:*** módulo operado por la Gerencia de Sistemas donde se administran los códigos de las unidades operativas que utiliza el Sistema de Receta Electrónica.
- ✓ ***ADMINISTRACIÓN EQUIVALENCIAS ESTRUCTURAS:*** módulo operado por la Gerencia de Sistemas donde se administran los códigos de estructura del Sistema de Administración de Recursos Humanos Automatizados (SARHA) asociados a las unidades operativas que tienen acceso al sistema.
- ✓ ***LIMPIEZA DATOS DE PRUEBA:*** módulo operado por la Gerencia de Sistemas para aplicar una baja lógica en las recetas que por motivos excepcionales el área de sistemas haya tenido que generar en el ambiente productivo, debido a que era imposible replicar el error indicado en los ambientes de desarrollo.
- ✓ ***PANEL ADMINISTRACIÓN MENSAJES EN IMPRESIÓN:*** panel para administrar el mensaje escrito que puede incluirse al pie de las recetas electrónicas.
- ✓ ***PANEL BAJAS AUDITOR:*** panel confeccionado para el personal de auditoría prestacional, con la funcionalidad de dar de baja recetas de forma masiva a partir de un archivo de entrada donde se indican cuáles son las recetas a eliminar, motivo de alguna denuncia o irregularidad detectada / denunciada al INSSJP.
- ✓ ***PANEL DE BÚSQUEDAS AUDITOR SEGURIDAD INFORMÁTICA:*** panel personalizado para las necesidades de búsqueda y respuesta del área de seguridad informática.

- **Sistema de Liquidación de Medicamentos:**

  Esta aplicación se utiliza para realizar el proceso de validación y conciliación de los datos de las liquidaciones de medicamentos. Se ejecuta el procesamiento de las liquidaciones de medicamentos enviadas por la industria farmacéutica.

  Desde la aplicación se importan los archivos recibidos por las farmacéuticas, se procesan, se realizan las distintas validaciones y conciliaciones, y se genera el archivo de salida para que lo reciba la Gerencia de Medicamentos para su correspondiente revisión y aprobación y luego, su posterior liquidación. Esta aplicación cuenta con las siguientes herramientas de trabajo:

- ✓ ***IMPORTACIÓN DE ARCHIVOS DE LIQUIDACIÓN:*** panel desde el cual se realiza la importación de los archivos de texto plano de las liquidaciones recibidas a la base de datos del sistema para poder realizar el proceso de validación de datos.
- ✓ ***VISUALIZACIÓN DE HISTORIAL DE EJECUCIONES:*** permite visualizar en la interfaz del sistema por año, segmento y mes, el estado de los archivos procesados. Allí puede verse si un archivo está en proceso, finalizado o anulado.
- ✓ ***VISUALIZACIÓN DE ARCHIVOS ACTIVOS:*** permite visualizar los archivos que están siendo procesados actualmente y desde allí disparar las acciones del procesamiento y validaciones.
- ✓ ***PROCESAMIENTO DE ARCHIVOS DE LIQUIDACIÓN:*** desde esta sección el operador va ejecutando las diferentes acciones del procesamiento, como valorización del archivo contra las bases del Instituto, ejecución de las diferentes validaciones de control, inserción final en la base de datos, generación del archivo de entrega para el dueño de datos, y cambio del estado del proceso a "finalizado" para dicho archivo.
- ✓ ***PANEL DE USUARIOS:*** panel de administración de usuarios, al que solo tiene acceso el perfil de administrador. Desde allí se asignan los roles a los usuarios y se gestionan las bajas.

- **Sistema de *Vademecum* de Medicamentos:**

  La aplicación *Vademecum,* como su nombre lo indica, tiene por objetivo la administración del *vademecum* de medicamentos que utiliza el Instituto. A través de esta herramienta, la Gerencia de Medicamentos, puede gestionar las actualizaciones de los atributos de los medicamentos, información que es utilizada por los otros sistemas relacionados con la materia, por ejemplo, el Sistema de Recetas Electrónicas y el Sistema de Medicamentos sin Cargo. También desde esta aplicación se puede administrar el padrón de farmacias que operan con el Instituto.

  Esta aplicación cuenta con las siguientes herramientas de trabajo:

- ✓ ***PANEL CONSULTA GENERAL DE MEDICAMENTOS:*** panel de búsqueda general de especialidades medicinales, donde se pueden utilizar diferentes filtros para encontrar el

resultado deseado, y desde allí se accede al detalle del medicamento, así como a la posibilidad de la edición de su contenido en el caso de poseer el rol que habilite dicha funcionalidad.

- ✓ ***ABM DE MEDICAMENTOS:*** panel que muestra en detalle los atributos de los medicamentos, y desde el cual, con el rol correspondiente pueden editarse los mismos.
- ✓ ***ABM GENÉRICOS:*** panel que muestra en detalle los atributos de los genéricos, y desde el cual, con el rol correspondiente pueden editarse los mismos.
- ✓ ***ABM LABORATORIOS:*** panel que muestra en detalle los atributos de los laboratorios, y desde el cual, con el rol correspondiente pueden editarse los mismos.
- ✓ ***GRUPO TERAPEUTICOS:*** panel que muestra el detalle de los grupos terapéuticos, grupos creados para aplicar reglas de exclusión en el Sistema de Medicamentos Sin Cargo.
- ✓ ***ABM BANDEJAS NIVEL CENTRAL MEDICAMENTOS SIN CARGO:*** panel que administra las bandejas de trabajo de nivel central para el personal auditor médico de la Gerencia de Medicamentos.
- ✓ ***ACTUALIZACIÓN MASIVA:*** panel de carga de medicamentos con el cual, a partir de una planilla de cálculo como archivo de entrada se pueden subir a la base e impactar modificaciones masivas de atributos (precio, coberturas, descuentos, etc.).
- ✓ ***EXPORTACIÓN Y ENVÍO DE INFORMACIÓN:*** panel que permite la exportación del *vademécum* a planilla de cálculo y su posterior envío a PRAXYS S.A[14] (Empresa que brinda la plataforma tecnológica de hardware y software para el sistema de dispensa y liquidación de medicamentos ambulatorios que se prescriben mediante PAMI a las farmacias) para que sea actualizado luego por ellos en su base de datos.
- ✓ ***ABM FARMACIAS:*** panel desde el cual se pueden buscar con diversos filtros las farmacias con las que opera el Instituto. También se puede acceder a su detalle y si el rol lo permite, editar atributos y dar de alta o baja farmacias.
- ✓ ***ABM INTERACCIONES MEDICAMENTOSAS:*** panel donde se pueden administrar la base de interacciones medicamentosas y sus efectos para ser mostrados en el sistema de Recetas Electrónicas.
- ✓ ***ABM DROGUERÍAS:*** panel para la visualización y edición de datos de las droguerías.

[14] PRAXYS S.A. se dedica al desarrollo e implementación de soluciones informáticas para el sector farmacéutico. Esto es aplicable en las distintas etapas de la cadena de comercialización de medicamentos. http://www.praxys.com.ar

- **Sistema de Padrón de Diabéticos:**

  El sistema de padrón de afiliados con diabetes es una aplicación web alojada en la Plataforma de Sistemas CUP, creada con la finalidad de identificar a aquellos afiliados del Instituto que han informado (o desean hacerlo) su patología diabética y de esta manera, recibir la cobertura al 100% de los medicamentos necesarios para su tratamiento continuo.

  Esta aplicación cuenta con las siguientes herramientas de trabajo:

- ✓ ***BÚSQUEDA AFILIADOS EN PADRÓN:*** es el módulo de gestión de información exclusivo para personal del INSSJP, a través del cual se puede realizar la búsqueda de afiliados que permite identificar si el mismo se encuentra dentro del padrón de diabéticos. Allí se puede encontrar información tal como, datos afiliatorios, usuario que empadronó, último diagnóstico y perfil de la persona afiliada, entre otros.
- ✓ ***FORMULARIO DE ALTA PERFIL/ACTUALIZACIÓN DIAGNÓSTICO:*** ficha digital a completar por el médico tratante o usuario de carga que contiene los datos clínicos y patológicos del afiliado. Una vez completado y enviado el formulario, se toma al mismo de alta en el padrón de diabético.
- ✓ ***HISTORIAL DEL BENEFICIARIO:*** contiene el detalle de las fichas/formularios cargados para un afiliado/a específico.
- ✓ ***SOLICITUD DE LECTOR:*** es una bandeja de gestión utilizada por parte de los usuarios del INSSJP habilitados para realizar la solicitud de medidores de glucemia.

- **Sistema de Protocolos Oncológicos (ONCO):**

  Protocolos Oncológicos (ONCO) es un sistema alojado en la Plataforma CUP desarrollado por el proveedor Praxys S.A, que permite organizar la prescripción de tratamientos oncológicos, dentro de los protocolos definidos por el INSSJP, para cada una de las diferentes patologías:

  - Tratamientos (*dentro* de los protocolos establecidos) de autorización Local.
  - Tratamientos (*dentro* de los protocolos establecidos) de autorización Central.
  - Tratamientos (*fuera* de los protocolos establecidos) que se gestionan como Vía de Excepción.

El sistema dispone de una aplicación de Escritorio que permite a los Auditores Médicos aprobar, observar y rechazar aquellos tratamientos que requieran una elevación a Nivel Central.

Los módulos que componen el sistema ONCO son:

- ✓ ***APLICACIÓN DE ESCRITORIO PARA AUDITORÍA/AUTORIZACIÓN:*** aplicación de escritorio para la gestión de tratamientos oncológicos y especiales por parte de la auditoría de medicamentos central del INSSJP. Este escritorio cuenta con las siguientes herramientas de trabajo:
  - ➢ **Tratamientos:** visualización de los tratamientos iniciados (prescripción, mensajes e imágenes de tratamiento)
  - ➢ **Modificación de Tratamientos:** carga de datos faltantes o erróneos de un tratamiento (por ejemplo, afiliado, fecha de prescripción y diagnóstico, tipo de tratamiento, etc.)
  - ➢ **Menú de Trabajo:** permite guardar información modificada, autorizar, rechazar u observar un tratamiento para su devolución al remitente, ante el caso de necesitar más información/disponer de datos erróneos. También es posible reactivar o derivar un tratamiento en caso que el operador del Centro Autorizador encuentre que un tratamiento debe ser evaluado por algún grupo de médicos auditores en particular.
  - ➢ **Seguimiento:** visualización de los acontecimientos de un trámite.
  - ➢ **Gestión de Tratamientos especiales:** desde esta funcionalidad se podrá modificar, buscar e imprimir tratamientos.
  - ➢ **Consulta de Trámites Oncológicos:** disponer de una visión personalizada como el remitente del tratamiento, es decir que el operador podrá tener la misma visualización a la que accede el remitente.
  - ➢ **Consultas:** visualizar los consumos por obra social, tratamientos autorizados para un afiliado específico, tratamientos con acontecimientos.
  - ➢ **Gestión de anulaciones:** desde esta funcionalidad se podrá iniciar resolución, actualizar, filtrar o dar por resuelto.
- ✓ ***APLICACIÓN WEB DE ONCOLOGÍA/ PROTOCOLOS:*** aplicación web para la gestión de tratamientos oncológicos y especiales por parte de las delegaciones (UGLs y agencias) y médicos prescriptores. Esta aplicación cuenta con las siguientes herramientas de trabajo:

- **Solicitud de Tratamiento:** carga de un nuevo tratamiento desde cero, independientemente del motivo que genere su ingreso (ya sea un inicio de tratamiento, una renovación, un cambio por toxicidad, un cambio por progresión, un mantenimiento o un complemento).
- **Consulta de Tratamientos:** visualización de todos los tratamientos que se gestionen durante la carga y/o tramitación diaria: Tratamientos de cada delegación del INSSJP – ya sea la Sede Central, Agencia, Boca de Atención – (con la posibilidad de consultar también todos los tratamientos cargados en el ámbito/jurisdicción de su UGL). Los tratamientos aparecen clasificados/ordenados en distintas 'bandejas', dependiendo el estado o instancia en la cual el tratamiento se encuentre dentro del proceso de tramitación.
- **Médicos:** gestión para alta, baja y/o modificación de los datos de los médicos tratantes.
- **Avisos Afiliados:** listado con los cambios de estado de los tratamientos de los afiliados por delegación o la UGL en general. Funciona como una "lista de control" para confirmar en el sistema que el afiliado fue notificado respecto al estado de un tratamiento oncológico solicitado.
- **Tratamiento por Afiliado:** consulta de todos los tratamientos de los afiliados del INSSJP en todo el país. Gestión del traslado de un afiliado de una delegación a otra.
- **Historial del Tratamiento:** consultar el historial de la gestión del trámite, incluyendo las observaciones cargadas, los cambios de estado y los usuarios intervinientes.
- **Devolver un Tratamiento:** esta función le permite al médico de UGL/Agencia, devolver el tratamiento al usuario administrativo que lo cargó/inició.
- **Reclamar un Tratamiento:** para los tratamientos elevados a nivel central (ya sea por protocolos o por vía de excepción), se podrá cargar un reclamo a través del sistema para solicitar la evaluación del mismo y generarle una alerta a ese nivel.
- **Solicitar Anulación:** funcionalidad para cuando sea necesario anular un tratamiento.
- **Imprimir Ficha:** impresión de la ficha (resumen de lo cargado en el sistema).
- **Imprimir Ficha para Afiliado:** constancia al afiliado con la información completa del tratamiento y los medicamentos cargados.
- **Consultar mensajes:** permite revisar la información cargada hasta el momento y también comunica qué falta completar para finalizar con la carga del tratamiento.

- **Sistema para el Circuito de Identificación de Talonarios de Recetas (CIT):**
  El Circuito de Identificación de Talonarios (CIT) posibilita la trazabilidad de la impresión y logística de los talonarios de recetas manuales (recetarios celestes) del Instituto. Se asignan diferentes estados a los talonarios, conforme van sucediendo los distintos movimientos de las cajas que los contienen. Esta aplicación cuenta con las siguientes herramientas de trabajo:

✓ ***EMISIÓN TALONARIOS:*** instancia donde el proveedor confirma la emisión/impresión correcta de los talonarios/cajas de recetas, que posteriormente serán enviadas a las distintas Unidades Operativas del INSSJP.
✓ ***RECEPCIÓN TALONARIOS:*** evento por el cual, en cada una de las Unidades Operativas del Instituto, se confirmará la recepción de los talonarios / cajas enviadas desde imprenta.
✓ ***RECEPCIÓN AGENCIA:*** en el caso de que un talonario sea enviado a una agencia, el mismo tomará un estado intermedio denominado "*enviado a agencia*".
✓ ***ENVÍO A PRESTADORES:*** estado que toma un talonario cuando el mismo es entregado desde una Agencia/UGL al prestador. En esta instancia, se validará claramente que el prestador al cual se le entregan los talonarios, cuente con una relación contractual con el INSSJP.
✓ ***ACTIVACIÓN PRESTADORES:*** a través de este módulo se genera la activación de los talonarios. Un talonario activado permite que la receta que se prescriba pueda ser dispensada.

3.2. Marco normativo e institucional

En 1971, a través de la Ley Nº 19.032[15], se crea el Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP) , persona jurídica de derecho público no estatal que posee individualidad financiera y administrativa. Esta ley fue reglamentada a través del Decreto Nº 1157/71[16]. La Ley 19.032, de acuerdo al artículo 15 expresa lo siguiente, … *"El Instituto queda comprendido en las disposiciones de la Ley 18610 estando excluido del control del Tribunal de Cuentas de la Nación y del régimen de la ley de contabilidad"…*

[15] http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16081/norma.htm
[16] http://servicios.infoleg.gob.ar/infolegInternet/resaltaranexos/50000-54999/53259/norma.htm

Con posterioridad, ya transcurriendo el año 2002, se dicta la Ley Nº 25.615[17] que modifica la ley de creación del Instituto e introduce cambios, estableciendo en su artículo primero que la auditoría externa del mencionado organismo, estará a cargo de la Auditoría General de la Nación:

"ARTICULO 1º — Modifícase el artículo 1º de la Ley Nº 19.032, el que quedará redactado de la siguiente manera:

Artículo 1º: Créase el Instituto Nacional de Servicios Sociales para Jubilados y Pensionados, que funcionará como persona jurídica de derecho público no estatal, con individualidad financiera y administrativa, de acuerdo con las normas de la presente ley.

Su acción queda sometida al contralor de la Sindicatura que se instituye en su seno, quedando su auditoría externa a cargo de la Auditoría General de la Nación.".

A su vez, la misma Ley 25.615 instituye que el Instituto será el encargado de brindar, por si o por terceros, atención a jubilados y pensionados de ANSES (Administración Nacional de la Seguridad Social); junto con sus familiares a cargo, y además se hace extensivo sus servicios a los pensionados. Asimismo, en el 2005 se creó el Programa Nacional de Atención de Veteranos de la Guerra de Malvinas y a su grupo familiar (que son los ex soldados y civiles que se encontraban cumpliendo funciones de servicio y/o apoyo a las FF.AA. o de Seguridad, entre el 2 de abril y el 14 de junio de 1982), a personas mayores de 70 años que no tengan ningún tipo de cobertura de obra social, personas sujetas a curatela, entre otros.

Al momento de realizar esta auditoría, el INSSJP es la obra social más grande de Latinoamérica, contando con casi 5 millones de afiliados.[18]

El Articulo 2 de la Ley Nº 19.032 establece que este Instituto tiene como objeto brindar a sus afiliados y familiares asistencia médica integral que incluya:*..."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*

[17] http://servicios.infoleg.gob.ar/infolegInternet/anexos/75000-79999/76149/texact.htm
[18] https://www.pami.org.ar/historia

particularidades e idiosincrasia propias de las diversas jurisdicciones provinciales y de las regiones del país." ...

Este articulo también dicta que … "*Estas prestaciones son consideradas servicios de interés público, siendo intangibles los recursos destinados a su financiamiento."...* Y que …"*el Instituto no podrá delegar, ceder o de algún modo transferir a terceros las funciones de conducción, administración, planificación, evaluación y control que le asigna la presente ley. Todo acto, disposición u omisión por parte de sus autoridades que infrinja este enunciado será declarado nulo de nulidad absoluta.*" …

A su vez, dentro de la Ley, y tal como lo establece el Art. 3 …"*podrá prestar otros servicios destinados a la promoción y asistencia social de los afiliados, tales como subsidios, préstamos con o sin garantía real, vivienda en comodato mediante programas y asistencia financiera de la Secretaría de Estado de Vivienda, asesoramiento y gestoría previsional gratuitos, promoción cultural, proveeduría, recreación, turismo y todo otro servicio que el Directorio establezca."...*

El gobierno y la administración del Instituto están a cargo de un Directorio Ejecutivo Nacional (DEN) y Unidades de Gestión Local (UGL).

A su vez, el Órgano Ejecutivo de Gobierno está integrado por un Director Ejecutivo y un Subdirector Ejecutivo, los cuales son designados por el Poder Ejecutivo Nacional (Art. 2 y 3, DNU Nº 2/2004[19]).

El Directorio Ejecutivo Nacional (DEN), tiene a cargo las siguientes funciones y responsabilidades según lo establecido por el Art. 6 de la Ley Nº 19.032:

- *"Administrar los fondos y bienes del Instituto, conforme a las necesidades de prestaciones y servicios planteados por las distintas regiones";*
- *"formular y diseñar las políticas globales en materia sanitaria y social, garantizando la equidad en la cantidad y calidad de los servicios ofrecidos por el Instituto en todo el territorio nacional, coordinando la planificación de las políticas del Instituto con las autoridades sanitarias jurisdiccionales respectivas";*

[19] http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=91557

- *"resolver sobre las propuestas formuladas por las Unidades de Gestión Local, dentro del marco de las políticas trazadas por el Instituto";*
- *"ejercer la administración general del Instituto, asimilando para sí los criterios de administración financiera y sistemas de control que en la materia rigen para el sector público nacional, en función de los cuales deberá dictar las reglamentaciones necesarias para regular la relación entre el Instituto y su personal —garantizando la carrera administrativa y programas de capacitación en todos sus estamentos—; con los afiliados y terceros; con las autoridades sanitarias jurisdiccionales a los fines de articular acciones en la materia; previendo en su caso los recursos";*
- *"establecer y controlar administrativa y técnicamente las prestaciones, reglamentar sus modalidades y beneficiarios y fijar, en su caso, los aranceles correspondientes";*
- *"dictar normativas que regulen la relación entre afiliados e Instituto, estableciendo un régimen de sanciones ante conductas dolosas contra este último";*
- *"Dictar todas las resoluciones y actos de disposición necesarios para el mejor desempeño de sus funciones";*
- *"Instituir nuevos servicios sociales destinados a asegurar una mejor calidad de vida de los afiliados, reglamentando su naturaleza, cuando razones de necesidad, como la incapacidad económica manifiesta, y otras urgencias ameriten su otorgamiento".*

Las Unidades de Gestión Local (UGL) reglamentadas bajo el Art. 6 bis de la Ley Nº 19.032 actúan …*"como unidad de ejecución de todos los programas implementados por el Instituto, elaborando propuestas y programas prestacionales para la jurisdicción, basados en los factores socio-demográficos, epidemiológicos, tasas de uso estimativas y costos de cada jurisdicción, de acuerdo a las normas establecidas por el DEN, asumiendo la responsabilidad de mantener a tal fin actualizado el padrón de afiliados de su área de cobertura."…*

Las Agencias de atención son las oficinas del INSSJP donde se realizan todos los trámites y solicitudes de los afiliados. Al momento de realizar esta auditoría, el Instituto cuenta con más de 600 Agencias de Atención y 38 Unidades de Gestión Local (UGL).

En cada UGL funcionará un Consejo Asesor que tiene carácter honorario y consultivo con las siguientes funciones que le asigna el Art. 6 bis de la Ley Nº 19.032:

- "*Elaborar propuestas y programas prestacionales para la U.G.L;*
- *Asesorar sin carácter vinculante al Director Ejecutivo local;*
- *Realizar todas las acciones que fueran necesarias para garantizar la calidad y transparencia de la gestión".*

La Ley Nº 19.032 creó el Consejo Federal de Servicios Sociales para Jubilados y Pensionados, que se encuentra presidido por el presidente del DEN. Los candidatos son propuestos por entidades representativas del sector pasivo (jubilados y pensionados), que tengan personería jurídica otorgada.

Este Consejo tiene como principales funciones las siguientes (Art. 15 bis, Ley Nº 19.032, incorporado por la Ley Nº 25.615):

- *"Seleccionar a los representantes de los beneficiarios que integraran el Directorio Ejecutivo Nacional;*
- *Analizar el funcionamiento integral del Instituto en todo el país, proponiendo al DEN acciones tendientes a garantizar la cantidad y calidad de las prestaciones, resguardando su equidad en todo el territorio nacional;*
- *Conforman en sus jurisdicciones de origen un Consejo Asesor de la respectiva UGL que representa los intereses de los beneficiarios."*

Por Decreto de Necesidad y Urgencia-DNU 297/20, en el marco de la pandemia del virus COVID-19, entre sus considerandos se dispuso …"*proteger la salud pública como una obligación inalienable del Estado nacional, se estableció para todas las personas que habitan en el país o se encuentren en él, la medida de "aislamiento social, preventivo y obligatorio", por un plazo determinado*[20]…, durante el cual todas las personas debían permanecer en sus residencias habituales o en el lugar en que se encuentren y abstenerse de concurrir a sus lugares de trabajo, debiendo cumplir sus obligaciones mediante modalidad de trabajo remoto (Decisión Administrativa (DA) 280/21)[21]. Asimismo, se estableció la prohibición de

[20] https://servicios.infoleg.gob.ar/infolegInternet/anexos/335000-339999/335741/texact.htm
[21] https://www.boletinoficial.gob.ar/detalleAviso/primera/242410/20210329

desplazarse por rutas, vías y espacios públicos, a fin de prevenir la circulación y el contagio del mencionado virus. La DA 390/20 estableció la dispensa del deber de asistencia a su lugar de trabajo, a las personas que estén comprendidas en alguno de los grupos de riesgo.[22]

En este sentido, las medidas de aislamiento social, el trabajo remoto y las restricciones de movilidad implementadas por los Decretos 297/2020, 325/2020, 355/2020, 408/2020, 459/2020, 493/2020, 520/2020, 576/2020, 605/2020, 641/2020, 677/2020, 714/2020, 754/2020 y subsiguientes[23], para controlar la propagación del virus implicaron, entre otros, desafíos operativos para los organismos gubernamentales.

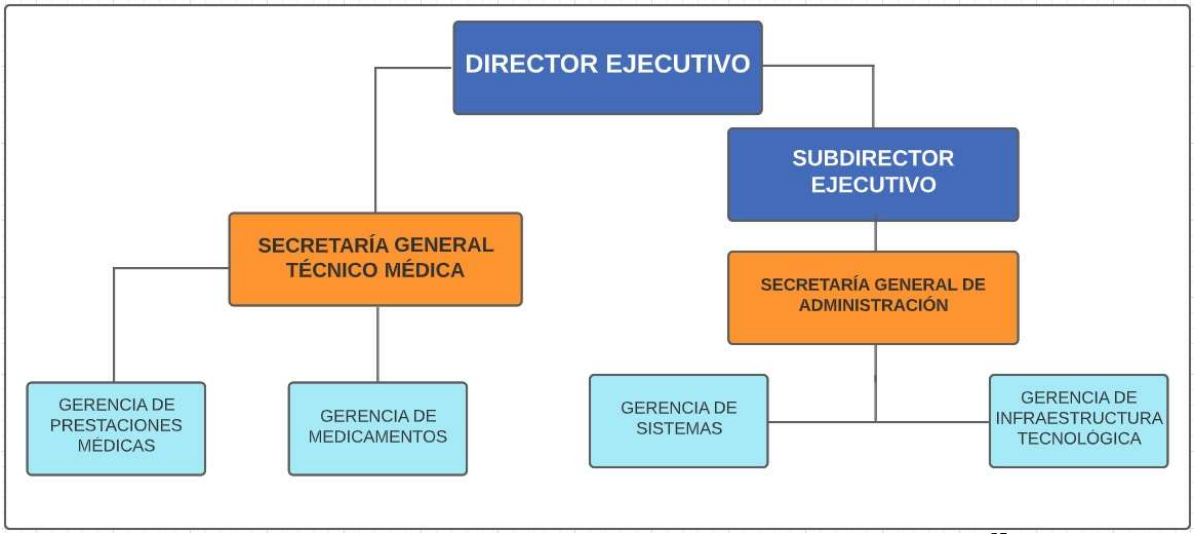
En lo relacionado específicamente a los procesos destacados para su análisis, el área del INSSJP vinculada es la Gerencia de Medicamentos, dependiente de la Secretaria General Técnico Médica, a su vez dependiente de la Dirección Ejecutiva. (Resolución N° 810/DE/18[24]).

Esta Secretaria General Técnico Médica, asiste al órgano de gobierno en la planificación estratégica de las políticas de salud implementadas en el ámbito de competencia del INSSJP, tendientes a favorecer la atención y cuidado de la salud de los afiliados. (Resolución Nº 678/DE/17[25], anexo X) y la Gerencia de Medicamentos es la encargada de dar cumplimiento a la política de medicamentos establecida por la Dirección Ejecutiva del Instituto, definiendo los protocolos de fiscalización y control técnico operativo. (Resolución Nº 899/DE/19[26])

A continuación, se presenta el organigrama de las áreas que involucran el objeto de auditoría y los procesos destacados:

[22] https://www.boletinoficial.gob.ar/detalleAviso/primera/226846/20200317
[23] https://www.boletinoficial.gob.ar/detalleAviso/primera/235132/20200920
[24] https://institucional.pami.org.ar/files/boletines_inssjp/01-08-18.pdf
[25] https://institucional.pami.org.ar/files/boletines_inssjp/12-07-17.pdf
[26] https://institucional.pami.org.ar/files/boletines_inssjp/13-05-19.pdf

Ilustración N°1: Organigrama de las áreas que involucran el objeto de auditoría y los procesos destacados



Fuente: elaboración propia –DAI - Resolución RESOL-2021-369-INSSJP-DE#INSSJP[27]

En el año 2016 se estableció la obligatoriedad del uso del Sistema de Receta Electrónica para todos los agentes médicos que trabajen en las dependencias del Instituto o en efectores sanitarios propios, médicos de cabecera y prestadores médicos con convenio, de acuerdo a las pautas técnicas vigentes. Al momento de realizar sus recetas, los prestadores deberán cumplir con los requisitos establecidos en la Ley Nº 25.649, de *Especialidades Medicinales- "Promoción de la utilización de medicamentos por su nombre genérico",* que tiene por objeto proteger al consumidor de medicamentos y drogas farmacéuticas y su utilización como medio de diagnóstico en tecnología biomédica y todo otro producto de uso y aplicación en la medicina humana. (Resolución N° 1304/DE/16[28]).

Es importante mencionar que se ha delegado en la Secretaría General de Planificación y Modernización, la facultad para elaborar los procedimientos, normas, cronogramas de implementación a cargo de los distintos profesionales vinculados al Instituto y demás herramientas necesarias, a fin de instrumentar la utilización del Sistema de Receta Electrónica, así como también es facultad de esta Secretaría, coordinar con el conjunto de las demás áreas

[27] http://institucional.pami.org.ar/files/boletines_inssjp/RESOL-2021-369-INSSJP-DE-INSSJP.pdf
[28] https://institucional.pami.org.ar/files/boletines_inssjp/25-07-16.pdf

del Instituto inherentes, y arbitrar los medios necesarios para efectivizar la obligatoriedad del uso del Sistema de Receta Electrónica. (Resolución N°1304/DE/16).

Antes de la implementación de la receta electrónica, los prestadores expedían recetas manuales color verde, este tipo de receta ya no podrá ser emitida por los prestadores, salvo que hayan solicitado la excepción por las vías comunicacionales formalmente establecidas por el Instituto.

En este sentido, la Secretaría aprobó un cronograma de implementación para la utilización del Sistema, el cual incluyó a los agentes internos y a los prestadores con convenio. Aquellos prestadores que demuestren no poder cumplir, deberán solicitar una excepción ante la Unidad de Gestión Local correspondiente. (Disposición Nº 4/SGPM/2016[29])

En 2019 se incorpora la firma digital como otro medio válido de suscripción de las recetas por parte de los médicos prescriptores en el Sistema de Receta Electrónica. De esta manera, los médicos de cabecera del INSSJP, pueden firmar las recetas digitalmente y prescribir medicamentos sin sello ni firma manuscrita. Este punto es importante, dado que tiene por objetivo agilizar el proceso de realización de una prescripción y, en consecuencia, busca optimizar la dispensa de medicamentos a los afiliados. (Resolución Nº 1162/2019.INSSJP[30]). Por su parte, el Decreto 182/19[31] menciona al respecto de la firma digital entre sus considerandos lo siguiente ...*" Que la creación de un clima de confianza en el entorno digital es esencial para el desarrollo económico y social, por lo que resulta conveniente reforzar la confianza en las transacciones electrónicas en nuestro país, para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas y la Administración Pública e incrementar, en consecuencia, la economía digital, la prestación de servicios en línea públicos y privados y el comercio electrónico" ...*

Durante el periodo auditado, el INSSJP implementó dos tipos de recetas que pueden ser brindadas por los prestadores a los afiliados:

1) La receta electrónica (blanca), medio obligatorio según lo que será indicado y se emana de las resoluciones que se expondrán en el párrafo siguiente, la cual contiene una serie de medidas

[29] https://institucional.pami.org.ar/files/boletines_inssjp/05-08-16.pdf
[30] https://institucional.pami.org.ar/files/boletines_inssjp/21-06-19.pdf
[31] https://www.argentina.gob.ar/normativa/nacional/decreto-182-2019-320735/texto

de seguridad que permiten garantizar que se reciban los medicamentos que el médico le prescribió al afiliado.

2) Las recetas manuales (celestes), para casos puntuales (por ejemplo, en el caso que recete una ambulancia que acudió al domicilio del afiliado) respaldados con un proceso de validación y autorización, debidamente activadas a través del Circuito de Identificación de Talonarios (CIT), medida de seguridad que incluye un sistema de activación que garantiza la validez de la receta al momento de la entrega de los medicamentos e insumos. Las recetas celestes no activadas no son aceptadas en farmacias[32].

En el ámbito de recetas electrónicas, el INSSJP tiene implementada la siguiente normativa vigente al momento de las tareas de campo de esta auditoría:

- Establecer con carácter obligatorio para todos los agentes médicos que trabajen en las dependencias del INSSJP o en efectores sanitarios propios, médicos de cabecera en relación de dependencia y prestadores médicos con convenio la utilización del Sistema de Receta Electrónica. (RESOLUCIÓN Nº 1304/DE/16)

- Establecer con carácter obligatorio a partir de la entrada en vigencia de la Resolución Nº 636/DE/18, que los insumos e insulinas deberán prescribirse y dispensarse en receta electrónica exclusivamente no pudiendo hacerse en receta manual. (RESOLUCIÓN Nº 636/DE/18[33])

- Establecer que todos los medicamentos oncológicos para los afiliados del Instituto deberán prescribirse y dispensarse en receta electrónica exclusivamente, no pudiendo hacerse en receta manual. (RESOLUCIÓN Nº 2018-848-INSSJP-DE#INSSJP[34])

- Establecer la prescripción electrónica de medicamentos mediante el uso del Sistema de Receta Electrónica, como condición suficiente para el acceso de las personas afiliadas al INSSJP a la dispensa de medicamentos en farmacia (RESOLUCIÓN Nº 2020-1110-INSSJP-DE#INSSJP[35])

[32] www.pami.org.ar/validador-receta-manual
[33] https://institucional.pami.org.ar/files/boletines_inssjp/27-06-18.pdf
[3434] https://institucional.pami.org.ar/files/boletines_inssjp/24-08-18.pdf
[35] https://institucional.pami.org.ar/files/boletines_inssjp/30-03-20.pdf

A su vez, y concordantemente existe la Unidad Fiscal para la Investigación de Delitos Cometidos en el ámbito de actuación del INSSJP y su Programa de Atención Médica Integral (UFI-PAMI), encargada de recibir denuncias de particulares, afiliados, agentes del Instituto o de prestadores, referidas a acciones u omisiones que puedan constituir un delito en el ámbito de actuación del INSSJP-PAMI, entre otras funciones. (Resolución PGN N°155/04[36])

Finalmente, atento lo expuesto en todo este acápite, es dable destacar la importancia de la Ley 27.553 de Recetas Electrónicas o Digitales[37], en donde se manifiesta entre sus fundamentos lo siguiente … *"La receta digital es una herramienta en la gestión sanitaria que permite un mejor control de las prescripciones, reducción de errores médicos, aceleración o simplificación del proceso en los centros de salud, aumento en la adherencia a los tratamientos crónicos, optimización de gestión en farmacias, crecimiento y ordenamiento en las capacidades de fiscalización y auditoria de la gestión de medicamentos, y disminución de los costos financieros entre otras ventajas"*[38] ...y del Decreto 98/2023[39], publicado el 28 de febrero de 2023 en el Boletín Oficial, qué reglamenta dicha ley, y en donde se centra especial atención a su principal objetivo …"*permitir que la prescripción y dispensa de medicamentos y toda otra indicación puedan ser elaboradas y firmadas a través de firmas electrónicas o digitales, en recetas electrónicas o digitales, en todo el territorio nacional. También contempla que puedan utilizarse en todo el país plataformas de tele asistencia en salud"*…. Así mismo menciona al respecto que… "*la presente Reglamentación no altera la vigencia de la receta con firma manuscrita, conforme la normativa que la regula"*…

Adicionalmente, el mencionado decreto reglamentario crea la **Licencia Sanitaria Federal**, que consiste en una única identificación que incluirá todas las matrículas habilitantes de los y las profesionales de la salud, registrados y registradas en la Red Federal de Registros de Profesionales de la Salud (REFEPS), y que será complementaria de las mismas. En este sentido, la Licencia Sanitaria Federal asignará una **Clave Única de Identificación de Profesional Sanitario**, que permitirá identificar de manera unívoca a las y los profesionales

[36] https://www.mpf.gov.ar/resoluciones/pgn/2004/pgn-0155-2004-001.pdf
[37] https://servicios.infoleg.gob.ar/infolegInternet/anexos/340000-344999/340919/texact.htm
[38] https://www.hcdn.gob.ar/proyectos/proyectoTP.jsp?exp=3979-D-2019
[39] https://servicios.infoleg.gob.ar/infolegInternet/anexos/380000-384999/380005/norma.htm

de la salud, como también acceder a los sistemas interoperables para la implementación de las Tecnologías de la Información y la Comunicación (TIC) en el Sistema Sanitario Argentino

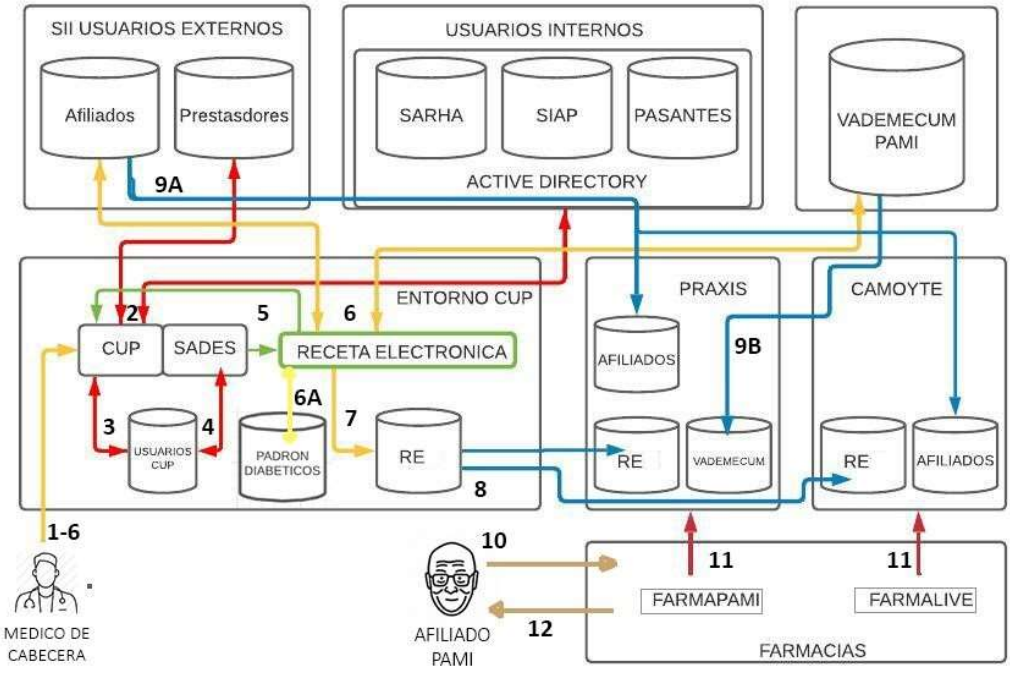
3.3. Descripción de los procesos sujetos al análisis de esta auditoría

Los principales procesos de control de la plataforma tecnológica CUP que serán motivo de análisis en función del objeto de auditoría establecido, se encuentran incluidos en el Sistema de Recetas Electrónicas, desde la prescripción de un medicamento hasta la liquidación al INSSJP por parte de los proveedores que dispensan los medicamentos recetados a los afiliados, a través de las farmacias adheridas al Instituto.

A continuación, se describen los procesos indicados.

3.3.1 Proceso de ingreso al sistema CUP - Receta Electrónica, prescripción y dispensa de medicamentos:

Ilustración N°2: Diagrama del proceso.



Fuente: elaboración propia –DAI- en base a la información provista por la Gerencia de Sistemas y la Gerencia de Medicamentos del INSSJP y de los relevamientos realizados con personal de estas áreas durante las tareas de campo.

INTERVENCION DE LA INFRAESTRUCTURA TECNOLÓGICA DEL INSSJP (1-7)

1- El médico de cabecera accede al Sistema CUP mediante la página web correspondiente (https://cup.pami.org.ar/) donde ingresa su usuario y contraseña.

2- El sistema valida que el usuario sea efectivamente un usuario activo en los padrones del INSSJP. En caso de ser un usuario externo del INSSJP, el sistema validará buscando su estado en la base de prestadores del Sistema Interactivo de Información (SII), en caso de ser un usuario interno del INSSJP, el sistema va a validar su estado en el *Active Directory* que contiene las diferentes bases de datos de personal del Instituto según su situación contractual[40].

3- Si el usuario no está activo en ninguno de estos dos sistemas, no le permitirá el acceso a la plataforma CUP. Si el usuario está habilitado para ingresar al sistema, CUP va a validar que se encuentre registrado en la base de datos de usuarios propia de la plataforma.

4- Si el usuario no está registrado en el sistema CUP, deberá completar el formulario de registro. Si el usuario está registrado, el SADES chequeará en la base de datos, el rol, los permisos y las aplicaciones que tiene habilitadas.

5- En esta descripción tomamos como ejemplo a un usuario que tiene acceso al Sistema de Receta Electrónica, razón por la cual el SADES, desde la pantalla de la plataforma CUP, habilitará el acceso del usuario a esta aplicación en el menú correspondiente.

6- En esta instancia, el profesional ya está habilitado para prescribir recetas a través del Sistema de Receta Electrónica. Cuando el médico cargue el número de afiliado, el sistema va consultar en el padrón de afiliados del SII que el mismo esté activo y vigente como tal, y para la carga del medicamento, el sistema buscará en el VADEMECUM PAMI. Si ambos datos son correctos, podrá finalizar la generación de la receta.

[40] Usuarios de Planta: Válida en sistema Sarha de RRHH, Usuarios contratados: Válida en contra Sistema Sap y Usuarios Pasantes: Active Directory - Login y Alta de usuario.

6A- Si el medicamento recetado se corresponde con la enfermedad de diabetes, el Sistema de Receta Electrónica verificará también que dicho afiliado se encuentre inscripto en el padrón de diabéticos.

7- Una vez generada la receta, la misma se guarda en la base de datos del Sistema de Receta Electrónica.

INTERVENCIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DE PRAXYS Y CAMOyTE-[41] (8-11)

8- Cuando la receta ya está generada en la base de datos del Sistema de Receta Electrónica, su información es enviada online mediante un *web service*[42] en formato XML[43] a la base de datos de recetas de los sistemas provistos por PRAXYS y CAMOyTE. Si el medicamento recetado es de tipo ambulatorio, la información será enviada a la red de PRAXYS, y si el medicamento es especial o de alto costo (oncológicos, HIV), la información será enviada al sistema de CAMOyTE. Esta validación sobre el tipo de medicamento se realiza a través del vademécum.

9- **A**- Una vez por semana el INSSJP envía a las proveedoras PRAXYS y CAMOyTE el padrón de afiliados en forma completa, utilizando un *job*[44] automatizado a un sitio

[41] CAMOyTE: Centro de Autorización de Medicamentos Oncológicos y Tratamientos Especiales) es la denominación usualmente utilizada en el ámbito del PAMI para referirse a la ACE – ONCOLOGÍA (Agrupación para la administración de contratos de Oncología y Tratamientos Especiales), con quien el INSSJP suscribió un contrato para la administración de los medicamentos "OYTE" (Oncología y Tratamientos Especiales), hemofilia y suplementos nutricionales (Convenio Marco de Adhesión 2018, disponible en https://prestadores.pami.org.ar/medicamentosPAMI/convenio_marco_v4.pdf). ACE– ONCOLOGÍA es una persona jurídica constituida como *agrupación* en los términos de los artículos 1453 a 1462 del Código Civil y Comercial de la Nación. Este tipo de organización tiene por finalidad facilitar o desarrollar determinadas fases de la actividad de sus miembros, no pueden tener fines de lucro y su plazo no puede superar los diez años (Arts. 1453º, 1454º y 1455º). En el sitio web de la agrupación se encuentra el link de acceso al software Farmalive (https://www.aceoncologia.com.ar), que utilizan las farmacias adheridas al INSSJP para cumplir con la dispensa de medicamentos.

[42] Un servicio web (en inglés, *web service* o *web services*) es una tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones. Distintas aplicaciones desarrolladas en lenguajes de programación diferentes, y ejecutadas sobre cualquier plataforma, pueden utilizar los servicios web para intercambiar datos en redes de computadoras como Internet. La interoperabilidad se consigue mediante la adopción de estándares abiertos.

[43] XML, por sus siglas en inglés *Extensible Markup Language,* que en español significa Lenguaje de Marcas Extensibles, es un estándar informático abierto, flexible ampliamente utilizado para almacenar, publicar e intercambiar cualquier tipo de información.

[44] En informática, un *job es un c*onjunto de programas que producen un trabajo útil al usuario y que son procesados uno a continuación de otro y que se ejecutan cada cierto tiempo.

FTP[45] dispuesto por estas empresas. A su vez, si hubiera alguna novedad en este padrón se realiza el envío el mismo día en que se produce la actualización un *web service.*

B- Desde el sistema VADEMECUM PAMI se exporta el vademécum en formato de planilla de cálculo y por medio de un web service, se envía a un servidor FTP de PRAXYS las novedades que haya/n sobre el vademécum de medicamentos, con el fin de que la empresa pueda actualizar esta información en sus bases.

10- El afiliado debe presentarse en la farmacia (puede optar por cualquier farmacia que opere con el INSSJP) con el DNI y el carnet de la obra social.

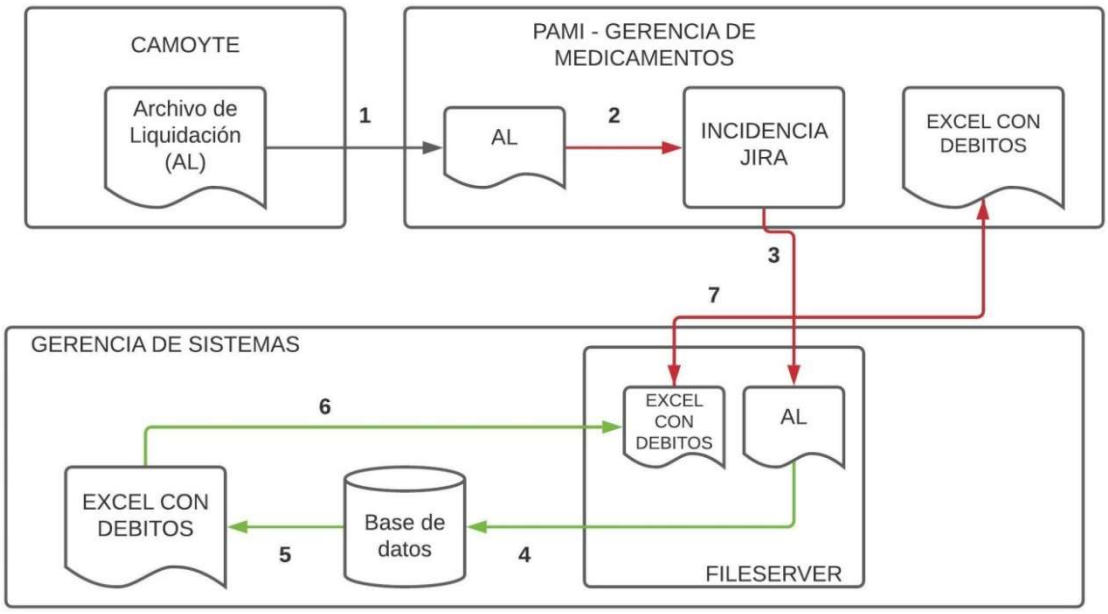
11- Si el medicamento recetado es ambulatorio, el farmacéutico utilizará la aplicación FARMAPAMI[46], desarrollada y mantenida por la empresa PRAXYS, con el fin de conectar a sus servidores para validar la receta, el afiliado y el vademécum de medicamentos, así como para proceder a su liquidación y facturación. Y si el medicamento es especial o de alto costo, el farmacéutico utilizará la aplicación FARMALIVE[47], desarrollada y mantenida por CAMOyTE, con el fin de conectar a sus servidores para validar la receta, el afiliado y el vademécum de medicamentos, así como para proceder a su liquidación y facturación.

12- Si las validaciones que realice el sistema FARMAPAMI o FARMALIVE son exitosas, el farmacéutico está habilitado para dispensar el medicamento al afiliado.

[45] FTP, por sus siglas en inglés *File Transfer Protocol,* que en español significa Protocolo de Transferencia de Archivos, es un protocolo que se utiliza para transferir todo tipo de archivos entre equipos conectados a una red, por ejemplo, Internet.
[46] https://farma.pami.org.ar/seguridad/iniciar-sesion
[47] https://www.farmalive.com.ar/login.html

3.3.2 Proceso de liquidación de medicamentos mediante el sistema FARMALIVE

Ilustración N°3: Diagrama del proceso.



Fuente: elaboración propia-DAI- en base a la información provista por la Gerencia de Sistemas y la Gerencia de Medicamentos del INSSJP, así como de los relevamientos realizados con personal de estas áreas durante las tareas de campo.

El proceso de liquidación comienza con el envío de una liquidación provisoria en archivo .txt[48] y en formato papel (digitalizado), luego sobre esta liquidación se realiza un control preliminar administrativo que habilita el desembolso del 75% de dicha facturación y que será la base de la liquidación final, posteriormente conformada por parte de CAMOyTE, siguiendo el siguiente proceso:

1- CAMOyTE genera y envía por email al Departamento Único de Recepción de Facturas (DURF) los archivos de liquidación. La liquidación para validar el total de los medicamentos dispensados a los afiliados del INSSJP, se envía en formato de texto

[48] Un **archivo TXT** es un archivo de texto sin formato que no requiere de ningún programa especial para su creación y apertura.

plano (archivo del tipo .txt y archivo del tipo .prn[49]) y también en formato papel. El DURF caratula el expediente y lo envía al Departamento de Ingreso de Facturación (DIF) donde registra contablemente la liquidación.

2- El DIF remite el expediente a la Gerencia de Medicamentos, donde el Departamento de Contabilidad crea una incidencia en Jira[50] del tipo GD (Gestión de la Demanda), en la que se adjuntan los archivos de la liquidación (En caso que por su tamaño los archivos no pudieran ser adjuntados al sistema Jira, se subirán a un file server[51] compartido entre las áreas) y en el cual solicita la tarea de procesamiento de la información al Departamento de Desarrollo de Sistemas de Provisión de Medicamentos, dependiente de la Gerencia de Sistemas.

3- El Departamento de Desarrollo de Sistema de Provisión de Medicamentos toma el ticket y descarga los archivos adjuntos en el ticket del Jira o bien si fueron depositados por la Gerencia de Medicamentos, en el servidor de recurso compartido (*Fileserver*) para el caso de que el tamaño de los archivos no permita adjuntarlos al ticket del Jira.

4- Se importan los archivos a la base de datos y se ejecutan los procesos de conciliación y control de datos con el objetivo de realizar el control correspondiente sobre la liquidación y así poder obtener los débitos que correspondieran aplicar a la liquidación enviada por CAMOyTE.

5- Se genera el archivo de resultados en formato de planilla de cálculo con la liquidación y las marcas de errores encontrados.

6- El Departamento de Desarrollo de Sistema de Provisión de Medicamentos de la Gerencia de Sistemas responde el ticket de Jira generado por la Gerencia de Medicamentos (Punto 2), adjuntando, si su tamaño lo permitiese, la planilla de cálculo

[49] Un **Archivo** con extensión **PRN** almacena contenido listo para imprimir. **PRN** es una extensión genérica utilizada por muchas aplicaciones.
[50] **Jira** es una herramienta en línea utilizada por las áreas de sistemas de las organizaciones para la administración de tareas de un proyecto, el seguimiento de errores e incidencias reportados por la comunidad usuaria y los propios agentes del área de sistemas y para la gestión operativa de proyectos.
[51] Un file server o servidor de archivos es un tipo de servidor que almacena y distribuye diferentes tipos de archivos informáticos entre los clientes de una red de computadoras. Su función es permitir el acceso remoto a los archivos que almacena o sobre los que tiene acceso.

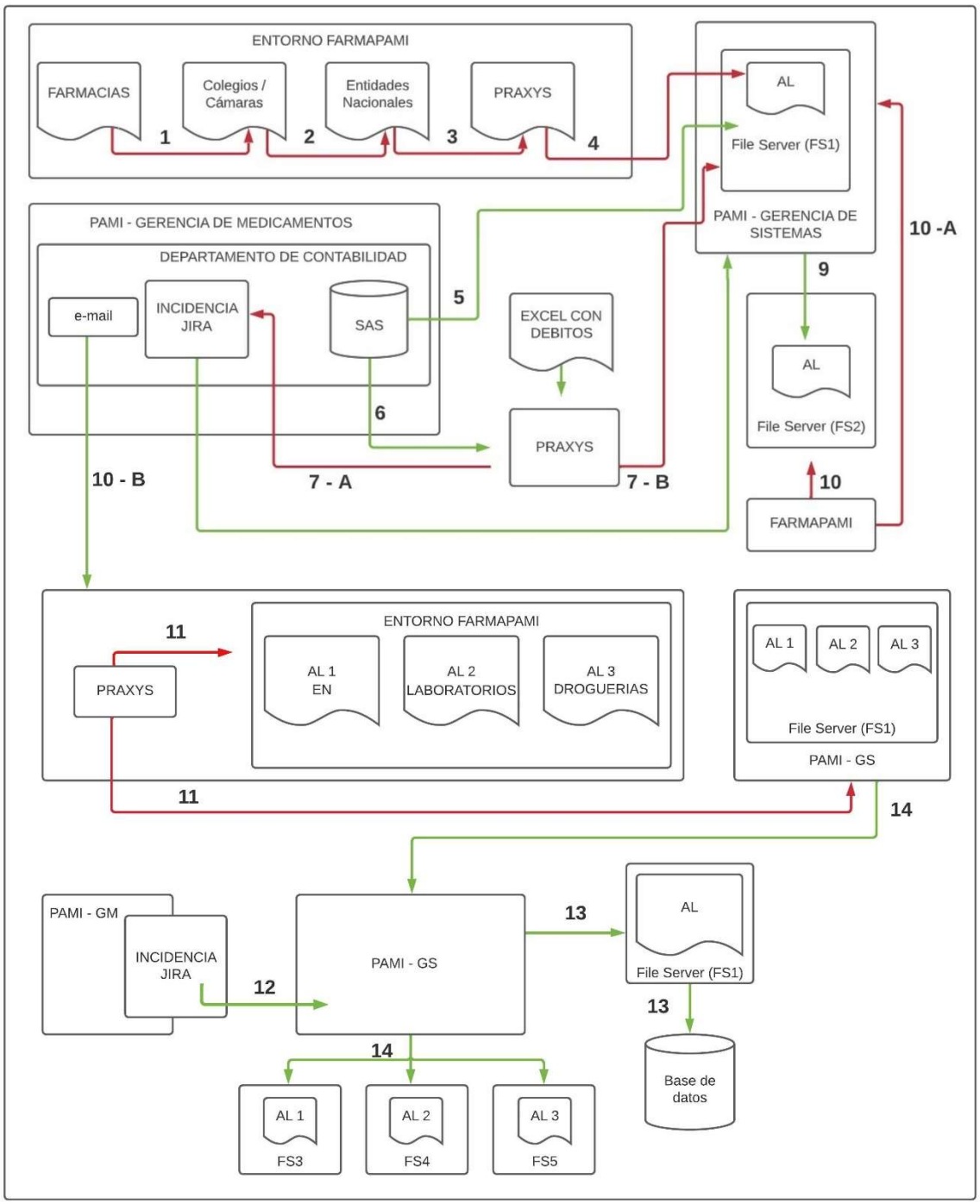
generada y en el caso de que el mismo no pudiera ser adjuntado al Jira, se deposita en el servidor de recurso compartido (*fileserver*) accedido por ambas gerencias.

7- El Departamento de Desarrollo de Sistema de Provisión de Medicamentos de la Gerencia de Sistemas solicita la validación en ticket de Jira a los fines de cerrar la tarea demandada por la Gerencia de Medicamentos y darla por concluida. Una vez cerrada la tarea, la Gerencia de Medicamentos inicia un proceso administrativo para gestionar los pagos y débitos que correspondan sobre la liquidación procesada.

El Departamento de Contabilidad valida el ticket Jira y comienza a trabajar sobre el análisis de los archivos resultantes del proceso de control. Analizados los archivos, se envían a CAMOyTE para la eventual subsanación de errores y la correcta trazabilidad de los productos faltantes. CAMOyTE, subsanados los errores, remite nuevamente los archivos y vuelve a comenzar el proceso indicado en el punto 4. Finalizado el mismo, se elabora un informe final con el resultado y los conflictos aplicables. En base al informe, la Gerencia de Medicamentos convalida los débitos a aplicar y remite el expediente a la Gerencia Económico Financiera dando por concluido el circuito.

3.3.3 Proceso de liquidación de medicamentos mediante el sistema FARMAPAMI:

Ilustración N°4: Diagrama del proceso.



Fuente: elaboración propia-DAI- en base a la información provista por la Gerencia de Sistemas y la Gerencia de Medicamentos del INSSJP, así como de los relevamientos realizados con personal de estas áreas durante las tareas de campo.

El proceso de liquidación se describe de la siguiente manera:

1. Quincenalmente las farmacias conforman la liquidación en el sistema FARMAPAMI, al cerrar la liquidación el mismo sistema las pone a disposición para ser validadas por los Colegios o Cámaras en la que cada farmacia se encuentre adherida.
2. Cuando los Colegios o Cámaras validan las mismas, esta información es consolidada y puesta a disposición de las cinco (5) entidades nacionales (EN): COFA, FACAF, FEFARA, FARMASUR y AFSMRA.
3. De esta manera el sistema FARMAPAMI les da acceso a estas cinco (5) entidades para cerrar el periodo y así consolidar toda la base de datos en una sola liquidación total.
4. Ese único archivo de liquidación (AL) es exportado del sistema FARMAPAMI por la empresa PRAXYS en formato de texto (.txt) y enviado al file server (FS1) del INSSJP que comparte la empresa con la Gerencia de Medicamentos y la Gerencia de Sistemas.
5. El Departamento de Contabilidad (DC), dependiente de la Subgerencia de Validación y Control de Medicamentos (SV), Gerencia de Medicamentos (GM), toma el archivo del file server (FS1) y utiliza el software SAS para analizarlo a los fines de detectar marcas de error.
6. El resultado de dicho análisis es un archivo de planilla de cálculo (.xls), el cual se analiza de forma manual para ratificar o rectificar los errores detectados por el software SAS[52].
7. Con el archivo Excel resultante se toman dos cursos de acción:

    A) De no existir errores (o subsanados los mismos), se establece el archivo de texto final de liquidación.

    B) De encontrarse errores, se envía por email un archivo Excel con el detalle de correcciones a realizar a la empresa PRAXYS, quien deberá proceder a

[52] SAS, es un aplicativo de análisis y gestión de datos de la empresa SAS Solutions (www.sas.com).

efectuar los cambios solicitados y el proceso se vuelve a repetir a partir del punto 4.

8. Una vez generado el archivo de texto final de liquidación, el DC genera un ticket de JIRA, solicitando a la Gerencia de Infraestructura Tecnológica (GIT) que tome el archivo de texto de liquidación del file server (FS1) y lo ponga a disponibilidad de la empresa

   FARMALINK[53] (empresa que actúa como representante o administrador de los laboratorios en este punto del proceso) en un file server (FS2) compartido por el administrador, la Gerencia de Sistemas (GS) y la Gerencia de Medicamentos.

9. La Gerencia de Sistemas toma el archivo de texto de liquidación del file server (FS1) y lo pone a disposición de la empresa FARMALINK (como representante de los laboratorios) en un file server (FS2) compartido entre la empresa, la GS y GM.

10. FARMALINK tiene 48 horas para revisar y objetar la liquidación del INSSJP. En este punto la empresa tiene dos opciones:

    A) Si la empresa objeta la liquidación del INSSJP, el proceso se repite y reinicia nuevamente desde el punto 4.

    B) Si el archivo de liquidación enviado es aceptado, el INSSJP le notifica por email a PRAXYS que puede continuar con la liquidación.

11. PRAXYS utilizando el sistema FARMAPAMI, genera en base a la liquidación final, los archivos para las EN, los laboratorios y las droguerías. Todos estos archivos son puestos a disposición del INSSJP en el FS1.

12. Mediante un ticket de JIRA, la Gerencia de Medicamentos solicita a la Gerencia de Infraestructura Tecnológica que exporte el archivo final de liquidación (AL) (Ver punto 7A) a una tabla maestra de la base de datos del INSSJP y que ponga a disposición de las Entidades Nacionales, laboratorios y droguerías, los archivos de liquidación generados, descriptos en el punto 10, en el file server que corresponda según el acceso de cada actor.

[53] Empresa especializada en la administración y auditoría de **la dispensación de medicamentos ambulatorios en las farmacias** para agentes del Seguro de salud (obras sociales, empresas de medicina prepaga, etc.) en todo el país. https://www.farmalink.com.ar/home/#/#empresa

13. Gerencia de Medicamentos exporta el archivo final de liquidación (AL) a la base de datos maestra.

14. Gerencia de Medicamentos pone a disposición de las Entidades, laboratorios y droguerías, los archivos de liquidación generados y descriptos en el punto 10 dentro del file server que corresponda según el acceso de cada actor (FS 3, FS 4 y FS 5, de acuerdo a la Ilustración Nº 4).

Finalmente, la Gerencia de Medicamentos envía a cada entidad el valor a facturar (y corroborar contra el archivo que tiene disponible en el file server) y a la Gerencia Económico Financiera del INSSJP, se le remite una nota convalidando los montos para que esta pueda luego, cruzarla con la facturación que remitan las entidades.

3.4. Cumplimiento de Disposiciones AGN (Nº 62/22, Nº 198/18 y Nº 182/12)

3.4.1. Cumplimiento Ley 27.499, Ley Micaela, de Capacitación Obligatoria en Género para todas las personas que integran los Tres Poderes del Estado (Disposición AGN Nº 62/22)

El INSSPJ, a través de la Gerencia de Recursos Humanos, está llevando a cabo la capacitación obligatoria en género según lo dispuesto por la Ley 27.499 (Ley Micaela, de Capacitación Obligatoria en Género para todas las personas que integran los Tres Poderes del Estado).

El INSSJP cuenta con las certificaciones por parte del MINISTERIO DE LAS MUJERES, GÉNEROS Y DIVERSIDAD que por Decreto N° 7/2019[54], modificatorio de la Ley de Ministerios N° 22.520, suprimió el Instituto Nacional de la Mujer (INAM) que era su antecesor y a quién la Ley 27.499 [55] nombraba cómo autoridad de aplicación de la Ley Micaela, en consecuencia, y dada la actualización efectuada por el Decreto 7/2019, el MMGYD, es competente para establecer el procedimiento administrativo tendiente a la certificación de los programas de capacitación en la temática de género y violencia contra las mujeres elaborados por los diferentes organismo y áreas del Estado y es quién expide el informe técnico que fue elaborado por la Dirección de Capacitación del Sector Público en

[54] https://servicios.infoleg.gob.ar/infolegInternet/anexos/330000-334999/333138/norma.htm
[55]https://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318666/norma.htm

Género y Diversidad dependiente del MINISTERIO DE LAS MUJERES, GÉNEROS Y DIVERSIDAD mediante Providencia Nro. PV – 2022 – 108276310 – APN – DNFYCGDYE # MMGYD de fecha 12 de octubre de 2022 y el cual ratifica que los documentos presentados (programa de capacitación y el plan de trabajo) cumplen con los lineamientos para la elaboración de propuestas de capacitación en el marco de la Ley Micaela y los contenidos establecidos.

Del análisis de la documentación provista por el INSSJP sobre las capacitaciones realizadas surge que:

El 58% de los trabajadores de Planta Permanente realizaron el curso, quedando el porcentaje restante (42%) pendiente de cumplimiento. En tanto, en lo que refiere al personal contratado, solo el 10% de los trabajadores han realizado la capacitación. Todo ello se ve reflejado a continuación de acuerdo a la siguiente Ilustración:

Ilustración N°5: Trabajadores que realizaron la capacitación.

Situación laboral	Capacitadas/os	No capacitadas/os	Totales
Trabajadoras/es de planta permanente	7.398	5.440	12.838
Trabajadoras/es contratadas/os	159	1.441	1.600
Totales	7.557	6.881	14.438

Fuente: Información provista por el INSSJP en el marco de la presente auditoria.

3.4.2. Cumplimiento ODS (Disposición AGN Nº 198/18).

En lo que refiere al cumplimiento de los Objetivos de Desarrollo Sostenible (ODS), el auditado manifestó por Nota de respuesta ante el requerimiento de la AGN, que al respecto de la temática en cuestión, …*"este Organismo no posee una asignación o adhesión formal suscripta con dicha organización o bien con el estado nacional que establezca compromisos y metas."*…

3.4.3. Cumplimiento leyes 22.431, 25.689, 25.785 y modificatorias (Disposición AGN Nº 182/12).

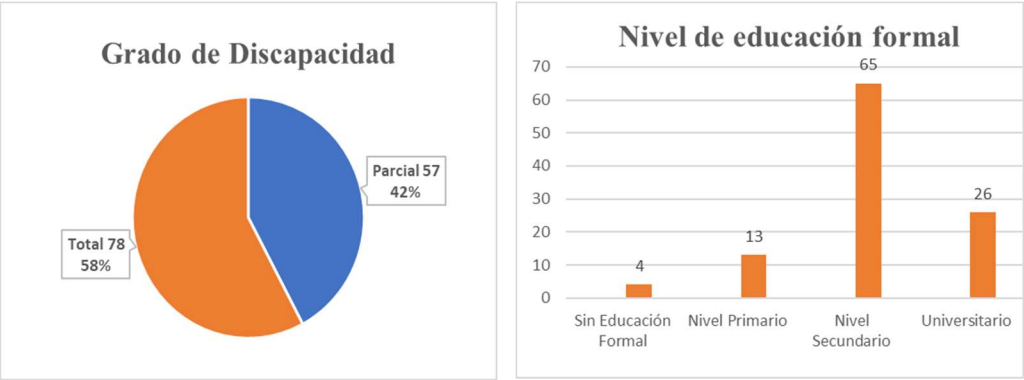
Sobre el cumplimiento del cupo laboral del 4% de ocupación de personas con discapacidad establecido en el artículo 8º Ley 22.431, la Gerencia de Recursos Humanos del Instituto informó a este equipo de auditoria que al 31/12/2022, contaba con una planta permanente de 12.845 empleados y una planta de trabajadores contratados de 1.522 personas.

Si bien el organismo expresa que no cuenta con la información del total de agentes con discapacidad ocupados, manifiesta que 135 agentes de planta permanente certifican discapacidad, y que a su vez, de esa cantidad, 57 agentes poseen una discapacidad parcial y los restantes 78, tienen discapacidad total. En este sentido, de acuerdo a lo informado a los efectos de la presente auditoria, estas cifras representan el 1% del total de los agentes de planta permanente.

Así mismo, sobre los niveles de educación de estos agentes se nos informa que 4 de ellos, no tienen educación formal, 13 cuentan con educación primaria, 65 con educación secundaria y 26 con educación universitaria.
El cuadro a continuación, proporcionado por el auditado, identifica lo antes descripto:

Planta Permanente	Contratados	Total	Discapacidad	% Total
12845	1522	14367	135	0,93965337

Ilustración N°6: Porcentajes de grado de discapacidad y nivel de educación formal.



Fuente: Realización propia del DAI, en base a información suministrada por el auditado.

4. HALLAZGOS

4.1. Gobierno de TI

4.1.1. *El INSSJP no realiza relevamientos con la comunidad usuaria en cuanto al nivel de satisfacción sobre la disponibilidad y las funcionalidades que ofrece el sistema de Receta Electrónica y sus sistemas relacionados. Esto conlleva al desconocimiento de la opinión de los usuarios respecto a los problemas, debilidades y requerimientos funcionales sobre el aplicativo, y del nivel de satisfacción sobre el soporte brindado por el instituto a los usuarios.*

En base al análisis de la documentación provista y de las entrevistas mantenidas con las áreas de servicio de la Gerencia de Sistemas y la de Tecnología, se pudo verificar que no se realizan relevamientos con la comunidad usuaria en cuanto al nivel de satisfacción sobre la disponibilidad y las funcionalidades que ofrecen los Sistemas del INSSJP.

Las buenas prácticas referidas a la gestión de usuarios indican que los relevamientos y encuestas de satisfacción de los usuarios respecto a los niveles de servicios de TI brindados, constituyen una herramienta de vital importancia para realizar las acciones correctivas, evolutivas y adaptativas sobre servicios de TI y las aplicaciones de acuerdo a los requerimientos dinámicos del negocio (ITIL v4 fase: Operación del Servicio y CobIT v4.1 DS8: Administrar la Mesa de Servicio y los Incidentes y DS10: Administración de Problemas).

La carencia de estos relevamientos impacta sobre el nivel de conocimiento del Instituto, sobre los problemas, así como también en las necesidades técnicas y funcionales de los usuarios de la plataforma CUP (Receta electrónica y relacionados). A raíz de esto, no se toman acciones correctivas, evolutivas y adaptativas de manera planificada sobre el sistema como parte integrante de un plan formalizado de mejora continua.

4.1.2. *El INSSJP no cuenta, para su plataforma tecnológica y para los servicios de soporte y mantenimiento continuo brindados por las Gerencias de Sistemas y Tecnología, con un adecuado ambiente de control interno que garantice la detección temprana de riesgos de TI y las acciones pertinentes para gestionarlos.*

A partir de las entrevistas mantenidas con las Gerencias de Sistemas y de Tecnología, y con los responsables de la UAI del organismo y de la evaluación de la documentación provista en materia de informes de auditoría, se constató que no se realizaron auditorías internas de TI sobre el Sistema de Recetas Electrónicas y sus procesos asociados durante el período auditado. Este escenario evidencia la falta de un efectivo control interno sobre los procesos y procedimientos llevados a cabo por la Gerencia de Sistemas y la Gerencia de Tecnología para la prestación de los servicios de TI al instituto, principalmente, sobre los procesos operativos del servicio de receta electrónica con alcance en la prescripción, dispensa y liquidación de medicamentos.

En función de lo establecido en la Res. 87/22 - SIGEN – Anexo-Normas de Control Interno para la Tecnología de la Información-, punto 12.1 -, las Unidades de Auditoría Interna definidas en la Ley 24.156, deben contemplar la ejecución de auditorías de sistemas, debiendo reunir los responsables de llevarlas a cabo los requisitos de competencia técnica, independencia y autoridad para efectuar revisiones objetivas de los controles informáticos y preparar informes sobre sus hallazgos y recomendaciones. Asimismo, en la Res. 87/22 - SIGEN – mismo punto, se establece que - la unidad de TI debe presentar informes periódicos de gestión a la dirección de la organización para que ésta supervise el cumplimiento de los objetivos planteados. De igual forma, deben elevarse reportes periódicos sobre la situación de la seguridad de la información.

Por último, las buenas prácticas referidas al control de TI (CobIT v4.1 - ME2.1: Monitorización del Marco de Trabajo de Control Interno y ME2.2: Revisiones de Auditoría), establecen que se debe monitorear de forma continua, comparar y mejorar el ambiente de control de TI y el marco de trabajo de control de TI para satisfacer los objetivos

organizacionales, y se debe evaluar la eficiencia y efectividad de los controles internos de revisión de la gerencia de TI.

La falta de un adecuado ambiente de control interno de TI sobre la plataforma tecnológica y los servicios brindados por las Gerencias de Sistemas y Tecnología, exponen al INSSJP a riesgos no detectados y, que por lo tanto, no son tratados.

4.2. Seguridad de la información

4.2.1. *El organismo no cuenta con una estructura organizacional adecuada para atender y gestionar las políticas y procedimientos de seguridad de la información aplicables transversalmente a toda la organización, ni tampoco tiene un Comité de Seguridad de la Información. Esta situación expone la vulnerabilidad del organismo ante la falta de implementación y correcto control sobre las políticas y procedimientos de seguridad de la información organizacionales y de un equipo especializado que las gestione para su debido cumplimiento, las revise y actualice periódicamente.*

Luego de evaluada la documentación técnica provista por el organismo y de las entrevistas mantenidas con la Gerencia de Tecnología, se constató que si bien el INSSJP aprobó su "Política de Seguridad de la Información" a través de la Disposición 0002/15 GYTC, y en la misma se designó al Subgerente de Seguridad Informática como Responsable de Seguridad de la Información del organismo, el mencionado cargo, incluso desde la aprobación de dicha política, luego durante el periodo auditado y aun mientras se llevaban adelante las tareas de campo, se encontraba acéfalo, evidenciándose la falta de constitución de un Comité de Seguridad de la Información que implemente, revise y gestione un Plan de Seguridad de la Información que abarque a todo el organismo, alineado a la política de seguridad de la información aprobada que se encargue de la ejecución operativa del plan, así como del cumplimiento de las políticas y procedimientos pertinentes.

En función de lo que establecen las buenas prácticas en la materia (ISO 27001 - Aspectos organizativos para la Seguridad de la Información; CobIT V4 - DS5.1: Administración de la Seguridad de TI y CobIT V4 - DS5.2: Plan de Seguridad de TI), toda organización debe

administrar adecuadamente la Seguridad de la Información a partir de los siguientes aspectos: i) concientizar internamente a la organización sobre la necesidad de implementar y cumplir con políticas y procedimientos que garanticen la salvaguarda de los activos de información de la organización y del negocio; ii) conformar un Comité de Gestión de Seguridad de la Información que dicte, formalice, controle y actualice las políticas y procedimientos de Seguridad de la Información; iii) asignar una estructura técnica especializada contando con todos los medios, recursos e insumos técnicos necesarios, dependiente de las máximas autoridades de la organización, para que se responsabilice de la administración integral de la Seguridad de la Información.

Que el organismo no implemente y mantenga en el tiempo estas buenas prácticas vinculadas a la Seguridad de la Información a nivel organizacional, pone en riesgo el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información.

4.2.2. *La estructura organizacional para administrar eficiente y efectivamente la seguridad de la información del INSSJP no es funcional respecto a lo establecido en la Política de Seguridad de la Información del organismo. Escenario que pone en riesgo la confidencialidad, integridad y disponibilidad de la información del Instituto.*

La Política de Seguridad de la Información del INSSJP (Disposición 0002/15 GYTC) designa al Subgerente de Seguridad Informática como Responsable de Seguridad de la Información del organismo. Sin embargo del análisis de la información suministrada por el auditado y de las entrevistas mantenidas con las áreas responsables de implementar dichas políticas, se ha podido comprobar que: i) la Subgerencia de Seguridad Informática no existe dentro de la estructura organizacional del organismo, motivo por el cual no se ha designado un subgerente de seguridad que pueda llevar adelante el rol que le impone la mencionada política de seguridad; ii) durante el periodo auditado y las tareas de campo el área “División de la Seguridad de la información y Seguridad Informática” se mantuvo acéfala; iii) la mencionada división se encuentra formalizada bajo la órbita de la Gerencia de Tecnología; y iv) durante las tareas de campo y en forma transitoria se le asignó la responsabilidad de la seguridad de la información a la Subgerencia de Gestión de la Demanda, dependiente también de la

Gerencia de Tecnología. No obstante, y ante la renuncia del subgerente, se volvió a la situación inicial de acefalia respecto de la gestión de la seguridad de la información en el INSSJP.

Respecto de lo expresado en este punto, las buenas prácticas establecen que: i) los organismos deben administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio (CobiT 4.1 - DS5.1: Administración de la Seguridad de TI); ii) establecer la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel superior apropiado; iii) definir y asignar roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento. Puede ser necesario asignar responsabilidades adicionales de administración de la seguridad a nivel de sistema específico (CobIT v4.1 - PO4.8: Responsabilidad sobre el riesgo, la seguridad y el cumplimiento); y iv) la Res. 87/22-SIGEN: 1.4 establece que la asignación de responsabilidades debe garantizar una adecuada separación de funciones, que fomente el control por oposición de intereses.

Teniendo en cuenta el escenario evidenciado en el organismo por este equipo de auditoria, y en base a lo que establecen las buenas prácticas en la materia, se puede aseverar que la estructura de seguridad de la información del INSSJP no tiene el nivel jerárquico y estratégico apropiado dentro de la estructura orgánica del Instituto, con las capacidades para garantizar que las acciones de la administración de la seguridad estén en línea con los requerimientos de la organización, poder definir y asignar roles críticos para administrar los riesgos de TI y garantizar la adecuada separación de funciones para fomentar el control por oposición de intereses. Esta situación pone en riesgo la capacidad del Instituto de asegurar adecuadamente la integridad, disponibilidad y confidencialidad de la información y la seguridad sobre la infraestructura tecnológica que da servicio al procesamiento de la información, con el objetivo de minimizar vulnerabilidades e incidentes de seguridad.

4.2.3. *La Gerencia de Tecnología (responsable del área de seguridad de la información) no realiza pruebas de seguridad e intrusión sobre la plataforma tecnológica del organismo, en*

especial sobre los entornos que dan soporte a los procesos de receta electrónica en lo referido a la prescripción, dispensa y liquidación de medicamentos. Esta situación no permite medir el grado de seguridad en que se encuentran estos entornos, diagnosticar y tomar acciones correctivas que minimicen los riesgos que pudieran comprometer la confidencialidad, integridad y disponibilidad de la información.

Del análisis de la documentación técnica entregada y de las entrevistas mantenidas con personal del área de informática del instituto, se constató que, durante el período auditado, no se han aplicado procedimientos de pruebas y análisis de seguridad informática que incluyan testeos de intrusión sobre la plataforma tecnológica del organismo, en especial sobre los entornos que dan soporte a los procesos de receta electrónica en lo referido a la prescripción, dispensa y liquidación de medicamentos.

Las buenas prácticas en seguridad de los sistemas señalan que la necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye, entre otros, realizar pruebas periódicas, así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad. (CobIT v4.1 - DS5: Garantizar la seguridad de los sistemas)

La falta de pruebas de seguridad informática sobre los activos de TI del INSSJP generan las siguientes limitaciones: i) no permite medir, en materia de seguridad, el grado de solidez de los sistemas y herramientas informáticas utilizadas para dar soporte a los procesos críticos del organismo; ii) podrían no detectarse vulnerabilidades que puedan comprometer la confidencialidad, integridad y disponibilidad de la información; y iii) posibles fallas en las acciones correctivas para minimizar el impacto de las vulnerabilidades o incidentes de seguridad.

4.3. Continuidad de las operaciones organizacionales.

4.3.1. *El INSSJP no cuenta con un Plan de Continuidad del Negocio (BCP, por sus siglas en inglés). Esta carencia pone en riesgo la operación de los procesos críticos de la organización.*

A partir de la evaluación de la documentación técnica provista por el organismo y de las entrevistas mantenidas con los responsables de áreas clave del INSSJP, se constató que el Instituto no cuenta con un Plan de Continuidad del Negocio (BCP, por sus siglas en inglés), ni si quiera evaluado ni aprobado.

Las buenas prácticas en esta cuestión (ISO 22.301 – Directrices para garantizar la Continuidad del Negocio; ISO 27.001 – Sistemas de gestión de la seguridad de la información; CobiT 4.1 – DS4 Garantizar la continuidad del servicio), indican que un Plan de Continuidad del Negocio es un proceso de recuperación operacional que le permite a la organización estar preparada frente a una contingencia causada por una interrupción mayor e inesperada, con el objetivo de garantizar la continuidad de la operación crítica de la empresa durante y posteriormente a una crisis, como desastres naturales o incidencias de seguridad informática a los que se encuentran continuamente amenazadas todas las organizaciones públicas y privadas, más aún un organismo como el INSSJP que gestiona una infraestructura tecnológica catalogada como infraestructura crítica.
Según las mejores prácticas anteriormente indicadas, un Plan de Continuidad del Negocio debe contener, desarrollar y ejecutar como mínimo los siguientes pasos:

a) Determinar el perfil de riesgos a los cuales está sometida la organización a través de una autoevaluación sobre las personas, los procesos críticos del negocio y el contexto en el cual se desarrollan.
b) Identificar los procesos, productos, servicios y/o funciones clave.
c) Establecer los objetivos del plan de continuidad de la actividad.
d) Evaluar el impacto potencial de las interrupciones para la organización y sus trabajadores.

e) Determina los tiempos necesarios para lograr la recuperación de los procesos críticos del negocio ante una contingencia.
f) Enumerar las acciones necesarias para asegurar la protección de la organización y sus procesos, productos, servicios y/o funciones clave.
g) Organizar las listas de contactos de todas aquellas personas que deben actuar en situación de contingencia.
h) Concienciar, difundir y capacitar periódicamente a todos los RRHH de la organización sobre el plan de continuidad del negocio.
i) Probar, mantener, revisar y actualizar periódicamente el plan de continuidad del negocio.

La implementación de un Plan de Continuidad del Negocio le permite al INSSJP estar preparado ante una catástrofe, minimizando impactos sobre sus objetivos estratégicos, así como procesos críticos internos y aquellos que dan servicio sus clientes del Sector Público Nacional y privados

.Ilustración N°. 7 Principales etapas de un BCP

Fuente: elaboración propia-DAI- en base a ISO 22.301.

Ilustración N° 8. Cronología de procesos en un BCP

Fuente: elaboración propia -DAI- en base a ISO 22.301.

Que el INSSJP no cuente con un Plan de Continuidad del Negocio, ni su debida aprobación, evaluación y actualización, acorde a lo que establecen las buenas prácticas y su correspondiente difusión, capacitación, plan de pruebas, documentación de simulacros y ajustes continuos, pone en riesgo la disponibilidad de las operaciones críticas de la propia organización, como así también de los servicios comprometidos con sus afiliados y prestadores.

4.3.2. *La Gerencia de Tecnología, a cargo de la gestión y administración de la infraestructura tecnológica que da soporte de TI al organismo, no cuenta con un Plan de Recuperación ante Desastres (DRP, por sus siglas en inglés), situación que pone en riesgo el aseguramiento de la continuidad de los servicios de TI ante la ocurrencia de eventualidades o amenazas de cualquier tipo.*

A partir del análisis realizado sobre la documentación técnica provista por el auditado, y de las entrevistas mantenidas con el responsable la Gerencia de Tecnología, se verificó que no se cuenta con la existencia de un Plan de Recuperación ante Desastres que asegure la continuidad de los servicios de TI que dan soporte al INSSJP.

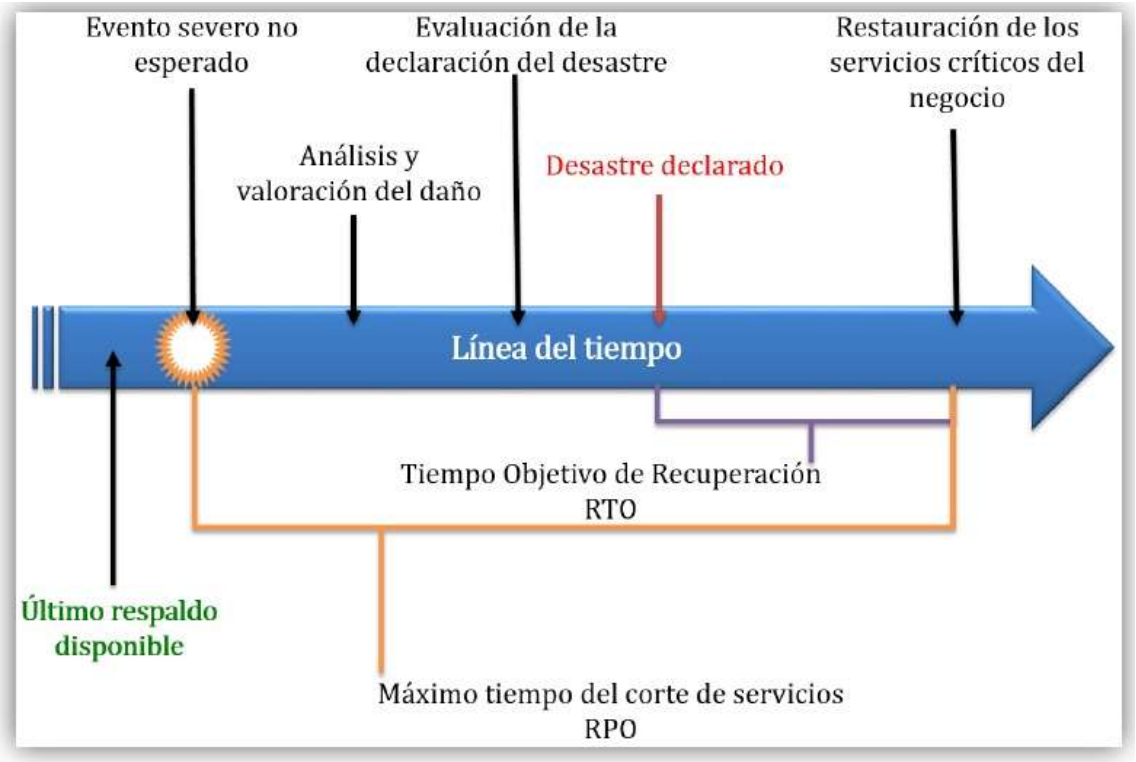
En función de lo que establecen las buenas prácticas en la materia, un Plan de Recuperación ante Desastres (DRP, por sus siglas en inglés) es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de ocurrencia de un desastre natural, errores humanos, ciberataques o ataques causados por terceros de cualquier tipo, que atenten contra la continuidad del funcionamiento de la organización. En este proceso no solo intervienen las áreas técnicas responsables de su ejecución sino también las áreas críticas de la organización, incluida la alta dirección, que deben formar parte de un comité de crisis para actuar al momento de su activación (ISO 22.301, directrices para garantizar la Continuidad del Negocio; ISO 24.762, directrices para asegurar la Continuidad de los Servicios de TI; ISO 27.001, Sistemas de gestión de la seguridad de la información; CobIT 4.1, proceso DS4 - Garantizar la continuidad del servicio).

Según las mejores prácticas anteriormente indicadas, un Plan de Recuperación ante Desastres debe contener, desarrollar y ejecutar como mínimo los siguientes pasos:

a) desarrollar una política de continuidad del negocio;
b) realizar una evaluación de riesgos;
c) realizar un análisis de impacto al negocio;
d) desarrollar estrategias de recuperación y continuidad del negocio;
e) concientizar, capacitar y probar los planes;
f) mantener y mejorar el plan de recuperación ante desastres.

La consideración de este plan ofrece la ventaja de responder de forma planeada y proactiva ante una catástrofe y minimizar su impacto en los objetivos y misión del INSSJP y sobre los sistemas de información que constituyen el soporte informático a los servicios que ésta presta.

Ilustración N° 9: Etapas de un DRP



Fuente: elaboración propia-DAI- en base a ISO 24.762.

Que la Gerencia de Tecnología, a cargo de la gestión y administración de la infraestructura tecnológica del organismo, no cuente con un Plan de Recuperación ante Desastres acorde a lo que establecen las buenas prácticas y su correspondiente plan de pruebas, documentación de simulacros y ajustes continuos, implica un riesgo de alto impacto sobre la disponibilidad de la información ante una interrupción de los servicios de TI, sobre los cuales todas las áreas operativas del INSSJP tienen una alta dependencia.

4.3.3. *La Gerencia de Tecnología del INSSJP no cuenta con políticas y procedimientos formalizados de resguardo de la información (backups) que establezcan las formas técnicas de ejecución y los períodos en los que se deben efectivizar las copias de respaldo de la información y sus debidas pruebas de restauración en virtud de los requerimientos que exijan*

los procesos críticos de la organización. Esta carencia pone en riesgo la disponibilidad de la información.

Del estudio realizado sobre la documentación técnica provista por el auditado, y de las entrevistas mantenidas con el responsable de la Gerencia de Tecnología se constató que las medidas de respaldo de la información aplicadas por los responsables técnicos de esta tarea son insuficientes e inadecuadas debido a que: i) no existen políticas y procedimientos formalizados de resguardo de la información que permitan monitorear el efectivo cumplimiento de esta actividad clave y crítica para la organización y que establezcan revisiones periódicas con las áreas usuarias respecto a las nuevas necesidades de backups; y ii) no se realizan procesos de pruebas de restauración que permitan comprobar la eficacia de las copias realizadas y garantizar la disponibilidad de la información ante una contingencia que amerite tener que restaurar una copia de resguardo.

Las buenas prácticas sobre políticas y procedimientos de back-ups y pruebas de restauración establecen que se debe garantizar la posesión de copias de resguardo de toda la información crítica utilizada por la organización, relevando de manera continua las necesidades de resguardo de información con las áreas usuarias. Además, se debe someter a la solución de back-up y recuperación de datos a pruebas formalizadas en forma periódica con la debida documentación de los resultados obtenidos en ellas, con la aceptación y control de las áreas usuarias. Estos testeos deben poner a prueba el funcionamiento de la tecnología utilizada, y es la forma más adecuada de detectar y resolver posibles fallos antes de que ocurra un incidente real (ISO 27.001 - Aspectos de seguridad - Información para la gestión de continuidad de negocio y CobIT v4.1 - DS4: Garantizar la continuidad del servicio).

Aplicar procedimientos de backups que no garanticen el resguardo exitoso de la información y que se ejecuten en períodos que no satisfagan las necesidades operativas de la organización, pone en riesgo la disponibilidad de dicha información ante un incidente que requiera aplicar una restauración.

4.4. Operaciones de TI.

4.4.1. *No se encuentra establecida una función de mesa de ayuda para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información de los sistemas CUP y Receta Electrónica.*

En las entrevistas mantenidas con los responsables de la Gerencias de Sistemas y Tecnología y del estudio de la documentación provista por el organismo, se constató que no existe actualmente dentro de la estructura del INSSJP una mesa de ayuda para el manejo de incidentes para el Sistema CUP y los aplicativos de Receta Electrónica y relacionados. En el año 2018 se disolvió la que brindaba este servicio, durante las tareas de campo y el periodo auditado se encontraba en proceso la extracción de requerimientos para la conformación de una nueva mesa de ayuda, mientras tanto, el INSSJP mantiene vigente un área exclusivamente para incidentes y problemas relacionados a ofimática[56].

En relación a lo expuesto, las buenas prácticas sobre la gestión de problemas e incidentes establecen que: i) se debe establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información; ii) deben existir procedimientos de monitoreo y escalamiento basados en los niveles de servicio acordados en los SLAs, que permitan clasificar y priorizar cualquier problema reportado como incidente, solicitud de servicio o solicitud de información; y iii) se debe medir la satisfacción del usuario final respecto a la calidad de la mesa de servicios y de los servicios de TI (CobIT v4.1 - DS8.1: Mesa de Servicios).

La falta de una Mesa de Ayuda (o servicios), le evita al organismo la obtención de reportes de la actividad que esta lleva adelante, impidiendo a la gerencia, la posibilidad de medir el desempeño del servicio y los tiempos de respuesta, así como identificar tendencias de

[56] **Ofimática** (acrónimo de *oficina* y de *informática*), designa al conjunto de técnicas, aplicaciones y herramientas informáticas que se utilizan en funciones de oficina para optimizar, automatizar, mejorar tareas y procedimientos relacionados.

problemas recurrentes de manera que el servicio pueda mejorarse de forma continua (CobIT v4.1 - DS8.5: Análisis de Tendencias).

4.5. Adquisiciones y contrataciones de TI.

4.5.1. *El INSSJP no realiza un control adecuado sobre el nivel de servicio prestado por los proveedores de los sistemas FarmaPami y FamaLive, que dan soporte a los procesos involucrados en la dispensa y liquidación de medicamentos prescriptos desde la receta electrónica.*

Del análisis de la información suministrada por el organismo y de las entrevistas mantenidas con las Gerencias de Tecnología y Sistemas del Instituto, se pudo constatar que no se realiza un control adecuado sobre la prestación de los servicios brindados por los proveedores de los sistemas *FarmaPami* y *Farmalive*. De los contratos con ambos, se desprende que se han establecido los acuerdos de nivel de servicio que debe cumplir el prestador y desde las áreas responsables se realizan los monitoreos sobre los servicios brindados. En este sentido, desde las áreas responsables se ha manifestado el desconocimiento sobre la existencia de los acuerdos de nivel de servicio establecidos en los contratos.

La falta de conocimiento sobre las pautas establecidas en estos acuerdos firmados con los proveedores, genera que el monitoreo de los mismos no sea acorde a los objetivos que establecen las buenas prácticas respecto de esta cuestión, como por ejemplo, la capacidad del organismo de revisar regularmente los acuerdos de niveles de servicios con quienes brindan el servicio, para asegurar que sean efectivos y acordes a las necesidades del negocio, que estén actualizados y que se han tomado en cuenta los cambios en requerimientos, así como la potestad de evaluar la aplicación por parte del INSSJP de sanciones o multas ante el incumplimiento de algún punto del acuerdo.

En tal sentido las buenas prácticas sostienen que el organismo debe revisar regularmente con los proveedores internos y externos los acuerdos de niveles de servicio y los contratos de apoyo, para asegurar que son efectivos, que están actualizados y que se han tomado en cuenta

los cambios en requerimientos (CobIT v4.1 - DS1.6: Revisión de los acuerdos de niveles de servicio y de los contratos) además de definir un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el cliente y el prestador de servicio. El marco de trabajo mantiene una alineación continua con los requerimientos y las prioridades de negocio y facilita el entendimiento común entre el cliente y el(los) prestador(es) de servicio. El marco de trabajo incluye procesos para la creación de requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio (SLAs), acuerdos de niveles de operación (OLAs) y las fuentes de financiamiento. Estos atributos están organizados en un catálogo de servicios. El marco de trabajo define la estructura organizacional para la administración del nivel de servicio, incluyendo los roles, tareas y responsabilidades de los proveedores externos e internos y de los clientes. (CobIT v4.1 - DS1.1: Marco de trabajo de la administración de los niveles de servicio).

El desconocimiento por parte de las áreas responsables del Instituto sobre los acuerdos de nivel de servicio celebrados con los proveedores de TI, genera el riesgo de que los mismos no estén alineados a los requerimientos y las prioridades del negocio, que no sean efectivos y que, ante un incumplimiento a raíz de la ausencia de este control, pueda incurrirse en la falta de aplicación de sanciones o multas (Ejemplo de ello, el riesgo de abonar certificados o facturas de la contratista como si el cumplimiento hubiese sido integro, ocasionando, en este caso, pérdidas económicas para el Instituto) de acuerdo a la definición de roles y responsabilidades.

4.6. Desarrollo de software aplicativo.

4.6.1. *En la Gerencia de Sistemas del INSSJP (responsable del área de Desarrollo) no existen políticas, procedimientos y metodologías establecidos de manera formal para el ciclo de vida del desarrollo y mantenimiento continuo de la plataforma CUP y puntualmente sobre los sistemas de receta electrónica y relacionado, que permitan facilitar la asignación de prioridades, la coordinación de proyectos, la reducción de costos inesperados y la cancelación de proyectos.*

De la documentación técnica provista por el auditado y de las entrevistas mantenidas con los responsables de las Gerencias de Sistemas y Tecnología, se pudo constatar que, en el INSSJP, no se cuenta con procedimientos y metodologías establecidos de manera formal para el ciclo de vida del desarrollo y mantenimiento continuo de la plataforma CUP y del sistema de Receta Electrónica.

En este sentido, se verificó que el seguimiento de los proyectos de las áreas pertinentes se realiza utilizando el software aplicativo Microsoft Excel, que comienza con una solicitud del área demandante, enviada al área de desarrollo a partir del aplicativo Jira o bien, utilizando directamente la vía del correo electrónico y luego es la Subgerencia quien toma el rol de la carga de dicha solicitud en Jira. De esta forma, se evidencia la no existencia de acuerdos formales de nivel de servicio con las áreas usuarias, aunque el estimado de los tiempos de resolución, pueden ser consultados en el software Jira por los usuarios del área que realizo la solicitud.

En relación a lo expuesto, las buenas prácticas sobre la Administración de Proyectos establecen que: i) se debe establecer un marco de trabajo de administración de programas y proyectos para la administración de todos los proyectos de TI establecidos; ii) el marco de trabajo debe garantizar la correcta asignación de prioridades y la coordinación de todos los proyectos; iii) el marco de trabajo debe incluir un plan maestro, asignación de recursos, definición de entregables, aprobación de los usuarios, un enfoque de entrega por fases, aseguramiento de la calidad, un plan formal de pruebas, revisión de pruebas y post-implantación después de la instalación para garantizar la administración de los riesgos del proyecto y la entrega de valor para el negocio. (CobIT v4.1 - PO10: Administrar proyectos.)

La ausencia de un marco de trabajo que administre los programas y proyectos de desarrollo de TI, incrementa el riesgo de costos inesperados y de cancelación de los mismos. Así como también, dificulta la comunicación y el involucramiento del negocio y de los usuarios finales, reduciendo el valor y la calidad de los entregables de los programas y proyectos de desarrollo de TI.

4.7. Sistemas de información

4.7.1. *Los sistemas y procesos de liquidación de medicamentos en el INSSJP, no se encuentran suficientemente integrados con los sistemas de información de los proveedores habilitados para administrar la dispensa y la liquidación de medicamentos a los afiliados del INSSJP, situación que pone en riesgo la integridad y confidencialidad de la información.*

Del análisis de la información entregada por el organismo y de las entrevistas mantenidas con las áreas de Gerencia de Medicamentos, Gerencia de Sistemas y Subgerencia de Control y Validación de Medicamentos, se pudo verificar que para el proceso de liquidación de medicamentos, no se ha definido un modelo de arquitectura de la información gestionado a través de un sistema integrado que de soporte a este proceso, orientado a asegurar que los datos se encuentren organizados eficientemente y de manera homogénea.

Para el caso del proceso de liquidación del sistema *FarmaPami* se constató que: i) los archivos de liquidación son enviados por el prestador al INSSJP en archivos de formato de texto plano; ii) el archivo se analiza con herramientas ofimáticas sin intervención de la Gerencia de Sistemas y sin controles automáticos; iii) el resultado del análisis se exporta a una planilla de cálculo en formato xls (Excel); y iv) sobre el archivo en formato Excel, se realizan controles manuales previo a volver a importarlo a formato de texto plano para ser enviado al proveedor de servicios tecnológicos del sistema *FarmaPami*.

En cuanto al proceso para la liquidación del sistema *Farmalive*, se verificó que: i) el total de los medicamentos dispensados a los afiliados del INSSJP, se envía en formato de texto plano (archivo del tipo .txt) y también en formato papel; y ii) El resultado del proceso de búsqueda de errores en la liquidación es exportado en formato de planilla de cálculo (.xls) sobre el cual se realizan controles manuales.

Para estas cuestiones, las buenas prácticas destacan la necesidad de definir e implementar procedimientos formalizados para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y

archivos. (CobIT v4.1. - PO2.4). Asimismo, indican que se debe establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI, facilitando la creación, uso y compartimiento de la información por parte del negocio de tal manera que se garantice su integridad, sea flexible, funcional, rentable, oportuna, segura y tolerante a fallos. (CobIT v4.1. - PO2.1).

Adicionalmente, los criterios técnicos en la materia advierten sobre la necesidad de establecer un esquema de clasificación de la información que aplique a todo el organismo, basado en definir qué tan crítica y sensible es la información (esto es, pública, confidencial, secreta, etc.). Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para asegurar la confidencialidad de la información a través del control de acceso a la información, de la gestión segura de archivos o aplicando técnicas de cifrado. (CobIT v4.1. - PO2.3).

Por último, es oportuno destacar que las directrices establecidas en la Resolución 87/22-SIGEN-Anexo-Normas de Control Interno para la Tecnología de la Información-, punto 3.1, indican que la unidad de TI debe definir el modelo de arquitectura de la información de la organización, orientado a asegurar que los datos se encuentren organizados eficientemente y de manera homogénea, garantizando que estarán disponibles para su utilización, en concordancia con las necesidades operativas de las diferentes áreas usuarias en cuanto a oportunidad, integridad, exactitud o formato, entre otras. Este modelo de arquitectura de la información debe documentarse y mantenerse actualizado en un diccionario de datos corporativo, especificando los controles de consistencia, integridad, confidencialidad y validación aplicables.

Por todo lo expuesto, se advierte que la ausencia de sistemas integrados atenta contra la estandarización de procesos y la eliminación de procesos manuales como, por ejemplo, el control manual de liquidaciones en formato Excel. Situación que genera, además, la

intervención de áreas como la GS y la GIT en actividades operativas concernientes a las áreas encargadas de las liquidaciones a los prestadores, poniendo en riesgo la confiablidad, integridad y disponibilidad de la información que estas contienen. Además, las herramientas ofimáticas utilizadas en estos procesos manuales carecen de trazabilidad y auditabilidad, afectando la confiabilidad e integridad de los datos procesados.

En este sentido, el organismo se encuentra expuesto al riesgo de no poder proteger de manera óptima y oportuna la información que gestiona, siendo la misma un activo determinante para la salvaguarda de los fondos públicos en materia de salud, principalmente para los afiliados del INSSJP. Asimismo, los sistemas integrados permiten optimizar los tiempos de ejecución de las tareas y la gestión de la información y el conocimiento de las organizaciones facilitando la planificación y la mejora continua de sus sistemas.

5. ANÁLISIS DE LA VISTA

Por Nota N° 765/24-P, la AGN remite el día 10 de octubre de 2024, el proyecto de Informe de Auditoría, sujeto a discusión, cuyo objeto es *"Clave Única PAMI (CUP) y sistemas relacionados"* al INSSJP, otorgándole un plazo de 15 (quince) días corridos para la entrega de su respectivo descargo, a partir del momento de recibida la presente.

Por Nota Número: IF-2024-117020785-INSSJP-DE#INSSJP, el día 25 de octubre de 2024, reproducida en el Anexo I, el INSSJP remite vía casilla de correo institucional (mail), el documento electrónico conteniendo el descargo de la vista del mencionado proyecto de Informe.

6. RECOMENDACIONES

La secuencia de las recomendaciones aquí expuestas sigue el mismo orden que los hallazgos del capítulo 4.

6.1. Gobierno de TI

6.1.1. Implementar relevamientos con la comunidad usuaria referidos al nivel de satisfacción sobre la disponibilidad y las funcionalidades que ofrecen los sistemas de la plataforma CUP-PAMI. Desarrollar planes de acciones correctivas, evolutivas y adaptativas sobre el mismo a partir de los resultados obtenidos en estos relevamientos como parte de un plan de mejora continua.

6.1.2. Monitorear de forma continua el ambiente de control de TI y el marco de trabajo de control de TI sobre el contexto tecnológico del Instituto, evaluando la eficiencia y efectividad de los controles internos implementados por el área a cargo del servicio de TI del organismo**.**

6.2. Seguridad de la información

6.2.1. Conformar e implementar un Comité de Seguridad de la Información que opere de manera continua, que dicte, implemente, revise y gestione las políticas y procedimientos al respecto, que sean las más adecuadas a las necesidades del organismo, y designar una estructura especializada en la materia que haga cumplir las políticas y procedimientos de Seguridad de la Información establecidas por el Comité.

6.2.2. Tomar las medidas necesarias para que la estructura orgánica del Instituto permita la correcta aplicación de la Política de Seguridad de Información aprobada por Disposición 0002/15 GYTC y que dicha estructura se coloque al nivel adecuado para garantizar la separación de funciones, fomentado el control por oposición.

6.2.3. Realizar evaluaciones técnicas de vulnerabilidad sobre los activos de TI del organismo, en especial sobre los entornos tecnológicos que dan soporte a los procesos de receta electrónica en lo referido a la prescripción, dispensa y liquidación de medicamentos, de manera continua y ejecutando las acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Garantizar que la implementación de la seguridad en TI sea probada

y monitoreada de forma pro-activa y recurrente para mantener el nivel de seguridad requerido por la organización.

6.3. Continuidad de las operaciones organizacionales

6.3.1. Desarrollar, aprobar, probar y mantener en forma continua un Plan de Continuidad del Negocio aprobado formalmente por acto administrativo del organismo, siguiendo las directrices de las buenas prácticas al respecto y que asegure la continuidad de las operaciones críticas del Instituto, como así también de los servicios tecnológicos comprometidos con sus afiliados y prestadores ante una contingencia que amerite su activación.

6.3.2. Desarrollar, aprobar, probar y mantener en forma continua un Plan de Recuperación ante Desastres aprobado formalmente por acto administrativo de la organización, siguiendo las directrices de las buenas prácticas al respecto y que asegure la continuidad de los servicios y la disponibilidad de los sistemas y de la información del INSSJP.

6.3.3. Definir e implementar políticas y procedimientos formalizados de respaldo y de restauración de los sistemas, aplicaciones, datos y documentación, en línea con los requerimientos de la organización y el plan de continuidad de los servicios de TI, que permitan garantizar la disponibilidad de la información y definir la ejecución de pruebas de restauración que aseguren la eficiencia y el éxito ante una posible incidencia que requiera restaurar la información respaldada.

6.4. Operaciones de TI

6.4.1. Establecer una Mesa de ayuda (o servicios) y procedimientos correspondientes, con el objetivo de generar las herramientas necesarias para el tratamiento efectivo de incidentes y la mejora constante.

6.5. Adquisiciones y contratación de TI

6.5.1. Definir un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el cliente y el prestador, con el fin de adecuar los acuerdos a los requerimientos y las prioridades estratégicas del Instituto, así como también, considerar para los casos en que el proveedor incurra en algún incumplimiento, todo aquello vinculado a las facultades y potestades derivadas de los contratos en la aplicación de multas y/o sanciones.

6.6. Desarrollo de software aplicativo

6.6.1. Establecer, aprobar, implementar y comunicar un marco de trabajo de administración de programas y y proyectos para la administración de sistemas CUP y receta electrónica del INSSJP.

6.7. Sistemas de información

6.7.1. Implementar y mantener sistemas de información integrados a los sistemas *Farmalive* y *FarmaPami* que den soporte a los procesos de liquidación producidos por ambos sistemas. Así mismo, adquirir y mantener la infraestructura tecnológica de la que hacen uso estos sistemas, facilitando eficientemente la operación y el uso de los aplicativos a los usuarios finales con adecuadas medidas de seguridad para el acceso de los mismos y que se implementen controles automatizados, de forma tal que se garantice el procesamiento de la información de manera exacta, completa, oportuna, autorizada y auditable.

7. CONCLUSIONES

El sistema Clave Única PAMI (CUP) es un mecanismo de inicio de sesión unificada (*Single Sign On*) diseñado para proporcionar un acceso seguro y centralizado a más de 60 aplicaciones del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP), cuyo

origen se funda en la Ley 19.032, creación del INSSJP, modificada luego por Ley 25.615[57]. Este sistema permite a los usuarios autenticarse y solicitar autorización para acceder a las aplicaciones pertinentes según sus roles. No obstante, obtener acceso a CUP no implica contar con el permiso de acceso a todas estas aplicaciones, y esto debido a que la mencionada plataforma cuenta con su propio Sistema de Administración de Seguridad (SADES), el cual permite la autogestión de software de aplicaciones, funciones y perfiles, mediante la aprobación del dueño de datos de la aplicación solicitada (las áreas usuarias del INSSJP). El SADES es una herramienta integral de control de acceso que incluye módulos para la administración de usuarios, auditoría de permisos, gestión de noticias, desarrollo y administración de sistemas.

Entre las aplicaciones incluidas en la plataforma CUP relacionadas con la prescripción, valorización y dispensa de medicamentos, se encuentra el Sistema de Gestión de Medicamentos Sin Cargo (MSC), una aplicación web que permite la solicitud, evaluación, autorización y renovación de medicamentos con cobertura al 100% para los afiliados del INSSJP. Este sistema es vital para la sistematización del acceso a tratamientos farmacológicos a través de diversas vías administrativas, incluyendo subsidios sociales y urgencias locales.

Otra aplicación es el Sistema de Recetas Electrónicas (RE), que de acuerdo a los fundamentos en su Ley de creación[58], se marca un avance en la gestión de la salud al facilitar la transición de las recetas manuales a las electrónicas. Esta herramienta, en línea con lo establecido en la Ley 27.553, de Recetas Electrónicas o digitales, en pos de desarrollar y/o adecuar los sistemas electrónicos existentes y regular su implementación para utilizar recetas electrónicas o digitales, agiliza la dispensa de medicamentos y ofrece mayor seguridad en el acto médico de la prescripción, incluyendo módulos para la prescripción, búsqueda y administración de recetas, así como la gestión de datos médicos.

El Sistema de Liquidación de Medicamentos es otra aplicación clave que se utiliza para validar y conciliar los datos de las liquidaciones de medicamentos enviados por la industria

[57] https://servicios.infoleg.gob.ar/infolegInternet/anexos/75000-79999/76149/texact.htm
[58] https://www.hcdn.gob.ar/proyectos/proyectoTP.jsp?exp=3979-D-2019

farmacéutica. A través de este sistema, se pueden importar, procesar y validar los archivos de liquidación, generando así un proceso de revisión y aprobación efectivo para la Gerencia de Medicamentos.

En tanto, el Sistema de Vademécum de Medicamentos administra el listado de medicamentos utilizados por el Instituto e incluye la administración del padrón de farmacias que operan en el mismo, lo que facilita la gestión de medicamentos y la optimización del proceso de prescripción.

Por su parte, el Sistema de Padrón de Diabéticos permite la identificación de afiliados con patología diabética, garantizando la cobertura necesaria para su tratamiento continuo y el Sistema de Protocolos Oncológicos (ONCO), funciona como una herramienta fundamental para organizar la prescripción de tratamientos oncológicos, gestionando la administración de los protocolos definidos por el INSSJP para diferentes patologías.

Así las cosas, el presente Informe abarca un análisis exhaustivo de los sistemas integrados en la plataforma CUP, destacando la importancia de un marco de seguridad y control eficiente para gestionar los servicios de salud ofrecidos por el Instituto. En este sentido, la adopción de sistemas electrónicos busca e intenta mejorar la gestión y dispensa de medicamentos y como consecuencia de ello, incrementar la seguridad, eficiencia y control en el proceso de atención a los afiliados, aspectos claves que definen la evaluación de los objetivos abordados en esta auditoría.

Los procesos sujetos al análisis del equipo auditor en el ámbito del sistema Clave Única PAMI (CUP) estuvieron centrados en atención al objeto que nos ocupa, sobre el Sistema de Recetas Electrónicas (RE). Dentro de los módulos que componen el mencionado sistema, podemos destacar como principales a los siguientes i) ALTA DE RECETA; ii) BÚSQUEDA DE RECETA; iii) DATOS DEL MÉDICO: y iv) DISTINTOS PANELES DE ADMINISTRACIÓN.

Bajo este escenario, el equipo de auditoría realizó un relevamiento y análisis detallado de este Sistema de Recetas Electrónicas, abarcando los procesos que incluyeron desde la prescripción de un medicamento hasta la liquidación al INSSJP por parte de los proveedores que dispensan

los medicamentos recetados a los afiliados, a través de las farmacias adheridas al Instituto: i) Proceso de ingreso al sistema CUP - Receta Electrónica, prescripción y dispensa de medicamentos; ii) Proceso de liquidación de medicamentos mediante el sistema FARMALIVE[59] y iii) Proceso de liquidación de medicamentos mediante el sistema FARMAPAMI[60].

A partir del análisis efectuado sobre estos procesos, la auditoría se enfocó en 7 (siete) ejes principales: 1) Gobierno de TI, 2) Seguridad de la información, 3) Continuidad de las Operaciones Organizacionales, 4) Operaciones de TI, 5) Adquisiciones y Contrataciones de TI, 6) Desarrollo de Software Aplicativo, y 7) Sistemas de información.

Los principales hallazgos en el ámbito del Gobierno de TI evidencian que: i) El INSSJP no realiza relevamientos con la comunidad usuaria en cuanto al nivel de satisfacción sobre la disponibilidad y las funcionalidades que ofrece el sistema de Receta Electrónica y sus sistemas relacionados, lo que conlleva al desconocimiento de la opinión de los usuarios respecto a los problemas, debilidades y requerimientos funcionales sobre el aplicativo, y del nivel de satisfacción sobre el soporte brindado por el Instituto a los usuarios; y ii) El INSSJP no cuenta, para su plataforma tecnológica y para los servicios de soporte y mantenimiento continuo brindados por las Gerencias de Sistemas y Tecnología, con un adecuado ambiente de control interno que garantice la detección temprana de riesgos de TI y las acciones pertinentes para gestionarlos.

En cuanto a la Seguridad de la Información, la situación encontrada denota debilidades en la administración de los riesgos para garantizar la confidencialidad, integridad y disponibilidad de la información en niveles aceptables, pues se detectó que: i) El organismo no cuenta con una estructura organizacional adecuada para atender y gestionar las políticas y procedimientos de seguridad de la información aplicables transversalmente a toda la organización, ni tampoco tiene un Comité de Seguridad de la Información. Esta situación expone la vulnerabilidad del

[59] https://www.farmalive.com.ar/login.html
[60] https://farma.pami.org.ar/seguridad/iniciar-sesion

organismo ante la falta de implementación y correcto control sobre las políticas y procedimientos de seguridad de la información organizacionales y de un equipo especializado que las gestione para su debido cumplimiento, las revise y actualice periódicamente; ii) La estructura organizacional para administrar eficiente y efectivamente la seguridad de la información del INSSJP no es funcional respecto a lo establecido en la Política de Seguridad de la Información del organismo. Escenario que pone en riesgo la confidencialidad, integridad y disponibilidad de la información del Instituto; y iii) La Gerencia de Tecnología (responsable del área de seguridad de la información) no realiza pruebas de seguridad e intrusión sobre la plataforma tecnológica del organismo, en especial sobre los entornos que dan soporte a los procesos de receta electrónica en lo referido a la prescripción, dispensa y liquidación de medicamentos. Esta situación no permite medir el grado de seguridad en que se encuentran estos entornos, diagnosticar y tomar acciones correctivas que minimicen los riesgos que pudieran comprometer la confidencialidad, integridad y disponibilidad de la información.

En relación a la Continuidad de las Operaciones Organizacionales, se ha hallado que: i) El INSSJP no cuenta con un Plan de Continuidad del Negocio (BCP, por sus siglas en inglés). Esta carencia pone en riesgo la operación de los procesos críticos de la organización; ii) La Gerencia de Tecnología, a cargo de la gestión y administración de la infraestructura tecnológica que da soporte de TI al organismo, no cuenta con un Plan de Recuperación ante Desastres (DRP, por sus siglas en inglés), situación que pone en riesgo el aseguramiento de la continuidad de los servicios de TI ante la ocurrencia de eventualidades o amenazas de cualquier tipo; y iii) La Gerencia de Tecnología del INSSJP no cuenta con políticas y procedimientos formalizados de resguardo de la información (backups) que establezcan las formas técnicas de ejecución y los períodos en los que se deben efectivizar las copias de respaldo de la información y sus debidas pruebas de restauración en virtud de los requerimientos que exijan los procesos críticos de la organización. Esta carencia pone en riesgo la disponibilidad de la información.

Respecto a las Operaciones de TI, se pudo constatar que no se encuentra establecida una función de mesa de ayuda para registrar, comunicar, atender y analizar todas las llamadas,

incidentes reportados, requerimientos de servicio y solicitudes de información de los sistemas CUP y Receta Electrónica.

En lo relacionado con las Adquisiciones y Contrataciones de TI, se verificó que el INSSJP no realiza un control adecuado sobre el nivel de servicio prestado por los proveedores de los sistemas FarmaPami y FamaLive, que dan soporte a los procesos involucrados en la dispensa y liquidación de medicamentos prescriptos desde la receta electrónica.

En referencia al Desarrollo de Software Aplicativo, se detectó que en la Gerencia de Sistemas del INSSJP (responsable del área de Desarrollo) no existen políticas, procedimientos y metodologías establecidos de manera formal para el ciclo de vida del desarrollo y mantenimiento continuo de la plataforma CUP y puntualmente sobre los sistemas de receta electrónica y relacionado, que permitan facilitar la asignación de prioridades, la coordinación de proyectos, la reducción de costos inesperados y la cancelación de proyectos.

Por último, en relación a los Sistemas de Información, se constató que los sistemas y procesos de liquidación de medicamentos en el INSSJP, no se encuentran suficientemente integrados con los sistemas de información de los proveedores habilitados para administrar la dispensa y la liquidación de medicamentos a los afiliados del INSSJP, situación que pone en riesgo la integridad y confidencialidad de la información.

En lo que hace al cumplimiento normativo interno que aplica en forma transversal, al respecto de la Ley 27.499, Ley Micaela, de Capacitación Obligatoria en Género para todas las personas que integran los Tres Poderes del Estado (Disposición 62/22-AGN), el INSSPJ, a través de la Gerencia de Recursos Humanos, informa que está llevando a cabo la capacitación obligatoria en género según lo dispuesto por la mencionada Ley. En el cumplimiento de los Objetivos de Desarrollo Sostenible (ODS), el auditado manifestó por Nota de respuesta ante el requerimiento de la AGN (Disposición 198/18-AGN), que al respecto de la temática en cuestión, …"*este Organismo no posee una asignación o adhesión formal suscripta con dicha organización o bien con el estado nacional que establezca compromisos y metas."...* y en lo que hace al cumplimiento de las Leyes 22.431, 25.689, 25.785 y modificatorias

(Disposiciones 182/12 y 232/14-AGN), si bien el organismo expresa que no cuenta con la información del total de agentes con discapacidad ocupados, manifiesta que 135 agentes de planta permanente certifican discapacidad, y que a su vez, de esa cantidad, 57 agentes poseen una discapacidad parcial y los restantes 78, tienen discapacidad total.

En conclusión, a partir del escenario descripto, resulta necesario que las autoridades del INSSJP, conjuntamente con la Gerencia de Tecnología, Auditoría Interna y las Gerencias operativas usuarias que están estrechamente vinculadas a los sistemas de Recetas Electrónicas, a los sistemas de dispensa de medicamentos y al sistema de liquidación de medicamentos, pongan en marcha un plan de estratégico de TI, de la seguridad de la Información, de la continuidad de los servicios de TI, de gestión del software aplicativo y de administración de los sistemas de información críticos, con eficientes y efectivos procesos de planificación que se encuentren debidamente alineados a los objetivos estratégicos del Instituto, garantizando un adecuado ambiente de control sobre los servicios de TI y considerando los principios fundamentales de disponibilidad, integridad y confidencialidad de la información del organismo; todo en concordancia con los aspectos que se encuentran indicados en los puntos 4 (HALLAZGOS) y 6 (RECOMENDACIONES) del presente Informe.

8. LUGAR Y FECHA

BUENOS AIRES, septiembre de 2024

9. FIRMA

MARTINEZ
Maria Virginia

Cdra. María Virginia Martínez
Jefa de Departamento de Auditoría Informática
Gerencia de Planificación y Proyectos Especiales
Auditoría General de la Nación
AGN REPÚBLICA ARGENTINA

VILLA Federico
Gaston

Cdor. Federico G. Villa
Subgerente de Planificación
y Proyectos Especiales
Auditoría General de la Nación

10. ANEXOS

ANEXO I – Comentarios del auditado

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

Informe

Número: IF-2024-117020785-INSSJP-DE#INSSJP

CIUDAD DE BUENOS AIRES
Viernes 25 de Octubre de 2024

Referencia: Respuesta a NOTA Nº 765/24-P - Ref. S-050600994/2021, ACT. Nº 127/21-AGN

Sr. Presidente de la Auditoría General de la Nación

Dr. Juan Manuel Olmos

Tengo el agrado de dirigirme a Ud. a los efectos de brindar respuesta a la NOTA Nº 765/24-P, Ref. S-050600994/2021, ACT. Nº 127/21-AGN, cursada el 10 de octubre del corriente, mediante la cual nos remite copia del Proyecto de Informe de Auditoría, *sujeto a discusión*, cuyo objeto es *"Clave Unica PAMI (CUP) y sistemas relacionados"*, que esa Auditoría General de la Nación (AGN) a su cargo está llevando a cabo en el Instituto Nacional de Servicios Sociales Para Jubilados y Pensionados (INSSJP).

Es importante poner de resalto, tal como se menciona en el proyecto de informe, que el periodo auditado se extiende del 01/02/2018 al 31/03/2021 y que las tareas de campo se desarrollaron, por parte de esa Auditoría, entre los meses de mayo de 2021 y agosto de 2023.

En virtud de lo expuesto, se considera relevante, poner a disposición de esa Auditoría General de la Nación, el conjunto de acciones llevadas adelante en la materia de que trata la presente, en el marco de la estrategia institucional 2024-2027, la cual responde a la necesidad de brindar seguridad y protección a los datos de los 5.33 millones de afiliados de PAMI, así como también generar las políticas de resguardo de los activos digitales que forman parte del patrimonio del INSSJP.

A continuación, en el **Anexo I "Consideraciones vertidas a las observaciones del informe preliminar de AGN"**, se exponen las acciones llevadas adelante, en la materia de que se trata.

Quedando a disposición para cualquier consulta que esa AGN requiera, aprovecho la ocasión para saludarlo Atte.

Anexo I

Consideraciones vertidas a las observaciones del informe preliminar de AGN

4.2.1 / Referente a la observación que señala la carencia de contar con una estructura organizacional adecuada para atender y gestionar las políticas y procedimientos, en lo que respecta a Seguridad de la Información, se informa a esa Auditoría General de la Nación lo siguiente:

Con fecha 12/abr/2024, mediante DI-2024-1-INSSJP-JGA#INSSJP fue aprobado el Plan Estratégico de Seguridad de la Información. (EX-2024-36547616-INSSJP-JGA#INSSJP), cuyo propósito central es el de desarrollar los lineamientos de la Estrategia de Seguridad de la Información del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP), necesarios para propender a aumentar la confidencialidad, integridad y disponibilidad de la información, mitigando riesgos y asegurando el cumplimiento de regulaciones y estándares relevantes. Asimismo, esta estrategia busca fomentar una cultura de seguridad dentro de la organización, promoviendo la conciencia y responsabilidad de todos los empleados en la protección de la información sensible.

Por otra parte, con fecha 30/abr/2024, mediante Resolución RESOL-2024-1272-INSSJP-DE#INSSJP el Director Ejecutivo del INSSJP aprobó la estructura orgánico-funcional del organismo, donde se crea la Gerencia de Seguridad de la Información y Activos Digitales, que depende orgánicamente de la Jefatura de Gabinete de Asesores, con el propósito de que tenga un rol de desarrollo y control por oposición de las políticas gestionadas por la Gerencia de Tecnología. En cuanto a la estructura de la Gerencia de Tecnología, dependiente de la Coordinación Ejecutiva del Instituto, la misma Resolución, crea la Subgerencia de Gestión de la Calidad y Gestión de la Información y la Subgerencia de Seguridad Informática, (EX-2024-23688759-INSSJP-GRRHH#INSSJP).

Asimismo, con fecha 22/ago/2024, mediante Resolución RESOL-2024-2407-INSSJP-DE#INSSJP el Director Ejecutivo de PAMI, aprobó la estructura orgánico-funcional de la Jefatura de Gabinete de Asesores creando bajo la órbita de la Gerencia de Seguridad de la Información y Activos Digitales, el Departamento de Gestión de Procesos de Seguridad de la Información y el Departamento de Normas de Protección de Datos y Seguridad de la Información, (EX-2024-86504196-INSSJP-GRRHH#INSSJP).

La creación de las áreas antes mencionadas, así como sus misiones y funciones, forman parte de una estrategia diseñada en consonancia con las normas ISO 27000 y las normas vigentes en el país, en materia de calidad y seguridad de la información.

Respecto de la observación en la que se hace referencia a no contar con un Comité de Seguridad de la Información, se informa a esa Auditoría General de la Nación lo siguiente:

Con fecha 20/mar/2024, mediante Resolución RESOL-2024-28738857-INSSJP-DE#INSSJP, el Director Ejecutivo creó el Comité de seguimiento y Seguridad de la Información - CSSI y su Reglamento de Funcionamiento, en la órbita de la Jefatura de Gabinete de Asesores dependiente de la Dirección Ejecutiva. (EX-2024-28738857-INSSJP-USA#INSSJP). En tal instancia se convoca a todos los gerentes del organismo, con el objeto de poner en conocimiento y realizar intercambio de propuestas, respecto de las políticas de seguridad de la información de que se trate. De esta forma, se produce el involucramiento de todas las áreas institucionales. Asimismo, es dable mencionar que, a la fecha de la presente, se llevaron adelante cuatro (4) encuentros del CSSI en fechas 22/mar/2024, 17/abr/2024, 31/may/2024 y 25/sep/2024 respectivamente.

En sintonía con todo lo antes mencionado, con fecha 30/agos/2024, mediante Resolución RESOL-2024-2491-INSSJP-DE#INSSJP, el Director Ejecutivo de PAMI, aprobó el Plan Anual Operativo 2024, en el que se aborda, desde el EJE 4 del mencionado plan, la Transformación digital, disponibilidad, integridad y seguridad de la información (EX-2024-90093505-INSSJP-JGA#INSSJP).

En cuanto a las capacitaciones efectuadas al personal, se informa lo siguiente:

a. Se llevan a cabo capacitaciones virtuales, mediante la plataforma EDUPAMI, que es el soporte digital de los cursos que se brindan al personal del Instituto, sobre las siguientes temáticas:
   1. Seguridad de la información, conceptos fundamentales
   2. Riesgos para la seguridad de la información
   3. Introducción a los datos personales
   4. Clasificación de la información y gestión de riesgos
   5. Aspectos esenciales sobre términos y condiciones de uso y políticas de privacidad

a. b. Por otra parte, se llevan adelante talleres presenciales sobre las siguientes temáticas:
   1. Seguridad de la Información y Clasificación de la Información (30/may/2024)
   2. Gestión de Riesgos de Seguridad de la Información (13/jun/2024)
   3. Integrador de Clasificación de la Información y Gestión de Riesgos (04/jul/2024)
   4. Gestión de Incidentes de Seguridad de la Información (08/ago/2024)
   5. Aspectos legales sobre la Protección de Datos Personales y el Derecho de Acceso a la Información Pública (22/ago/2024)
   6. Introducción a la Continuidad de las Operaciones (18/09/2024)
   7. Mapeo de Procesos orientados a Seguridad de la información (10/oct/2024)
   8. Ciclo de vida de las TICs – parte 1 (a definir fecha)
   9. Ciclo de vida de las TICs – parte 2 (a definir fecha)

4.2.2 / Referente a la estructura organizacional y la Política de Seguridad de la Información y adicionalmente a lo respondido en 4.2.1, puntos a), b) y c), se señala:

Mediante EX-2024-96625303- INSSJP-GSIYAD#INSSJP se encuentra en curso de aprobación por el Director Ejecutivo el Proyecto de Resolución de la **Política de Seguridad de la Información** del INSSJP, basada en ISO 27.001/2022-

1. / **Referente a las Pruebas de seguridad e intrusión**

Mediante Licitación pública nº 17/2024 se encuentra en proceso el procedimiento para la adquisición de equipamiento y soluciones para la actualización y fortalecimiento de las infraestructuras de ciberseguridad del instituto, en tal marco se contempla la contratación de herramientas para la medición de grados de seguridad de los entornos de infraestructura digital.

4.3.1 / Referente al BCP – Plan de Continuidad de Negocio

La Gerencia de Seguridad de la Información y Activos Digitales presentó un proyecto, el cual se encuentra en curso, con apoyo del Banco Interamericano de Desarrollo (BID) - número de cooperación técnica NO REEMBOLSABLE CT AR-T1384, denominado "Apoyo a la Transformación en Seguridad de la Información del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP)". Este proyecto forma parte de la estrategia de diseño como aporte al Plan de Continuidad de Negocio que se encuentra en proceso de elaboración, luego de haber atravesado el relevamiento y diagnóstico inicial previo.

4.3.2 / Referente a no contar con un DRP – Plan de Recuperación ante Desastres

Por EX-2024-96625303- -INSSJP-GSIYAD#INSSJP se encuentra en curso de aprobación por el Director Ejecutivo el Proyecto de Resolución de la "Política de Seguridad de la Información" del INSSJP actualizada a ISO 27.001/2022- la que incluye el proceso a desarrollar por la Gerencia de Tecnología de la Información.

4.3.3 / Referente a no contar con políticas y procedimientos formalizados de resguardo de la información Back-Up.

Por EX-2024-96625303- -INSSJP-GSIYAD#INSSJP se encuentra en curso de aprobación por el Director Ejecutivo el Proyecto de Resolución de la "Política de Seguridad de la Información" del INSSJP actualizada a ISO 27.001/2022- la que incluye el proceso a desarrollar por la Gerencia de Tecnología de la Información.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.10.28 11:21:38 -03'00'

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

ANEXO II – Análisis de los comentarios del Auditado

Acápite del Informe	Comentario del Auditado	Análisis del Comentario
4. Hallazgos **4.2. Seguridad de la información** **4.2.1.** ***El organismo no cuenta con una estructura organizacional adecuada para atender y gestionar las políticas y procedimientos de seguridad de la información aplicables transversalmente a toda la organización, ni tampoco tiene un Comité de Seguridad de la Información. Esta situación expone la vulnerabilidad del organismo ante la falta de implementación y correcto control sobre las políticas y procedimientos de seguridad de la información organizacionales y de un equipo especializado que las gestione para su debido cumplimiento, las revise y actualice periódicamente.*** Luego de evaluada la documentación técnica provista por el organismo y de las entrevistas mantenidas con la Gerencia de Tecnología, se constató que si bien el INSSJP aprobó su "Política de Seguridad de la Información" a través de la Disposición 0002/15 GYTC, y en la misma se designó al Subgerente de Seguridad Informática como Responsable de Seguridad de la Información del organismo, el mencionado cargo, incluso desde la aprobación de dicha política, luego durante el periodo auditado y aun mientras se llevaban adelante las tareas de campo, se encontraba acéfalo, evidenciándose la falta de constitución de un Comité de Seguridad de la Información que implemente, revise y gestione un Plan de Seguridad de la Información que abarque a todo el organismo, alineado a la política de seguridad de la información aprobada que se encargue de la ejecución operativa del plan, así como del cumplimiento de las políticas y procedimientos pertinentes.	*4.2.1 / Referente a la observación que señala la carencia de contar con una estructura organizacional adecuada para atender y gestionar las políticas y procedimientos, en lo que respecta a Seguridad de la Información, se informa a esa Auditoría General de la Nación lo siguiente:* *Con fecha 12/abr/2024, mediante DI-2024-1-INSSJP-JGA#INSSJP fue aprobado el Plan Estratégico de Seguridad de la Información. (EX-2024-36547616-INSSJP-JGA#INSSJP), cuyo propósito central es el de desarrollar loslineamientos de la Estrategia de Seguridad de la Información del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP), necesarios para propender a aumentar la confidencialidad, integridad y disponibilidad de la información, mitigando riesgos y asegurando el cumplimiento de regulaciones y estándares relevantes. Asimismo, esta estrategia busca fomentar una cultura de seguridad dentro de la organización, promoviendo la conciencia y responsabilidad de todos los empleados en la protección de la información sensible.* *Por otra parte, con fecha 30/abr/2024, mediante Resolución RESOL-2024-1272-INSSJP-DE#INSSJP el Director Ejecutivo del INSSJP aprobó la estructura orgánico-funcional del organismo, donde se crea la Gerencia de Seguridad de la Información y Activos Digitales, que depende orgánicamente de la Jefatura de Gabinete de Asesores, con el propósito de que tenga un rol de desarrollo y control por oposición de las políticas gestionadas por la Gerencia de Tecnología. En cuanto a la estructura de la Gerencia de Tecnología, dependiente de la Coordinación Ejecutiva del Instituto, la misma Resolución, crea la Subgerencia de Gestión de la Calidad y Gestión de la Información y la*	El comentario del auditado no desconoce ni objeta el hallazgo. Al contrario, lo toma y al respecto realiza manifestaciones que definen un plan de acción de mejoras. En este sentido, toda mejora posterior a la finalización de la presente auditoria, deberá ser tenida en cuenta en oportunidad de autorizarse futuros seguimientos o nuevas auditorías. Atento lo expuesto, se mantiene el hallazgo.

En función de lo que establecen las buenas prácticas en la materia (ISO 27001 - Aspectos organizativos para la Seguridad de la Información; CobIT V4 - DS5.1: Administración de la Seguridad de TI y CobIT V4 - DS5.2: Plan de Seguridad de TI), toda organización debe administrar adecuadamente la Seguridad de la Información a partir de los siguientes aspectos: i) concientizar internamente a la organización sobre la necesidad de implementar y cumplir con políticas y procedimientos que garanticen la salvaguarda de los activos de información de la organización y del negocio; ii) conformar un Comité de Gestión de Seguridad de la Información que dicte, formalice, controle y actualice las políticas y procedimientos de Seguridad de la Información; iii) asignar una estructura técnica especializada contando con todos los medios, recursos e insumos técnicos necesarios, dependiente de las máximas autoridades de la organización, para que se responsabilice de la administración integral de la Seguridad de la Información. Que el organismo no implemente y mantenga en el tiempo estas buenas prácticas vinculadas a la Seguridad de la Información a nivel organizacional, pone en riesgo el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información.	*Subgerencia de Seguridad Informática, (EX-2024-23688759-INSSJP-GRRHH#INSSJP).* *Asimismo, con fecha 22/ago/2024, mediante Resolución RESOL-2024-2407-INSSJP-DE#INSSJP el Director Ejecutivo de PAMI, aprobó la estructura orgánico-funcional de la Jefatura de Gabinete de Asesores creando bajo la órbita de la Gerencia de Seguridad de la Información y Activos Digitales, el Departamento de Gestión de Procesos de Seguridad de la Información y el Departamento de Normas de Protección de Datos y Seguridad de la Información, (EX-2024-86504196-INSSJP-GRRHH#INSSJP).* *La creación de las áreas antes mencionadas, así como sus misiones y funciones, forman parte de una estrategia diseñada en consonancia con las normas ISO 27000 y las normas vigentes en el país, en materia de calidad y seguridad de la información.* ***Respecto de la observación en la que se hace referencia a no contar con un Comité de Seguridad de la Información, se informa a esa Auditoría General de la Nación lo siguiente:*** *Con fecha 20/mar/2024, mediante Resolución RESOL-2024-28738857-INSSJP-DE#INSSJP, el Director Ejecutivo creó el Comité de seguimiento y Seguridad de la Información - CSSI y su Reglamento de Funcionamiento, en la órbita de la Jefatura de Gabinete de Asesores dependiente de la Dirección Ejecutiva. (EX-2024-28738857-INSSJPUSA# INSSJP). En tal instancia se convoca a todos los gerentes del organismo, con el objeto de poner en conocimiento y realizar intercambio de propuestas, respecto de las políticas de seguridad de la información de que se trate. De esta forma, se produce el involucramiento de todas las áreas institucionales. Asimismo, es dable mencionar que, a la fecha de la presente, se llevaron adelante cuatro (4) encuentros del*	

	CSSI en fechas 22/mar/2024,17/abr/2024, 31/may/2024 y 25/sep/2024 respectivamente. *En sintonía con todo lo antes mencionado, con fecha 30/agos/2024, mediante Resolución RESOL-2024-2491-INSSJP-DE#INSSJP, el Director Ejecutivo de PAMI, aprobó el Plan Anual Operativo 2024, en el que se aborda, desde el EJE 4 del mencionado plan, la Transformación digital, disponibilidad, integridad y seguridad de la información (EX-2024-90093505-INSSJP-JGA#INSSJP).* ***En cuanto a las capacitaciones efectuadas al personal, se informa lo siguiente:*** *Se llevan a cabo capacitaciones virtuales, mediante la plataforma EDUPAMI, que es el soporte digital de los cursos que se brindan al personal del Instituto, sobre las siguientes temáticas:* *1. Seguridad de la información, conceptos fundamentales* *2. Riesgos para la seguridad de la información* *3. Introducción a los datos personales* *4. Clasificación de la información y gestión de riesgos* *5. Aspectos esenciales sobre términos y condiciones de uso y políticas de privacidad* *a.b. Por otra parte, se llevan adelante talleres presenciales sobre las siguientes temáticas:* *1. Seguridad de la Información y Clasificación de la Información (30/may/2024)* *2. Gestión de Riesgos de Seguridad de la Información (13/jun/2024)* *3. Integrador de Clasificación de la Información y Gestión de Riesgos (04/jul/2024)* *4. Gestión de Incidentes de Seguridad de la Información (08/ago/2024)* *5. Aspectos legales sobre la Protección de Datos Personales y el Derecho de Acceso a la Información Pública (22/ago/2024)*	

	6. Introducción a la Continuidad de las Operaciones (18/09/2024) *7. Mapeo de Procesos orientados a Seguridad de la información (10/oct/2024)* *8. Ciclo de vida de las TICs – parte 1 (a definir fecha)* *9. Ciclo de vida de las TICs – parte 2 (a definir fecha)*	
4.2.2. ***La estructura organizacional para administrar eficiente y efectivamente la seguridad de la información del INSSJP no es funcional respecto a lo establecido en la Política de Seguridad de la Información del organismo. Escenario que pone en riesgo la confidencialidad, integridad y disponibilidad de la información del Instituto.*** La Política de Seguridad de la Información del INSSJP (Disposición 0002/15 GYTC) designa al Subgerente de Seguridad Informática como Responsable de Seguridad de la Información del organismo. Sin embargo del análisis de la información suministrada por el auditado y de las entrevistas mantenidas con las áreas responsables de implementar dichas políticas, se ha podido comprobar que: i) la Subgerencia de Seguridad Informática no existe dentro de la estructura organizacional del organismo, motivo por el cual no se ha designado un subgerente de seguridad que pueda llevar adelante el rol que le impone la mencionada política de seguridad; ii) durante el periodo auditado y las tareas de campo el área "División de la Seguridad de la información y Seguridad Informática" se mantuvo acéfala; iii) la mencionada división se encuentra formalizada bajo la órbita de la Gerencia de Tecnología; y iv) durante las tareas de campo y en forma transitoria se le asignó la responsabilidad de la seguridad de la información a la Subgerencia de Gestión de la Demanda, dependiente también de la Gerencia de Tecnología. No obstante, y ante la renuncia del subgerente, se volvió a la situación inicial de acefalia respecto de la gestión de la seguridad de la información en el INSSJP.	***4.2.2 / Referente a la estructura organizacional y la Política de Seguridad de la Información y adicionalmente a lo respondido en 4.2.1, puntos a), b) y c), se señala:*** *Mediante EX-2024-96625303- INSSJP-GSIYAD#INSSJP se encuentra en curso de aprobación por el Director Ejecutivo el Proyecto de Resolución de la* ***Política de Seguridad de la Información*** *del INSSJP, basada en ISO 27.001/2022-*	El comentario del auditado no desconoce ni objeta el hallazgo. Al contrario, lo toma y al respecto realiza manifestaciones que definen un plan de acción de mejoras. En este sentido, toda mejora posterior a la finalización de la presente auditoria, deberá ser tenida en cuenta en oportunidad de autorizarse futuros seguimientos o nuevas auditorías. Atento lo expuesto, se mantiene el hallazgo.

Respecto de lo expresado en este punto, las buenas prácticas establecen que: i) los organismos deben administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio (CobiT 4.1 - DS5.1: Administración de la Seguridad de TI); ii) establecer la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel superior apropiado; iii) definir y asignar roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento. Puede ser necesario asignar responsabilidades adicionales de administración de la seguridad a nivel de sistema específico (CobIT v4.1 - PO4.8: Responsabilidad sobre el riesgo, la seguridad y el cumplimiento); y iv) la Res. 87/22-SIGEN: 1.4 establece que la asignación de responsabilidades debe garantizar una adecuada separación de funciones, que fomente el control por oposición de intereses. Teniendo en cuenta el escenario evidenciado en el organismo por este equipo de auditoria, y en base a lo que establecen las buenas prácticas en la materia, se puede aseverar que la estructura de seguridad de la información del INSSJP no tiene el nivel jerárquico y estratégico apropiado dentro de la estructura orgánica del Instituto, con las capacidades para garantizar que las acciones de la administración de la seguridad estén en línea con los requerimientos de la organización, poder definir y asignar roles críticos para administrar los riesgos de TI y garantizar la adecuada separación de funciones para fomentar el control por oposición de intereses. Esta situación pone en riesgo la capacidad del Instituto de asegurar adecuadamente la integridad, disponibilidad y confidencialidad de la información y la seguridad sobre la infraestructura tecnológica que da servicio al procesamiento de la		

información, con el objetivo de minimizar vulnerabilidades e incidentes de seguridad.		
4.2.3. ***La Gerencia de Tecnología (responsable del área de seguridad de la información) no realiza pruebas de seguridad e intrusión sobre la plataforma tecnológica del organismo, en especial sobre los entornos que dan soporte a los procesos de receta electrónica en lo referido a la prescripción, dispensa y liquidación de medicamentos. Esta situación no permite medir el grado de seguridad en que se encuentran estos entornos, diagnosticar y tomar acciones correctivas que minimicen los riesgos que pudieran comprometer la confidencialidad, integridad y disponibilidad de la información.*** Del análisis de la documentación técnica entregada y de las entrevistas mantenidas con personal del área de informática del instituto, se constató que, durante el período auditado, no se han aplicado procedimientos de pruebas y análisis de seguridad informática que incluyan testeos de intrusión sobre la plataforma tecnológica del organismo, en especial sobre los entornos que dan soporte a los procesos de receta electrónica en lo referido a la prescripción, dispensa y liquidación de medicamentos. Las buenas prácticas en seguridad de los sistemas señalan que la necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye, entre otros, realizar pruebas periódicas, así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad. (CobIT v4.1 - DS5: Garantizar la seguridad de los sistemas)	*1. /* ***Referente a las Pruebas de seguridad e intrusión*** *Mediante Licitación pública nº 17/2024 se encuentra en proceso el procedimiento para la adquisición de equipamiento y soluciones para la actualización y fortalecimiento de las infraestructuras de ciberseguridad del instituto, en tal marco se contempla la contratación de herramientas para la medición de grados de seguridad de los entornos de infraestructura digital.*	El comentario del auditado no desconoce ni objeta el hallazgo. Al contrario, lo toma y al respecto realiza manifestaciones que definen un plan de acción de mejoras. En este sentido, toda mejora posterior a la finalización de la presente auditoria, deberá ser tenida en cuenta en oportunidad de autorizarse futuros seguimientos o nuevas auditorías. Atento lo expuesto, se mantiene el hallazgo.

La falta de pruebas de seguridad informática sobre los activos de TI del INSSJP generan las siguientes limitaciones: i) no permite medir, en materia de seguridad, el grado de solidez de los sistemas y herramientas informáticas utilizadas para dar soporte a los procesos críticos del organismo; ii) podrían no detectarse vulnerabilidades que puedan comprometer la confidencialidad, integridad y disponibilidad de la información; y iii) posibles fallas en las acciones correctivas para minimizar el impacto de las vulnerabilidades o incidentes de seguridad.		
4.3. Continuidad de las operaciones Organizacionales. **4.3.1.** ***El INSSJP no cuenta con un Plan de Continuidad del Negocio (BCP, por sus siglas en inglés). Esta carencia pone en riesgo la operación de los procesos críticos de la organización.*** A partir de la evaluación de la documentación técnica provista por el organismo y de las entrevistas mantenidas con los responsables de áreas clave del INSSJP, se constató que el Instituto no cuenta con un Plan de Continuidad del Negocio (BCP, por sus siglas en inglés), ni si quiera evaluado ni aprobado. Las buenas prácticas en esta cuestión (ISO 22.301 – Directrices para garantizar la Continuidad del Negocio; ISO 27.001 – Sistemas de gestión de la seguridad de la información; CobiT 4.1 – DS4 Garantizar la continuidad del servicio), indican que un Plan de Continuidad del Negocio es un proceso de recuperación operacional que le permite a la organización estar preparada frente a una contingencia causada por una interrupción mayor e inesperada, con el objetivo de garantizar la continuidad de la operación crítica de la empresa durante y posteriormente a una crisis, como desastres naturales o incidencias de seguridad informática a	*1. / **Referente a las Pruebas de seguridad e intrusión*** *Mediante Licitación pública nº 17/2024 se encuentra en proceso el procedimiento para la adquisición de equipamiento y soluciones para la actualización y fortalecimiento de las infraestructuras de ciberseguridad del instituto, en tal marco se contempla la contratación de herramientas para la medición de grados de seguridad de los entornos de infraestructura digital.* ***4.3.1 / Referente al BCP – Plan de Continuidad de Negocio*** *La Gerencia de Seguridad de la Información y Activos Digitales presentó un proyecto, el cual se encuentra en curso, con apoyo del Banco Interamericano de Desarrollo (BID) - número de cooperación técnica NO REEMBOLSABLE CT AR-T1384, denominado "Apoyo a la Transformación en Seguridad de la Información del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP)". Este proyecto forma parte de la estrategia de diseño como aporte al Plan de Continuidad de Negocio que se encuentra en proceso de elaboración, luego de haber atravesado el relevamiento y diagnóstico inicial previo.*	El comentario del auditado no desconoce ni objeta el hallazgo. Al contrario, lo toma y al respecto realiza manifestaciones que definen un plan de acción de mejoras. En este sentido, toda mejora posterior a la finalización de la presente auditoria, deberá ser tenida en cuenta en oportunidad de autorizarse futuros seguimientos o nuevas auditorías. Atento lo expuesto, se mantiene el hallazgo.

los que se encuentran continuamente amenazadas todas las organizaciones públicas y privadas, más aún un organismo como el INSSJP que gestiona una infraestructura tecnológica catalogada como infraestructura crítica. Según las mejores prácticas anteriormente indicadas, un Plan de Continuidad del Negocio debe contener, desarrollar y ejecutar como mínimo los siguientes pasos: j) Determinar el perfil de riesgos a los cuales está sometida la organización a través de una autoevaluación sobre las personas, los procesos críticos del negocio y el contexto en el cual se desarrollan. k) Identificar los procesos, productos, servicios y/o funciones clave. l) Establecer los objetivos del plan de continuidad de la actividad. m) Evaluar el impacto potencial de las interrupciones para la organización y sus trabajadores. n) Determina los tiempos necesarios para lograr la recuperación de los procesos críticos del negocio ante una contingencia. o) Enumerar las acciones necesarias para asegurar la protección de la organización y sus procesos, productos, servicios y/o funciones clave. p) Organizar las listas de contactos de todas aquellas personas que deben actuar en situación de contingencia. q) Concienciar, difundir y capacitar periódicamente a todos los RRHH de la organización sobre el plan de continuidad del negocio. r) Probar, mantener, revisar y actualizar periódicamente el plan de continuidad del negocio. La implementación de un Plan de Continuidad del Negocio le permite al INSSJP estar preparado ante una catástrofe, minimizando impactos sobre sus objetivos estratégicos, así		

como procesos críticos internos y aquellos que dan servicio sus clientes del Sector Público Nacional y privados.

Ilustración N°. 7 Principales etapas de un BCP

Fuente: elaboración propia-DAI- en base a ISO 22.301.

Ilustración N° 8. Cronología de procesos en un BCP

Fuente: elaboración propia -DAI- en base a ISO 22.301.

Que el INSSJP no cuente con un Plan de Continuidad del Negocio, ni su debida aprobación, evaluación y actualización, acorde a lo que establecen las buenas prácticas y su correspondiente difusión, capacitación, plan de pruebas, documentación de simulacros y ajustes

continuos, pone en riesgo la disponibilidad de las operaciones críticas de la propia organización, como así también de los servicios comprometidos con sus afiliados y prestadores.		
4.3.2. ***La Gerencia de Tecnología, a cargo de la gestión y administración de la infraestructura tecnológica que da soporte de TI al organismo, no cuenta con un Plan de Recuperación ante Desastres (DRP, por sus siglas en inglés), situación que pone en riesgo el aseguramiento de la continuidad de los servicios de TI ante la ocurrencia de eventualidades o amenazas de cualquier tipo.*** A partir del análisis realizado sobre la documentación técnica provista por el auditado, y de las entrevistas mantenidas con el responsable la Gerencia de Tecnología, se verificó que no se cuenta con la existencia de un Plan de Recuperación ante Desastres que asegure la continuidad de los servicios de TI que dan soporte al INSSJP. En función de lo que establecen las buenas prácticas en la materia, un Plan de Recuperación ante Desastres (DRP, por sus siglas en inglés) es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de ocurrencia de un desastre natural, errores humanos, ciberataques o ataques causados por terceros de cualquier tipo, que atenten contra la continuidad del funcionamiento de la organización. En este proceso no solo intervienen las áreas técnicas responsables de su ejecución sino también las áreas críticas de la organización, incluida la alta dirección, que deben formar parte de un comité de crisis para actuar al momento de su activación (ISO 22.301, directrices para garantizar la Continuidad del Negocio; ISO 24.762, directrices para asegurar la Continuidad de los Servicios de TI; ISO 27.001, Sistemas de gestión de la seguridad de la	***4.3.2 / Referente a no contar con un DRP – Plan de Recuperación ante Desastres*** *Por EX-2024-96625303- -INSSJP-GSIYAD#INSSJP se encuentra en curso de aprobación por el Director Ejecutivo el Proyecto de Resolución de la "Política de Seguridad de la Información" del INSSJP actualizada a ISO 27.001/2022- la que incluye el proceso a desarrollar por la Gerencia de Tecnología de la Información.*	El comentario del auditado no desconoce ni objeta el hallazgo. Al contrario, lo toma y al respecto realiza manifestaciones que definen un plan de acción de mejoras. En este sentido, toda mejora posterior a la finalización de la presente auditoria, deberá ser tenida en cuenta en oportunidad de autorizarse futuros seguimientos o nuevas auditorías. Atento lo expuesto, se mantiene el hallazgo.

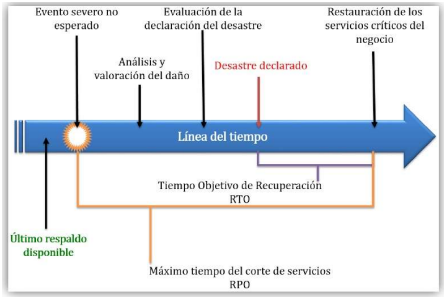
información; CobIT 4.1, proceso DS4 - Garantizar la continuidad del servicio).

Según las mejores prácticas anteriormente indicadas, un Plan de Recuperación ante Desastres debe contener, desarrollar y ejecutar como mínimo los siguientes pasos:

g) desarrollar una política de continuidad del negocio;
h) realizar una evaluación de riesgos;
i) realizar un análisis de impacto al negocio;
j) desarrollar estrategias de recuperación y continuidad del negocio;
k) concientizar, capacitar y probar los planes;
l) mantener y mejorar el plan de recuperación ante desastres.

La consideración de este plan ofrece la ventaja de responder de forma planeada y proactiva ante una catástrofe y minimizar su impacto en los objetivos y misión del INSSJP y sobre los sistemas de información que constituyen el soporte informático a los servicios que ésta presta.

Ilustración N° 9: Etapas de un DRP



Fuente: elaboración propia-DAI- en base a ISO 24.762.

Que la Gerencia de Tecnología, a cargo de la gestión y administración de la infraestructura tecnológica del

organismo, no cuente con un Plan de Recuperación ante Desastres acorde a lo que establecen las buenas prácticas y su correspondiente plan de pruebas, documentación de simulacros y ajustes continuos, implica un riesgo de alto impacto sobre la disponibilidad de la información ante una interrupción de los servicios de TI, sobre los cuales todas las áreas operativas del INSSJP tienen una alta dependencia.		
4.3.3. ***La Gerencia de Tecnología del INSSJP no cuenta con políticas y procedimientos formalizados de resguardo de la información (backups) que establezcan las formas técnicas de ejecución y los períodos en los que se deben efectivizar las copias de respaldo de la información y sus debidas pruebas de restauración en virtud de los requerimientos que exijan los procesos críticos de la organización. Esta carencia pone en riesgo la disponibilidad de la información.*** Del estudio realizado sobre la documentación técnica provista por el auditado, y de las entrevistas mantenidas con el responsable de la Gerencia de Tecnología se constató que las medidas de respaldo de la información aplicadas por los responsables técnicos de esta tarea son insuficientes e inadecuadas debido a que: i) no existen políticas y procedimientos formalizados de resguardo de la información que permitan monitorear el efectivo cumplimiento de esta actividad clave y crítica para la organización y que establezcan revisiones periódicas con las áreas usuarias respecto a las nuevas necesidades de backups; y ii) no se realizan procesos de pruebas de restauración que permitan comprobar la eficacia de las copias realizadas y garantizar la disponibilidad de la información ante una contingencia que amerite tener que restaurar una copia de resguardo. Las buenas prácticas sobre políticas y procedimientos de back-ups y pruebas de restauración establecen que se debe	***4.3.3 / Referente a no contar con políticas y procedimientos formalizados de resguardo de la información Back-Up.*** *Por EX-2024-96625303- -INSSJP-GSIYAD#INSSJP se encuentra en curso de aprobación por el Director Ejecutivo el Proyecto de Resolución de la "Política de Seguridad de la Información" del INSSJP actualizada a ISO 27.001/2022- la que incluye el proceso a desarrollar por la Gerencia de Tecnología de la Información.*	El comentario del auditado no desconoce ni objeta el hallazgo. Al contrario, lo toma y al respecto realiza manifestaciones que definen un plan de acción de mejoras. En este sentido, toda mejora posterior a la finalización de la presente auditoria, deberá ser tenida en cuenta en oportunidad de autorizarse futuros seguimientos o nuevas auditorías. Atento lo expuesto, se mantiene el hallazgo.

garantizar la posesión de copias de resguardo de toda la información crítica utilizada por la organización, relevando de manera continua las necesidades de resguardo de información con las áreas usuarias. Además, se debe someter a la solución de back-up y recuperación de datos a pruebas formalizadas en forma periódica con la debida documentación de los resultados obtenidos en ellas, con la aceptación y control de las áreas usuarias. Estos testeos deben poner a prueba el funcionamiento de la tecnología utilizada, y es la forma más adecuada de detectar y resolver posibles fallos antes de que ocurra un incidente real (ISO 27.001 - Aspectos de seguridad - Información para la gestión de continuidad de negocio y CobIT v4.1 - DS4: Garantizar la continuidad del servicio). Aplicar procedimientos de backups que no garanticen el resguardo exitoso de la información y que se ejecuten en períodos que no satisfagan las necesidades operativas de la organización, pone en riesgo la disponibilidad de dicha información ante un incidente que requiera aplicar una restauración.		