Auditoría General de la Nación

INFORME DE AUDITORÍA

Gestión de TI. Sistemas de información -
Registro de denuncias, Línea Telefónica 168 (Ex 0800) y sistemas y procesos relacionados -
INSTITUTO NACIONAL CONTRA LA DISCRIMINACIÓN, LA XENOFOBIA Y EL RACISMO (INADI)

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

Tabla de contenido

Glosario

AAIP: Agencia de Acceso a la Información Pública.

ABM: **A**ltas, **B**ajas y **M**odificaciones.

CIDyP: Coordinación de Investigaciones, Dictámenes y Patrocinio.

CIOD: Coordinación de Investigación y Observatorios sobre Discriminación

CISC: Coordinación de Instrucción y Seguimientos de Casos.

CobIT: Objetivos de Control para Información y Tecnologías Relacionadas, por sus siglas en inglés *Control Objectives for Information and Related Technology*. Se utiliza como marco de referencia de buenas prácticas en TI.

CPD: Centro de Procesamiento de Datos.

CRyED: Coordinación de Recepción y Evaluación de Denuncias.

DA: Decisión Administrativa.

DAVic: Dirección de Asistencia a la Víctima.

DB: Base de Datos, por sus siglas en inglés *Data Base.*

DG: Delegaciones del INADI.

DRP: Plan de recuperación ante desastres, por sus siglas en inglés *Disaster Recovery Plan*.

GDE: Sistema de Gestión Documental Electrónica.

GUID: Guías INTOSAI.

IDI: Iniciativa de Desarrollo de INTOSAI.

INADI: Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo.

INTOSAI: Organización Internacional de Entidades Fiscalizadoras Superiores, por sus siglas en inglés *International Organization of Suprime Audit Institutions*.

ISO: Organización Internacional de Normalización, 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*. Se utiliza como marco de referencia de buenas prácticas en TI.

ME: Mesa de Entradas.

ODS: Objetivos de Desarrollo Sostenible.

SIGEN: Sindicatura General de la Nación.

SLA: Acuerdos de Nivel de Servicio, por sus siglas en inglés *Service Level Agreement*.

SPSS: Paquete Estadístico para las Ciencias Sociales, por sus siglas en inglés *Statistical Package for the Social Sciences.*

TAD: Trámites a Distancia.

TI: Tecnologías de la Información.

UAI: Unidad de Auditoría Interna.

UNL: Universidad Nacional del Litoral.

WGITA: Grupo de Trabajo sobre Auditoría TI, por sus siglas en inglés *Working Group Information Technology Audit*.

INFORME DE AUDITORIA

A la Sra. Interventora
Dra. Greta Pena
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 CONTRA LA DISCRIMINACIÓN, LA XENOFOBIA Y EL RACISMO (INADI), con el objeto que se detalla en el apartado 1.

1. OBJETO DE AUDITORÍA

Gestión de TI. Sistemas de información – Registro de denuncias, Línea Telefónica 168[1] (Ex 0800) y sistemas y procesos relacionados, en el Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo (INADI).

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

[1] En el Programa de Acción Anual 2022 aprobado por Res. AGN 146/21, el objeto de auditoría referenciaba a la Línea Telefónica "0800", que luego, dentro del período auditado (Marzo 2021), fue reemplazada por la Línea "168".

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"[2], y aplicándose los procedimientos detallados en el punto 2.3.

El inicio de las tareas de auditoría se notificó al Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo mediante Nota Nº 41 /2022-GPyPE, recibida el 18/03/2022.

El período auditado se extiende del 01/12/19 al 31/01/22.
Las tareas de campo se desarrollaron entre los meses de abril de 2022 a noviembre de 2022.

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

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

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.[3]

La tarea abarcó el estudio y verificación de: i) la gestión informática aplicada en el organismo; ii) los procesos técnicos y administrativos practicados por la Dirección de Asistencia a la Víctima y las áreas dependientes de esta dirección en lo que respecta al tratamiento de denuncias y consultas sobre discriminación, xenofobia y racismo; iii) los procedimientos técnicos aplicados por la Coordinación de Investigación y Observatorios sobre Discriminación para la elaboración de estadísticas y del "Mapa Nacional de la Discriminación"[4], insumo clave para la confección del indicador para la meta ODS 10.3; iv) el soporte y mantenimiento continuo de las aplicaciones y herramientas informáticas utilizadas para los puntos ii) y iii); y v) 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[5] como las más importantes relativas al objeto de auditoría:

- Gobierno de TI;
- Seguridad de la Información;
- Seguridad de la infraestructura de TI;
- Continuidad de las operaciones organizacionales;

[3] 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.
[4] El **Mapa Nacional de la Discriminación** es un relevamiento que realiza periódicamente el Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo (INADI) con el objetivo de producir conocimiento sobre las formas en que se expresa la discriminación en Argentina. (https://www.argentina.gob.ar/inadi/mapa-nacional-de-la-discriminacion)
[5] 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.

- Operaciones de TI;
- Adquisiciones y contrataciones de TI;
- Sistemas de información.

Adicionalmente, por Disp. 62/22-AGN, se incorporó en el Plan de trabajo 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 practicas describen los procedimientos que una organización debe implementar para obtener resultados óptimos en la gestión de la información.

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[6].

Seguridad de infraestructura de TI:

- Evaluación del diseño del CPD.

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.

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

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 INADI.

Adquisiciones y contratación de TI:

- verificación y análisis de los acuerdos de niveles de servicio pactados con los proveedores, en especial con el proveedor Gradicom S.A. que presta el servicio integral del call center de atención en la línea telefónica 168 (Ex 0800).

Sistemas de información:

- evaluación de la integración de los procesos relacionados con las consultas y denuncias por discriminación, racismo y xenofobia;
- en el marco de los procesos relacionados a la elaboración y publicación de estadísticas sobre las consultas y denuncias por discriminación, racismo y xenofobia, se llevó a cabo el análisis de los mecanismos de control de salida de datos que deben garantizar la integridad y exactitud de la información;
- evaluación de las actividades y funciones habilitadas al administrador de la base de datos productiva de denuncias por discriminación, racismo y xenofobia;
- constatación de que en el INADI existan políticas y procedimientos de confidencialidad con los empleados que gestionan información sensible sobre las denuncias por discriminación, racismo y xenofobia.

Procedimientos transversales:

- inspección a la Sala de Servidores del INADI;
- inspección a la oficina que alberga al servidor de la base de datos de denuncias;
- inspección al Call Center de INADI para el servicio de la Línea Telefónica 168 (Ex 0800).

- 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.

3. ACLARACIONES PREVIAS

3.1. Marco conceptual

El INADI, en colaboración con la Secretaría de Derechos Humanos de la Nación, la Dirección de Derechos Humanos de Cancillería, la Secretaría de Gabinete de Ministros y especialistas en la materia elaboró un Plan Nacional contra la Discriminación[7] [8], según el cual las prácticas sociales discriminatorias abarcan cualesquiera de estas acciones:

1. Crear y/o colaborar en la difusión de estereotipos de cualquier grupo humano por características reales o imaginarias, sean estas del tipo que fueren, sean estas positivas o negativas y se vinculen a características innatas o adquiridas.
2. Hostigar, maltratar, aislar, agredir, segregar, excluir y/o marginar a cualquier miembro de un grupo humano del tipo que fuere por su carácter de miembro de ese grupo.
3. Establecer cualquier distinción legal, económica, laboral, de libertad de movimiento o acceso a determinados ámbitos.

[7] http://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/109501/norma.htm
[8] https://www.argentina.gob.ar/sites/default/files/hacia_un_plan_nacional_contra_la_discriminacion.pdf

En el Marco Estratégico de Cooperación de las Naciones Unidas para el Desarrollo de Argentina (MECNUD), se conformó el Grupo de Trabajo "Cero Discriminación a 2030, para la reducción del estigma y la discriminación en Argentina", que cuenta con la colaboración del Sistema de las Naciones Unidas en Argentina (SNU) y de la que participan funcionarios de distintas agencias de las Naciones Unidas brindando asistencia técnica y financiera al INADI, a fin de alcanzar la meta "Cero Discriminación" y los Objetivos de Desarrollo Sostenible (ODS) a 2030[9].

Para el INADI, el trabajo en este marco de cooperación con el Sistema de Naciones Unidas en Argentina comprende la colaboración de los organismos internacionales en tres ejes: la finalización del Mapa de la Discriminación; la elaboración de un documento de diagnóstico del Plan Nacional contra la Discriminación, que presente un estado de situación actualizado de la discriminación en Argentina e incluya una metodología para desarrollar el plan y el desarrollo de proyectos específicos para un trabajo federal[10].

En este sentido, el último mapeo elaborado por *el INADI a través de encuestas realizadas a 11.700 personas en sus hogares durante 2019,* revela los siguientes datos:[11]

- *Mientras que en 2013 solo un 12% de la población consideraba a la discriminación como vulneración de derechos, en el 2019 un 36% indicó esta respuesta.*

[9] https://www.argentina.gob.ar/noticias/reunion-del-grupo-de-trabajo-cero-discriminacion-2030
[10] https://www.argentina.gob.ar/noticias/reunion-del-grupo-de-trabajo-cero-discriminacion-2030
[11] Mapa Nacional de la Discriminación 2019", Tercera Edición, INADI https://www.argentina.gob.ar/noticias/el-inadi-presenta-el-nuevo-mapa-nacional-de-la-discriminacion

Ilustración Nº1 – Interpretación de la discriminación en 2013 vs. 2019

Fuente: INADI. Mapa Nacional de la Discriminación, 2019, Tercera Edición

- *La discriminación es identificada por el 72 % de la población, lo que implica que hay un 28 % de personas que aún mantiene naturalizadas tales situaciones de vulneración de derechos que ocurren día a día en la sociedad.*

Ilustración Nº2 – Personas que experimentaron discriminación 2013 vs. 2019

Fuente: INADI. Mapa Nacional de la Discriminación, 2019, Tercera Edición

- *En cuanto al comportamiento de la discriminación, el relevamiento del INADI identificó tres grandes grupos, los que se aprecian en la Ilustración Nº 3:*

Ilustración Nº3 – Tipos de discriminación

Fuente: INADI. Mapa Nacional de la Discriminación, 2019, Tercera Edición

- *Por último, dentro del imaginario social sobre los ámbitos donde se presenta la discriminación, crecieron notoriamente las menciones acerca de las redes sociales. Sin embargo, cabe aclarar que no muchas personas expresaron haber vivido esas situaciones en primera persona.*

Ilustración Nº4 – Opinión sobre cómo debería actuar el Estado

Fuente: INADI. Mapa Nacional de la Discriminación, 2019, Tercera Edición

Diagnóstico técnico elaborado por la Dirección de Asistencia a la Víctima (DAVIC) del INADI:[12]

A continuación, se transcribe el informe técnico elaborado por la DAVIC.

"En los últimos años, el trabajo de la Dirección de Asistencia a la Víctima del INADI se vio incrementado paulatina pero sostenidamente. De un promedio de 1900 denuncias anuales que se registraron entre el 2008 y el 2010, se llegó a un promedio de 2500 denuncias para los años 2017 a 2019, lo que implicó un crecimiento del 33%. Esta variación no tuvo un correlato en el incremento de la planta de personal ni en la modernización de los procedimientos, lo que fue generando un paulatino atraso en la tramitación de las denuncias.

[12] IF-2020-38543634-APN-DAVIC#INADI – INFORME - Referencia: Fundamentación y formalización de la propuesta, punto 2. Diagnóstico del funcionamiento. (Documento provisto por el auditado)

Este atraso sostenido generó que las denuncias por discriminación puedan demorar hasta tres años en obtener un dictamen de fondo, lo que atenta contra la garantía de obtener un pronunciamiento en un plazo razonable, y contra la eficiencia administrativa. Teniendo en cuenta aquellos casos que se resuelven de modo temprano y aquellos en los que se dicta resolución de fondo, la respuesta del organismo insume, en promedio, 18 meses. Sin embargo, si los casos no son conciliados de modo temprano (lo que sucede en promedio en 4 meses y medio), o las partes no llegasen a un acuerdo (que de lograrse ocurre en promedio en 8 meses), la resolución final demorará aproximadamente 20 meses.

Al mismo tiempo, lo que resulta más preocupante aún es que en los últimos años, un porcentaje muy elevado de estas denuncias terminan obteniendo una resolución negativa, ya sea por no contar con las pruebas suficientes o por no haberse podido acreditar el hecho. Así, en el año 2018, el 79% de los dictámenes de fondo que se pronunciaron fueron de rechazo de la denuncia y sólo el 21% positivo (603 resoluciones negativas frente a 156 positivas). Algo similar ocurrió durante el 2019, donde se rechazaron el 75% de los casos en los que se emitió dictamen y se dictaron resoluciones de fondo positivas sólo en el 25% de ellos (343 negativas frente a 113 positivas).

De este modo, puede observarse que, en la actualidad, el caso medio de denuncia de discriminación que tramita la Dirección de Asistencia a la Víctima demora casi dos años y obtiene un dictamen negativo. Esto sucede por una sumatoria de factores: por un lado, un procedimiento fragmentado, con numerosos pases e intervenciones de diversas áreas que deben estudiar el caso desde cero; por el otro, criterios vetustos sobre la prueba producida o sus cargas; y, en tercer lugar, falta de articulación suficiente entre las diversas coordinaciones y con las delegaciones intervinientes.

Para garantizar el acceso a un recurso efectivo a las víctimas de discriminación –como parte de las obligaciones del Estado Nacional referidas anteriormente— el INADI actualmente se plantea el objetivo inmediato de mejorar en estos aspectos. Por un lado, revisar el procedimiento de tramitación para hacerlo más efectivo, ágil y flexible. Al mismo

tiempo, implementar estándares de pruebas actuales, contando con una mirada integral entre las coordinaciones centrales y las actuaciones de las delegaciones provinciales."

3.2. Marco normativo e institucional

El INADI fue creado por la Ley 24.515[13] del año 1995, como organismo descentralizado en la órbita del Ministerio del Interior. Por Decreto 184/05[14], desde 2005 pasa a depender del Ministerio de Justicia y Derechos Humanos y se encuentra bajo supervisión de la Secretaría de Derechos Humanos (Decreto 988/05[15]).

El Instituto tiene por objeto elaborar políticas nacionales y medidas concretas para combatir la discriminación, la xenofobia y el racismo, impulsando y llevando a cabo acciones a tal fin, y resulta de suma importancia en el esquema institucional de prevención y sanción de la discriminación del Estado, pues son funciones del INADI: recibir consultas de los habitantes y brindar contención y asesoramiento a las víctimas de discriminación, elaborar dictámenes técnicos y patrocinar jurídicamente a quienes quieran recurrir a la justicia.

El INADI es el órgano Nacional encargado de recibir todo tipo de denuncias relacionadas con discriminación, actos de xenofobia y/o racistas. En su ley de creación establece que: "*corresponde al INADI* […] *Recibir y centralizar denuncias sobre conductas discriminatorias, xenofóbicas o racistas y llevar un registro de ellas*"[16]. En base a ello, la Dirección de Asistencia a la Víctima organizó un sistema por el cual se atienden consultas y se tramitan las denuncias recibidas para concluir con un dictamen de opinión técnica sobre el hecho denunciado.

A los efectos de la presente auditoría es importante destacar que los actos discriminatorios que hacen al objeto bajo análisis, se encuentran tipificados en la Ley 23.592[17] de Actos

[13] http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=25031
[14] http://servicios.infoleg.gob.ar/infolegInternet/anexos/100000-104999/104402/norma.htm
[15] http://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/108997/norma.htm
[16] Ley 24.515, art. 4, inciso e).
[17] http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20465/texact.htm

Discriminatorios y concurrentes, y contemplados en los Pactos Internacionales de rango Constitucional referidos en el art. 75 inc. 22 de la Constitución Nacional y en los restantes Tratados Internacionales sobre Derechos Humanos

De este modo, se cumplen los compromisos asumidos internacionalmente, entre los que se puede mencionar:

- *Los Estados partes asegurarán a todas las personas que se hallen bajo su jurisdicción, protección y recursos efectivos, ante los tribunales nacionales competentes y otras instituciones del Estado, contra todo acto de discriminación racial que, contraviniendo la presente Convención, viole sus derechos humanos y libertades fundamentales, así como el derecho a pedir a esos tribunales satisfacción o reparación justa y adecuada por todo daño de que puedan ser víctimas como consecuencia de tal discriminación*. (Convención sobre la Eliminación de todas las formas de Discriminación Racial, art. 6),[18] ratificado por Ley 17.722 Contra la Discriminación Racial.
- *Los Estados partes condenan la discriminación contra la mujer en todas sus formas, convienen en seguir, por todos los medios apropiados y sin dilaciones, una política encaminada a eliminar la discriminación contra la mujer y, con tal objeto, se comprometen a:*

  c) *Establecer la protección jurídica de los derechos de la mujer sobre una base de igualdad con los del hombre y garantizar, por conducto de los tribunales nacionales competentes y de otras instituciones públicas, la protección efectiva de la mujer contra todo acto de discriminación*; (Convención sobre la eliminación de todas las formas de discriminación contra la mujer, Art. 2 inciso c),[19] ratificado por Ley 23.179[20] Contra la Discriminación de la Mujer.
- Igualdad y no discriminación

[18] https://www.ohchr.org/es/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial
[19] https://www.un.org/womenwatch/daw/cedaw/text/sconvention.htm
[20] http://servicios.infoleg.gob.ar/infolegInternet/anexos/25000-29999/26305/norma.htm

Los Estados partes prohibirán toda discriminación por motivos de discapacidad y garantizarán a todas las personas con discapacidad protección legal igual y efectiva contra la discriminación por cualquier motivo. (Convención sobre los derechos de las personas con discapacidad, art. 5 inciso 2),[21] ratificado por Ley 26.378[22] Derechos de las Personas con Discapacidad.

El Decreto 218/12[23] del Poder Ejecutivo Nacional, que aprueba la estructura organizativa del primer nivel operativo del INADI, establece en su anexo II que es responsabilidad primaria de la Dirección de Asistencia a la Víctima *"entender en la recepción, registro, evaluación, investigación y análisis de denuncias presentadas sobre conductas discriminatorias, xenófobas o racistas, como así también prestar el servicio de asesoramiento y patrocinio jurídico gratuito a las personas damnificadas".* Con ese fin realizará, entre otras, las siguientes acciones:

- Recibir toda denuncia sobre conductas discriminatorias, xenófobas o racistas y llevar un registro de las mismas.
- Investigar los hechos denunciados, reunir y producir las pruebas pertinentes de acuerdo a los medios previstos en el Reglamento de Procedimientos Administrativos […]
- Analizar y evaluar las denuncias presentadas y elaborar los dictámenes técnicos especializados respectivos […]"

En virtud de este decreto, el entonces del Instituto a través de la Disposición 208/12[24], estableció la estructura de segundo nivel operativo. Así, para la Dirección de Asistencia a la Víctima se crearon dos coordinaciones:

[21] https://www.un.org/esa/socdev/enable/documents/tccconvs.pdf
[22] http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141317/norma.htm
[23] http://servicios.infoleg.gob.ar/infolegInternet/anexos/190000-194999/194121/norma.htm

[24] http://servicios.infoleg.gob.ar/infolegInternet/anexos/200000-204999/202801/norma.htm

- "Recepción y Evaluación de Denuncias" tiene las acciones de "atender las consultas […] brindándoles orientación e información" y también las de "Analizar, evaluar y emitir opinión sobre los casos de las denuncias recibidas".
- "Investigación y Seguimiento de Casos" realizará las acciones de "Investigar los casos denunciados, cuando a criterio de la Coordinación de Recepción y Evaluación […] resulte necesario para una mejor evaluación".

Esta estructura de la Dirección, con dos coordinaciones se mantuvo a lo largo del tiempo estando vigente durante el periodo auditado y las tareas de campo. El Decreto 174/18[25] ratificó al INADI bajo la órbita del Ministerio de Justicia y Derechos Humanos y la DA 823/19 reformó y sistematizó la estructura de primer y segundo niveles del Instituto. En dicha oportunidad, la Dirección de Asistencia a la Víctima no fue modificada, manteniendo lo establecido por la Disposición 208/12, con sólo un cambio de nombre de las coordinaciones. Sin embargo, el artículo 4 de la DA 823/19[26], sí facultó a la Titular del organismo a modificar la estructura del segundo nivel organizativo, sin que ello implique incremento de las unidades organizativas que la componen ni sus partidas presupuestarias.

Los objetivos del INADI más relevantes, a los fines del objeto de auditoria, son:

ATRIBUCIONES Y FUNCIONES[27]:

a) Actuar como organismo de aplicación de la mencionada ley, velando por su cumplimiento y la consecución de sus objetivos, a través del análisis de la realidad nacional en materia de discriminación, xenofobia y racismo y la elaboración de informes y propuestas con respecto a dichos temas;

[25] http://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/307419/norma.htm
[26] http://servicios.infoleg.gob.ar/infolegInternet/anexos/325000-329999/329381/norma.htm

[27] http://servicios.infoleg.gob.ar/infolegInternet/anexos/25000-29999/25031/norma.htm

b) Difundir los principios normados por la Ley 23.592[28], normas concordantes y complementarias, así como los resultados de los estudios que realice o promueva y las propuestas que formule;
c) Recibir y centralizar denuncias sobre conductas discriminatorias, xenofóbicas o racistas y llevar un registro de ellas;

Según su ley de creación y su decreto reglamentario (Decreto PEN 419/15), el INADI debe estar dirigido y administrado por un Directorio, asistido por un Consejo Asesor con funciones consultivas. El Directorio debe estar compuesto por nueve miembros: un Presidente y un Vicepresidente elegidos por el Poder Ejecutivo Nacional, a propuesta en terna del Congreso de la Nación, cuatro representantes de Ministerios Nacionales (Ministerio del Interior; Ministerio de Relaciones Exteriores, Comercio Internacional y Culto; Ministerio de Justicia y Derechos Humanos; y Ministerio de Educación) y *"tres representantes* de las Organizaciones No Gubernamentales serán designados por el Ministro de Justicia y Derechos Humanos, de las ternas propuestas por las organizaciones que hayan sido sorteadas, previa inscripción en el Registro de Organizaciones de la Sociedad Civil del INSTITUTO NACIONAL CONTRA LA DISCRIMINACIÓN, LA XENOFOBIA Y EL RACISMO (INADI). Dichas Organizaciones No Gubernamentales deberán poseer reconocida trayectoria en la lucha a favor de los derechos humanos y contra la discriminación, la xenofobia y el racismo. "[29].

Sin embargo, desde 1997 el INADI fue intervenido de manera intermitente, lo que merece un párrafo aparte analizar la cantidad de años que ha estado intervenido el INADI, desde su creación por Ley 24.515 de fecha 05/07/1995.

La intervención es una institución por la que la máxima autoridad administrativa central (Poder Ejecutivo Nacional), designa a un funcionario para que regularice una situación de

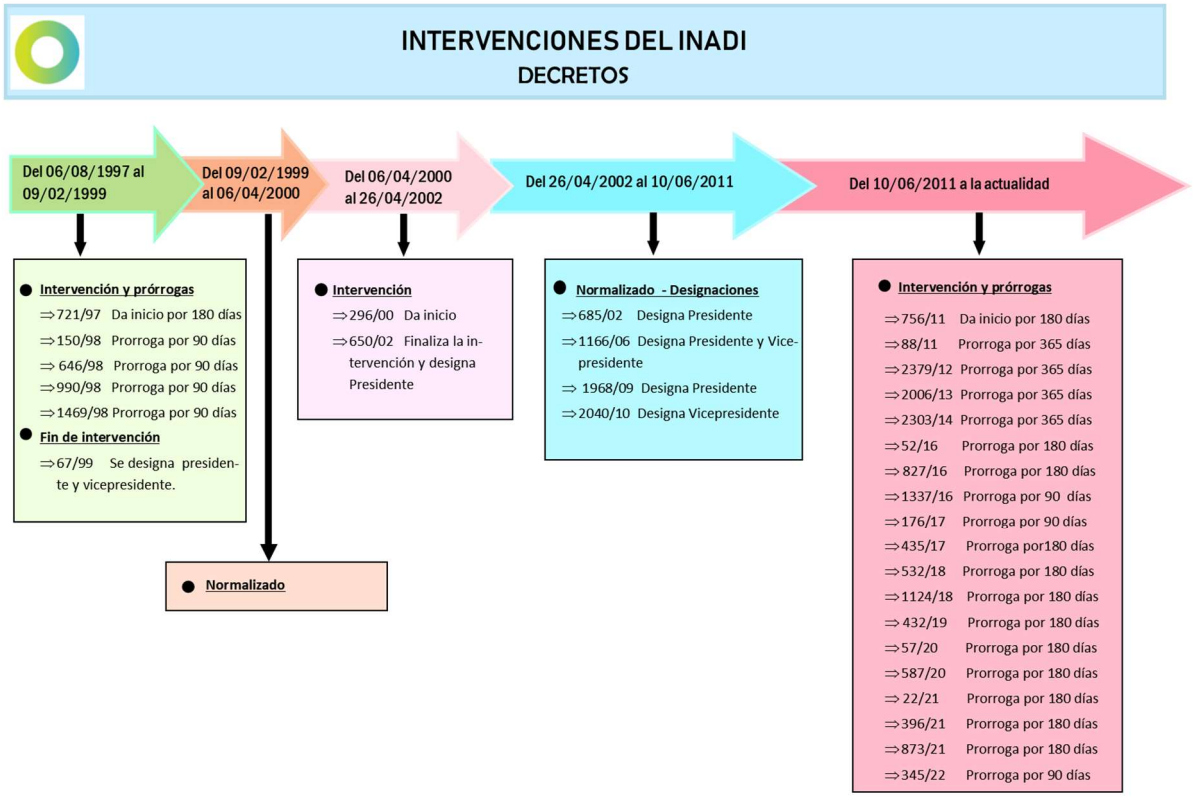
[28] http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=20465
[29] https://www.argentina.gob.ar/normativa/nacional/decreto-419-2015-245009/texto

anormalidad que impide el correcto funcionamiento de un ente descentralizado y hacer cumplir las funciones que la ley le ha dado.

El hecho de que INADI este intervenido, hace que no funcione el Consejo Asesor integrado por un máximo de diez (10) miembros tal cual lo establece la Ley 24.515, y que las decisiones de políticas públicas en los temas relevantes del Instituto sean tomadas unipersonalmente, sin participación del Consejo mencionado, situación que pone de manifiesto que el organismo no funcionaría de acuerdo a lo que establece el espíritu de la Ley que le da creación; no obstante, la intervención es una facultad que tiene el Poder Ejecutivo y está en su órbita ejercerla.

En el período auditado 01/12/19 al 31/01/22, el INADI se encontraba a cargo de la Interventora Dra. Victoria Analía DONDA PÉREZ y a continuación, se detallan los periodos de intervención con los decretos que establecieron las mismas.

Ilustración Nº5 – Intervenciones del INADI



Fuente: Elaboración propia DAI – (Infoleg).

En consecuencia, durante el período auditado, no estuvo vigente la estructura organizativa prevista en la legislación. Las atribuciones y obligaciones otorgadas al Directorio y al Presidente del INADI (Ley 24.515 y Decreto 218/12), son ejercidas por el Interventor designado por el Poder Ejecutivo Nacional.

AUTORIDADES:

A continuación, se presenta el organigrama del INADI vigente al cierre de las tareas de campo de esta auditoría, que surge de la DA-2019-823-APN-JGM .

Cabe mencionar que, la gestión de TI recae sobre la Dirección de Administración, ya que tiene entre sus funciones, "*Dirigir y optimizar la utilización de la información y las Comunicaciones en el Organismo y brindar soporte técnico informático a las áreas del Instituto*".

Asimismo, en lo que respecta a la Dirección de Asistencia a la Víctima, se realizó una modificación a las Coordinaciones de segundo nivel, conforme lo establecido en el artículo 4 de la DA DA-2019-823-APN-JGM , a través de la Resolución INADI 135/20[30], publicada en el Boletín Oficial el 16/07/2020.

Ilustración Nº6 – Organigrama del INADI

[30] http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=339952

Fuente: ***https://www.argentina.gob.ar/inadi***

Objetivos de Desarrollo Sostenible (ODS) en INADI:

Por último, enumeramos los ODS a los que ha adherido el organismo y cuál es la situación al momento de la realización de las tareas de campo de esta auditoria, así como las proyecciones establecidas en el corto y mediano plazo para cada uno de ellos.

El INADI reporta periódicamente a través de la Dirección Nacional de Asuntos Internacionales del Ministerio de Justicia y Derechos Humanos de la Nación, la evolución de un indicador para la medición de la Meta adaptada 10.3: *Garantizar la igualdad de oportunidades y reducir la desigualdad de resultados, incluso eliminando las leyes, políticas y prácticas discriminatorias y promoviendo legislaciones, políticas y medidas adecuadas a ese respecto (Objetivo Global 10)*, formulado a partir del estudio que se realiza a nivel nacional sobre la auto percepción de haber transitado alguna vez una situación discriminatoria (Mapa Nacional de la Discriminación): 10.3.1 Porcentaje de la población que declara haberse sentido personalmente víctima de discriminación, arrojando un resultado del 44% al 2019, según lo informado por INADI a este equipo de auditoría en el documento "3.d.6.7 ODS.pdf", con fecha 29/04/2022.

Asimismo, según lo informado por el Organismo, en el año 2021 el INADI se comprometió a iniciar la medición de un nuevo indicador para la meta adaptada 16.3 "*Promover el estado de derecho en los planos nacional e internacional y garantizar la igualdad de acceso a la justicia para todos*", a saber: *16.3.3. Porcentaje de personas que accedieron a algún mecanismo oficial de resolución de controversias por discriminación* (de medición bianual); cuya composición se basa en el porcentaje de denuncias resueltas a través de mecanismos de resolución de controversias, como las gestiones de buenos oficios ante la parte denunciada, o las conciliaciones de mutuo acuerdo entre partes denunciante y denunciada.

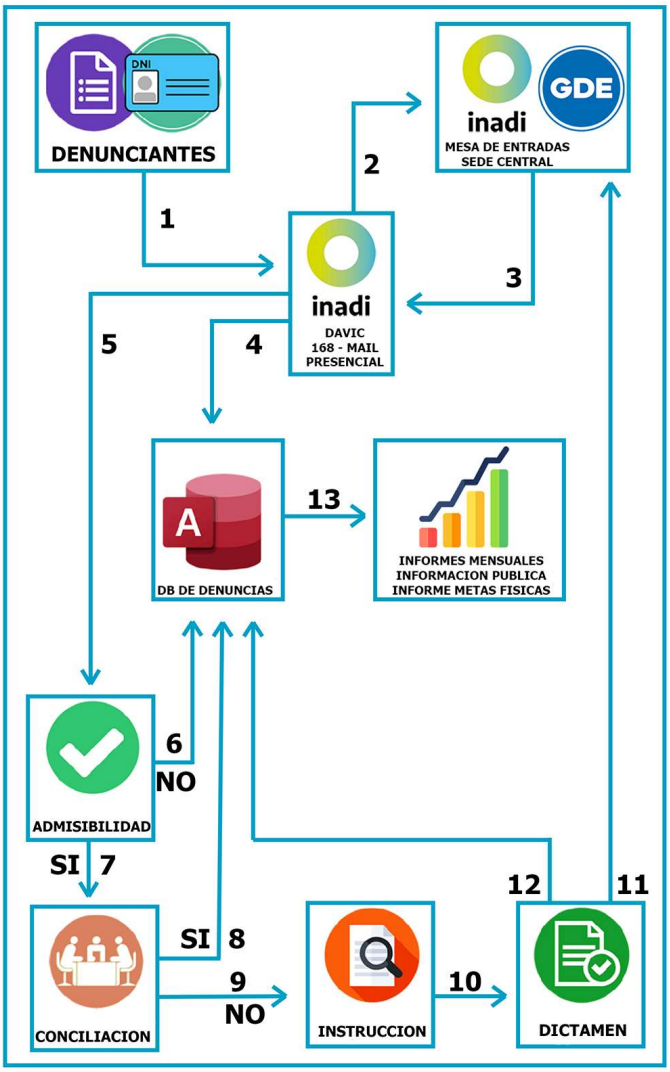
3.3. Descripción de los procesos sujetos al análisis de esta auditoría

Los principales procesos detectados con altos niveles de riesgos de TI y que fueron analizados en función del objeto de auditoría establecido, son: i) el proceso de tratamientos de denuncias; ii) el proceso del tratamiento de consultas. Estos dos procesos son indistintos uno de otro, independientemente de que una consulta evolucione en una denuncia, ya que ambos se tramitan por canales administrativos e informáticos diferentes; y iii) el proceso de elaboración estadística del "Mapa de la Discriminación".

3.3.1 Proceso de tratamiento de denuncias:

- **Denuncias recibidas en la Sede Central**

Ilustración Nº7 – Proceso de denuncias recibidas en la Sede Central del INADI



Fuente: elaboración propia en base a la documentación provista por el organismo y lo relevado por el equipo de auditoría con la Dirección de Asistencia a la Víctima de INADI.

1. Para iniciar una denuncia, los denunciantes deben completar el formulario de denuncia que provee el INADI y acreditar identidad. Los canales para completar y/o enviar este formulario pueden ser la Línea168 (Ex 0800) de atención telefónica, correo electrónico, plataforma de Trámites a Distancia (TAD), o presencialmente.

2. La Dirección de Asistencia a la Víctima (DAVic) recibe la denuncia y la envía a la Mesa de Entradas (ME) de la Sede Central para que cree la carátula e inicie el expediente en el Sistema de Gestión Documental Electrónica (GDE)[31].
3. La ME gira el expediente a la DAVic.
4. La DAVic carga la denuncia en la "Base de Datos de Denuncias", creada y administrada por personal de la DAVic que utiliza el aplicativo Microsoft Access como motor de la misma.
5. La DAVic remite a la Coordinación de Recepción y Evaluación de Denuncias (CRyED), que estudia la admisibilidad de la misma (para que una denuncia sea admisible por el INADI debe estar encuadrada dentro de las previsiones de la Ley 23.592 de Actos Discriminatorios). Asimismo, intenta una resolución rápida de conflictos vía gestión telefónica.
6. En caso que la denuncia no sea admisible, se cierra el expediente y se registra en la "Base de datos de denuncias".
7. Si la denuncia es admitida por el INADI, se le da curso a la Coordinación de Instrucción y Seguimientos de Casos (CISC), dependiente de la DAVic. La misma, convoca a las partes a una conciliación voluntaria.
8. Si las partes logran un acuerdo mediante la conciliación, se cierra el expediente y se registra en la "Base de datos de denuncias".
9. Si las partes no aceptan presentarse a la fase de conciliación o no acuerdan en ella, el expediente sigue su curso en la etapa de instrucción.
10. La Coordinación corre traslado de la denuncia al denunciante y se abre a prueba. Al producirse las pruebas, se adjuntan al expediente y una vez finalizado son revisadas por parte de la Coordinación de Investigaciones Dictámenes y Patrocinio (CIDyP), dependiente de la DAVic.

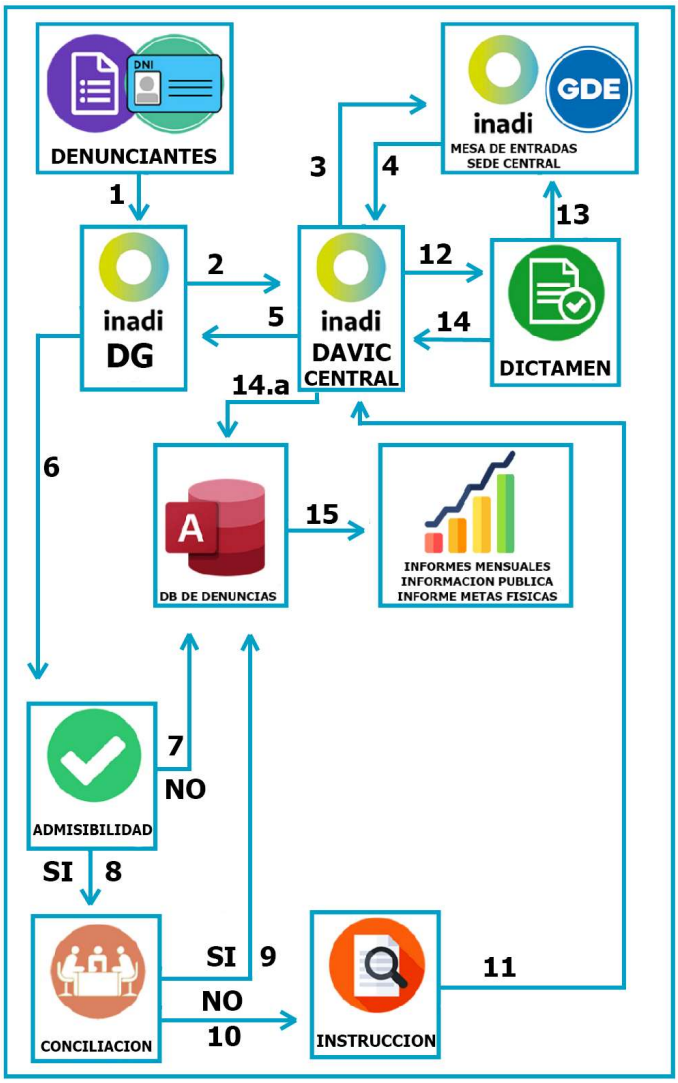
[31] El Sistema de Gestión Documental Electrónica (GDE) es un sistema integrado de caratulación, numeración, seguimiento y registración de movimientos de todas las actuaciones y expedientes del Sector Público Nacional

11. Un asesor de la de la DAVic elabora un proyecto de dictamen, que es revisado internamente, aprobado por la Coordinadora de la CIDyP, y remitido al Director para su suscripción. Una vez firmado por el Director, el mismo se adjunta al expediente[32].
12. Se cierra y se registra en la "Base de datos de denuncias".
13. La Base de datos de denuncias se utiliza para la confección de informes mensuales, a demanda de solicitud de información pública, y trimestralmente para el informe de metas físicas que solicita la Oficina Nacional de Presupuesto del Ministerio de Economía. Las metas físicas que debe informar INADI son: Cantidad de asesoramientos, cantidad de denuncias, cantidad de pronunciamientos y tiempo de respuesta.

[32] Información provista y ratificada por el auditado.

- **Denuncias recibidas en las Delegaciones**

Ilustración Nº8 – Proceso de denuncias recibidas en las Delegaciones del INADI



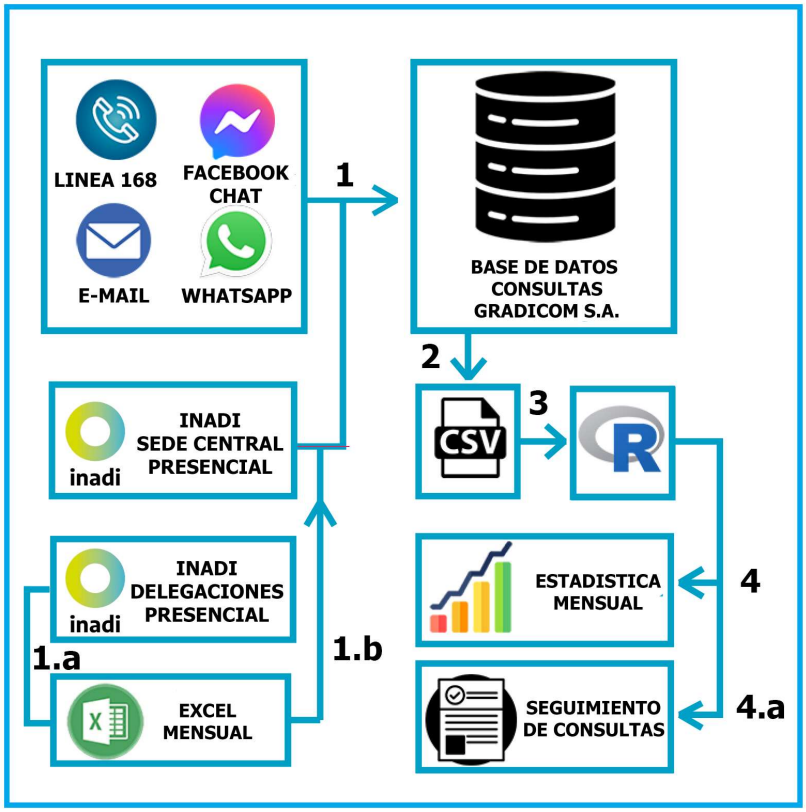
Fuente: elaboración propia en base a la documentación provista por el organismo y a lo relevado por el equipo de auditoría con la Dirección de Asistencia a la Víctima de INADI.

1. Para iniciar una denuncia, los denunciantes deben completar el formulario que provee el INADI y acreditar identidad. El canal para la recepción de las denuncias en las delegaciones es solo presencial.
2. La Delegación envía el formulario a la SEDE Central para que caratule el expediente mediante el Sistema GDE.
3. La Dirección de Asistencia a la Víctima (DAVic) recibe la denuncia y la envía a la Mesa de Entradas (ME) de la Sede Central para que cree la carátula e inicie el expediente en el Sistema GDE.
4. La ME gira el expediente a la DAVic.
5. La DAVic gira el expediente a la Delegación donde se originó la denuncia.
6. La Delegación estudia la admisibilidad de la misma (para que una denuncia sea admisible por el INADI debe estar encuadrada dentro de las previsiones de la Ley 23.592, de Actos Discriminatorios).
7. En caso que la denuncia no sea admisible, se la remite a la Coordinadora de RyED, y si comparte la resolución, se cierra el expediente y se gira a la DAVic para que lo registre en la "Base de datos de denuncias".
8. Si la denuncia es admitida por la Delegación, la misma llama a las partes a una conciliación.
9. Si las partes logran un acuerdo mediante la conciliación, se cierra el expediente y se gira a la DAVic para que lo registre en la "Base de datos de denuncias".
10. Si las partes no aceptan presentarse a la conciliación o no acuerdan en ella, el expediente sigue su curso en la etapa de instrucción.
11. La Delegación corre traslado de la denuncia al denunciante y se abre a prueba. Al producirse las pruebas, se adjuntan al expediente y una vez finalizado se remite a la Coordinación de IdyP en Sede Central para su revisión (aquí finaliza la participación de la Delegación en el proceso de denuncia).
12. El expediente es asignado a un asesor por la Coordinación de Recepción, Evaluación y Dictámenes de Denuncias dependiente de la DAVic a fin de elaborar el proyecto de dictamen.

13. Una vez elaborado el Dictamen por la coordinación y firmado por la DAVic, se adjunta al expediente.
14. (14.a) Se cierra y se registra en la "Base de datos de denuncias".
15. La Base de datos de denuncias se utiliza para la confección de informes mensuales, a demanda de solicitud de información pública, y trimestralmente para el informe de metas físicas que solicita la Oficina Nacional de Presupuesto del Ministerio de Economía. Las metas físicas que debe informar INADI son: Cantidad de asesoramientos, cantidad de denuncias, cantidad de pronunciamientos y tiempo de respuesta.

3.3.2. Proceso de tratamiento de consultas

Ilustración Nº9 - Proceso de tratamiento de consultas



Fuente: elaboración propia en base a la documentación provista por el organismo y lo relevado por el equipo de auditoría con la Dirección de Asistencia a la Víctima de INADI.

1. Para la recepción de consultas en el INADI el sistema cuenta con los siguientes canales de admisión.

   En formato a distancia:

   - **Línea Telefónica 168 (Ex 0800):** El Call Center ubicado en el INADI Central (Av. de Mayo 1401 - CABA) cuenta con cuatro operadores por turno y trabaja los siete días de la semana, de 9.00 a 19.00 hs. El Call Center cuenta con cuatro líneas de telefonía IP[33] contratadas a la empresa Gravicom S.A.
   - **Facebook Chat**[34]: Desde la página oficial de Facebook, la ciudadanía tiene la opción de realizar una consulta, la cual será atendida por el operador de Facebook del INADI.
   - **E-MAIL:** El INADI también recibe y atiende consultas por correo electrónico (0800@inadi.gob.ar).
   - **Whatsapp:** Este medio se utiliza para el caso de ciudadanos hipoacúsicos que deseen enviar un video en lenguaje de señas para realizar una consulta. (Tanto la línea como el dispositivo móvil utilizado, son propiedad del INADI).

   En formato presencial:

   - **INADI Central:** Las oficinas de INADI central (Av. de Mayo 1401 - CABA) atienden consultas de forma presencial en el horario de atención al público, de 9.00 a 16.00 hs. Para todos estos casos las denuncias se cargan en la "base de datos de consultas" en el momento del ingreso. El proveedor

[33] La telefonía IP es la telefonía que establece las comunicaciones mediante Internet y donde la transición de voz se realiza mediante Voz por IP. La telefonía IP funciona a través de conexión a Internet y los teléfonos se conectan al enrutador para tener línea. Esta telefonía usa "protocolos de Internet" para comunicarse por medios digitales. Dirección IP significa "dirección del Protocolo de Internet". Este protocolo es un conjunto de reglas para la comunicación a través de Internet, ya sea el envío de correo electrónico, la transmisión de video o la conexión a un sitio web. Una dirección IP identifica una red o dispositivo en Internet.

[34] Es una aplicación de mensajería instantánea que se creó en 2008 como un chat interno de la red social Facebook. En 2010 cambió su nombre de Facebook Chat a Facebook Messenger y se lanzó como aplicación independiente.

de la base de datos y de la interfaz de carga de datos es Gravicom S.A. (mismo proveedor de las líneas de telefonía IP del Call Center).

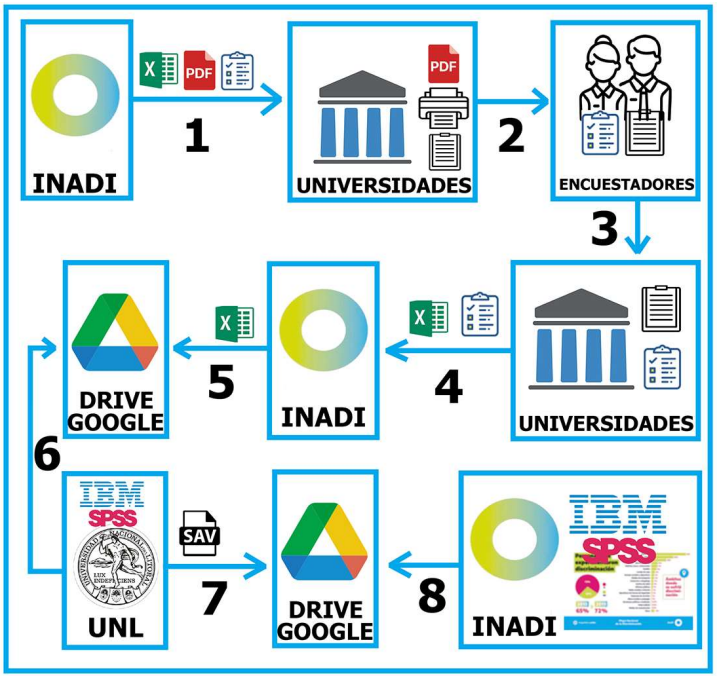
- **Delegaciones INADI[35]:** Las delegaciones de INADI no tienen acceso a la carga de datos en la "Base de datos de consultas", motivo por el cual registran las mismas en una planilla de cálculo que (1a.) mensualmente es enviada al INADI Central (1b.), para que desde INADI Central se cargue la información remitida en la planilla de cálculo en la base de consultas.

2. La Dirección de Asistencia a la Víctima (DAVic) exporta la información contenida en la "base de datos de consultas" a formato "CSV"[36] para ser procesada.
3. Utilizando la plataforma "R"[37] se realizan los procesos necesarios sobre el archivo "CSV" para confeccionar las estadísticas mensuales (con el fin de detectar patrones y realizar informes) y llevar el seguimiento de consultas. (4 y 4a.).

[35] Además de la Sede Central, el INADI cuenta con 25 delegaciones y 18 subdelegaciones esparcidas por todo el territorio argentino.
[36] Un archivo CSV (valores separados por comas) es un tipo especial de archivo que usualmente se puede crear o editar en una planilla de cálculo. En lugar de almacenar la información en columnas, los archivos CSV almacenan datos separados por comas. Cuando el texto y los números se guardan en un archivo CSV, es posible moverlos de un programa a otro.
[37] "R": Es un software (aplicativo) desarrollado con un lenguaje de programación creado para el análisis estadístico.

3.3.3. Proceso de confección del "Mapa Nacional de la Discriminación"[38]

Ilustración Nº10 - Proceso de confección del documento "Mapa Nacional de la Discriminación"



Fuente: elaboración propia en base a la documentación provista por el organismo y lo relevado por el equipo de auditoría.

1. La Coordinación de Investigación y Observatorios sobre Discriminación del INADI, envía a las universidades, quienes por convenio con INADI son las encargadas de realizar las encuestas para la toma de la muestra estadística en cada jurisdicción debido a que el organismo, no tiene la capacidad operativa para realizar la misma con personal propio[39], por correo electrónico los archivos que necesitarán para realizar las encuestas (formulario de encuesta en formato PDF[40] y matriz de

[38] El "Mapa Nacional de la Discriminación" fue publicado en el mes de junio de 2022, la recolección de datos se realizó durante el año 2019 y el procesamiento de los mismos durante el periodo auditado.
[39] Información provista y ratificada por el auditado.
[40] El formato PDF (del inglés, *Portable Document Format*, Formato de Documento Portátil) es un formato de archivo universal que conserva las fuentes, las imágenes y la maquetación de los documentos originales creados en una amplia gama de aplicaciones y plataformas.

carga en formato de planilla de cálculo). Además, diferentes instructivos (en video o escritos) para realizar las encuestas.

2. Las universidades reciben el correo electrónico y descargan el archivo en formato PDF para imprimirlo. Estos formularios impresos serán entregados a los encuestadores junto a las planillas de rastreo para la toma de datos.
3. Los encuestadores contratados por las universidades y capacitados por el INADI, proceden a la toma de datos completando los formularios en función de las cuotas establecidas y las planillas de rastreo. Cada universidad tiene un Jefe de Campo encargado de supervisar la obtención de información que realizan los encuestadores. Al finalizar la tarea de registro, los encuestadores devuelven a las universidades los formularios originales completos (en papel) y las planillas de rastreo. El equipo de CIOD controla el proceso a la distancia manteniendo reuniones con los jefes de campo.
4. Cada universidad realiza la carga de los formularios en la matriz de carga (planilla de cálculo) y realiza una limpieza (búsqueda y corrección de inconsistencias) de la base en función de las "*normas de clean*"[41] establecidas por la CIOD. A su vez, se escanean las planillas de rastreo completadas y se envían junto con la matriz cargada por correo electrónico a la CIOD.
5. La CIOD recibe los archivos en planillas de cálculo (matriz de carga)- que envía cada universidad- y realiza otra limpieza de cada una de las planillas de cálculo. Si se presenta alguna inconsistencia, se consulta a la universidad correspondiente para ver si se puede corregir en base a los originales que ellos poseen. Las planillas de datos que se terminan de limpiar por la CIOD, se suben a un disco compartido virtual (específicamente Google Drive[42]).
6. La Universidad Nacional del Litoral (UNL), encargada de la consolidación estadística, descarga los archivos en formato de planillas de cálculo del disco

[41] Se trata de un marco de trabajo estadístico que establece pautas de depuración de datos según las necesidades del estudio que se esté realizando.
[42] Google Drive es una aplicación de la compañía Google cuyo objetivo es ofrecer un servicio de almacenamiento de archivos en la nube (acceso a centros de almacenamiento por medio de internet).

compartido virtual y consolida todas las planillas en una sola planilla que se utilizará como base de datos final, la cual es importada al software "SPSS"[43]. Asimismo, la UNL realiza el cálculo de ponderación de la información contenida en la base de datos en función del censo 2010.

7. El archivo resultante de la ponderación realizada por la UNL es exportado en formato ".SAV" [44] y subido al disco virtual compartido con la CIOD para que esté a disposición del INADI.
8. En el INADI la base de datos enviada por la UNL (archivo .SAV) se abre en el software "SPSS" para su procesamiento. Los datos obtenidos en este son el insumo estadístico para la confección del "Mapa Nacional de la Discriminación".

Respecto del marco normativo relacionado específicamente al o los sistemas de información que dan soporte al procedimiento de denuncias y a las estadísticas producidas por el INADI, tras el relevamiento y el análisis de la documentación provista por el auditado, se pudo constatar que el Instituto, no ha formalizado normativa y/o decisiones administrativas y/o actos administrativos al respecto.

3.4. Cumplimiento Ley 27.499 (Ley Micaela)

El INADI, a través de la Dirección de Recursos Humanos, está llevando a cabo la capacitación obligatoria en género que establece la Ley 27.499 (Ley Micaela) de acuerdo a lo establecido por el INAM (Instituto Nacional de la Mujer) como organismo rector de dicha ley y el INAP (Instituto Nacional de la Administración Pública) como organismo a cargo de la capacitación del personal de la APN.

[43] SPSS (Por sus siglas en inglés, *Statistical Package for the Social Sciences*) es un programa estadístico informático creado por la empresa IBM que originalmente se usaba únicamente en las investigaciones de las ciencias sociales y en las ciencias aplicadas, y también se aplica ahora en el ámbito la de investigación de mercado.
[44] SAV es el formato de archivo de datos utilizado por el software SPSS.

El INADI cuenta con las certificaciones por parte del Instituto Nacional de la Mujer (INAM) quien certifica que las "Capacitaciones de sensibilización y concientización en el marco de la Ley Micaela: Introducción a la discriminación hacia las mujeres basada en el género" cuentan con los estándares de calidad para la capacitación en la temática de género y violencia contra las mujeres establecidos por ese Instituto y la certificación del Instituto de la Administración Pública (INAP) en calidad de órgano rector, el cual tiene acreditación sobre su diseño y el dictado de cursos.

Del análisis de la documentación provista por el INADI sobre las capacitaciones realizadas surge que, de 422 agentes, han cumplimentado la capacitación 257, lo que representa el 61% del total.

Capacitados		**INADI**	**INAP**	**AMBOS**	**Sin capacitar**
Hombres	84	37	40	7	59
Mujeres	173	73	79	21	106
Total	**257**	**110**	**119**	**28**	**165**
Porcentaje sobre el total del personal	61%				39%

Respecto a los 165 agentes (39% del total del personal) que aún no han sido capacitados en la Ley Micaela, la Coordinación de Recursos Humanos del INADI, manifestó que en el Plan de Capacitación 2023, se contempla la capacitación de la totalidad del personal del Instituto. Este plan no se encontraba oficialmente aprobado al momento de esta auditoría y según lo informado por el auditado deberá estar aprobado por el INADI para ser presentado en el INAP, durante el primer trimestre de 2023.

4. HALLAZGOS

4.1. Gobierno de TI

4.1.1. *El INADI no cuenta con un plan estratégico de TI alineado a los objetivos estratégicos del organismo. Esta carencia dificulta establecer una visión tecnológica de mediano y largo plazo y evidenciar el rol que la tecnología debe tener para brindar un adecuado soporte sobre los procesos críticos de la organización.*

En base al análisis de la documentación solicitada al auditado y de las entrevistas mantenidas con la Dirección de Administración, con el responsable del soporte informático del INADI y con el responsable de la administración de la base de datos de denuncias de discriminación, se verificó que el INADI no posee un plan estratégico de TI elaborado en base a las metas estratégicas del organismo.

Las buenas prácticas referidas a la definición, elaboración, aprobación y puesta en marcha de un plan estratégico de TI indican que las estrategias de negocio y de TI deben estar integradas, relacionando de manera clara las metas de la organización y las metas de TI y reconociendo las oportunidades, así como las limitaciones en la capacidad actual, y se deben comunicar de manera amplia. Identificar las áreas en que el negocio (estrategia) depende de forma crítica de TI, y mediar entre los imperativos del negocio y la tecnología, de tal modo que se puedan establecer prioridades concertadas. (CobIT V4.1 - PO1.2 Alineación de TI con el Negocio).

Sobre esta base, se debe crear un plan estratégico de TI de corto y mediano plazo que, entre otros, defina: i) cómo TI va a contribuir con los objetivos estratégicos de la organización (metas del negocio); ii) el presupuesto de la inversión que conlleva el plan, las fuentes de financiamiento, la estrategia de obtención, la estrategia de adquisición, y los requerimientos legales y regulatorios a cumplir; iii) los riesgos relacionados a su puesta en marcha; iv) cómo TI dará soporte a los programas de inversión establecidos en el plan; v)

cómo se cumplirán y medirán los objetivos y recibirán una autorización formal de los interesados; y vi) el plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI. (CobIT V4.1 - PO1.4 Plan Estratégico de TI).

Que el INADI no cuente con un plan estratégico de TI genera una considerable limitación sobre la ejecución eficiente de los procesos operacionales críticos que deben dar cumplimiento a los objetivos estratégicos de la organización. La falta de una visión estratégica de TI alineada con las metas del organismo reduce la posibilidad de identificar las oportunidades de evolución y mejora basadas en el soporte tecnológico, materia clave en la actualidad para toda organización.

4.1.2. *El INADI no posee políticas, normas y procedimientos de TI formalizados por la alta dirección y debidamente comunicados a las distintas áreas operativas de la estructura organizacional. Esto genera altos niveles de riesgos de TI e impacta sobre el ambiente de control en el ámbito de TI, provocando que el nivel de los servicios sea insuficiente para dar soporte a los objetivos estratégicos de la organización.*

A partir del análisis de la documentación provista por el auditado y de las entrevistas mantenidas con la Dirección de Administración, con el responsable del soporte informático del INADI y con diferentes referentes de las áreas operativas del Instituto, se constató que el organismo no cuenta con políticas, normas y procedimientos de TI debidamente formalizados y comunicados por las altas autoridades de la organización.

Para esta cuestión, las buenas prácticas de gobierno de TI indican que se deben definir políticas, normas y procedimientos que establezcan un ámbito de servicios formalizados por la alta dirección y debidamente comunicado a las áreas administrativas y operativas de la organización para garantizar un adecuado ambiente de control para TI. Este marco normativo en el contexto de TI debe estar alineado con la filosofía administrativa, con el estilo operativo y fundamentalmente con los objetivos estratégicos de la organización. (CobIT v4.1 – PO6: Comunicar las aspiraciones y la dirección de la gerencia.

La ausencia de políticas, normas y procedimientos aprobados por la alta dirección que establezcan formalmente cuáles deben ser las responsabilidades, y cuáles deben ser y cómo deben brindarse los servicios de TI que dan soporte a los procesos organizacionales, provocan que el ambiente de control de TI sea débil e informal, situación que además implica un alto nivel de riesgo en el gobierno de TI y trae como consecuencia que los servicios de TI resulten deficitarios e insatisfactorios en función de lo demandado por los procesos críticos que dan soporte a los objetivos estratégicos del organismo.

4.1.3. *La estructura organizacional de TI presentada por el INADI posee un diseño inadecuado e insuficiente para cumplir con eficiencia y eficacia las responsabilidades y funciones que le competen y que demanda la organización a partir de sus objetivos estratégicos.*

La evaluación de la documentación provista por el organismo para el caso –planillas de activos de TI, hoja *RRHH*- en la que se han analizado los perfiles, las funciones y las responsabilidades de cada uno de los integrantes del área de TI; y de las entrevistas mantenidas con la Dirección de Administración, con el responsable del soporte informático del INADI y con el administrador de la base de datos de denuncias por discriminación, permitieron a este equipo de auditoría constatar que la estructura organizacional del área de TI del INADI, al no estar formalizada y por lo tanto no tener establecidas oficialmente las misiones y funciones del área y sus integrantes, conduce a que el personal que se desempeña como soporte técnico, se encuentre frente a la necesidad de cumplir tareas de gestión de los sistemas y servicios de TI y de administración de bases de datos. Sin embargo, por formación y capacidades, la naturaleza del puesto informado a esta auditoría orienta a que este personal tenga capacidades de acción limitadas al soporte y mantenimiento de: i) entornos ofimáticos (informática de escritorio); ii) servidores de archivos y de telefonía; iii) correo electrónico; y iv) la red de área local del organismo.

Adicionalmente, se destaca que el administrador de la base de datos de denuncias no se encuentra dentro de la estructura operativa de TI, estando por fuera de ésta y prestando servicios desde la Dirección de Asistencia a la Víctima.

Esta situación permite aseverar que la estructura organizacional de TI existente en el INADI al momento de esta auditoría, no se encuentra formalizada y es inadecuada e insuficiente para poder dar respuesta a lo descrito en los hallazgos 4.1.1 y 4.1.2, y principalmente para acompañar con el soporte tecnológico que requieren los objetivos estratégicos de corto y mediano plazo del Instituto, entre ellos, implementar y mantener actualizado un sistema informático integrado para la registración unificada y simultánea de denuncias por discriminación a nivel nacional, ya sea que se reciban en la Sede Central o en las delegaciones del organismo en el interior del país; permitiendo la consulta pública y gratuita vía web del estado de trámite de las denuncias de la ciudadanía[45].

En esta materia, las buenas prácticas de gobierno de TI indican que: i) se debe definir un marco de trabajo para el proceso de TI para ejecutar el plan estratégico de TI. Este marco incluye una estructura organizacional adecuada para definir y llevar a cabo la ejecución del plan estratégico y que sea capaz de dar soporte a los objetivos del negocio; ii) se debe ubicar a la función de TI dentro de la estructura organizacional general con un modelo de negocios supeditado a la importancia de TI dentro de la organización, en especial en función de qué tan crítica es para la estrategia del negocio y el nivel de dependencia operativa sobre TI; y iii) se debe establecer una estructura organizacional de TI interna y externa que refleje las necesidades del negocio. Además, implementar un proceso para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos de personal y las estrategias internas para satisfacer los objetivos de negocio esperados y las circunstancias cambiantes. (CobIT v4.1 - PO4.1: Marco de Trabajo de Procesos de TI CobIT v4.1 - PO4.4: Ubicación Organizacional de la Función de TI, CobIT v4.1 - PO4.5: Estructura Organizacional)

[45] https://www.argentina.gob.ar/sites/default/files/mapa-de-riesgos-2018-spn.pdf

Que la estructura organizacional de TI de INADI sea inadecuada e insuficiente y sin estar formalizada oficialmente por el organismo para acompañar con eficiencia y eficacia el soporte tecnológico de las necesidades organizacionales, provoca considerables limitaciones operacionales, sobre todo en aquellas metas estratégicas en las cuales la tecnología de la información cumple un rol esencial para alcanzar su logro.

4.1.4. *El INADI no cuenta, para su plataforma tecnológica y para los servicios de soporte y mantenimiento continuo, brindados por el personal de soporte de TI, con una adecuada revisión del ambiente de control interno que garantice la detección temprana de riesgos de TI y las acciones pertinentes para gestionarlos.*

De la entrevista mantenida con la UAI del organismo y del análisis de la documentación provista en materia de informes de auditoría, se constató que no se realizaron auditorías internas de TI en el INADI durante el período auditado; este escenario evidencia la falta de un efectivo monitoreo del control interno sobre los procesos y procedimientos llevados a cabo por el área informática y por el responsable de la administración de la base de denuncias por discriminación para la prestación de los servicios de TI al Instituto, principalmente, sobre los procesos operativos del servicio de la Línea Telefónica 168 (Ex 0800), de denuncias y consultas por discriminación y de generación de estadísticas publicadas por el organismo.

En función de lo establecido en la Res. 87/22 - SIGEN - 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 - 11.2 -, 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 monitoreo del sistema de control interno de TI sobre la plataforma tecnológica y los servicios brindados por el área de informática del organismo, expone al INADI a riesgos no detectados y, por lo tanto, no mitigados.

4.2. Seguridad de la información

4.2.1. *El INADI no posee políticas de seguridad de la información aplicables transversalmente a toda la organización. Este escenario impacta sobre el adecuado cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información.*

Del estudio de la documentación técnica solicitada por este equipo de auditoría al organismo, se confirma que el INADI no posee un sistema de gestión de la seguridad de la información ya que no cuenta con políticas de seguridad de la información formalizadas que establezcan directrices, con alcance en todas las áreas de la organización, sobre cómo debe gestionarse la información garantizando su confidencialidad, integridad y disponibilidad. Esto coloca al organismo en una situación de alto nivel de riesgo y vulnerabilidad, más aún considerando que los procesos relacionados con las denuncias por discriminación, gestionan información sensible y de carácter reservado.

En función de lo que establecen las buenas prácticas en esta materia (ISO/IEC 27001, 27002 y CobIT v4.1 - DS11.6: Requerimientos de Seguridad para la Administración de Datos) es un deber estratégico de la organización disponer de políticas de seguridad de la información, y se deben definir e implementar con procedimientos que alcancen a todas las áreas, pudiendo identificar y atender todos los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos para conseguir los objetivos de negocio y cumpliendo con los requerimientos regulatorios pertinentes. Asimismo, el INADI, como uno de los organismos comprendidos en el inciso a) del artículo 8 de la Ley 24.156, debe desarrollar una política de seguridad de la información compatible con su responsabilidad primaria y las acciones de su competencia, sobre la base de una evaluación de los riesgos que pudieran afectarlo. Los términos de dicha política deben ser consistentes con las directrices de la DA 641/21 - DECAD-2021-641-APN-JGM - Requisitos mínimos de Seguridad de la Información para Organismos -.

Que el INADI no haya dictado e implementado políticas de seguridad de la información pone en riesgo la confidencialidad, integridad y disponibilidad de la información, instalando al organismo en un alto nivel de vulnerabilidad.

4.2.2. *El INADI no cuenta con un plan de seguridad de la información consistente, situación que conduce a un estado de vulnerabilidad sobre los procesos críticos de la organización y pone en riesgo la confidencialidad, integridad y disponibilidad de la información.*

La documentación solicitada por este equipo y entregada por el auditado permite aseverar que el INADI no tiene un plan de seguridad de la información implementado que conduzca a realizar un diagnóstico sobre el tratamiento que le da al manejo de la información y sobre los sistemas informáticos que utiliza, para detectar vulnerabilidades y posteriormente tomar las medidas de mitigación pertinentes.

En referencia a esta cuestión, las buenas prácticas (ISO/IEC 27001, 27002 y CobIT v4.1 - DS5.2: Plan de Seguridad de TI) indican que es clave para la organización trasladar los requerimientos del negocio, y los riesgos que se hayan ponderado dentro de un plan de seguridad de la información completo, teniendo en consideración la infraestructura de TI y los sistemas de información que dan soporte a los procesos críticos del negocio. Asegurando que el plan se encuentra implementado con procedimientos de calidad en materia de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Adicionalmente, es importante comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios de la organización.

Que no se cuente con un plan de seguridad de la información pone en riesgo la confidencialidad, integridad y disponibilidad de la información que gestiona el INADI, exponiendo al organismo a un estado de fragilidad ante esta situación.

4.2.3. *La gestión de usuarios aplicada por el organismo para acceder a la base de datos de denuncias por discriminación es inadecuada poniendo en riesgo la confidencialidad, integridad y disponibilidad de la información.*

A partir del estudio de la documentación técnica suministrada por el auditado, y de las entrevistas realizadas con el administrador de la base de datos de denuncias por discriminación, se constató que la gestión de usuarios utilizada por el INADI es inapropiada e insegura debido a que se permite que los usuarios autorizados accedan a la base de datos en forma directa para realizar ABM de datos, sin utilizar ningún sistema de accesos seguro a través de cuentas de usuarios que exijan la identificación personal, con la asignación de nombre de usuario y clave de acceso, y sin configurar el acceso a la información de la base de datos según las funciones asignadas para cada tipo de perfil (definición de roles y accesos a la información según cada rol).

Las buenas prácticas de gestión de usuarios (CobiT 4.1 - DS5.3: Administración de Identidad, CobiT 4.1 - DS5.4: Administración de Cuentas del Usuario y CobIT v4.1 -

PO7.3: Asignación de Roles), entre otros, establecen que se debe: i) asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de información (aplicación de negocio, entorno de TI, operación de sistemas, desarrollo y mantenimiento) deben ser identificables de manera única; ii) permitir que el usuario se identifique a través de mecanismos de autenticación confiables y seguros; iii) confirmar que los permisos de acceso del usuario al sistema y los datos están en línea con las necesidades del negocio definidas y documentadas y que los requerimientos de trabajo están adjuntos a las identidades del usuario; iv) asegurar que los derechos de acceso del usuario sean solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad; v) mantener las identidades del usuario y los derechos de acceso en un repositorio central; vi) garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de gestión de cuentas de usuario.

Que la gestión de usuarios para el acceso a la base de datos de denuncias aplicada por INADI sea inadecuada pone en riesgo la confidencialidad, integridad y disponibilidad de la información. La situación descrita permite aseverar que INADI no cumple con las normas básicas de gestión de usuarios generando un alto nivel de riesgo sobre la seguridad de la información de denuncias por discriminación, que tiene carácter de reservada y sensible.

4.2.4. *El personal de TI 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 denuncias, consultas y generación de estadísticas por discriminación, lo que 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.*

De las entrevistas mantenidas con personal del área de informática del Instituto y de la evaluación de la documentación técnica recibida, se constató que, durante el período auditado, no se han ejecutado 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 denuncias, consultas y generación de estadísticas por discriminación.

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 debe incluir, 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 INADI 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. Seguridad de la infraestructura de TI

4.3.1. *La sala de servidores que aloja a la infraestructura tecnológica que da soporte informático al INADI y la oficina donde se aloja el servidor de la base de datos de denuncias por discriminación no cumplen con las condiciones mínimas necesarias para resguardar la seguridad física de los servidores y sus datos, lo que pone en riesgo la continuidad de los servicios tecnológicos que sustentan los procesos críticos.*

Según las especificaciones básicas establecidas en las normas ISO 27001 "Sistemas de gestión de la seguridad de la información", CobiT 4.1 - DS12.1: Selección y Diseño del Centro de Datos, y en las ANSI/BICSI 002, "Mejores prácticas para el diseño y gestión de Data Centers", se debe realizar una gestión eficiente de los Centros de Procesamiento de Datos para garantizar la disponibilidad y confiabilidad de los servicios tecnológicos requeridos por los objetivos claves de una organización.

En las visitas realizadas a la sala de servidores donde se encuentran implementados los componentes de infraestructura tecnológica que dan soporte informático al INADI, y a la oficina que aloja al servidor de la base de datos de denuncias por discriminación, se verificaron, entre otras, las siguientes falencias: (ver Anexo IV, fotografías)

- El servidor de la base de datos de denuncias no debería estar en una oficina convencional sin una adecuada seguridad física y separado del resto de la infraestructura tecnológica;
- no cuentan con un sitio alternativo operativo para garantizar la continuidad de servicios ante la interrupción de los servicios del sitio principal;
- no cuentan con un sistema electrónico de control de acceso, sólo posen cerraduras de llaves convencionales;
- las paredes de la sala de servidores no se encuentran cubiertas por el encofrado correspondiente según Normas "IRAM 3691" (norma relativa de uso seguro de andamios y encofrados);
- no existe un procedimiento para controlar el acceso de los proveedores a la sala de servidores;
- no cuentan con piso técnico adecuado para el cableado eléctrico y de datos y para un adecuado sistema de refrigeración;
- no cuentan con un sistema de detección temprana de incendios, ni con un sistema de extinción adecuado para un CPD que aloja infraestructura tecnológica crítica;

- la puerta de acceso a la sala de servidores es una puerta convencional, no es una puerta cortafuego y no es del tipo *mantrap*[46];
- los cables de los servidores y de red no se encuentran bajo un esquema de conectividad normalizado y documentado como lo establecen las buenas prácticas relacionadas al cableado estructurado. Por el contrario, la conectividad de los servidores no es adecuada, ni cumple con las condiciones mínimas de buenas prácticas;
- no se encuentran definidos ni documentados los procedimientos relacionados a las rutinas de trabajo para la operación diaria en la sala de servidores;

Que el INADI no cuente con un CPD que cumpla con las normas elementales de seguridad requeridas para el diseño, implementación y gestión de un Data Center que aloja a la infraestructura tecnológica crítica de la organización, y mientras mantenga el escenario detectado y descrito por este equipo de auditoría, pone en un alto nivel de riesgo a la disponibilidad de la información, riesgo que pudo haberse materializado cuando, durante la ejecución de esta auditoría, durante el mes de junio de 2022, el organismo sufrió un hecho delictivo de público conocimiento[47], ocurrido fuera del horario de servicio y atención, en el cual fueron violentadas las puertas de algunas oficinas y de las cuales se hurtaron notebooks oficiales, verificando además que, entre las oficinas a las que accedieron, se encontraba la oficina que aloja al servidor de base de datos de denuncias por discriminación.

4.4. Continuidad de las Operaciones Organizacionales

[46] Los sistemas mantrap o portales de seguridad están diseñados para proteger áreas específicas dentro de un establecimiento mediante la verificación de ingreso de individuos e identificación de amenazas internas y externas. Se trata esencialmente de un pequeño cuarto o ambiente con dos puertas que limita el acceso a zonas seguras de personas no autorizadas y proporciona un medio eficaz para detener físicamente a sujetos sospechosos hasta que su identidad haya sido corroborada. Estos dispositivos son especialmente útiles para instalaciones que trabajan con información crítica o sensible y requieren un alto grado de seguridad, monitoreo y control de acceso

[47] https://www.telam.com.ar/notas/202206/596443-inadi-denuncia-robo-equipos-sede-central-caba.html

4.4.1. *El personal de TI, 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 formalizado y debidamente comunicado. Este escenario 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 INADI tienen una alta dependencia.*

A partir del análisis realizado sobre la documentación técnica provista por el auditado, y de las entrevistas mantenidas con el responsable del área de informática y con el administrador de la base de datos de denuncias por discriminación, se verificó que no se cuenta con un plan de recuperación ante desastres que asegure la continuidad de los servicios de TI que dan soporte al INADI.

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).

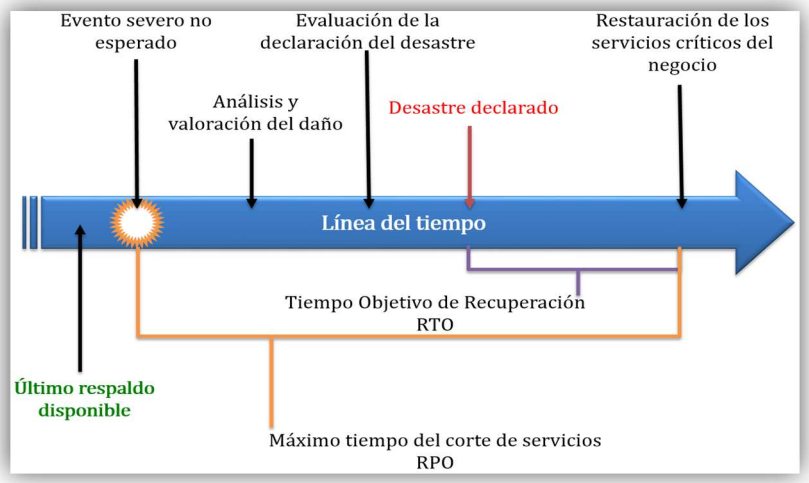
Según las mejores prácticas anteriormente indicadas, un DRP debe contener, desarrollar y ejecutar como mínimo los siguientes pasos:

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 INADI y sobre los sistemas de información que constituyen el soporte informático a los servicios que éste presta.

Ilustración Nº11 – Etapas de un DRP



Fuente: elaboración propia en base a ISO 24.762

Que el personal de TI, a cargo de la gestión y administración de la infraestructura tecnológica del organismo, no cuente con un Plan de Recuperación ante Desastres alineado con un Plan de Continuidad del Negocio, con el cual el Instituto debería contar según los requerimientos organizacionales en situación de contingencia y acorde a lo que establecen las buenas prácticas y su correspondiente plan de pruebas, documentación de simulacros y

ajustes continuos, pone en riesgo la disponibilidad de las aplicaciones y de la información crítica de la organización.

4.4.2. *El personal de TI del INADI 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 del soporte de TI y con el administrador de la base de datos de denuncias por discriminación, 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*; los criterios de resguardo de información son establecidos por los responsables técnicos de turno; ii) no se cuenta con herramientas especializadas en la materia que gestionen los *backups* y las restauraciones de la información con procesos automáticos que aseguren su eficiencia y que documenten los hitos de ejecución y sus resultados, sino que las copias son realizadas por los operadores en forma manual; iii) los períodos establecidos por los responsables técnicos para la realización de las copias de seguridad son mensuales, generando una brecha inaceptable de pérdida de información por parte del organismo ante la necesidad de ejecutar una restauración de la última copia; iv) no se realizan guardas externas de las copias de resguardo; y v)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 *backups* 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 *backup* 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, entre otros, la disponibilidad de dicha información ante un incidente que requiera aplicar una restauración

4.5. Operaciones de TI

4.5.1. *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 soporte e información. Esta situación impide a la organización contar con herramientas que permitan medir el desempeño de los servicios de TI y los tiempos de respuesta para resolver incidencias y problemas en el ámbito de TI.*

De la verificación de los procesos, la documentación provista por el auditado y de las entrevistas mantenidas con los responsables del área de soporte informático y con diversos usuarios que reciben soporte sobre los servicios de TI del organismo, se constató que no existe dentro del INADI, una mesa de ayuda establecida para la gestión de problemas e incidentes. El manejo de los mismos se realiza de manera informal y no cuentan con procedimientos formalizados, ni con herramientas especializadas en la gestión de centros

de atención a los usuarios. Los incidentes se reportan a través de correos electrónicos, llamadas telefónicas y mensajes mediante la aplicación de mensajería "*Whatsapp*"[48]. La resolución de los incidentes se realiza, dependiendo el caso, por alguna de las vías de comunicaciones anteriormente mencionadas o con el uso de la herramienta "*TeamViewer*"[49], para brindar soporte a las computadoras de las delegaciones desde la Sede Central.

Por otro lado, en la Sede central de INADI, donde desarrollan sus funciones los responsables del soporte informático, se responden a problemas e incidentes del total las sedes de INADI. Y en función del alcance de cobertura establecido, se verificó que no existen en el Instituto acuerdos de nivel de servicio (SLA, siglas del inglés, *Service Level Agreement*) establecidos que especifiquen los tiempos de respuesta comprometidos para la resolución de los incidentes. Asimismo, no se utiliza un sistema para gestionar el seguimiento de incidentes, por ejemplo, a través de tickets de consulta, lo cual hace imposible la trazabilidad segura de los reportes y su resolución.

Por todo lo dicho, se puede aseverar que el INADI no cuenta con un marco metodológico que permita: i) administrar eficientemente las prioridades de atención; ii) el escalamiento de problemas; y iii) la medición de satisfacción del usuario final con respecto a los servicios de mesa de ayuda. Además, al no existir un sistema de registros, queda imposibilitada la posibilidad de analizar eficientemente los datos de los incidentes y problemas a fin de determinar establecer un esquema de mejora continua del servicio.

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,

[48] *WhatsApp Messenger* es una aplicación de mensajería instantánea utilizada en teléfonos móvil.
[49] *TeamViewer* es una herramienta informática que se utiliza para acceder en forma remota para tomar control de uso de una computadora u otros dispositivos tecnológicos. Utilizado generalmente con fines de soporte para resolver problemas o incidencias en los equipos de usuarios finales.

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 no existencia de una mesa de servicios y/o ayuda con un marco metodológico eficiente y ajustado a las necesidades de servicio que demanda la organización, priva al organismo de reportes en esta materia, que permitan a las autoridades del Instituto medir el desempeño del servicio y los tiempos de respuesta, así como también, para identificar tendencias de problemas recurrentes, de forma tal que el servicio pueda encontrarse en mejora continua.

4.5.2. *La Coordinación de Recepción y Evaluación de Denuncias, dependiente de la Dirección de Asistencia a la Víctima, no realiza monitoreos sobre el servicio de conectividad utilizado por la línea 168 (Ex 0800) entregado por el proveedor a cargo de la prestación. Esta situación imposibilita medir adecuadamente el cumplimiento de los niveles de servicio acordados y establecer un plan de mejora continua, alineado a las necesidades y prioridades de la organización.*

Del análisis de la documentación técnica solicitada al auditado, del relevamiento *in-situ* efectuado por el equipo de auditoría en el Call Center de INADI, y de las entrevistas mantenidas con los responsables del área de informática, con la responsable de la Coordinación de Recepción (Call Center del servicio de la Línea Telefónica 168 (Ex 0800)), y con la Dirección de Asistencia a la Víctima, se pudo verificar que estas áreas referentes y responsables de la gestión del servicio dentro del organismo, no cuentan con un marco metodológico de trabajo que brinde un proceso formal de gestión y medición de los niveles de servicio acordados con el proveedor prestador de los mismos (empresa

GRADICOM S.A.)[50]. A su vez, pudo constatarse que no se realizan tareas de monitoreo sobre el servicio de telefonía IP, aplicación web, disponibilidad de la infraestructura tecnológica de la base de datos, entornos tecnológicos brindados por el proveedor.

Por último, en el relevamiento llevado a cabo por este equipo de auditoría se detectó que la Coordinación de Recepción y Evaluación de Denuncias, utiliza una planilla de cálculo para registrar los casos de incidentes que surgen con el servicio prestado por la empresa proveedora, los cuales se informan por correo electrónico a la empresa.

Las buenas prácticas sobre este tema, entre otras cuestiones, indican que: i) se debe 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 debe mantener una alineación continua con los requerimientos y las prioridades de negocio y facilitar el entendimiento común entre el cliente y el(los) prestador(es) de servicio; ii) se deben establecer y acordar convenios de niveles de servicio para todos los procesos críticos de TI con base en los requerimientos del negocio y las capacidades en TI; iii) se deben monitorear continuamente los criterios de desempeño especificados para el nivel de servicio. Los reportes sobre el cumplimiento de los niveles de servicio deben emitirse en un formato que sea entendible para los interesados. Las estadísticas de monitoreo deben ser analizadas con el fin de identificar tendencias positivas y negativas de los servicios brindados; y iv) es necesario 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 base a los requerimientos del negocio. (CobIT v4.1 - DS1.1: Marco de Trabajo de la Administración de los Niveles de Servicio, CobIT v4.1 DS1.2: Definición de Servicios, CobIT v4.1 - DS1.3: Acuerdos de Niveles de Servicio, CobIT v4.1 - DS1.5: Monitoreo y Reporte del Cumplimento de los Niveles de Servicio y CobIT v4.1 - DS1.6: Revisión de los Acuerdos de Niveles de Servicio y de los Contratos)

[50] Empresa que brinda soluciones tecnológicas (http://www.gradicom.com/)

El escenario descrito, limita monitorear y medir eficientemente los servicios de TI brindados por el proveedor en función de los niveles de servicios acordados y del nivel de satisfacción que requieran los usuarios y la organización. Asimismo, imposibilita consolidar un plan de mejora continua que esté alineado con las prioridades y los objetivos estratégicos del organismo

4.6. Adquisiciones y contratación de TI

4.6.1. *La Dirección de Asistencia a la Víctima y la Coordinación de Recepción y Evaluación de Denuncias, no realizan un control sobre el nivel de servicio establecido en el contrato por el servicio de la Línea Telefónica 168 (Ex 0800). Esto impide que las áreas usuarias puedan gestionar, controlar y medir adecuadamente la calidad de la prestación brindada por el proveedor.*

A partir de la evaluación de la información técnica, y de las entrevistas mantenidas con la Dirección de Asistencia a la Víctima y con la responsable de la Coordinación de Recepción y Evaluación de Denuncias, se verificó que, si bien se registran y se reclaman al proveedor las anomalías que se presenten con el servicio de la línea de atención telefónica 168 (Ex 0800), las áreas usuarias de este servicio, además de lo expuesto en el hallazgo 4.5.2., no realizan un control del SLA (siglas en inglés: *Service Level Agreement*, traducido como Acuerdo de Nivel de Servicio), que debe cumplir el proveedor del servicio según lo comprometido en el contrato analizado por este equipo de auditoria. Esto impide gestionar eficientemente la prestación brindada por el proveedor, pues al no monitorear el SLA, por ejemplo, no se aplican las penalidades establecidas por contrato cuando corresponda por incumplimiento de los niveles de servicios comprometidos.

Las buenas prácticas en gestión de proveedores de TI establecen que: i) se debe definir y acordar convenios de niveles de servicio para todos los procesos críticos de TI con base en los requerimientos del cliente y las capacidades en TI. Esto incluye los compromisos del cliente, los requerimientos de soporte para el servicio, métricas cualitativas y cuantitativas

para la medición del servicio firmado por los interesados, en caso de aplicar, los arreglos comerciales y de financiamiento, y los roles y responsabilidades, incluyendo la revisión del SLA. Los puntos a considerar son disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte, planeación de continuidad, seguridad y restricciones de demanda (CobIT v4.1 - DS1.3: Acuerdos de niveles de servicio); y ii) se debe monitorear continuamente los criterios de desempeño especificados para el nivel de servicio. Los reportes sobre el cumplimiento de los niveles de servicio deben emitirse en un formato que sea entendible para los interesados. Las estadísticas de monitoreo son analizadas para identificar tendencias positivas y negativas tanto de servicios individuales como de los servicios en conjunto (CobIT v4.1 - DS1.5: Monitoreo y reporte del cumplimento de los niveles de servicio).

La falta de un monitoreo y control del SLA imposibilita evaluar con objetividad y eficiencia el rendimiento y cumplimiento del servicio prestado por el proveedor y hacer valer lo comprometido en el contrato.

4.7. Sistemas de información

4.7.1. *Los sistemas de información y procesos aplicados por el INADI para el tratamiento de denuncias y consultas por discriminación, racismo y xenofobia, no se encuentran suficientemente integrados. La ausencia de procesos automáticos e integrados para el tratamiento de la información, pone en riesgo su integridad al momento de ser recibida y posteriormente al momento de su procesamiento.*

Del estudio de la documentación entregada por el auditado y de las entrevistas mantenidas con la Dirección de Asistencia a la Víctima, con el administrador de la base de datos de denuncias, con la Coordinación de Recepción y Evaluación de Denuncias y con usuarios intervinientes en los procesos de denuncias, este equipo de auditoría verificó que para el proceso de recepción de denuncias y consultas, no se ha definido un modelo de arquitectura de la información gestionado a través de un sistema integrado que les dé soporte con el

objetivo de asegurar que los datos se encuentren organizados eficientemente y de manera homogénea, y que garantice además que las bases de datos se encuentren en alta disponibilidad para su acceso y que los usuarios intervinientes accedan al sistema mediante un protocolo de identificación y autenticación unívoca (con identificador y clave de acceso).

Para el caso del proceso de recepción de denuncias, se constató que: i) el proceso de recopilación de datos se realiza mediante el soporte de herramientas ofimáticas, las cuales carecen de controles automáticos, supliendo esta carencia con controles manuales que no se encuentran formalizados, y son implementados por el mismo personal de DAVIC; ii) el aplicativo utilizado como motor de la base de datos de denuncias es *MS- Access*, Versión 2013[51], el cual al momento de esta auditoría no se encontraba licenciado[52].

En cuanto al proceso para recepción de consultas, el organismo opera y accede a una base de datos que se encuentra tercerizada, bajo un sistema desarrollado por la empresa Gradicom S.A. que requiere el licenciamiento de usuarios para su operación e ingreso de datos sobre la misma. El INADI solo ha licenciado la cantidad de usuarios que trabajan sobre las consultas recibidas en la Sede Central, motivo por el cual las delegaciones no tienen acceso a la carga de datos sobre este entorno tecnológico, lo que genera que éstas deban enviar mensualmente por correo electrónico las planillas de cálculo conteniendo las consultas recibidas localmente. Además, el proceso de recepción de datos aplicado por la DAVIC para las delegaciones, no cuenta con procedimientos documentados y formalizados para cada uno de los subprocesos involucrados, como ser: i) para el envío de las planillas por parte de las delegaciones; ii) para la guarda de esta información, tanto en correos

[51] Microsoft Access es un sistema de gestión de bases de datos incluido en las ediciones profesionales de la suite Microsoft Office. Es un gestor de datos que utiliza los conceptos de bases de datos relacionales y pueden manejarse por medio de consultas e informes.

[52] Las licencias de software son los permisos que un fabricante o desarrollador proporciona para la distribución, uso y/o modificación del software. Las licencias pueden estar limitadas a periodos de tiempo, variar según el territorio donde se aplica, ya que, entre otros, las licencias deben cumplir con las leyes locales. Por otro lado, las licencias de software conllevan un contrato de uso en el cual el usuario adquiere derechos de uso aceptando los términos y condiciones del fabricante o los que acuerden entre ambas partes, entre ellas, las condiciones de actualización y soporte que ofrecerá el fabricante.

electrónicos como en carpetas de red compartidas; ni iii) para la gestión de la información de consultas recibida desde las delegaciones.

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: Administración de Integridad). 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: Modelo de Arquitectura de Información Empresarial).

Además, 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 (pública, confidencial, secreta). Este esquema debe incluir 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 : Esquema de Clasificación de Datos).

Por último, es oportuno destacar que las directrices establecidas en la Res. 87/22-SIGEN (art. 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 pudo observar que la ausencia de sistemas integrados obstaculiza la estandarización de procesos y la eliminación de procesos manuales como, por ejemplo, las planillas de cálculo que mensualmente envían las delegaciones por correo electrónico con las consultas recibidas, poniendo en riesgo la confiablidad, integridad y disponibilidad de la información sensible y de carácter reservada que estas contienen. Además, las herramientas ofimáticas utilizadas en estos procesos manuales carecen de trazabilidad y auditabilidad, afectando la confiabilidad, integridad y el control de los datos procesados.

En este sentido, el organismo se encuentra expuesto al riesgo de no poder salvaguardar de manera óptima y oportuna la información sensible que gestiona.

Adicionalmente es importante resaltar que el uso de software sin licencia pone en riesgo la disponibilidad de información y es violatoria de las leyes de propiedad intelectual[53]. Esta situación presenta el riesgo de que, en caso de prescindir del uso del software sin licencia, el proceso de creación de la base y todo reporte que dependa de dicho software no pueda realizarse oportunamente hasta tanto se regularice su situación licenciataria. Además, la situación hace pasible al organismo de posibles demandas por el uso de software ilegal

4.7.2. *La falta de procedimientos formalizados y estandarizados con procesos de control automáticos e integrados para asegurar un eficiente y seguro tratamiento de la información que garanticen la integridad y consistencia de los datos almacenados y su recopilación, impacta contra la confiabilidad de la información que se utiliza para la*

[53] La legislación argentina ha incluido al software dentro de la tutela de la Ley de Propiedad Intelectual Nº 11.723 y la utilización de sistemas sin licencia constituye delito penal y atribuye responsabilidad civil por daños y perjuicios

elaboración del "Mapa Nacional de la Discriminación" y de los informes estadísticos publicados por el INADI sobre la discriminación, racismo y xenofobia.

Mediante entrevistas con la CIOD (responsable y el equipo técnico de trabajo), se ha podido constatar que: i) la Coordinación de Investigación y Observatorios sobre Discriminación no cuenta con una aplicación que permita ejecutar procesos automáticos e integrados para recibir la información de las universidades, procesar la información y consolidar la base de datos del "Mapa Nacional de la Discriminación"; ii) los procesos manuales aplicados y descriptos en el punto "3.3. Descripción de los procesos sujetos al análisis de esta auditoría", presentan las siguientes falencias: ii.i) no se encuentran documentadas y formalizadas las funciones y responsabilidades de quienes realizan el control de calidad sobre la información; ii.ii) no existe una adecuada segregación de funciones y controles por oposición formalmente establecidos; ii.iii) el proceso de control de calidad no cuenta con un manual de procedimientos; y ii.iv) las autoridades del INADI no han realizado, hasta el momento de las tareas de campo, un relevamiento dentro de la Coordinación de Investigación y Observatorios sobre Discriminación, a fin de detectar las necesidades informáticas con el objetivo de implementar herramientas tecnológicas que contribuyan a la sistematización y aseguramiento de la integridad de la información procesada sobre los procesos implementados al momento de esta auditoria; iii) no existen procesos automatizados para recabar, controlar y procesar la información estadística, la digitalización y procesamiento de los datos. El proceso de recopilación de datos se realiza con soporte de herramienta ofimáticas carentes de controles automáticos, aplicando en su lugar controles manuales implementados por el propio personal de la Coordinación; iv) no está contemplada la digitalización y envío de originales por parte de las universidades hacia el INADI, y solo en algunos casos se reciben los originales en papel; v) no se han firmado acuerdos de confidencialidad con las universidades; vi) las universidades envían los archivos "matriz de carga" (de tipo .xls) por correo electrónico sin ninguna medida de protección que garantice confidencialidad e integridad de la información; y vii) los archivos y las bases resultantes (en .xls) de los mismos, se guardan en una unidad de red, con características de nube pública (Google drive), escenario que no permite al organismo,

gestionar la gobernanza de la seguridad de la información, poniendo en riesgo la confidencialidad, la disponibilidad y la integridad de información crítica y sensible, al ser administrada en este tipo de entorno tecnológico, y sin contar con un procedimiento formalizado para tal administración.

Asimismo, pudo detectarse que la Coordinación de Investigación y Observatorios sobre Discriminación, no guarda la información generada en los servidores del INADI, y el organismo no brinda soporte de infraestructura tecnológica para el mantenimiento de estas bases de datos generadas en este proceso.

Por último, se verificó que el aplicativo utilizado como parte del procesamiento de la base de datos para la generación de estadísticas y para la creación del "Mapa Nacional de la Discriminación", "SPSS", no se halló en el inventario de aplicativos entregado a requerimiento de esta auditoría, constatándose que dicho software no se encuentra oficialmente licenciado por el INADI.

Las buenas prácticas exponen que: i) se debe administrar la integridad de la información definiendo e implementando procedimientos 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: Administración de integridad); ii) se deben implementar controles de negocio, cuando aplique, en controles de aplicación automatizados tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable (CobIT v4.1. - AI2.3: Control y Posibilidad de Auditar las Aplicaciones); iii) las Transacciones de datos sensibles se intercambien solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen (CobIT v4.1. – DS5.11: Intercambio de Datos Sensitivos); iv) se deben definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos para conseguir los objetivos de negocio, las políticas de seguridad de la organización y requerimientos regulatorios. (CobIT v4.1. – DS11.6:

Requerimientos de Seguridad para la Administración de Datos); y v) para mitigar los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de entrega de forma segura y eficiente sobre una base de continuidad se debe considerar, además, acuerdos de confidencialidad, contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos, etc. (CobIT v4.1. DS2.3: Administración de Riesgos del Proveedor)

En base a lo expuesto es pertinente observar que: i) la falta de procesos automatizados e integrados colisiona contra el objetivo de aplicar normas y procedimientos uniformes para la recepción de la información y el procesamiento de los datos estadísticos. Asimismo, la carencia de dichos procesos no satisface los criterios de integridad, eficiencia y efectividad; ii) la ausencia de procesos de control automáticos e integrados para el tratamiento de la información (ingreso, procesamiento y salida) pone en riesgo la integridad de la información al momento de que ésta es recibida y posteriormente procesada; iii) existe el riesgo inherente al proceso, de que la información contenida en los archivos enviados por las universidades y las bases resultantes puedan ser modificadas y/o alteradas por personal de la Coordinación, o cualquier persona ajena al sector que tenga acceso a la carpeta compartida de Google Drive donde residen los archivos originales, y no queden registros de tales alteraciones o eventuales filtraciones de datos; iv) el uso de software, programas o aplicativos sin licencia pone en riesgo la disponibilidad de la información y es violatoria de las leyes de propiedad intelectual, esta situación presenta el riesgo de que, en caso de prescindir del uso del software sin licencia, el proceso de creación del Mapa y todo reporte estadístico que dependa de dicho software no pueda realizarse oportunamente hasta tanto se regularice su situación licenciataria. Además, la situación hace pasible al organismo de posibles demandas por el uso de software ilegal.

Atento lo expuesto, se concluye que la falta de integración entre las fuentes de información y los mecanismos para su ingreso, procesamiento y salida, no permiten garantizar su integridad, y por lo tanto existe un alto nivel de riesgo sobre la confiabilidad de la base de

datos nacional utilizada para la publicación de las estadísticas oficiales y para la confección del "Mapa Nacional de la Discriminación".

Por último, y en vinculación con los ODS, es importante destacar que el ODS 10 (Reducción de las desigualdades) en su meta 10.3 (Garantizar la igualdad de oportunidades y reducir la desigualdad de resultados, incluso eliminando las leyes, políticas y prácticas discriminatorias y promoviendo legislaciones, políticas y medidas adecuadas a ese respecto) que es uno de los ODS que presenta periódicamente el INADI, utiliza como fuente, del indicador 10.3.1. (Porcentaje de la población que declara haberse sentido personalmente víctima de discriminación), al "Mapa Nacional de la Discriminación", trasladando los riesgos citados precedentemente a dicho indicador.

4.7.3. *No se cuenta con políticas y procedimientos formalizados para la administración de la base de datos de denuncias por discriminación, racismo y xenofobia que puedan garantizar la seguridad lógica y la confidencialidad de la información.*

Del estudio de la documentación técnica recibida y de las entrevistas mantenidas con el administrador de la base de datos de denuncias por discriminación, racismo y xenofobia, se verificó que no existen políticas y procedimientos formalizados institucionalmente para la administración de la base de datos que almacena y gestiona información de carácter sensible y reservada, que incluya además las pautas y lineamientos establecidos en la Ley 25.326, de Protección de Datos Personales. A su vez, durante las labores de auditoria,-se constató que: i) los usuarios habilitados acceden a la base de datos sin ejecutar una autenticación previa (usuario y contraseña), lo que imposibilita delimitar y establecer responsabilidades y funciones sobre las actividades que ejecuta cada usuario dentro de la base de datos; ii) no existen reportes de monitoreos periódicos sobre la base de datos y sobre el servidor que la soporta que emitan resultados sobre las actividades ejecutadas; iii)

no existe un *log*[54] activo que genere pistas de las acciones ejecutadas por los usuarios y las del propio administrador de la base de datos que permita realizar auditorías sobre los eventos registrados en la base de datos; iv) en línea con lo observado en el hallazgo 4.4.2, no existen políticas y procedimientos formalizados para las tareas de resguardos y recuperaciones de la base de datos (plan de contingencia sobre los datos); y v) el motor de base de datos utilizado por el organismo – *MS-Access,* Versión 2013 – dadas las características, es una herramienta muy básica para el almacenamiento y explotación de la información que además presenta considerables limitaciones en cuanto al volumen de almacenamiento, a la cantidad de usuarios con acceso simultáneo, a la capacidad de procesamiento de la información, y principalmente en el aspecto de seguridad. Esto deja de manifiesto, que no es el motor de base de datos más adecuado y confiable para el INADI para el tratamiento de información corporativa de carácter crítico, como son las denuncias por discriminación, racismo y xenofobia, información sobre la cual se generan informes estadísticos que luego el Instituto utiliza para la toma de decisiones y el establecimiento de acciones estatales en cuestiones de discriminación.

Las buenas prácticas sobre el seguimiento y control en la gestión de operaciones, establecen que: i) para detectar las actividades no autorizadas de procesamiento de información es recomendable que los sistemas se monitoreen y controlen para asegurar que los usuarios realicen solamente las actividades para las cuales fueron autorizados explícitamente (ISO 27.002 - 10.10 Seguimiento y control); ii) se produzcan y mantengan pistas de auditoría en las cuales se registren las actividades, excepciones y eventos de seguridad de la información de los usuarios, por un período acordado para ayudar en futuras investigaciones y en el seguimiento del control de acceso. En todos los sistemas, sean automatizados o no, las pistas de auditoría deben estar siempre presentes, y deben cumplir el requisito básico de que cualquier transacción generada automáticamente, pueda ser

[54] En informática, se usa el término log, historial de log o registro, que se refiere 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.

rastreada hasta el evento o condición que la generó (ISO 27.002 - 10.10.1 Registro de auditoría); iii) que la información de registro esté protegida contra la manipulación y procesos no autorizados (ISO 27.002 - 10.10.3 Protección de la información de los registros de actividad); y iv) realizar una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en la organización causado por vulnerabilidades o incidentes de seguridad (CobIT v4.1 - DS5: Garantizar la seguridad de los sistemas).

La falta de políticas y procedimientos formales para la administración de la base de datos de denuncias por discriminación, racismo y xenofobia y el uso de un motor de base de datos que presenta evidentes limitaciones para su aplicación en un ambiente corporativo, ponen en riesgo la confidencialidad, integridad y disponibilidad de la información, que además, y en cumplimiento de la Ley 25.326[55] de Protección de Datos Personales y de la Resolución 40/2018-AAIP[56] Política de Protección de Datos Personales para Organismos Públicos, tiene carácter de sensible y reservada.

4.7.4. *El INADI, a través de Dirección de Asistencia a la Víctima, no ha formalizado la firma de un acuerdo de confidencialidad con cada uno de los empleados que gestionan y/o tienen acceso a información sensible y reservada, generada por las denuncias de discriminación, xenofobia y racismo que le asegure al organismo la no divulgación interna y/o externa de dicha información.*

De las entrevistas mantenidas con la Dirección de Asistencia a la Víctima, se constató que el INADI no ha puesto en práctica la firma de un acuerdo de confidencialidad con cada uno de los empleados que por sus funciones y responsabilidades gestionan y/o tienen acceso a información sensible y reservada generada por las denuncias de discriminación, xenofobia y racismo, que permita establecer un marco legal de no divulgación de este tipo de información.

[55] http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm
[56] https://www.argentina.gob.ar/aaip/datospersonales/politica-modelo-organismos-publicos

Las mejores prácticas relacionadas con la gestión de la seguridad de información organizacional, en relación al acceso e intercambio de información reservada, sugieren la firma de acuerdos de confidencialidad corporativos entre el empleador y sus empleados y entre el prestador del servicio y sus clientes (Serie ISO 27.000). Asimismo, la DA 641/21 establece que se deben: i) incorporar acuerdos y cláusulas de confidencialidad y no divulgación según las necesidades del organismo en todos los acuerdos que se suscriban; y ii) incorporar acuerdos y cláusulas de confidencialidad y no divulgación cuando el organismo entienda que resulta conveniente para el tipo de información que trate.

La ausencia de estos acuerdos no brinda garantías de confidencialidad y de no divulgación de información que tiene carácter sensible y reservado.

5. ANÁLISIS DE LA VISTA

Por Nota Nº 124/23-GPyPE, la AGN remite el día 16 de Mayo del corriente, el proyecto de Informe de auditoría sujeto a discusión sobre *"Gestión de TI Sistemas de información – Registro de denuncias, Línea Telefónica 168 (Ex 0800) y sistemas y procesos relacionados*", en el Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo (INADI), otorgándole como tiempo máximo de respuesta un plazo de 15 (quince) días corridos de recibida la presente.

El día 31 de Mayo de 2023, a través de un correo electrónico institucional, enviado por la Interventora del INADI, Dra. Greta Penna, al Sr. Gerente de Planificación y Proyectos Especiales, fue solicitada una prórroga de tres (3) días para dar respuesta a la vista de dicho Informe. En virtud de ello, la Gerencia responde el mismo día y por la misma vía otorgando el requerimiento de la prórroga favorablemente. Por Nota Nº NO-2023-64799193-APN-DADM#INADI, fechada el 6 de Junio de 2023 (reproducida en el Anexo I), el día 7 de Junio de 2023, el INADI remite el documento electrónico conteniendo el descargo de la vista del Informe en cuestión.

Luego de dar acabada lectura al documento que contenía la formulación de las respuestas propinadas por parte del organismo auditado, se concluyó que no hubo formulación de comentarios que ameriten análisis, dado que en pasajes de la lectura y en el acápite final de su contestación, el INADI reafirma los hallazgos identificados, así como las Recomendaciones provistas por la AGN, refiriendo a lo siguiente: […] *"Se aceptan, pues, todas las observaciones formuladas por el Órgano Auditor, en la inteligencia de que el diagnostico efectuado resulta concordante con el de esta Dirección"* […] *"Las citadas conclusiones, se reitera, resultan convergentes con las del Informe de Auditoria".* (véase Anexo I).

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. Definir, elaborar, aprobar e implementar un plan estratégico de TI alineado con las metas estratégicas del INADI que permita obtener mecanismos de soporte tecnológico eficientes, eficaces y económicamente adecuados sobre los procesos críticos de los servicios que brinda el organismo, contribuyendo además en su mejora continua.

6.1.2. Elaborar, aprobar, implementar y comunicar a toda la organización las políticas, normas y procedimientos debidamente alineados a los objetivos estratégicos del organismo y al plan estratégico de TI que formalicen servicios de TI eficientes y eficaces.

6.1.3. Establecer una estructura organizacional de TI que refleje las necesidades operativas y estratégicas del organismo. Implementar un proceso para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos del personal y las

estrategias internas para satisfacer los objetivos estratégicos esperados por la organización, y que sea capaz de adaptarse a las circunstancias cambiantes que se vayan presentando.

6.1.4. 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. Dictar, implementar y comunicar a todas las áreas del Instituto las políticas de seguridad de la información que permitan garantizar un eficiente y eficaz sistema institucional de gestión de la seguridad de la información.

6.2.2. Diseñar, implementar y comunicar a toda la organización un plan de seguridad de la información consistente, eficiente y eficaz que permita gestionar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información sensible y reservada que gestiona el Instituto.

6.2.3. Poner en marcha un sistema de gestión de usuarios adecuado y seguro que permita que todos los usuarios que tengan acceso autorizado a la base de datos de denuncias por discriminación sean identificables de manera única y con perfiles y funciones por perfil definidos. Y que además garantice la posibilidad de auditar las actividades que ejecutan los usuarios dentro de la base de datos.

6.2.4. 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 denuncias, consultas y generación de estadísticas por discriminación, 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 proactiva y recurrente para mantener el nivel de seguridad requerido por la organización.

6.3. Seguridad de la infraestructura de TI

6.3.1. Readecuar los espacios físicos e implementar las medidas de seguridad que correspondan para garantizar el óptimo funcionamiento del Centro de Procesamiento de Datos, a fin de llevar a cabo una correcta administración y resguardo de los sistemas de información y de las bases de datos que brindan servicio a los procesos críticos del INADI.

6.4. Continuidad de las operaciones organizacionales

6.4.1. Desarrollar, probar y mantener en forma continua un Plan de Recuperación ante Desastres, alineado a un Plan de Continuidad del Negocio (BCP por sus siglas en inglés, *Business Continuity Plan*), aprobado formalmente por un 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 de información y de la información de acuerdo a los requerimientos operativos y administrativos del INADI.

6.4.2. 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. Adquirir e implementar una herramienta especializada en la ejecución de copias de respaldo y de restauración que asegure la eficiencia, el éxito y la documentación de los respaldos externos de la información crítica del organismo.

6.5. Operaciones de TI

6.5.1. Implementar una mesa de ayuda con sus correspondientes procedimientos formalizados, con el objetivo de generar las herramientas necesarias para el tratamiento eficiente de incidentes y problemas, permitiendo además la medición y evaluación de los servicios TI y su mejora continua.

6.5.2. Establecer un marco formal de administración y monitoreo de los niveles de servicios acordados con el/los proveedores de TI, en especial con el prestador de la línea 168 (Ex 0800), con el objetivo de que el INADI se asegure un servicio eficiente y que cuente con los elementos técnicos y legales necesarios para exigirle a los proveedores los ajustes y las mejoras necesarias de las prestaciones que brindan en función de las necesidades estratégicas del organismo.

6.6. Adquisiciones y contratación de TI

6.6.1. Controlar y monitorear continuamente los criterios de desempeño del proveedor del servicio de la Línea Telefónica 168 (Ex 0800) en función de lo establecido en el contrato para el nivel de servicio comprometido.

6.7. Sistemas de información

6.7.1. Respecto a los procesos de denuncias y consultas por discriminación, racismo y xenofobia:

- Adquirir o desarrollar, implementar y mantener sistemas de información integrados que les den soporte. Adquirir y mantener la infraestructura tecnológica que requieran estos sistemas.
- Facilitar eficientemente la operación y el uso de los aplicativos a los usuarios finales con adecuadas medidas de seguridad para el acceso de los mismos.

- Implementar controles automatizados en las aplicaciones tal que se garantice el procesamiento de la información de manera exacta, completa, oportuna, autorizada y auditable.
- Actualizar el inventario de aplicaciones existente en el INADI y regularizar la situación en el caso de uso de software no licenciado.

6.7.2. Respecto a la elaboración del "Mapa Nacional de la Discriminación" y de los informes estadísticos publicados por el INADI sobre la discriminación, racismo y xenofobia:

- Confeccionar, aprobar por la máxima autoridad competente del INADI e implementar procedimientos para la administración de las bases de datos estadísticas dentro del marco de las políticas de seguridad de la información que dicte el organismo.
- Establecer políticas y procedimientos formalizados para el intercambio de datos claves y sensibles (secretos y confidenciales) que garanticen la autenticidad e integridad del contenido y el no repudio del origen.
- Celebrar acuerdos de confidencialidad con las universidades y con otros terceros que intervengan en los procesos de toma y procesamiento de datos referidos a la confección del "Mapa Nacional de la Discriminación" y otros informes estadísticos publicados por el INADI.
- Implementar controles automatizados en las aplicaciones tal que se garantice el procesamiento de la información de manera exacta, completa, oportuna, autorizada y auditable.
- Actualizar el inventario de aplicaciones existente en INADI, y regularizar la situación en caso de uso de software no licenciado.

6.7.3 Elaborar, aprobar, implementar y comunicar las políticas y procedimientos para la administración de la base de datos de denuncias por discriminación, racismo y xenofobia, incluyendo las pautas establecidas en la Ley 25326 Protección de Datos Personales, con el

objetivo de garantizar la seguridad de la información. Asimismo, se debe realizar un análisis del sistema de administración de base de datos más adecuado para gestionar la información sobre denuncias por discriminación, racismo y xenofobia que garantice la seguridad, confidencialidad, integridad y disponibilidad de la información.

6.7.4. Arbitrar los medios para que se firmen los acuerdos de confidencialidad pertinentes entre INADI y todos los empleados y terceros que por sus funciones y responsabilidades tienen acceso a información sobre las denuncias de discriminación, xenofobia y racismo la cual tiene carácter sensible y reservada, asegurando la confidencialidad de la información y dirimiendo las responsabilidades de cada parte en la administración de la seguridad de la información.

7. CONCLUSIONES

El INADI, en colaboración con la Secretaría de Derechos Humanos de la Nación, la Dirección de Derechos Humanos de Cancillería, la Secretaría de Gabinete de Ministros y especialistas en la materia, elabora el Plan Nacional contra la Discriminación, según el cual las prácticas sociales discriminatorias abarcan cualesquiera de estas acciones:

1. Crear y/o colaborar en la difusión de estereotipos de cualquier grupo humano por características reales o imaginarias, sean estas del tipo que fueren, sean estas positivas o negativas y se vinculen a características innatas o adquiridas.
2. Hostigar, maltratar, aislar, agredir, segregar, excluir y/o marginar a cualquier miembro de un grupo humano del tipo que fuere por su carácter de miembro de ese grupo.
3. Establecer cualquier distinción legal, económica, laboral, de libertad de movimiento o acceso a determinados ámbitos.

En el Marco Estratégico de Cooperación de las Naciones Unidas para el Desarrollo de Argentina (MECNUD), se conformó el Grupo de Trabajo *"Cero Discriminación a 2030, para la reducción del estigma y la discriminación en Argentina",* que cuenta con la

colaboración del Sistema de las Naciones Unidas en Argentina (SNU) y del que participan funcionarios de distintas agencias de las Naciones Unidas, brindando asistencia técnica y financiera al INADI, a fin de alcanzar la meta *"Cero Discriminación"* y los Objetivos de Desarrollo Sostenible (ODS) a 2030.

En esta instancia, para el INADI, este trabajo en el marco de cooperación con el Sistema de Naciones Unidas en Argentina, abarca la colaboración de los Organismos internacionales en tres Ejes: la finalización del Mapa de la Discriminación; la elaboración de un documento de diagnóstico del Plan Nacional contra la Discriminación que presente un estado de situación actualizado de la discriminación en Argentina e incluya una metodología para desarrollar el plan y finalmente, el desarrollo de proyectos específicos para un trabajo federal .

Es importante destacar que, desde su creación por Ley 24.515 del 05 de Julio de 1995, el INADI ha sido intervenido, a partir del año 1997, de manera intermitente, situación que ha generado como consecuencia inmediata el no funcionamiento del Consejo Asesor integrado por un máximo de diez (10) miembros tal cual lo establece su Ley de creación, y a su vez, que las decisiones de políticas públicas en los temas relevantes del Instituto sean tomadas unipersonalmente en oposición a lo que establece el espíritu de la mencionada Ley. No obstante, la intervención es una facultad que tiene el Poder Ejecutivo Nacional y está en su órbita ejercerla.

Durante el período auditado, 01/12/19 al 31/01/22, el INADI se encontraba a cargo de la Interventora, Dra. Victoria Analía DONDA PÉREZ.

El INADI como Institución, es el encargado de recibir todo tipo de denuncias relacionadas con discriminación, actos de xenofobia y/o racistas. En su Ley de creación establece que: *"corresponde al INADI [...] Recibir y centralizar denuncias sobre conductas discriminatorias, xenofóbicas o racistas y llevar un registro de ellas"*. En base a ello, dentro de su estructura organizacional, la Dirección de Asistencia a la Víctima, organizó

un sistema por el cual se atienden consultas y se tramitan las denuncias recibidas para concluir con un dictamen de opinión técnica sobre el hecho denunciado.

A los efectos de la presente auditoría, es importante destacar que los actos discriminatorios que hacen al objeto bajo análisis, se encuentran tipificados en la Ley 23.592, de Actos Discriminatorios y concurrentes, y contemplados en los Pactos Internacionales de rango Constitucional, referidos en el art. 75 inc. 22 de la Constitución Nacional y en los restantes Tratados Internacionales sobre Derechos Humanos.

El Decreto 218/12 del Poder Ejecutivo Nacional, que aprueba la estructura organizativa del primer nivel operativo del INADI, establece en su anexo II que es responsabilidad primaria de la Dirección de Asistencia a la Víctima,… "*entender en la recepción, registro, evaluación, investigación y análisis de denuncias presentadas sobre conductas discriminatorias, xenófobas o racistas, como así también prestar el servicio de asesoramiento y patrocinio jurídico gratuito a las personas damnificadas*". Con ese fin realizará, entre otras, las siguientes acciones:

- Recibir toda denuncia sobre conductas discriminatorias, xenófobas o racistas y llevar un registro de las mismas.
- Investigar los hechos denunciados, reunir y producir las pruebas pertinentes de acuerdo a los medios previstos en el Reglamento de Procedimientos Administrativos […]
- Analizar y evaluar las denuncias presentadas y elaborar los dictámenes técnicos especializados respectivos […]

En virtud de este decreto, se estableció, a través de la Disposición 208/12, la estructura de segundo nivel operativo. Así, para la Dirección de Asistencia a la Víctima se crearon dos coordinaciones:

1-"Recepción y Evaluación de Denuncias", tiene las acciones de *"atender las consultas […] brindándoles orientación e información"* y también la de *"Analizar, evaluar y emitir opinión sobre los casos de las denuncias recibidas"*.
2-"Investigación y Seguimiento de Casos", realizará las acciones de *"Investigar los casos denunciados, cuando a criterio de la Coordinación de Recepción y Evaluación […] resulte necesario para una mejor evaluación"*.

Cumplimiento Ley 27.499, *Ley Micaela de Capacitación Obligatoria en Género para todas las personas que integran los Tres Poderes del Estado*:

El INADI, a través de la Dirección de Recursos Humanos, está llevando a cabo la capacitación obligatoria en género que establece la Ley 27.499 (Ley Micaela) de acuerdo a lo establecido por el INAM (Instituto Nacional de la Mujer), como organismo rector de dicha ley y el INAP (Instituto Nacional de la Administración Pública), como organismo a cargo de la capacitación del personal de la Administración Pública Nacional (APN).

A su vez, el organismo cuenta con las certificaciones por parte del Instituto Nacional de la Mujer (INAM) quien indica que las *"Capacitaciones de sensibilización y concientización en el marco de la Ley Micaela: Introducción a la discriminación hacia las mujeres basada en el género",* cuentan con los estándares de calidad para la capacitación en la temática de género y violencia contra las mujeres establecidos por ese Instituto y la certificación del Instituto de la Administración Pública (INAP) en calidad de órgano rector, el cual tiene acreditación sobre su diseño y el dictado de cursos.

Del análisis de la documentación provista por el INADI sobre las capacitaciones realizadas surge que, de 422 agentes, han cumplimentado la capacitación 257, lo que representa el 61% del total.

Respecto a los 165 agentes (39% del total del personal) que aún no han sido capacitados en la Ley Micaela, la Coordinación de Recursos Humanos del INADI, manifestó que en el

Plan de Capacitación 2023, se contempla la capacitación de la totalidad del personal del Instituto. Este plan no se encontraba oficialmente aprobado al momento de esta auditoría y según lo informado por el auditado, debería estar aprobado por el INADI para ser presentado en el INAP, durante el primer trimestre de 2023.

Objetivos de Desarrollo Sostenible (ODS) en INADI:

En virtud de dar cumplimiento a lo dispuesto por la Disposición AGN 198/18, en vinculación con los ODS a los que ha adherido el Instituto y cuál es la situación al momento de la realización de las tareas de campo de esta auditoría, así como las proyecciones establecidas en el corto y mediano plazo para cada uno de ellos, el INADI reporta periódicamente a través de la Dirección Nacional de Asuntos Internacionales del Ministerio de Justicia y Derechos Humanos de la Nación, la evolución de un indicador para la medición de la Meta adaptada 10.3: *Garantizar la igualdad de oportunidades y reducir la desigualdad de resultados*, incluso eliminando las leyes, políticas y prácticas discriminatorias y promoviendo legislaciones, políticas y medidas adecuadas a ese respecto (Objetivo Global 10), formulado a partir del estudio que se realiza a nivel nacional (Mapa Nacional de la Discriminación) sobre la autopercepción de haber experimentado alguna vez una situación discriminatoria: (10.3.1 Porcentaje de la población que declara haberse sentido personalmente víctima de discriminación), arrojando como dato y según lo informado por INADI a este equipo de auditoría, que el 44% de los encuestados se han sentido afectados por actos discriminatorios.

Asimismo, según lo manifestado por INADI, en el año 2021 se comprometió a iniciar la medición de un nuevo indicador para la meta adaptada 16.3: *"Promover el estado de derecho en los planos nacional e internacional y garantizar la igualdad de acceso a la justicia para todos"*, a saber: *16.3.3. Porcentaje de personas que accedieron a algún mecanismo oficial de resolución de controversias por discriminación (de medición bianual)*; cuya composición se basa en el porcentaje de denuncias resueltas a través de mecanismos de resolución de controversias, como las gestiones de buenos oficios ante la

parte denunciada, o las conciliaciones de mutuo acuerdo entre partes denunciante y denunciada.

El trabajo de auditoría se centró en el análisis de los siguientes procesos destacados:

- Tratamiento de denuncias recibidas en Sede Central y en las Delegaciones del Interior del país.
- Tratamiento de las consultas sobre cuestiones de discriminación a través de los distintos canales de comunicación que pone a disposición el INADI.
- Confección del "Mapa Nacional de la Discriminación".

A través del relevamiento y análisis efectuado sobre estos procesos, la auditoría se enfocó en 7 (siete) Ejes principales: 1) gobierno de TI, 2) seguridad de la información, 3) seguridad de la infraestructura de TI, 4) continuidad de las operaciones organizacionales, 5) operaciones de TI, 6) adquisiciones y contratación de TI, y 7) sistemas de información (entendiéndose como la evaluación de cuán adecuados son los controles con los que cuentan las aplicaciones utilizadas, en cuanto a las interfaces de entrada, de salida, la integración, automatización, etc.); cuestiones que impactan sobre la confidencialidad, integridad y disponibilidad de la información en los procesos evaluados.

Los principales hallazgos en el ámbito del gobierno de TI, evidencian que la Dirección de Administración, a cargo de los servicios de TI de la Institución, no realizan una planificación estratégica de corto, mediano y largo plazo que permita demostrar el rol que la tecnología debe tener para brindar un adecuado soporte sobre los procesos críticos que la conforman, sumado a que la estructura organizacional de TI presentada por el INADI, posee un diseño inadecuado e insuficiente para cumplir con eficiencia y eficacia las responsabilidades y funciones que le competen y que demanda a partir de sus objetivos estratégicos.

Por otro lado, se ha detectado que el INADI no posee políticas, normas y procedimientos de TI formalizados por la alta dirección y debidamente comunicados a las distintas áreas operativas de la estructura organizacional, generando elevados niveles de riesgos de TI que impactan sobre el ambiente de control en dicho ámbito, y provocando, además, que el nivel de los servicios sea insuficiente para dar soporte a los objetivos estratégicos de la Institución. Por último, se destaca que no se cuenta 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 ha detectado que: i) no se cuenta con un plan de seguridad de la información consistente; ii) que el organismo no posee políticas de seguridad de la información aplicables transversalmente a toda la organización; y iii) que la gestión de usuarios aplicada por el INADI para acceder a la base de datos de denuncias por discriminación es inadecuada, careciendo de los mínimos protocolos de seguridad.

Respecto a la seguridad de la infraestructura de TI, se detectó que la sala de servidores que aloja a la infraestructura tecnológica que da soporte informático al INADI y la oficina donde se aloja el servidor de la base de datos de denuncias por discriminación, no cumplen con las condiciones mínimas necesarias para resguardar la seguridad física de los servidores y sus datos, lo que pone en riesgo la continuidad de los servicios tecnológicos que sustentan los procesos críticos evaluados en esta auditoría.

En relación a la continuidad de las operaciones organizacionales, el nivel de disponibilidad de los procesos críticos no está alineado a las necesidades de la organización, ni tampoco a lo que establecen las buenas prácticas en la materia, debido a que fue hallado lo siguiente: i) el personal de TI, a cargo de la gestión y administración de la infraestructura tecnológica que da soporte de TI a la Institución, no cuenta con un Plan de Recuperación ante Desastres

formalizado y debidamente comunicado; y ii) el personal de TI del INADI, tampoco tiene 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.

En cuanto a las operaciones de TI, se verificó que no se garantiza de manera apropiada el correcto funcionamiento de los procesos críticos, ya que se constató que: i) 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 soporte e información; y ii) la Coordinación de Recepción y Evaluación de Denuncias, dependiente de la Dirección de Asistencia a la Víctima, no realiza monitoreos sobre el servicio de conectividad utilizado por la Línea Telefónica 168 (Ex 0800), entregado por el proveedor a cargo de la prestación.

Por otro lado, en adquisiciones y contratación de TI, existe un inadecuado control del nivel de servicio establecido en el contrato por el servicio de la Línea Telefónica 168 (Ex 0800). Esto impide que las áreas usuarias puedan gestionar, controlar y medir adecuadamente la calidad de la prestación brindada por el proveedor.

Finalmente, en el ambiente de sistemas de información, se hallaron evidencias que identificaron lo siguiente:: i) los sistemas de información y procesos aplicados por el INADI para el tratamiento de denuncias y consultas por discriminación, racismo y xenofobia, no se encuentran suficientemente integrados; y ii) no existen procedimientos formalizados y estandarizados con procesos de control automáticos e integrados, para asegurar un eficiente y seguro tratamiento de la información, que garanticen la integridad y consistencia de los datos almacenados y su recopilación, impactando contra la confiabilidad de la información que se utiliza para la elaboración del *"Mapa Nacional de la Discriminación"* y de los informes estadísticos publicados por el INADI sobre la discriminación, racismo y xenofobia.

En conclusión, en este contexto, resulta necesario que la alta dirección del Instituto, principalmente las Direcciones de Administración y de Asistencia a la Víctima, pongan en marcha en forma conjunta un plan estratégico de TI con eficientes y efectivos procesos de planificación que se encuentren debidamente alineados a los objetivos estratégicos del INADI, garantizando un adecuado ambiente de control sobre los servicios de TI y considerando los principios fundamentales de disponibilidad, integridad y confidencialidad de la información de la Institución; todo en concordancia con los aspectos que se encuentran indicados en los acápites 4 (HALLAZGOS) y 6 (RECOMENDACIONES) del presente Informe.

8. LUGAR Y FECHA

BUENOS AIRES, junio de 2023

9. FIRMA

MARTINEZ Maria Virginia

Cdra. Maria Virginia Martinez
Jefa de Departamento de Auditoría Informática
Gerencia de Planificación y Proyectos Especiales
Auditoría General de la Nación
REPÚBLICA ARGENTINA

VILLA Federico Gaston

Firmado digitalmente por VILLA Federico Gaston

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

MASSACCESI Leandro Horacio

Firmado digitalmente por MASSACCESI Leandro Horacio

10. ANEXOS

ANEXO I – Comentarios del auditado

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Nota

Número: NO-2023-64799193-APN-DADM#INADI

CIUDAD DE BUENOS AIRES
Martes 6 de Junio de 2023

Referencia: Opinión del auditado - AGN

A: Greta Marisa Pena (INADI#MJ),

Con Copia A:

De mi mayor consideración:

Tengo el agrado dirigirme a usted en relación con el Informe relacionado con Tecnologías de la Información del INADI. A continuación, se emite opinión del auditado.

Anexo I - Comentarios del auditado

a. CUESTIONES PRELIMINARES

A fin de contextualizar la "Opinión del Auditado", cabe efectuar algunas consideraciones previas.

En tal sentido, se destaca que mediante Decreto N° 15 de fecha 9 de enero de 2023 se dio por prorrogada la Intervención de este Instituto Nacional, designándose Interventora a la Dra. Greta Marisa Pena desde esa fecha y hasta el 10 de diciembre del corriente año.

Así las cosas, la Suscripta fue designada en sus funciones mediante Decisión Administrativa N° 128 de fecha 24 de febrero de 2023, a partir del 1° de febrero del corriente año. A partir de ese momento, se iniciaron tareas de relevamiento y diagnóstico de cada uno de los puntos axiales de la Dirección; esto es:

- Tecnologías de la Información y de las Comunicaciones;

- Infraestructura y Servicios Generales;
- Seguridad e Higiene;
- Automotores;
- Patrimonio;
- Administración Financiera;
- Recursos Humanos; y
- Gestión Documental.

En términos generales, sobre la base de las mencionadas tareas, se han desarrollado los respectivos Estados de Situación de cada punto axial, sustancialmente coincidentes con los "hallazgos" contenidos en los respectivos informes de auditoría y, en función de ello, se ha establecido un Plan de Acción y Regularización de las diversas áreas internas de la DIRECCIÓN DE ADMINISTRACIÓN ("el Plan"), que comenzó a ejecutarse durante el mes de febrero de 2023, se encuentra actualmente en plena realización y posee acciones que deberían continuar durante los próximos ejercicios.

Específicamente, con relación a las Tecnologías de la Información y de las Comunicaciones ("TI"), debe enfatizarse que una de las primeras medidas adoptadas por la Suscripta, desde el inicio de su gestión, ha sido la de efectuar un relevamiento exhaustivo del estado de situación de este Organismo Nacional en la referida materia y, sobre esa base, se ha elaborado el documento titulado: "Plan Estratégico de Tecnologías de la Información 2023-2025" ("PETI"), que busca definir -entre otras cuestiones- la forma en que las TI van a contribuir con los objetivos estratégicos del INSTITUTO NACIONAL CONTRA LA DISCRIMINACIÓN, LA XENOFOBIA Y EL RACISMO.

Asimismo, corresponde apuntar que, con anterioridad al inicio de la gestión de la Suscripta, no existía plan estratégico alguno.

Ahora bien, es importante destacar que el diagnóstico efectuado en el Plan coincide, sustancialmente, con el del Informe de Auditoría. Se aceptan, pues, todas las observaciones formuladas por el Órgano Auditor, en la inteligencia de que el diagnóstico efectuado resulta concordante con el de esta Dirección.

Partiendo de las mencionadas premisas y en aras de obtener la mayor claridad expositiva posible, la "Opinión del Auditado" se estructurará de la siguiente manera:

*En primer término, se hará referencia a los "Hallazgos" que constan en el "Proyecto de Informe de Auditoría. Gestión de TI...", siguiendo sus ejes temáticos; a saber:

1. Gobierno de TI (punto 4.1.);
2. Seguridad de la Información (punto 4.2.);
3. Seguridad en la Infraestructura de TI (punto 4.3.);
4. Continuidad de las Operaciones Organizacionales (punto 4.4.);
5. Operaciones de TI (punto 4.5.);

6. Adquisiciones y contratación de TI (punto 4.6.); y

7. Sistemas de Información (punto 4.7.).

Seguidamente, se enumerarán las recomendaciones que constan en el Informe de Auditoria (punto 6) y, junto a cada una de ellas, se hará mención a las acciones del Plan de corto, mediano y largo plazo (respectivamente: 2023-2024, 2024-2025 y 2025 en adelante) que se han realizado, se vienen realizando o realizarán desde la DIRECCIÓN DE ADMINISTRACIÓN, en aras de abordar los problemas identificados por el Órgano Auditor.

b. ESTADO DE SITUACIÓN. HALLAZGOS

Sentado lo anterior, es importante destacar, una vez más, que esta Dirección coincide y comparte las consideraciones formuladas en el Informe de Auditoría, ya que el diagnóstico de situación que se formula es, en sustancia, análogo al efectuado a partir de las tareas de relevamiento encaradas por la Suscripta, cuyos resultados han quedado plasmados en el Plan.

En el Informe de Auditoría (punto 4), se detallan los siguientes "hallazgos" con relación al estado de situación en materia de "Gobierno de TI" (punto 4.1.) de este Organismo Descentralizado; a saber:

- carencia de "...políticas, normas y procedimientos de TI formalizados por la alta dirección y debidamente comunicados a las distintas áreas operativas de la estructura organizacional. Esto genera altos niveles de riesgos de TI e impacta sobre el ambiente de control en el ámbito de TI, provocando que el nivel de los servicios sea insuficiente para dar soporte a los objetivos estratégicos de la contratación..." (punto 4.1.2.);
- diseño inadecuado e insuficiente de la estructura organizacional de TI "...para cumplir con eficiencia y eficacia las responsabilidades y funciones que le competen y que demanda la organización a partir de sus objetivos estratégicos". Ello así, en tanto dicha estructura organizacional no está "formalizada" y, por lo tanto, no tiene "...establecidas oficialmente las misiones y funciones del área y sus integrantes...", lo cual "...conduce a que el personal que se desempeña como soporte técnico, se encuentre frente a la necesidad de cumplir tareas de gestión de los sistemas y servicios de TI y de administración de bases de datos...", pese a su formación y capacidades limitadas. La situación descripta provoca "...considerables operacionales, sobre todo en aquellas metas estratégicas en las cuales la tecnología de la información cumple un rol esencial para alcanzar su logro..." (punto 4.1.3.); y
- ausencia, en la plataforma tecnológica y los servicios de soporte y mantenimiento continuo brindados por el personal de soporte de TI, de "...una adecuada revisión del ambiente de control interno que garantice la detección temprana de riesgos de TI y las acciones pertinentes para gestionarlos...", siendo que "...no se realizaron auditorías internas de TI en el INADI durante el período auditado...", lo que evidencia "...la falta de un efectivo monitoreo del control interno sobre los procesos y procedimientos llevados a cabo por el área informática y por el responsable de la administración de la base de denuncias por discriminación para la prestación de los servicios de TI al Instituto, principalmente, sobre los procesos operativos del servicio de la Línea 168 (Ex 0800), de denuncias y consultas por discriminación y de generación de estadísticas publicadas por el organismo..." (punto 4.1.4);

Se deja constancia de que si bien durante el período auditado no existía un "Plan Estratégico de TI" (punto 4.1.1.), tal como se ha dicho, en la actualidad se cuenta con el "Plan Estratégico de Tecnologías de la Información (2023-2025)", elaborado en el seno de la DIRECCIÓN DE ADMINISTRACIÓN.

En lo que respecta a la estructura organizacional de TI, su modificación escapa a las facultades y atribuciones de la DIRECCIÓN DE ADMINISTRACIÓN, siendo ello un resorte exclusivo de la INTERVENCIÓN de este Organismo Federal, desde que involucra cambios en su organigrama y posibles aperturas de áreas o

dependencias dentro del mismo. Ello, claro está, sin perjuicio de los señalamientos al respecto que la Suscripta viene haciendo, desde el inicio de su gestión en febrero de 2023, a la máxima autoridad de este Instituto Nacional.

En cuanto al tópico "Seguridad de la Información" (punto 4.2.), en el Informe de Auditoría se señalan los siguientes "hallazgos"; a saber:

- ausencia de "…políticas de seguridad de la información aplicables transversalmente a toda organización. Este escenario impacta sobre el adecuado cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información". Este Instituto Nacional "…no posee un sistema de gestión de la seguridad de la información…", lo cual coloca a este Organismo "…en una situación de alto nivel de riesgo y vulnerabilidad, más aún considerando que los procesos relacionados con las denuncias por discriminación, gestionan información sensible y de carácter reservado…" (punto 4.2.1.);
- carencia de un "…plan de seguridad de la información consistente, situación que conduce a un estado de vulnerabilidad sobre los procesos críticos de la organización y pone en riesgo la confidencialidad, integridad y disponibilidad de la información…" (punto 4.2.2.);
- carácter inadecuado de la "…gestión de usuarios aplicada por el organismo para acceder a la base de datos de denuncias por discriminación […] poniendo en riesgo la confidencialidad, integridad y disponibilidad de la información…" (punto 4.2.3.);
- omisión del personal de TI en cuanto a "…pruebas de seguridad e intrusión sobre la plataforma tecnológica del organismo, en especial sobre los entornos que dan soporte a los procesos de denuncias, consultas y generación de estadísticas por discriminación, lo que 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…" (punto 4.2.4.).

En lo que respecta a la "Seguridad de la Infraestructura de TI" (punto 4.3.), se han indicado los siguientes "hallazgos"; a saber:

- incumplimiento, en cuanto a "…la sala de servidores que aloja la infraestructura tecnológica que da soporte informático al INADI y la oficina donde se aloja el servidor de la base de datos de denuncias por discriminación…" de "…las condiciones mínimas necesarias para resguardar la seguridad física de los servidores y sus datos, lo que pone en riesgo la continuidad de los servicios tecnológicos que sustentan los procesos críticos…" (punto 4.3.1.);

Acerca de la "Continuidad de las Operaciones Organizacionales" (punto 4.4), se hace alusión a los "hallazgos" detallados debajo; a saber:

- inexistencia de un "…Plan de Recuperación ante Desastres formalizado y debidamente comunicado…", a disposición del "…personal de TI, a cargo de la gestión y administración de la infraestructura tecnológica que da soporte de TI al organismo", lo que "…implica un riesgo de alto impacto sobre la disponibilidad de la información ante una interrupción de los servicios de TI, sobre las cuales todas las áreas operativas del INADI tienen una alta dependencia…" (punto 4.4.1.);
- ausencia de "…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…" (punto 4.4.2.);

En lo que atañe a "Operaciones de TI", en el Informe de Auditoría se consignan los siguientes "hallazgos"; a saber:

- inexistencia de "...una función de mesa de ayuda para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de soporte e información. Esta situación impide a la organización contar con herramientas que permitan medir el desempeño de los servicios de TI y los tiempos de respuesta para resolver incidencias y problemas en el ámbito de TI..." (punto 4.5.1.);
- ausencia de "...monitoreos sobre el servicio de conectividad utilizado por la línea 168 (Ex 0800)...", por parte de la COORDINACIÓN DE RECEPCIÓN Y EVALUACIÓN DE DENUNCIAS, dependiente de la DIRECCIÓN DE ASISTENCIA A LA VÍCTIMA. "Esta situación imposibilita medir adecuadamente el cumplimiento de los niveles de servicio acordados y establecer un plan de mejora continua, alineado a las necesidades y prioridades de la organización..." (punto 4.5.2.).

En materia de "Adquisiciones y Contratación de TI", se han apuntado los "hallazgos" que se especifican a continuación; a saber:

- ausencia de un "...control sobre el nivel de servicio establecido en el contrato por el servicio de la Línea Telefónica 168 (Ex 0800)...", por parte de la DIRECCIÓN DE ASISTENCIA A LA VÍCTIMA y la COORDINACIÓN DE RECEPCIÓN Y EVALUACIÓN DE DENUNCIAS. "Esto impide que las áreas usuarias puedan gestionar, controlar y medir adecuadamente la calidad de la prestación brindada por el proveedor...", además de que no resulta posible "...evaluar con objetividad y eficiencia el rendimiento y cumplimiento del servicio prestado por el proveedor y hacer valer lo comprometido en el contrato..." (punto 4.6.1.)".

Sobre los "Sistemas de información" (punto 4.7), se han destacado los "hallazgos" que se exponen seguidamente; a saber:

- insuficiencia de la integración de "Los sistemas de información y procesos aplicados por el INADI para el tratamiento de denuncias y consultas por discriminación, racismo y xenofobia [...] La ausencia de procesos automáticos e integrados para el tratamiento de la información, pone en riesgo su integridad al momento de ser recibida y posteriormente al momento de su procesamiento..." (punto 4.7.1.);
- "...falta de procedimientos formalizados y estandarizados con procesos de control automáticos para asegurar un eficiente y seguro tratamiento de la información que garanticen la integridad y consistencia de los datos almacenados y su recopilación...". Ello "...impacta contra la confiabilidad de la información que se utiliza para la elaboración del "Mapa Nacional contra la Discriminación" y de los informes estadísticos publicados por el INADI sobre la discriminación, racismo y xenofobia" (punto 4.7.2.);
- carencia de "...políticas y procedimientos formalizados para la administración de la base de datos de denuncias por discriminación, racismo y xenofobia que puedan garantizar la seguridad lógica y la confidencialidad de la información..." (punto 4.7.3.); y
- falta de formalización, "...a través de la Dirección de Asistencia a la Víctima..." de "...un acuerdo de confidencialidad con cada uno de los empleados que gestionan y/o tienen acceso a la información sensible y reservada, generada por las denuncias de discriminación, xenofobia y racismo que le asegure al organismo la no divulgación y/o externa de dicha información".

c. RECOMENDACIONES Y ACCIONES ASOCIADAS DE CORTO, MEDIANO Y LARGO PLAZO

Las "Recomendaciones" del Informe de Auditoría (punto 6) están agrupadas temáticamente siguiendo el criterio utilizado para los "Hallazgos" (punto 4).

En materia de "Gobierno de IT" (punto 6.1. del Informe de Auditoría) se han hecho las recomendaciones que se detallan debajo; a saber:

- "Definir, aprobar, elaborar e implementar un plan estratégico de TI alineado con las metas estratégicas del INADI que permita obtener mecanismos de soporte tecnológico eficiencias, eficaces y económicamente adecuados sobre los procesos críticos de los servicios que brinda el organismo, contribuyendo además en su mejora continua" (punto 6.1.1.);
- "Elaborar, aprobar, implementar y comunicar a toda la organización las políticas, normas y procedimientos debidamente alineados a los objetivos estratégicos del organismo y al plan estratégico de TI que formalicen servicios de TI eficientes y eficaces" (punto 6.1.2.);
- "Establecer una estructura organizacional de TI que refleje las necesidades operativas y estratégicas del organismo. Implementar un proceso para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos del personal y las estrategias internas para satisfacer los objetivos estratégicos esperados por la organización, y que sea capaz de adaptarse a las circunstancias cambiantes que se vayan presentando" (punto 6.1.3.);
- "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" (punto 6.1.4.);

Ahora bien, el Plan de esta Dirección contiene una serie de acciones que, desde ya, permiten mejorar los procesos de gobierno de TI en el sentido propiciado por el Órgano Auditor; a saber:

ACCIÓN 1 (de corto plazo): redacción de procedimientos para la gestión de TI que guíen el accionar de usuarios y técnicos en las tareas de operación y mantenimiento de la infraestructura de TI:

- Gestión de usuarios

1. alta y baja de usuarios en los diferentes sistemas;
2. políticas de acceso y gestión de claves;
3. requisitos de ingreso de personal.

- Gestión de bienes

1. gestión y actualización de inventarios y patrimonio;
2. ingresos y egreso de bienes y materiales informáticos.

- Gestión del soporte

1. gestión de los pedidos de soporte técnico;
2. manuales de usuarios de los diferentes sistemas.

- Gestión de la infraestructura de TI

1. políticas de back ups;
2. plan de disaster recovery;

3. procedimientos técnicos;

4. procedimientos de mejora continúa.

ACCIÓN 2 (de corto plazo): firma de un convenio con la Universidad Tecnológica Nacional ("UTN"), dada la escasez de personal técnico del INADI, tendiente a que dicha casa de estudios aporte personal que pueda ayudar en la implementación de las siguientes mejoras tecnológicas:

- relevamiento de la estructura tecnológica de este Organismo;
- reorganización del datacenter;
- sistema de monitoreo del datacenter;
- sistema de refrigeración adicional;
- implementación del sistema de ticket;
- desarrollo de aplicaciones.

En lo que respecta a la "Seguridad de la Información" (punto 6.2. del Informe de Auditoría), se han hecho las recomendaciones que lucen enumeradas debajo; a saber:

- "Dictar, implementar y comunicar a todas las áreas del Instituto las políticas de seguridad de la información que permitan garantizar un eficiente y eficaz sistema institucional de gestión de la seguridad de la información" (punto 6.2.1).
- "Diseñar, implementar y comunicar a toda la organización un plan de seguridad de la información consistente, eficiente y eficaz que permita gestionar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información sensible y reservada que gestiona el Instituto" (punto 6.2.2).
- "Poner en marcha un sistema de gestión de usuarios adecuado y seguro que permita que todos los usuarios que tengan acceso autorizado a la base de datos de denuncias por discriminación sean identificables de manera única y con perfiles y funciones por perfil definidos. Y que además garantice la posibilidad de auditar las actividades que ejecutan los usuarios dentro de la base de datos" (punto 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 denuncias, consultas y generación de estadísticas por discriminación, de manera continua y ejecutando las acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Garantizar que la implementación de la seguridad en IT sea probada y monitoreada de forma proactiva y recurrente para mantener el nivel de seguridad requerido por la organización" (punto 6.2.4).

Debe puntualizarse que el Plan contempla acciones que van en clara convergencia con las recomendaciones supra aludidas, y que se detallan a continuación:

ACCIÓN 22 (de largo plazo): desarrollo de una política de seguridad de la información que cumpla con los requisitos establecidos en la Decisión Administrativa N° 641/2021 de la JEFATURA DE GABINETE DE MINISTROS, aprobatoria de los "REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL.

La mencionada política debe incluir lineamientos y procedimientos para la protección de la información, gestión de riesgos, acceso a los recursos informáticos, resguardo de datos, continuidad del negocio y concientización

del personal en materia de seguridad de la información.

ACCIÓN 23 (de corto plazo): fortalecimiento de seguridad de Firewall: configuración y puesta en marcha de funcionalidades dentro del Firewall existente, que permita fortalecer los niveles de seguridad, contemplando, entre otras tareas:

- configuración de políticas de acceso y navegación. Implementación de filtros;
- implementación de políticas de análisis y priorización de tráfico;
- implementación de políticas para la detección y control de intrusos;
- implementación del servicio de Proxy;
- autenticación de usuarios dentro de los equipos, con miras a la identificación de los usuarios y sus políticas de uso de los diferentes servicios (para doscientos —200— usuarios aproximadamente);
- configuración de la funcionalidad de antivirus;
- implementación de la conexión VPN mediante el uso de la aplicación FortiCliente;
- provisión de toda la documentación topológica, de configuración y conexión de cada uno de los servicios, una vez configurados.

ACCIÓN 24 (de mediano plazo): implementación de antivirus: a través de la contratación de un sistema de antivirus, adecuadamente licenciado y con soporte para la infraestructura de computadoras de escritorio del INADI. Esto ayudará a proteger los sistemas contra malware, virus y otras amenazas cibernéticas. Además, es necesario mantener el software actualizado de manera regular y realizar escaneos periódicos en los equipos informáticos.

En lo que atañe a la "Seguridad en la Infraestructura de TI" (punto 6.3 del Informe de Auditoría), se ha efectuado la recomendación que se menciona ut infra; a saber:

- "Readecuar los espacios físicos e implementar las medidas de seguridad que correspondan para garantizar el óptimo funcionamiento del Centro de Procesamiento de Datos, a fin de llevar a cabo una correcta administración y resguardo de los sistemas de información y de las bases de datos que brindan servicio a los procesos críticos del INADI" (punto 6.3.1).

Cuadra señalar que esta Dirección ha previsto diversas acciones para superar los problemas apuntados por el Órgano Auditor, cuya naturaleza ha llevado a que se las detalle al momento de abordar el punto axial de Seguridad e Higiene, al cual se remite en honor a la brevedad.

Sobre el tópico de "Continuidad de las Operaciones Organizacionales" (punto 6.4. del Informe de Auditoría), se efectúan las siguientes recomendaciones; a saber:

- "Desarrollar, probar y mantener en forma continua un Plan de Recuperación ante Desastres, alineado a un Plan de Continuidad del Negocio (BCP por sus siglas en inglés, Business Continuity Plan), aprobado formalmente por un 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 de información y de la información de acuerdo a los requerimientos operativos y administrativos del INADI" (punto 6.4.1).

- "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. Adquirir e implementar una herramienta especializada en la ejecución de copias de respaldo y de restauración que asegure la eficiencia, el éxito y la documentación de los respaldos externos de la información crítica del organismo" (punto 6.4.2).

El Plan elaborado por esta Dirección se halla en sintonía con las recomendaciones antedichas, en lo que respecta a las acciones que se refieren a continuación; a saber:

ACCIÓN 14 (de corto plazo): mejoras en el datacenter: enmarcadas en el convenio que se propicia con la UTN y abarcativas de las siguientes tareas:

- Reorganización del datacenter:

1. acondicionamiento de la iluminación;

2. luz de emergencia y accesorios necesarios para la instalación;

3. provisión de bandejas deslizables para el soporte de equipos no rackeables;

4. reorganización de rack dentro del datacenter;

5. provisión e instalación de un rack de cuarenta (40) unidades para recambio de rack situado cerca de la entrada, en orden a la migración de los equipos existentes.

- Sistema de monitoreo: provisión e instalación de un sistema compuesto por:

1. un (1) controlador central con gestión y visualización remota;

2. un (1) sensor de temperatura cableado;

3. un (1) sensor de humedad cableado;

4. un (1) detector de incendios cableado;

5. un (1) censor de puerta cableado.

- Sistema de refrigeración adicional: provisión e instalación de un sistema de aire acondicionado de tipo split de cuatro mil quinientas (4.500) frigorías, para refrigeración del datacenter, adicional al ya existente.

ACCIÓN 15 (de corto plazo): mejora en la infraestructura de cableado de red: con miras a mejorar la calidad y confiabilidad de la red en la Sede Central del INADI, abarcativa de las siguientes acciones:

- reemplazo de los switches sin mantenimiento y discontinuados por modelos actuales de marcas reconocidas que ofrezcan soporte y actualizaciones regulares;

- actualización de la velocidad de conexión entre los switches y el datacenter a una velocidad de 10 GBps;

- implementación de un backbone o montante de fibra óptica para aumentar la capacidad y confiabilidad de la red;

- reorganización de la estructura de cableado en cada piso, para reducir la cantidad de racks concentradores y minimizar los saltos en las conexiones de red;

- mejoramiento del cableado horizontal para evitar la exposición de cables a la vista y reducir los riesgos asociados. Esto podría incluir la instalación de canalizaciones adecuadas para el tendido de cables o la búsqueda de soluciones alternativas para la colocación de los puestos de red;

- análisis exhaustivo de las necesidades de cableado en cada piso y realización de las expansiones necesarias para garantizar una cobertura adecuada sin necesidad de agregar switches adicionales en las oficinas;

- mantenimiento regular de los switches y el cableado para garantizar su buen funcionamiento y detectar posibles problemas a tiempo.

ACCIÓN 3 (de corto plazo): suscripción de un convenio con la Empresa Argentina de Soluciones Satelitales S.A. ("ARSAT") para que el INADI puede contar con la infraestructura de servidores, procesadores, disco y memoria suficiente para albergar allí las aplicaciones y sistemas a implementar, el cual tiene que contemplar:

- servicio de hosting IaaS;

- servicio de firewall y networking;

- conectividad Internet;

- monitoreo.

En otro orden de ideas, sobre las "Operaciones de TI" (punto 6.5. del Informe de Auditoría), se han efectuado las recomendaciones a las que se hace referencia debajo; a saber:

- "Implementar una mesa de ayuda con sus correspondientes procedimientos formalizados, con el objetivo de generar las herramientas necesarias para el tratamiento eficiente de incidentes y problemas, permitiendo además la mediación y evaluación de los servicios TI y su mejora continua" (punto 6.5.1).
- "Establecer un marco formal de administración y monitoreo de los niveles de servicios acordados con el/los proveedore[/]s de TI, en especial con el prestador de la línea 168 (Ex 0800), con el objetivo de que el INADI se asegure un servicio eficiente y que cuente con los elementos técnicos y legales necesarios para exigirle a los proveedores los ajustes y las mejoras necesarias de las prestaciones que brindan en función de las necesidades estratégicas del organismo" (punto 6.5.2).

El Plan, por su parte, contiene varias acciones tendientes a solucionar los problemas que han motivado las citadas recomendaciones; a saber:

ACCIÓN 11 (de corto plazo): implementación de sistemas internos de gestión, a través de convenios de servicios con la UTN:

- sistema de ticket para la gestión de pedidos informáticos;

- sistema de ticket para la gestión de servicios generales;

- sitio Web de Intranet donde se consolide la información de apoyo para las diferentes áreas del INADI.

En materia de "Adquisiciones y Contratación de TI" (punto 6.6.), se ha formulado la recomendación que se glosa a continuación; a saber:

- "Controlar y monitorear continuamente los criterios de desempeño del proveedor del servicio de la Línea Telefónica 168 (Ex 0800) en función de lo establecido en el contrato para el nivel de servicio comprometido" (punto 6.6.1).

Con relación a la recomendación que antecede, es de destacar que se le ha requerido el servicio de mapping telefónico a la firma Gradicom S.A.

En lo referente a los "Sistemas de Información" (punto 6.7.), se hacen las recomendaciones que se aluden seguidamente; a saber:

"Respecto a los procesos de denuncias y consultas por discriminación, racismo y xenofobia [punto 6.7.1.]:

- Adquirir, desarrollar, implementar y mantener sistemas de información integrados que les den soporte. Adquirir y mantener la infraestructura tecnológica que requieran estos sistemas.
- Facilitar efectivamente la operación y el uso de los aplicativos a los usuarios finales con adecuadas medidas de seguridad para el acceso de los mismos.
- Implementar controles automatizados en las aplicaciones tal que se garantice el procesamiento de la información de manera exacta, completa, oportuna, autorizada y auditable.
- Actualizar el inventario de aplicaciones existentes en el INADI y regularizar la situación en el caso de software no licenciado".

"Respecto a la elaboración del "Mapa Nacional de la Discriminación" y de los informes estadísticos publicados por el INADI sobre la discriminación, racismo y xenofobia [punto 6.7.2.]:

- Confeccionar, aprobar por la máxima autoridad competente del INADI e implementar procedimientos para la administración de las bases de datos estadísticas dentro del marco de las políticas de seguridad de la información que dicte el organismo.
- Establecer políticas y procedimientos formalizados para el intercambio de datos claves y sensibles (secretos y confidenciales) que garanticen la autenticidad e integridad del contenido y el no repudio del origen.
- Celebrar acuerdos de confidencialidad con las universidades y con otros terceros que intervengan en los procesos de toma y procesamiento de datos referidos a la confección del "Mapa Nacional de la Discriminación" y otros informes estadísticos publicados por el INADI.
- Implementar controles automatizados en las aplicaciones tal que se garantice el procesamiento de la información de manera exacta, completa, oportuna, autorizada y auditable.
- Actualizar el inventario de las aplicaciones existentes en INADI, y regularizar la situación en caso de uso de software no licenciado".

"Elaborar, aprobar, implementar y comunicar las políticas y procedimientos para la administración de las bases de datos de denuncias por discriminación, racismo y xenofobia, incluyendo las pautas establecidas en la Ley 35.326 [de] Protección de Datos Personales, con el objetivo de garantizar la seguridad de la información. Asimismo, se debe realizar un análisis del sistema de administración de bases de datos más adecuado para gestionar la información sobre denuncias por discriminación, racismo y xenofobia que garantice la seguridad, confidencialidad, integridad y disponibilidad de la información" (punto 6.7.3.).

"Arbitrar los medios para que se firmen los acuerdos de confidencialidad entre INADI y todos los empleados y terceros que por sus funciones y responsabilidades tienen acceso a información sobre las denuncias de discriminación, xenofobia y racismo la cual tiene carácter sensible y reservada, asegurando la confidencialidad de la información y dirimiendo las responsabilidades de cada parte en la administración de la seguridad de la

información" (punto 6.7.4.).

El Plan de esta Dirección contempla una serie de acciones que van en el mismo sentido de las aludidas recomendaciones; a saber:

ACCIÓN 5 (de mediano plazo): desarrollo de un sistema integral de gestión de consultas y denuncias por discriminación, xenofobia y racismo:

- características funcionales del sistema:

1. completamente Web, por lo que será accesible tanto desde la Sede Central como desde las delegaciones del INADI;

2. diferentes perfiles de usuarios;

3. posibilidad de registros de las denuncias ingresadas por diferentes medios: Línea 168, formulario Web, sistema TAD, actuación presencial en la Sede Central y en las delegaciones provinciales;

4. posibilidad de seguimiento y gestión de todas las denuncias;

5. reportes y consultas de estado de avance de cada denuncia;

- registro centralizado: abarcativo de la Sede Central tanto como de las delegaciones del interior de la República Argentina, evitando así las habituales inconsistencias entre el registro de denuncias aportado por la DIRECCIÓN DE ASISTENCIA A LA VÍCTIMA y el suministrado por las delegaciones;

- integración de la información sobre medios alternativos para la gestión de conflictos: esto facilitará la planificación y la evaluación de los resultados de los diferentes mecanismos utilizados para la solución de conflictos relacionados con la discriminación. El desarrollo e implementación de este aspecto requerirá un nuevo convenio de servicios con la UTN. El sistema correrá por los servidores contratados por INADI en la plataforma de ARSAT.

ACCIÓN 10 (de largo plazo): sistemas de inventario y patrimonio: implementación de un sistema informático de gestión de patrimonio que permita una administración más eficiente y precisa de los bienes del INADI.

- Beneficios de la implementación:

1. en la posibilidad de registrar y almacenar todos los bienes del INADI en una base de datos centralizada y accesible;

2. en la clasificación y categorización de los bienes del INADI de acuerdo con diferentes criterios, como ubicación, tipo de activo, fecha de adquisición, entre otros;

3. posibilidad de realizar un seguimiento más preciso de los activos, incluyendo detalles como movimientos, reparaciones y bajas;

4. posibilidad de generar informes y reportes actualizados sobre el estado del patrimonio, su valoración, depreciación y otros aspectos relevantes.

- Pasos a seguirse para la implementación;

1. Investigación y evaluación de diferentes soluciones informáticas;

2. Selección de la mejor de esas soluciones que se ajuste a las necesidades y presupuesto del INADI;

3. Capacitación del personal a cargo de utilizar y administrar el sistema y migración de los datos existentes, volcados en planillas de Excel.

ACCIÓN 7 (de mediano plazo): fortalecimiento tecnológico del Mapa Nacional de la Discriminación: tendiente a la generación de este tipo de informes con herramientas de probada utilidad.

- adquisición de licencias SPSS: de análisis estadístico avanzado, con algoritmos de machine learning, análisis textual, big data, entre otras funcionalidades;

- adquisición de licencias de Power BI: herramienta que permite visualizar y analizar datos de manera interactiva y compartir información en tiempo real, permitiendo recopilar datos de diversas fuentes, transformarlos y modelarlos y, luego, generar informes, paneles de control y visualizaciones interactivas;

- cursos de formación en R: lenguaje de programación de uso libre, útil para el análisis estadístico, visualización de datos, ciencia de datos y aprendizaje automático.

d. CIERRE

Esta DIRECCIÓN DE ADMINISTRACIÓN comprende la importancia estratégica que tiene una buena gestión en materia de Tecnologías de la Información y las Comunicaciones y, a partir de ello, se encuentra abocada a solucionar los problemas detectados gracias al relevamiento efectuado al comienzo de su gestión, cuyas conclusiones dieron lugar al Plan.

Las citadas conclusiones, se reitera, resultan convergentes con las del Informe de Auditoría. Partiendo del estado de situación oportunamente relevado, se ha elaborado un plan de acción de carácter integral que permite un abordaje global de los mentados problemas, mediante la concreción de un conjunto de acciones coordinadas de corto, mediano y largo plazo que, en definitiva, buscan poner en línea las Tecnologías de la Información y las Comunicaciones con las necesidades específicas de este Instituto Nacional, definidas en orden a su elevada misión institucional.-

Sin otro particular saluda atte.

Digitally signed by Gestion Documental Electronica
Date: 2023.06.06 15:00:19 -03:00

Noelia Carreño
Directora
Dirección de Administración
Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.06 15:00:20 -03:00

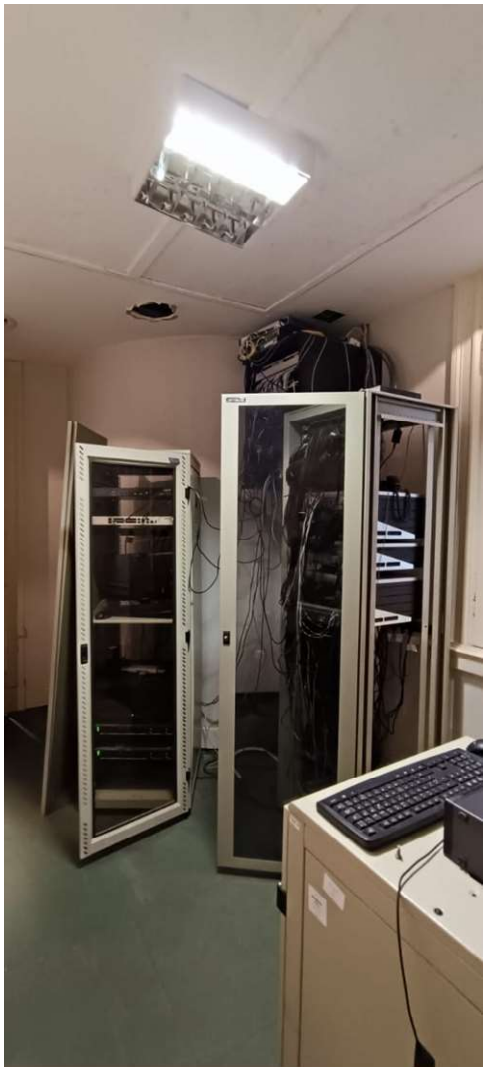
ANEXO II – Documentación fotográfica del hallazgo 4.3.1.[57]

1) Fotografías de la oficina destinada como Sala de Servidores:

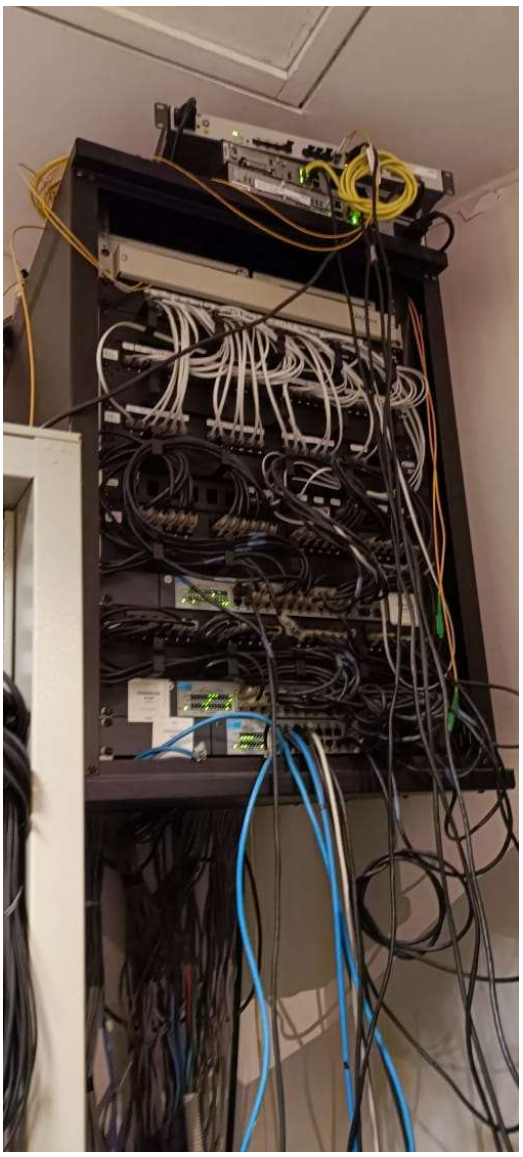
Fotografías N°1 y N°2 – Puertas de acceso a la Sala de Servidores

[57] Fotografías tomadas por el equipo de auditoría.

Fotografías N°3 y N°4 – Estado de las instalaciones en el interior de la Sala de Servidores



Fotografías N°5 y N°6 – Estado del cableado de red en los racks ubicados de la Sala



Fotografías de la oficina administrativa donde se encuentra alojado el servidor de la base de datos de denuncias:

Fotografías N°7 y N°8 – Ubicación del Servidor (PC) de la base de datos de denuncias


computer
kernel
Debian
basic
operating
system
programs
LG