Políticas de Seguridad de la Información Proveedores

Versión 1.0

Instituto Autárquico Provincial de Seguro (IAPS)

Revisión	Fecha	Descripción de la modificación	Causa de emisión o modificación
1.0	14/09/2021	Primera edición del documento corresponde a la versión 1.0 generada por la inclusión del Gestor Documental.	

Contenido

1. Política de Seguridad de la Información con Proveedores

1.1. Introducción

El Instituto Autárquico Provincial del Seguro, (en adelante "IAPS" o la "Organización") depende en forma crítica de la Información, las redes de comunicaciones y los sistemas de información implementados. La información tiene un rol preponderante en el inventario de activos de la empresa; siendo prioridad generar políticas, protocolos y procedimientos que ayuden a protegerla.

Todas las empresas, públicas o privadas, necesitan contratar servicios especializados externos que den soporte a parte de su actividad. Estas organizaciones acceden, administran, examinan o manipulan en alguna forma, información que el IAPS considera sensible. La gestión de los proveedores del IAPS, representa una actividad que requiere tercerizar un servicio para el logro de los objetivos de negocio, incrementando la productividad y mejorando los procesos por medio de estrategias que se proveen desde partes externas.

La complejidad de los sistemas de información actuales, la multiplicidad de conexiones y redes existentes y la sensibilidad de la información operada, hacen indispensable mantener el control sobre la seguridad de la información del IAPS, con el objetivo de preservar la Confidencialidad, Integridad y Disponibilidad de la misma, aun cuando esta esté siendo gestionada por terceros. Es necesario, entonces, exigir a los proveedores externos del IAPS que gestiona parte de la información sensible del organismo, cumplir con ciertas normas, directrices y prácticas de buen uso, detalladas en el presente documento.

1.2. Declaración de la Política

IAPS establecerá contratos de servicio y acuerdos de confidencialidad con Terceros Contratados y subcontratados (Proveedores) que por sus funciones requieran de acceso a información, infraestructura de la organización o de los clientes. Los proveedores serán responsables de definir de manera consensuada con el IAPS, implementar, mantener y revisar a intervalos planificados los controles de seguridad que permitan mitigar los riesgos derivados de la interacción entre dichos proveedores y el IAPS.

Los proveedores deberán hacer uso de las políticas de clasificación de la información para identificar, etiquetar y tratar la información de forma correcta. También deberán cumplir en todos los aspectos con la **Política de Seguridad de la Información** vigente del IAPS en todos los apartados que le sean referentes.

1.3. Objetivo de la Política

Es necesario establecer lineamientos que permitan el relacionamiento con los proveedores de acuerdo a los objetivos establecidos por los procesos de la organización, generando confianza entre las partes. Es objeto de la presente política establecer directrices y controles para proteger los Activos de Información y los Acuerdos de

Niveles de Servicios (ANS) con los proveedores del IAPS, en relación a la Confidencialidad, Integridad, Disponibilidad y Responsabilidad Legal de la Información. Esta protección debe contemplarse antes, durante y a la finalización del servicio contratado.

1.4. Alcance

Esta Política aplica a todos los proveedores y terceras partes vinculadas con IAPS según los ANS y Acuerdos de Confidencialidad establecidos entre las partes.

1.5. Términos y Definiciones

- **ANS:** Acuerdos de Niveles de Servicio o SLA (*Service Level Agreement*, SLA por sus siglas en inglés).
- **Análisis de Impacto al Negocio (BIA):** identificar los impactos asociados con la pérdida de los servicios o de la Gestión de los proveedores de IAPS, permitiendo obtener información para el desarrollo de los planes de restauración de los servicios de los procesos de Infraestructura física y tecnológica, soporte TIC y personal (Recurso Humano) ofrecidos a los clientes de IAPS.
- **Contingencia:** actividades de control que permite la continuidad de operaciones en eventos no programados que suspendan la funcionalidad del negocio.
- **Hosting:** servicio de alojamiento externo de recursos de Tecnologías de Información.
- **Intranet:** servicio corporativo interno.
- **Propietario de la información:** la persona responsable de la Confidencialidad, Integridad, y Disponibilidad de la información.
- **Proveedores vinculados:** todas aquellas terceras partes que tienen una relación comercial activa o lo vincule un acuerdo de cumplimiento previamente firmado luego de la terminación de la relación contractual.
- **Situación de crisis:** es la pérdida de control sobre las operaciones de Infraestructura física y tecnológica, Soporte TIC y Personal (Recurso Humano), por una falla inesperada o no programada de alguno de sus componentes en operación.
- **VPN:** Red Privada Virtual.

1.6. Disposiciones Generales

1. Esta Política se integra a la normativa básica de la empresa, incluyendo su difusión y las sanciones

correspondientes por incumplimiento de la misma.

2. El componente legal y las implicaciones del incumplimiento de la presente política serán analizados y ejecutados por el área Jurídica, Compras, Sistemas, la Alta Dirección, o cualquier responsable de administrar al proveedor.
3. Todo proveedor de servicios del IAPS que implique acceso o manejo de información considerada para el organismo como sensible deberá cumplir con la presente política.
4. El IAPS es consciente de la importancia de las buenas prácticas y acuerdos establecidos e implementados con los proveedores, dando cumplimiento mediante actividades de monitoreo, revisión y mejora continua para garantizar la satisfacción entre las partes.
5. Para asegurar que los proveedores que prestan servicios en el tratamiento de información propiedad de IAPS cuenten con estándares y niveles adecuados en materia de seguridad, IAPS se reserva el derecho de solicitar evidencia de la ejecución de auditorías independientes relacionadas a riesgo tecnológico, control interno, o auditorías de certificación relacionados con dicha materia, los que para cualquier efecto serán facilitados de manera temporal y con el objeto de revisar el alcance del trabajo realizado y el detalle de los resultados obtenidos.

1.7. Normas referentes

La presente política se basa en las buenas prácticas de seguridad de la información y toma como referencia las siguientes normas:

- ISO/IEC – 27001: sistema de Gestión de Seguridad de la Información publicado por La Organización Internacional de Normalización (ISO) y en especial su dominio “A.15.Relacion con los proveedores”.
- ISO/IEC – 27032: estándar de Ciberseguridad publicado por La Organización Internacional de Normalización (ISO). Ofrece orientación para fortalecer el estado de la Ciberseguridad en la organización, utilizando los puntos técnicos y estratégicos más importantes para esa actividad.
- ISO/IEC – 22301: Gestión de la continuidad del negocio. Gestión de los Proveedores.
- ISO/IEC – 20000: Gestión de los Servicios de TI.
- ISO/IEC – 27036: Seguridad de la información en las relaciones con los proveedores – Parte 1: Visión general y conceptos; Parte 2: Requisitos; Parte 3: Directrices para la seguridad en la cadena de suministro de las tecnologías de la información y la comunicación.

2. Cláusula: Notificaciones de Eventos de Seguridad

2.1. Introducción. Motivación

Cuando no constan procedimientos para reportar debilidades en la seguridad de la información, existe la posibilidad de que personal inexperto pueda intentar corregir una debilidad de la seguridad en programas de aplicación o sistemas operativos, lo cual podría interrumpir la continuidad de procesos críticos del negocio.

El atraso en darle inicio a las investigaciones pertinentes puede incrementar las pérdidas potenciales asociadas al incidente detectado.

Si el personal, propio, contratado o tercerizado, no está consciente de la importancia de reportar brechas potenciales de seguridad de la información, los incidentes podrían permanecer sin investigación por un período inaceptable. Esta política busca mitigar estos riesgos.

2.2. Definición de la Cláusula

La identificación de cualquier brecha o debilidad de la seguridad de la información se debe reportar inmediatamente a los responsables de tecnología y Seguridad de la Información a través de los canales y procesos definidos por la empresa con el objeto de proceder con la identificación de cualquier daño causado, efectuar cualquier restauración o reparación requerida además de facilitar la recopilación de cualquier evidencia asociada

2.3. Objetivo

Es objetivo de esta política identificar cualquier brecha de seguridad de la información que resulte o no de incidentes de seguridad cuyo último efecto es el daño o pérdida de datos de un sistema. El reporte oportuno de los errores, debilidades y vulnerabilidades es vital para tomar las acciones correctivas necesarias de acuerdo al caso.

2.4. Alcance

Esta política está dirigida al área Tecnología, Seguridad de la Información y a todos los empleados, contratados y proveedores de IAPS, quienes son corresponsables de velar por la seguridad de los activos de información de la organización.

2.5. Responsabilidades

Todo Director, Gerente, Empleado o proveedor del IAPS que tenga acceso a información, sistemas o cualquier recurso de la organización tiene la responsabilidad y obligación de notificar ante una brecha de seguridad descubierta o identificada.

3. Cláusula: Servicios asociados al tratamiento de la información

3.1. Introducción. Motivación

Las empresas contratadas para brindar servicios a IAPS se deben caracterizar por el cumplimiento de todas las normas, estándares y buenas prácticas existentes. Para los servicios tercerizados de infraestructura, plataforma tecnológica, procesamiento y almacenamiento de información física o digital y recursos humanos, IAPS verifica que el proveedor cuenta con mecanismos de protección y controles de seguridad de información adecuados al objeto del servicio contratado.

La organización debe validar todos estos requisitos antes de sellar una contratación, con el fin de salvaguardar la imagen institucional y los datos de todos sus clientes.

3.2. Definición de la Cláusula

En las situaciones en que se requiera contratar servicios de tratamiento o resguardo de activos de información, tales como servicios de hosting e infraestructura, plataforma tecnológica, centros de datos y procesamiento, almacenaje de información física o digital, entre otros, se deberá verificar que el proveedor cuenta con mecanismos y controles de seguridad adecuados, los que deberán tener, a lo menos, el mismo estándar que los existentes en IAPS.

Asimismo, en estas situaciones, se deberá realizar una evaluación de riesgos de seguridad asociados al servicio entregado por el proveedor, con la finalidad de identificar brechas que puedan ser potenciales vulnerabilidades que expongan la continuidad operativa de los procesos o puedan dañar la imagen Institucional, para lo cual el área requirente en conjunto con el resposansable de Seguridad de la Información, deberán realizar este análisis previo a la contratación del servicio o adquisición del producto.

Por su parte, para el caso en que existan proveedores que desarrollen sistemas de información para la Institución, se deberá considerar la revisión de los productos elaborados a partir de revisiones técnicas por parte del Departamento de Informática, Área de Desarrollo o quien corresponda.

Finalmente, en caso que los sistemas de información sean expuestos a la red de Internet, se deberá considerar además la ejecución de pruebas de seguridad que permitan garantizar razonablemente la Confidencialidad, Integridad y Disponibilidad de los datos manipulados en el sistema.

3.3. Objetivo

IAPS debe asegurarse que las terceras partes contratadas para el almacenamiento, administración, resguardo o cualquier otra tarea sobre información propia del organismo y/o de sus clientes, se trate de manera debida, siguiendo la legislación vigente.

3.4. Alcance

Esta política alcanza a todos los proveedores que sean contratados por IAPS en cuyas tareas estén involucrados servicios de tratamiento o resguardo de activos de información de cualquier tipo, tanto se tratare de acceso, administración, almacenamiento o consulta e indistintamente si se tratase de información corporativa o de los clientes de la compañía.

3.5. Responsabilidades

Todo proveedor del IAPS que tenga o trabaje con información de la organización o de sus clientes tiene la responsabilidad y obligación de seguir las pautas establecidas en la presente política.

4. Cláusula: Autorización y Entrega de Material Adicional

4.1. Introducción. Motivación

Por motivos de servicios, puede resultar que un proveedor contratado por IAPS requiera información, de la organización o de sus clientes, adicional a aquella establecida en los acuerdos contractuales, o que no sea inherente a la naturaleza del mismo. Se deben regular estos procedimientos y es objeto de esta política hacerlo.

4.2. Definición de la Cláusula

En cada ocasión en que un proveedor requiera información del IAPS, que sea adicional a aquella que el Servicio se ha obligado a entregar en virtud del contrato respectivo, o que no sea inherente a la naturaleza del mismo, el propietario de la información analizará los motivos de dicho requerimiento y procederá a aprobar o rechazar la entrega de la misma.

La solicitud de información adicional se hará según los procedimientos establecidos por IAPS, explicando las necesidades y motivos del nuevo requerimiento, y la aprobación o no de la misma será notificada al proveedor por parte del propietario de la información previa consulta al responsable de Sistemas y/o de Seguridad de la Información.

4.3. Objetivo

IAPS debe resguardar al máximo la información propia y de clientes. La organización establece el principio de mínimo privilegio y en consecuencia solo brinda acceso a la información requerida para realizar la tarea enmendada. El objetivo principal de esta política es mantener la confidencialidad de la información propia y de los clientes.

4.4. Alcance

Esta política alcanza a todos los proveedores y terceros que sean contratados por IAPS y que requieran mayores accesos o más cantidad de información que la acordada de manera inicial y pactada en el contrato.

4.5. Responsabilidades

Todo proveedor del IAPS que necesite mayor información que la acordada para cumplir su tarea, debe seguir los procedimientos desprendidos de la presente política. El propietario de la información, conjunto con el responsable de Sistemas y de Seguridad de la Información, deberán analizar la necesidad de acceso, la factibilidad y la correspondencia entre lo solicitado y la tarea enmendada antes de entregar lo solicitado por el proveedor.

5. Cláusula: Acceso Remoto a través de Herramientas Informáticas

5.1. Introducción. Motivación

Los proveedores de servicios informáticos contratados por IAPS necesitan acceder de manera remota a información, sistemas, aplicaciones, servicios o cualquier otro activo digital de la organización. Estos activos son vitales para el funcionamiento del IAPS, siendo necesario resguardar su acceso de manera debida.

5.2. Definición de la Cláusula

Los proveedores podrán acceder en forma remota a los activos tecnológicos a través de herramientas tales como Red Privada Virtual (VPN) y cualquier otro que IAPS defina, cuando ello fuere necesario para el cumplimiento de las obligaciones que emanan del contrato respectivo. En caso contrario, deberá solicitarse una autorización especial al propietario de la información, quien analizará los motivos de dicho requerimiento y procederá a otorgarla o denegarla.

En cualquier caso, dicho acceso será gestionado por el área de Sistemas de IAPS y sólo podrá tener por finalidad dar soporte a equipos tecnológicos o sistemas de información, revisar errores de funcionamiento o prestar servicios de seguridad y/o monitoreo. Para garantizar lo anterior, el Área de Sistemas deberá implementar controles que permitan limitar su acceso, registrar acciones para seguimiento y/o, supervisar visualmente el trabajo realizado.

Deberá existir un registro de los accesos que se han realizado a través de las herramientas señaladas en el párrafo primero de este apartado para efectos de trazabilidad y posterior revisión en caso de ser requerido.

5.3. Objetivo

IAPS debe resguardar al máximo la información propia y de clientes. Se debe generar registro de cada acceso interno o externo. Corresponde al IAPS especificar estándares para la conectividad remota de manera de salvaguardar la Confidencialidad, Integridad y Disponibilidad de la información propia y de terceros.

5.4. Alcance

Esta política alcanza a todos los proveedores, empleados y terceros que necesiten acceder de manera remota a servicios, equipos información o cualquier otro activo digital propiedad de IAPS o sus clientes.

5.5. Responsabilidades

Toda persona que necesite acceder de manera remota a los servicios del IAPS debe solicitar las credenciales al área Sistemas y/o Seguridad de la Información y este establecerá los permisos necesarios, siguiendo el concepto de mínimo privilegio.

El área de Seguridad de la Información será el encargado de velar por el cumplimiento de la presente política, asegurando que se lleven registro de los accesos y estos se otorguen de manera debida según lo acordado.

6. Cláusula: Acuerdos de Confidencialidad de la Información

6.1. Introducción. Motivación

La correcta gestión de la información, propia y de los clientes, es fundamental para proteger no solo la imagen Institucional, sino también los tres pilares fundamentales de la Seguridad de la Información que guían la presente política: Confidencialidad, Integridad y Disponibilidad. Los terceros que reciben la información pueden no tratarla de manera confidencial, dando por resultado que esta sea accedida por personas no autorizadas

Proteger activos confidenciales y vitales para la organización es uno de los objetivos principales que guían esa política.

6.2. Definición de la Cláusula

En los casos en que se requiera entregar información a proveedores, o que producto de la prestación del servicio acceda a información de IAPS o sus clientes, se deberán aplicar Acuerdos de Confidencialidad y No Divulgación (en inglés *Non-Disclosure Agreement* o NDA) entre Seguridad de la Información y los proveedores, los que deberán dar cuenta de los responsables, la información en cuestión, las medidas mínimas de seguridad aplicadas, la forma de proceder frente a incidentes, la extensión del acuerdo a terceros subcontratados, la propiedad de los productos desarrollados, el tiempo de vigencia del acuerdo, las sanciones frente a su incumplimiento y su aceptación formal.

En todo intercambio de información entre IAPS y los proveedores de servicios o productos, se deberán implementar estándares y procedimientos formales asociados al intercambio de información, que permitan garantizar razonablemente la seguridad en el acceso y la transferencia de información, considerando la aplicación de cifrado en las comunicaciones y la validación de identidad.

6.3. Objetivo

Mantener la información de los clientes como confidencial es un requisito legal y esencial para la credibilidad de la empresa.

La información, como activo crítico de la organización, debe ser protegido, y su acceso controlado. La presente política, basada en el privilegio de necesidad de conocer, busca regular el acceso e intercambio de la información por parte de los proveedores.

6.4. Alcance

Esta política alcanza a todos los proveedores que, con motivos de sus tareas, requieran acceso a información propiedad de IAPS o sus clientes.

6.5. Responsabilidades

El área de Sistemas y Seguridad de la Información es responsable de asegurar que cada uno de los proveedores de IAPS que requieran información de la institución o de sus clientes, basado en las tareas que realizan, tenga como premisa los principios de mínimo privilegio y necesidad de conocer. Aquellos que tienen bajo su responsabilidad la manipulación de activos de información críticos para la empresa, son también responsables de asegurar su manipulación bajo esquemas seguros.

Los proveedores que accedan a información del IAPS y/o de sus clientes son responsables del tratamiento de la misma, incluido su gestión y transferencia; debiendo cumplir las pautas establecidas en la presente política.

7. Cláusula: Acceso físico a los activos de información y equipos tecnológicos

7.1. Introducción. Motivación

El Centro de Datos (en inglés *Datacenter*) de la organización, en conjunto con los demás equipos y bienes tangibles que almacenan, transfieren o procesan información, conforman parte de la infraestructura crítica de IAPS y por lo tanto su acceso debe ser controlado y fiscalizado.

7.2. Definición de la Cláusula

El acceso físico por parte de los proveedores a los activos de información deberá ser controlado y supervisado por personal administrativo o técnico, según sea el caso, perteneciente al área de Sistemas de IAPS.

En las áreas protegidas o de alto riesgo, como es el caso de la sala de procesamiento de datos, se deberán establecer procedimientos documentados formales que tengan por objeto gestionar la forma en que se realizarán los trabajos en su interior, el que deberá contar con medidas de registro de proveedores, como también controles detectivos y preventivos; además de establecer normas que tengan por objeto gestionar la forma en que se realizarán los trabajos en su interior, y restricciones de acceso preventivas, como el lector de tarjeta o biométrico para el ingreso a la instalación.

7.3. Objetivo

El Datacenter, como centro crítico para el almacenamiento, procesamiento y resguardo de datos e información de IAPS debe ser protegido contra accesos no deseados. Es objetivo de la presente política gestionar de manera adecuada los accesos físicos por parte de terceros a los centros de procesamiento de información, considerados críticos para IAPS.

7.4. Alcance

Esta política alcanza a todos los proveedores que, con motivos de sus tareas, requieran acceso al Datacenter, a la sala de procesamiento de datos o a cualquier otro bien de carácter informático de IAPS.

7.5. Responsabilidades

El área de Soporte de Sistemas será la encargada de controlar el acceso a empleados y terceros por medio de controles de acceso, que dependen de la finalidad de la prestación del servicio o de una visita programada.

Todos los proveedores contratados por IAPS que deseen acceder al Datacenter de la organización deberán cumplir todos los procedimientos desprendidos de la presente política y cualquier otro control adicional que Seguridad de la Información disponga.

8. Cláusula: Gestión de Incidentes de Seguridad

8.1. Introducción. Motivación

Un proceso de respuesta y gestión en caso de incidentes contribuye a garantizar que estos se contengan rápidamente y a evitar tener que remitirlos a instancias superiores.

8.2. Definición de la Cláusula

Para los proveedores que tengan relación con almacenamiento, comunicación, infraestructura, plataforma o software que sean entregados a IAPS en modalidad de servicio, (también conocidos como SaaS, IaaS, PaaS) además de los equipos tecnológicos que sean adquiridos o sistemas de información que sean desarrollados por terceros y sobre los cuales existan garantías del fabricante, se deberán establecer y documentar procedimientos para la gestión de incidentes de seguridad, los que deberán ser gestionados a través de la mesa de servicios bajo los procedimientos internos ya definidos.

Los procedimientos para la gestión de incidentes que estén relacionados con proveedores, en los términos referidos en el párrafo anterior, deberán ser comunicados y formalizados entre las partes. Asimismo el área de Sistemas y/o Seguridad de la Información, podrá solicitar informes relacionados con las mediciones de incidentes de algún período en particular, información que deberá estar disponible durante lo que dure la relación entre el proveedor y IAPS.

El procedimiento de seguridad para la gestión de incidentes en cada caso deberá señalar, a lo menos, la persona de contacto, así como el número telefónico y/o correo electrónico al cual habrá que dirigir las solicitudes deberá contemplar:

- La comunicación inmediata al Área de Sistemas sobre infracciones relacionadas con datos y los incidentes de seguridad que hayan afectado o se hayan dirigido a los activos y/o servicios prestados a IAPS.
- Acceso a información actualizada sobre los progresos realizados con las medidas correctivas.
- Plan de reparación (acción, persona responsable y fecha de entrega) donde se incluyan las medidas correctivas a emprender en caso de que se produzca un incidente. Este plan se pondrá en conocimiento de IAPS.

8.3. Objetivo

Es necesario establecer y gestionar un proceso de respuesta a incidentes para tratar y notificar de forma oportuna y periódica los incidentes que afecten a la información de IAPS y/o a los servicios utilizados por la organización.

Esta política tiene como objetivo generar estándares mínimos de reporte, planes de reparación y acceso a estado de incidentes de cada uno de los proveedores contratados por IAPS de manera de proteger la Confidencialidad, Integridad y Disponibilidad de la información propia y de los clientes.

8.4. Alcance

Esta política alcanza a todos los proveedores que hayan sido contratados por IAPS para brindar servicios relacionados al almacenamiento, infraestructura, plataforma o software que sean entregados a IAPS en modalidad de servicio.

8.5. Responsabilidades

Todo proveedor contratado por IAPS que brinde alguno de los servicios alcanzados por la presente política debe contar con procedimientos acordes a los establecidos. El área de Seguridad de la Información es responsable de asegurarse que cada uno de los proveedores de IAPS cuenten con procedimientos conformes a la presente política.

9. Cláusula: Gobernanza de riesgos. Posibilidad de inspeccionar y auditar las condiciones del servicio

9.1. Introducción. Motivación

Los servicios tercerizados por IAPS, en relación a tecnología, almacenamiento de información, software o cualquier otro activo tecnológico, son factibles de ser atacados o dañados. Esta posibilidad se amplía de manera exponencial en la medida que el proveedor no cumpla con estándares en materia de Seguridad de la Información, pudiendo dañar la imagen institucional de IAPS y poniendo en peligro la Confidencialidad, Integridad y Disponibilidad de la información propia de la organización y sus clientes.

De no aplicarse este control, los proveedores de IAPS podrían no ser capaces de demostrar y no disponer de una supervisión adecuada de la Seguridad de Ia Información.

Las normas y las políticas documentadas son elementos cruciales de la gobernanza y la gestión de riesgos, ya que definen la perspectiva de la dirección sobre los controles necesarios para gestionarlo.

9.2. Definición de la Cláusula

El proveedor dispondrá de procesos de gobernanza para los riesgos de seguridad de la información/ciberseguridad que garanticen el conocimiento de su entorno tecnológico y del estado de los controles de seguridad de la información/ciberseguridad, así como de un programa de seguridad para proteger al proveedor contra ataques a la seguridad de la información o ciberataques, con arreglo a los códigos de prácticas recomendadas del sector (por ejemplo, NIST, SANS, ISO 27001 e ISO 27032).

Para asegurar que los proveedores que prestan servicios cuenten con estándares de industria en materia de seguridad, IAPS se reserva el derecho de solicitar evidencia de la ejecución de auditorías independientes relacionadas al riesgo tecnológico, control interno, o auditorías de certificación relacionados con dicha materia, los cuales deben ser facilitados de manera confidencial y con el objeto de revisar el alcance del trabajo realizado y el detalle de los resultados obtenidos.

Adicionalmente, IAPS también podrá realizar visitas programadas y supervisadas a las instalaciones de los proveedores, específicamente aquellos que presten servicios de resguardo de activos de información, esto con el objeto de verificar en campo las condiciones de seguridad implementadas, todo esto coordinado con anterioridad. El proveedor también permitirá a IAPS o quien esta designe en su representación a realizar una inspección inmediatamente después de un incidente de seguridad.

Todo incumplimiento de controles identificado por IAPS durante una inspección se someterá a una evaluación de riesgos por parte de la organización y este especificará un plazo para que se corrija. El proveedor se encargará

entonces de implantar cualquier medida correctiva que sea necesaria en el plazo establecido. El proveedor prestará a IAPS toda la asistencia necesaria durante una inspección.

9.3. Objetivo

Es objetivo de la presente política asegurar por parte de IAPS que los servicios contratados a terceros tratan de manera correcta la información, su resguardo y su procesamiento; siguiendo estándares de la industria que ayuden a disminuir las posibilidades de sufrir ataques de cualquier tipo.

9.4. Alcance

Todos los proveedores que presenten servicios tecnológicos al IAPS; fundamentalmente aquellos que sean referidos al almacenamiento, procesamiento o gestión de la información, incluidos aquellos que brindan soluciones de tipo SaaS, PaaS o IaaS, están alcanzados por la presente política.

9.5. Responsabilidades

El área de Seguridad de la Información acordará con los proveedores las visitas programadas y es quien definirá si el mismo cumple los estándares en materia de Seguridad de la Información; elaborando los informes correspondientes.

El proveedor contratado por IAPS tiene la responsabilidad de gestionar de manera adecuada los activos propiedad de IAPS y sus clientes; tomando las medidas se seguridad acorde a los estándares demandados por la industria. El proveedor se compromete a realizar las mejoras propuestas por IAPS, que deberán estar basadas en mejores prácticas y estándares conocidos.

10. Cláusula: Acuerdos de Niveles de Servicios (ANS) y planes de recuperación

10.1.Introducción. Motivación

Los servicios tercerizados por IAPS deben mantener un adecuado nivel de servicio (ANS), ya que representan actividades, tareas o servicios que brinda la institución y que esta, por cuestiones de actividad, económica o procedimental decide tercerizar. Los servicios que se brindan, sean propios o hayan sido encargados a terceras partes, forman parte de la imagen institucional que debe mantenerse.

10.2.Definición de la Cláusula

IAPS considera relevante mantener la disponibilidad permanente de los servicios entregados por los proveedores, para lo cual se deberán establecer acuerdos de niveles de servicio que permitan garantizar razonablemente este principio, los que deberán ser formalizados a través de bases de licitación, actos administrativos o acuerdos complementarios, siendo estos medidos y monitoreados permanentemente.

Para el caso de los servicios relacionados con Tecnología, se considerarán como criterios relevantes relacionados con el nivel de servicio la entrega continua del mismo, los tiempos de respuesta de atención para su entrega, los tiempos de resolución de problemas, entre otros, los que serán aplicados por el área respectiva que solicita el servicio y asesorados por el departamento técnico de la Institución.

El área requirente del servicio, conjuntamente con el área de Sistemas y Seguridad de la Información, deberán verificar la existencia de planes de contingencia para efectos de validar que estos cumplen de buena forma con el criterio de disponibilidad del servicio y los datos.

En la medida que el área requirente necesite información detallada del servicio o sus equipos, podrá solicitar un informe sobre la disponibilidad del servicio dentro de un período determinado, incluyendo el rendimiento de los equipos en caso que se haya sido acordado previamente entre las partes.

10.3.Objetivo

Los servicios brindados por IAPS, ya sean propios o tercerizados, deben mantener un adecuado nivel de servicio para no afectar la continuidad del negocio y la imagen institucional; esta política tiene como objetivo generar los lineamientos para salvaguardar ambas.

10.4.Alcance

Todos los proveedores que sean contratados para brindar un servicio referente a tecnología, incluidas plataformas de servicios, conectividad, infraestructura o cualquier otro relacionado a sistemas e informática deben cumplir con adecuados niveles de servicio y tener planes de recuperación, por lo que se encuentran alcanzados por la presente política.

10.5.Responsabilidades

El área de Sistemas será el encargado de validar que las empresas contratadas cuenten con ANS y planes de recuperación acordes a los demandados por el objeto de negocio, asegurándose que cumplen con los requisitos, salvaguardando la imagen institucional de IAPS.

El área de Seguridad de la Información podrá auditar, en conjunto con el área de Sistemas, estos ANS y planes de contingencia y recuperación para determinar si efectivamente cumplen con lo requerido.

Los proveedores contratados por IAPS deberán tomar todas las medidas necesarias para cumplir con los ANS acordados con la institución.