POLITICA DE SEGURIDAD DE LA INFORMACION DE LA SOCIEDAD
LADFI CONSULTING LATAM S.A.S

INTRODUCCIÓN

La sociedad **LADFI CONSULTING LATAM S.A.S** en adelante (**LADFI**), se establece la siguiente política que regula el manejo de la información en **LADFI**, orientada a definir las medidas que resguarden la confidencialidad, integridad y disponibilidad de la información propia de la organización, el acceso a la información en conformidad con la constitución, las leyes, y demás normas jurídicas, así como asegurar la continuidad de los servicios que le son propios.

Es por ello por lo que la misma asume la responsabilidad de implantar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (**SGSI**), de manera tal de garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Para tal fin, se establece una Política de la Seguridad de la Información, como marco de trabajo de la organización en lo referente al uso adecuado de los recursos, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

OBJETIVOS

Este documento formaliza el compromiso de la dirección frente a la gestión de la seguridad de la información y presenta de forma escrita a los usuarios de sistemas de información el compendio de acciones con las cuales la **LADFI** establece las normas para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos de la Empresa, los cuales están en constante cambio y evolución de acuerdo con el avance de la tecnología y los requerimientos de la Entidad.

El presente documento define los lineamientos que debe seguir **LADFI** con relación a la seguridad de la Información. Estos lineamientos están escritos en forma de políticas.

ALCANCE

Esta política se aplica a todo el personal interno de **LADFI**, bien sea por contrata u honorarios, y también al personal externo que preste o prestare servicios, remunerados o no, a **LADFI** ya sean integrantes de las diferentes comisiones o comités que tienen acceso privilegiado a la información.

También es aplicable a todo activo de información que la organización posea en la actualidad o en el futuro, de manera que la no inclusión explícita en el presente documento no constituye argumento para no proteger estos activos de información. La política cubre toda la información, entre otros, la impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, o hablada en una conversación. La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado y conocido por toda la organización basándose en metodologías de mejoramiento continuo.

DEFINICIONES

- **Información:** La información es la interpretación que se da a un conjunto de datos, pudiendo residir esta en medios electromagnéticos, físicos o en el conocimiento de las personas. En el caso de la presente política, se entenderá como información a toda forma proveniente de datos relacionados con los procesos de negocio de la Comisión Nacional de Investigación Científica y Tecnológica, así como antecedentes proporcionados tanto por los usuarios internos como los externos, siempre que sea dentro del contexto del ejercicio de sus funciones y del cumplimiento de sus obligaciones.

- **Información Pública:** Toda aquella información no catalogada como secreta o reservada, tal como lo establece el ordenamiento jurídico vigente.

- **Información reservada:** (conocimiento reservado): son aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter, cuando la naturaleza misma de la información requiera ser tratada de manera reservada.

- **La información secreta (solamente a quien le atañe la información debe conocerlo):** Son aquellos documentos cuyo conocimiento está circunscrito a las autoridades o personas a las que vayan dirigidos y a quienes deban intervenir en su estudio y resolución, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter. Una norma que establece restricciones claras es la ley de datos personales.

- **Seguridad de la Información:** Es el nivel de confianza que la organización desea tener de su capacidad para preservar la confidencialidad, integridad y disponibilidad de la información. Tiene como objetivo proteger el recurso información de una amplia gama de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el daño y, cumplir su misión y objetivos estratégicos.

- **Confidencialidad:** Es asegurar que la información es accesible sólo para las personas autorizadas para ello.

- **Integridad:** Es salvaguardar la exactitud y totalidad de la información en su procesamiento, transmisión y almacenamiento.

- **Disponibilidad:** Es asegurar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando estos sean requeridos.

- **Buen uso:** Se entiende por "buen uso" de los activos de información de la organización, a las expectativas que **LADFI** tiene con respecto al cuidado que su personal debe tener con los activos que la organización les entregue para el desempeño de sus funciones.

- **Personal:** Es toda persona a la cual se le concede autorización para acceder a la información y a los sistemas de **LADFI**. El personal puede ser interno o externo a la organización.

- **Supervisor:** Es toda persona encargada de un grupo de personas, área, división, programa o departamento en **LADFI**.

- **Tercero:** Se refiere a empresas prestadoras de servicios, las empresas contratistas, subcontratistas y cualquiera que, por cuenta propia o de terceros, desarrolle trabajos para o por cuenta de **LADFI**.

- **Responsable de la Información:** Es el usuario a cargo de la información y de los procesos que la manipulan sean estos manuales, mecánicos o electrónicos.

- **Encargado de Seguridad:** Es la persona que la autoridad máxima del servicio designa para la definición, diseño, implementación y supervisión de las medidas de seguridad de la información.

- **Comité de Seguridad:** es el equipo conformado por supervisores que representan a las áreas de la organización, responsable de la toma de decisiones en temas de la seguridad de la información.

- **Activo de Información:** Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.

Frente a los activos podemos distinguir 3 tipos de activos:

a) La Información propiamente dicha, en sus múltiples formatos (papel o digital, texto, imagen, audio, video, etc.).
b) Los Equipos/Sistemas que la soportan.
c) Las Personas que la utilizan.

Los activos poseen valor para la organización, y necesitan por tanto ser protegidos adecuadamente, para que el "negocio" no se vea perjudicado (implica detectar vulnerabilidades y establecer controles).

RESPONSABILIDADES Y CUMPLIMIENTO

➢ RESPONSABILIDADES

Director Ejecutivo de LADFI: En su calidad de tal, responde ante la sociedad por la existencia y cumplimiento de las medidas que mantengan un nivel de seguridad de la información acorde con el rol de la organización y los recursos disponibles.

Encargado de Seguridad: Es el principal responsable en la definición de los criterios de seguridad de la información en **LADFI**, para lo cual deberá analizar periódicamente el nivel de riesgo existente, proponiendo soluciones. Una vez autorizada la implementación de las medidas, deberá coordinar con quienes corresponda su materialización oportuna y correcta.

Responsable del Documento: tiene que mantener la aplicabilidad de este documento acorde a las prácticas operacionales de **LADFI**, por lo que es responsable de generar las modificaciones necesarias para que esté siempre actualizado. Además es responsable de publicar y dar a conocer nuevas versiones del documento.

Personal de LADFI: tiene la responsabilidad de cumplir con lo formalizado en este documento y aplicarlo en su entorno laboral. Además, tiene la obligación de alertar de manera oportuna y adecuada, según lo determine la política de manejo de incidentes, cualquier incidente que atente contra la seguridad de la información.

➢ CUMPLIMIENTO

La presente Política de Seguridad de la Información entra en vigencia una vez oficializada por el Director Ejecutivo de **LADFI**, y las demás áreas y dependencias de **LADFI** serán responsables de ponerlas en conocimiento de su personal subordinado.

Para el caso del personal que se contrate con posterioridad a la fecha de publicación, se le deberá entregar una copia del presente documento y hacer firmar una declaración de toma de conocimiento y aceptación de la misma.

La presente política está alineada con las directrices de las leyes y regulaciones existentes. Cualquier conflicto con estas regulaciones debe ser informado inmediatamente al responsable de este documento.

POLÍTICA

A. REQUISITOS SOBRE EL CONTROL DEL ACCESO

Todos los colaboradores y contratistas activos de **LADFI** deben tener una cuenta institucional asociada a los servicios que **LADFI** considere debe tener de acuerdo con su perfil, ejemplo: directorio activo, correo electrónico, Visión WEB, etc.

La cuenta institucional debe ser el identificador único de cada usuario mientras esté activo en la organización, en caso contrario, esta cuenta debe deshabilitarse junto con los servicios que tenga asociados.

Las personas que posean una cuenta institucional estarán obligadas a leer y entender las políticas de seguridad, aplicables y vigentes de la organización.

Algunos servicios podrán tener otros métodos de acceso diferente a la cuenta institucional en cuyo caso, los administradores de estos aplicativos deberán cumplir las disposiciones de seguridad vigentes.
Todos los activos de información deben asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados.

Los administradores de los activos de información deberán establecer los procedimientos formales para controlar la asignación de derechos o cuentas de acceso. Estos procedimientos deben comprender todas las fases del ciclo de vida de los datos, teniendo correspondencia con el ciclo de vida de acceso al usuario.

B. DE LA INFORMACIÓN INTERNA

La información es un activo vital y todos sus accesos, usos y procesamiento, deberán ser consistentes con las políticas y estándares emitidos por **LADFI** en cada ámbito en particular. La información debe ser protegida, por sus custodios, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas específicas de seguridad de la información, sus procedimientos asociados y en las recomendaciones dadas por el responsable designado de dicha información. Para ello, la Dirección de **LADFI** deberá proveer los recursos que permitan implementar los controles necesarios para otorgar el nivel de protección correspondiente al valor de los activos.

Toda la información creada o procesada por la organización debe ser considerada como “Pública”, a menos que se determine otro nivel de clasificación, pudiendo ser “Reservada” o “Secreta” de acuerdo con lo establecido en el ordenamiento jurídico vigente. Periódicamente se deberá revisar la clasificación, con el propósito de mantenerla o modificarla según se estime apropiado.

LADFI proveerá los mecanismos para que la información sea accedida y utilizada por el personal que de acuerdo a sus funciones así lo requiera. Sin embargo, se reserva el derecho de revocar al personal, el privilegio de acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameriten.

C. DE LA INFORMACIÓN DE LOS USUARIOS EXTERNOS

Si la institución procesa y mantiene información de usuarios externos que sean datos personales y/o sensibles de acuerdo a la normativa vigente, la organización se compromete a asegurar que esta información no será divulgada sin previa autorización y estará protegida de igual manera que la información interna. En el caso que la información de usuarios externos que se procese y mantenga y que no tenga las características anteriormente mencionadas, esta podrá ser divulgada sin previa autorización. Si se requiere compartir información de los usuarios externos de **LADFI** con instituciones externas, con motivo de externalizar servicios, a éstas se le exigirá la firma de un contrato de confidencialidad y no divulgación previo a la entrega de la información.

D. DE LAS AUDITORÍAS

Con el fin de velar por el correcto uso de los activos de información de su propiedad, **LADFI** se reserva el derecho de auditar en todo momento y sin previo aviso, el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los activos de información.

LADFI se reserva el derecho de tomar medidas administrativas en contra del personal que no dé cumplimiento a lo dispuesto en la presente política, las políticas específicas que se deriven y en su documentación de referencia, acciones que pueden ser solicitadas por el responsable de Recursos Humanos o el Encargado de Seguridad.

E. DEL COMPROMISO DE LA DIRECCIÓN DEL SERVICIO

La Dirección del Servicio velará por la existencia de un plan formal de difusión de esta política y las políticas específicas que la sustenten. La Dirección del Servicio, mediante la estructura que se defina en la política específica “Aspectos Organizativos de la Seguridad de la Información”, procurará que todo el personal reciba un entrenamiento suficiente en materia de seguridad, consistente con sus necesidades y su rol dentro de **LADFI**.

La Dirección del Servicio propiciará la existencia de mecanismos o procedimientos formales que permitan asegurar la continuidad del negocio ante situaciones que impidan el acceso a la información imprescindible para el funcionamiento de la organización.

F. DEBERES DEL PERSONAL Y USO DE MEDIOS ELECTRONICOS

La información y las tecnologías de información deben ser usadas sólo para propósitos relacionados con el servicio y autorizados por los supervisores, debiéndose aplicar criterios de buen uso en su utilización. Las claves de acceso a la información y a las tecnologías de información son individuales, intransferibles y de responsabilidad única de su propietario.

El personal está en la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política según procedimientos establecido en el manejo de incidentes.

Está absolutamente prohibido al personal de la organización divulgar cualquier información que según el ordenamiento jurídico esté catalogada como "Reservada" o "Secreta", Organización y Mantención de las Políticas.

Con el objetivo de garantizar el cumplimiento de la Política General de Seguridad de la Información y las políticas específicas que se definan posteriormente, **LADFI** ha establecido una estructura organizacional de seguridad que contempla la definición de funciones específicas en el ámbito de seguridad, las cuales serán ejecutadas por un Comité de Seguridad y un Responsable de Seguridad.

Las características de esta instancia organizacional y roles se detallan en el documento Política Específica

- Aspectos Organizativos de la Seguridad de la Información.

G. GENERALIDADES SOBRE EL PERSONAL PARA EL USO DE MEDIOS ELECTRONICOS

- **Prohibición de uso de Internet para propósitos personales.**

Para los funcionarios que atienden los registros públicos, el uso de Internet está ceñido a las páginas requeridas para realizar los trámites de registro, es de anotar que cualquier otro tipo de consulta está prohibida. Los usuarios de Internet deben ser advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas, de ser el caso.

- **Formalidad del correo electrónico.**

Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto podrá ser supervisada por el superior inmediato del empleado.

- **Preferencia por el uso del correo electrónico.**

Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.

- **Uso de correo electrónico**.

La cuenta de correo asignada es de carácter individual por lo cual ningún empleado bajo ninguna circunstancia debe usar la cuenta de otro empleado.

- **Revisión del correo electrónico.**

Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo al menos tres veces diarias. Así mismo, es su responsabilidad mantener espacio libre en el buzón.

.

- **Mensajes prohibidos.**

Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o personales o en beneficio de terceros o que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.

- **Acciones para frenar el SPAM.**

En el caso de recibir un correo no deseado y no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente al área de sistemas.

- **Todo buzón de correo debe tener un responsable.**

Todo buzón de correo asignado debe tener una persona responsable de su administración, incluidos los buzones de las aplicaciones.

- **Enviando software e información sensible a través de Internet.**

Software e información sensible de la **LADFI** que requiera ser enviado por Internet debe transmitirse con la mayor seguridad posible acordada entre las partes.

- **Intercambio de información a través de Internet.**

La información interna puede ser intercambiada a través de Internet pero exclusivamente para propósitos laborales, con la debida aprobación y usando los mecanismos de seguridad apropiados.

H. MANEJO DE LA INFORMACION FISICA

- **Reporte de pérdida o robo de identificación.**

Todo empleado debe reportar con la mayor brevedad, cualquier sospecha de pérdida o robo de carnés de identificación y tarjetas de acceso físico a las instalaciones.

- **Orden de salida para equipos electrónicos.**

Ningún equipo electrónico podrá salir de las instalaciones de la empresa **LADFI** sin una orden de salida otorgada por el personal adecuado o sin haber sido registrado en el momento de su ingreso.

- **Orden de salida de activos.**

Todos los activos que afecten la seguridad de la información de la sociedad **LADFI** como medios de almacenamiento, CDs, DVDs., USB entre otros, y que necesiten ser retirados de la empresa, deben tener la autorización escrita de salida.

Cuando se da una terminación laboral, los privilegios de acceso a las sedes de la **LADFI** deben ser revocados.

Cuando exista una terminación laboral, el usuario deberá devolver los objetos de acceso físico a las instalaciones (carnés, tarjetas de acceso, etc.) y a su vez todos sus privilegios de acceso deberán ser revocados.

I. COPIAS DE RESPALDO DE INFORMACIÓN (BACKUP):

Como método de seguridad para el mantenimiento de la información y la procura en evitar la pérdida de la misma, se definen las siguientes:

- Se debe contar con un sistema automático para la recolección de copias de respaldo.
- Las copias de respaldo deben tener el mismo nivel de protección de la información que poseen en su fuente original.
- Los medios magnéticos que contienen información deben ser almacenados en lugares físicamente seguros.
- Los usuarios responsables por respaldar la información también son responsables de facilitar la oportuna restauración de la información.
- Los medios magnéticos deben tener rótulos visibles y legibles tanto internos como externos.
- Se debe mantener suficientes respaldos de la información para que en caso de contingencia se pueda recuperar la información oportunamente.
- Para responder adecuadamente a una contingencia, los respaldos de la información se deben almacenar en sitios externos.

- Cualquier medio magnético que contenga información clasificada como restringida o confidencial, debe estar claramente identificada.
- Al enviar información clasificada como restringida o confidencial a terceros se debe exigir un acuse de recibo.
- Todos los medios que contengan información clasificada como restringida o confidencial y que finalice su ciclo de vida, deben ser sobre escritos destruidos físicamente para que la información no pueda ser recuperada.

J. DE LOS INCIDENTES FRENTE A LA SEGURIDAD

Todo incidente de seguridad en los activos de información en los que estén involucrados funcionarios podrá ser investigado por **LADFI** de acuerdo con los procedimientos establecidos, con el fin de determinar responsabilidades e imponer las sanciones previstas en la normatividad a este respecto, para ello contará con el apoyo técnico del Oficial de Seguridad de la Información.

En los incidentes de seguridad de la información en los que estén involucrados terceras partes, que sean reportadas al Oficial de Seguridad de la Información, serán informadas por éste, de forma inmediata, el que a su vez informará a la Oficina Jurídica para el inicio de las acciones judiciales pertinentes.

K. ENCARGADO DE LA SEGURIDAD DE LA INFORMACIÓN

El Coordinador de Sistema es el encargado de la Seguridad de la Información y tendrán las siguientes funciones:

a) Identificar y satisfacer las necesidades de capacitación en temas de seguridad de la información a los funcionarios de **LADFI**.
b) Actualización y seguimiento periódico a los riesgos de **LADFI**, validando con cada proyecto que se tomando siempre como base esta política para cualquier proyecto nuevo que se implemente.
c) Dirigir el programa de manejo y seguimiento de incidente.
d) Crear y establecer una metodología de clasificación de la información según su importancia e impacto dentro de **LADFI**.
e) Revisión y valoración de la Política de Seguridad de la Información.
f) Crear y mantener un Programa de Concienciación en seguridad de la información.
g) Seguimiento a la aplicación de las políticas, programas y planes adoptados para la protección de los sistemas, recursos informáticos y servidores de la Red Interna y Cómputo de **LADFI**.

L. DIFUSIÓN DE LA POLÍTICA

Resulta clave para que la presente política se integre en la cultura organizacional, la existencia de un plan formal de difusión, capacitación y sensibilización en torno a la seguridad de la información.

El Director Ejecutivo de **LADFI** será el responsable de la existencia permanente y el cumplimiento de un plan formal de difusión, capacitación y sensibilización de la seguridad de la información.

El Encargado de Seguridad de la información es el responsable de la ejecución del plan y el cumplimiento de sus objetivos, así como la existencia de un plan comunicacional que lo complemente.

M. MANTENCIÓN DE LA POLÍTICA

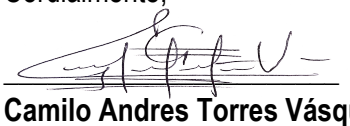
- La mantención de la presente política será realizada por el Encargado de Seguridad de la Información y sus cambios aprobados por el Director Ejecutivo de **LADFI**.
- Las políticas específicas asociadas a la presente política general deberán ser aprobadas por el Director Ejecutivo de **LADFI**. Los procedimientos asociados serán aprobados por el Director Ejecutivo mediante resolución exenta.
- El presente documento debe ser revisado a lo menos 1 vez al año y actualizado cada vez que se realicen cambios relevantes en la sociedad **LADFI** que afecten la adecuada protección de la información, considerando como tales entre otros, cambios en la misión, objetivos estratégicos, productos estratégicos, infraestructura, personal y/o procedimientos relacionados con la protección de la información.
- El Director Ejecutivo solicitará al área de comunicaciones interna que difunda la política dependiendo del alcance de la misma y su importancia para el negocio.

N. DOCUMENTACIÓN DE REFERENCIA

El presente documento constituye una política adecuada a la Ley, destinada a normar los aspectos más relevantes de la gestión de seguridad de la información, con una vigencia de largo plazo, por lo cual la Dirección promulgará documentos adicionales que explicitan en mayor detalle las medidas de seguridad de alto nivel dispuestas en el presente documento.

Fecha de actualización: veintiséis (26) de septiembre de 2022.

Cordialmente,



Camilo Andres Torres Vásquez
Representante Legal
LADFI CONSULTING LATAM S.A.S