Política de uso de sistemas informáticos

1. Objetivos

La presente política, en el marco de la Ley de Delitos Económicos, tiene por objetivo establecer los lineamientos y regulaciones para el manejo de los recursos informáticos y la información de Latin America Power S.A. y de todas las sociedades que conforman el grupo, señaladas en el Modelo de Prevención de Delitos (en adelante también "LAP" o la "Compañía"). Se busca definir las medidas que salvaguarden la Confidencialidad, así como la continuidad operativa de sistemas y activos digitales de la Compañía, incluidos los documentos y archivos sensibles, y para prevenir intentos de ataques cibernéticos desde los equipos de LAP, estableciendo las medidas y controles necesarios para ello.

Estas medidas tienen como objetivo prevenir filtración, pérdida, destrucción, acceso no autorizado, ataques cibernéticos y cualquier forma de mal uso de los activos informáticos.

En definitiva, el propósito de esta política es prevenir y evitar cualquier situación que pueda resultar en una violación de la normativa legal vigente, especialmente en lo establecido en la Ley N°20.393 sobre la responsabilidad penal de la persona jurídica (en adelante la "Ley"), incluidas las modificaciones introducidas por la Ley N°21.595 sobre Delitos Económicos.

2. Alcance

Lo establecido en este documento es aplicable a todos los directores, altos ejecutivos, miembros de la administración, dueños, accionistas, controladores y Trabajadores (en adelante los "Colaboradores") o cualquier persona que realice actividades de dirección y supervisión en LAP y sus sociedades, o represente sus intereses ante terceros, cuando el contenido de la presente política le sea aplicable en lo que corresponda.

En particular, y sin que el listado sea taxativo, la presente política aplica a las siguientes sociedades de la Compañía, a saber: Latin America Power S.A. y las sociedades Nehuén SpA, Pirita SpA, Empresa Eléctrica Carén S.A., Transmisora Valle Allipen S.A. y Transmisora Pitrufquén S.A. Adicionalmente, será aplicable a sociedades que pueda formar parte de la Compañía en un futuro.

Por su parte, LAP promoverá que sus contratistas, proveedores, prestadores de servicios, Colaboradores, asesores y clientes, la adopción de pautas de conducta consistentes con las que se definen en esta política y adoptará medidas para mantener relación sólo con aquellos que estén alineados con los objetivos de la Compañía.

3. Definiciones

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

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

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

- **Información**: La Información es la interpretación que se da a un conjunto de datos, pudiendo residir está 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, 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 de Identificación Personal ("PII")**: Cualquier dato que pueda identificar potencialmente a un individuo específico, como nombre, correo electrónico, Información financiera, número de seguro social, número de pasaporte, etc.

- **Seguridad de la Información**: Procesos y metodologías diseñados e implementados para proteger la Información, para así mantener 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.

4. Responsabilidad

- **Encargado de Prevención de Delitos**: Colaborador designado por la Administración de LAP para gestionar el Modelo de Prevención de Delitos, su diseño, implementación, actualización, control y cumplimiento.

- **Jefe de Tecnología**: Quien velará 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.

- **Equipo de Tecnologías de la Información (TI):** Área responsable de gestionar, mantener, procesar y resguardar los sistemas de seguridad de LAP.

- **Personal**: Es toda persona a la cual se le concede autorización para acceder a la Información y a los sistemas de LAP.

5. Lineamientos y directrices

La generalización de la informática y los flujos de Información presentan nuevos desafíos en materia de seguridad, haciendo cada vez más necesario establecer medidas para proteger los activos críticos de la Compañía. En este contexto, LAP se compromete a implementar los mejores mecanismos, herramientas y prácticas de seguridad y control aplicables.

Para lograr este objetivo, ha desarrollado y continuará desarrollando un conjunto de proyectos y acciones que permitan alcanzar los niveles de protección deseados. Se ejecutarán un conjunto de prácticas que evolucionen constantemente frente a los nuevos desafíos y amenazas en relación con la ciberseguridad y tratamiento de datos, convirtiéndose en una respuesta preventiva basada en datos, bajo el gobierno de nuestra área de Tecnologías de la Información.

El propósito principal es reducir el riesgo de error humano, robo, fraude o mal uso de las instalaciones y equipos. Dado que la seguridad de los activos críticos de LAP es un componente clave de su modelo comercial, por esto es indispensable que todos los Colaboradores estén sujetos a determinadas normas para garantizar la credibilidad y la seguridad en todo momento.

6. La Información

La Información es un activo vital para LAP y, por ende, todos los accesos, usos y procesamiento de esta deben regirse por las políticas y estándares establecidos por la Compañía en cada ámbito particular. Es crucial que esta Información sea protegida de manera consistente con su importancia, valor y criticidad, tanto por sus custodios como por el Jefe de Tecnología.

En este sentido, los ejecutivos de LAP deben comprometerse a proveer los recursos necesarios para la implementación de los controles requeridos, con el fin de garantizar el nivel de protección adecuado acorde al valor de los activos críticos. Esta medida no solo implica una inversión en tecnología y herramientas de seguridad, sino también en la capacitación y concientización del Personal para fortalecer la cultura de Seguridad de la Información dentro de la organización. De esta manera, se establece una sólida base para mitigar los riesgos asociados a posibles vulneraciones y amenazas cibernéticas.

6.1. Clasificación de la Información

Es fundamental para LAP considerar que toda la Información creada o procesada por la organización se clasifique inicialmente como “Pública”, a menos que se determine otro nivel de clasificación, como Confidencial, reservada o secreta.

Es importante establecer un proceso periódico de revisión de esta clasificación, con el fin de mantenerla actualizada o modificarla según sea necesario. La clasificación de la Información determinará el nivel de tratamiento y resguardo que requiere. LAP se compromete a proporcionar los mecanismos necesarios para que la Información sea accesible y utilizada por el Personal que lo requiere en el ejercicio de sus funciones.

Sin embargo, la empresa se reserva el derecho de revocar el acceso a la Información y tecnologías que la respaldan en caso de que la situación o condiciones lo ameriten. Esto refuerza la importancia de establecer políticas y procedimientos claros para el manejo y protección de la Información sensible, garantizando así la integridad y Confidencialidad de los activos de la Compañía.

6.2. Uso de la Información

LAP implementará procedimientos para un correcto uso de la Información, adoptando diferentes medidas de acuerdo con la clasificación asignada a esta. Es compromiso y responsabilidad de todos sus Colaboradores el uso, trato y resguardo adecuado de la Información, así como de los activos de Información.

6.3. Propiedad y Seguridad de la Información

Los Colaboradores de LAP deben tener presente que la empresa será propietaria de la Información, datos y derechos de uso y explotación de programas de software, equipos, sistemas, aplicaciones y cualquier documento instalado en los dispositivo propiedad de la Compañía. En este sentido, los Colaboradores no deben tener ninguna expectativa de privacidad para sus actividades mientras utilicen equipos informáticos de la empresa, a excepción de la Información Personal.

En virtud de lo anterior, los archivos, datos, documentos o correos electrónicos enviados o recibidos a través de las cuentas de la Compañía, serán considerados propiedad de ésta, al igual que los archivos almacenados en sus sistemas informáticos y en los sistemas de la Compañía.

Con el fin de garantizar la seguridad y el mantenimiento de la plataforma y sistemas, las personas autorizadas dentro de LAP podrán supervisar los equipos, sistemas y el tráfico de la red en cualquier momento. La Compañía se reserva el derecho de llevar a cabo auditorias periódicas de todas las plataformas tecnológicas para asegurar el cumplimiento de esta política.

Si la institución procesa y mantiene Información de usuarios externos que sean datos personales y/o sensibles de acuerdo con la normativa vigente, la Compañía se compromete a asegurar que esta Información no será divulgada sin previa autorización y estará protegida de igual manera que la Información interna.

6.4. Información Confidencial, Reservada o Secreta.

La Información almacenada en los sistemas de LAP, considerada como Información de Identificación Personal, será claramente etiquetada como Confidencial, conforme a los estipulado en esta política. Esta medida tiene como objetivo proteger derechos fundamentales como el honor, intimidad Personal y familiar, y la propia imagen, a través del establecimiento de mecanismos para regular el tratamiento de los datos. Es responsabilidad de los usuarios esforzarse por mantener segura esta Información en todo momento.

Se prohíbe terminalmente el envío de Información Confidencial, especialmente la Información de Identificación Personal almacenada en los archivos de la Compañía, mediante soportes materiales o a través de cualquier medio de comunicación, incluida la simple visualización o acceso.

Todo Colaborador que tenga acceso a los sistemas de Información está obligado a mantener la máxima reserva de manera indefinida y a no divulgar ni utilizar directa o indirectamente los datos, documentos, claves, programas, archivos y demás Información a la que tenga acceso propio por su posición o relación laboral con LAP.

6.5. Fuga, destrucción y protección de Información

El área de TI se enfrenta constantemente a desafíos relacionados con el almacenamiento y la Seguridad de la Información. Sin embargo, los incidentes pueden ocurrir debido al acceso no autorizado del Personal o a la pérdida de control en el sistema. Es fundamental que como empresa estemos preparados para responder rápidamente ante tales eventualidades.

Para prevenir estos escenarios, es esencial proporcionar capacitación y formación a todos los Colaboradores sobre buenas prácticas para evitar la fuga de Información. Se debe prestar especial atención y garantizar un mayor resguardo en el manejo de dispositivos críticos, el uso adecuado de los dispositivos extraíbles como USBs y CDs, el correo electrónico, la impresión de documentos, el uso de Internet y el mantenimiento de escritorios limpios y ordenados, entre otros aspectos.

Los respaldos de los activos críticos de Información, junto con los datos sensibles de la empresa, la Información de Identificación Personal y cualquier otro dato externo obsoleto o no relevante para las operaciones de LAP, serán eliminados de manera segura.

Además, se prohíbe estrictamente el uso de los recursos tecnológicos de la empresa para realizar o facilitar ataques informáticos contra otros sistemas, ya sea de manera activa o pasiva.

Para proteger nuestra red, implementaremos diversas herramientas como firewalls, sistemas de detección de intrusiones, monitoreos de red y otras medidas para salvaguardar la infraestructura contra amenazas tanto internas como externas. Es crucial mantener actualizados los sistemas, con las últimas versiones y parches de seguridad disponibles, que sean compatibles y soportados por sus hardware y software.

7. Control de acceso

La Información y las tecnologías de Información deben ser utilizadas exclusivamente para fines relacionados con las labores especificadas dentro de la estructura de LAP, aplicando criterios de Buen Uso en su utilización.

En este sentido, es imperativo que todos los sistemas de Información estén equipados con mecanismos de control y autenticación cifrados para el acceso, tales como la identificación de inicio de sesión por el usuario, permisos, contraseñas seguras, doble autenticación y registro de acceso, entre otras herramientas, según la naturaleza y capacidad de la plataforma que lo soporta.

El control de acceso reviste una importancia fundamental. Para esto, el proceso de asignación de permisos por las áreas funcionales debe ser únicamente a personas o usuarios autorizados, previniendo así el acceso indiscriminado a los sistemas de Información o de personal no calificado. Esto incluye medidas de protección mediante contraseñas, las cuales deben ser individuales, intransferibles y de responsabilidad única de su propietario (se trata a mayor profundidad en el **Anexo N°2**).

La creación de contraseñas debe regirse por las buenas prácticas de seguridad que contemple la periodicidad, la robustez y factores adicionales de validación, según la capacidad técnica de las soluciones a acceder.

El equipo tecnológico y los privilegios de acceso otorgados al Personal de LAP deben ser considerados de vital importancia, siendo su resguardo responsabilidad exclusiva de cada individuo como parte de sus deberes y obligaciones contractuales. Además, el Personal tiene la obligación de alertar de manera oportuna y adecuada cualquier incidente que viole lo establecido en esta política, utilizando los canales de comunicación preestablecidos.

8. Uso de dispositivos

Es política de LAP que los dispositivos entregados a los Colaboradores sean utilizados exclusivamente para fines de la actividad de la empresa. El acceso a estos y a los sistemas de Información estarán siempre controlado y gestionado a través de un nombre de usuario y una contraseña segura, personal e intransferible, comprometiéndose el usuario a tratar el empleo de los dispositivos con el máximo cuidado y diligencia, siendo este el único responsable del Buen uso de los aparatos y sistemas. También pondrá a disposición de los trabajadores las herramientas tecnológicas necesarias para la realización eficaz y eficiente de sus labores (software y hardware). Estas herramientas tecnológicas deben ser utilizadas únicamente para los fines que han sido dispuestas y no otros fines de carácter personal o comercial.

El uso de ordenadores, teléfonos fijos y móviles entregados por LAP estará destinado exclusivamente al uso profesional para actividades de LAP. Los contactos, mensajes, correos electrónicos, archivos que se creen o se compartan por medio de estas herramientas son propiedad exclusiva de la Compañía y no del usuario.

Lo anterior, posee ciertas excepciones, los usuarios podrán tener un limitado uso Personal de estas herramientas, en cuanto a la navegación en Internet, envío de correos electrónicos (el asunto debe establecer que es “Personal”), llamadas o recepción de mensajes o Información segura.

Al proveer la compañía los insumos tecnológicos para el desarrollo de las funciones quedan estrictamente prohibido utilizar herramientas tecnológicas no entregadas por la compañía para el desarrollo de las funciones, a mayor abundancia esto implica que se encuentra prohibido el uso de equipos propios como computadores de casa, notebooks personales, Tablet, entre otros, y está estrictamente prohibido el uso de softwares no entregados por la compañía, como cuentas de correo personal o plataformas para compartir información en la nube, y otras NO autorizadas directamente por la Compañía.

El mal uso de estas herramientas puede acarrear serios riesgos para LAP como la introducción de virus, malware, ransomware, fuga de información , etc.

Se prohíbe expresamente a todos los Colaboradores la utilización de los equipos de LAP para realizar cualquiera acto ilegal o contrario a la ética, especialmente los contemplados en la Ley 21.459.

8.1. Equipamiento

Tanto hardware como software serán entregados por la Compañía a los trabajadores según la necesidad que cada cargo requiera para el eficaz y eficiente desempeño de sus funciones. Dicho lo anterior, dependiendo de la naturaleza del cargo se determinará si este requiere o no de algún tipo de hardware o software específico, algunos ejemplos son:

a) Hardware:

- Notebook Marca Lenovo Core I7, 16Gb RAM

- Pantalla Adicional de 21’ Pulgada (LG o Samsung) (en caso de requerir)
- Teclado y Mouse
- Teléfono Fijo (Solo si el cargo lo requiere y es autorizado por su jefatura)
- Teléfono Móvil (iPhone o Samsung) (Solo si el cargo lo requiere y es autorizado por su jefatura)

b) Software:

- Windows 11 Profesional
- Office 365 (Outlook, Excel, Word, Power Point) Standard
- WinRAR (Software que permite comprimir y descomprimir archivos)
- Acrobat Reader (solo lectura) Standard
- Antivirus Panda Defense 360
- Mobile VPN with SSL client (acceso seguro a la red desde fuera de la oficina)
- SAP (solo en el caso que requiera utilizar este sistema) Bussiness One
- Power BI – adicional de Office 365
- Cognos – Complemento de Cognos de IBM
- Meet de Google (sistema para Video Conferencia)
- Teams (sistema Chat y Video y Video Conferencia)

8.2. Monitoreo de softwares usados y Actualizaciones

LAP dispone de herramientas tecnológicas para el monitoreo de softwares usados en cada equipo otorgado por la Compañía, así como también cuenta con sistemas de monitoreo para las actualizaciones de los softwares, por lo cual cualquier uso indebido será reportado a la jefatura para inmediatamente corregir la desviación a este protocolo con las consecuencias que esta violación al protocolo indica.

8.3. Control de inventario de hardware y actualizaciones.

La Compañía cuenta con un sistema de inventario, el cual nos permite mantener actualizado todos los datos del equipo.

8.4. Situaciones especiales.

En el caso que el trabajador en conjunto con su jefatura determine que los equipos tecnológicos entregados por la compañía son insuficientes pare el desarrollo eficaz y eficiente de sus funciones, estos se podrán solicitar mediante el formulario “Solicitudes Especiales de Tecnología”, para poder realizar esta solicitud se debe realizar un levantamiento de las funciones y aplicaciones que se requieren.

a) Ejemplo de software:

- AutoCAD (solicitado para proyecto o dpto. ingeniería).
- Acrobat Pro (Software que permite modificar archivos PDF).
- Project Estándar o Pro (solicitado para proyecto o dpto. ingeniería).
- Entre otros.

b) Ejemplo de Hardware:

- Pantalla 21' adicional a la que actualmente tienen.
- Impresora.
- Servidor Virtual para correr algún tipo de sistema.

En el caso de que el software o hardware requerido no esté disponible, se procederá con el proceso de aprobación de abastecimiento standard.

8.5. Entrega de equipos tecnológicos:

La entrega de hardware se realizará mediante acta de entrega FO-091 y mediante el acta FO-092 de claves de accesos a los equipos y sistemas (Acceso a Windows, Correo, , VPN, impresora. Será responsabilidad del trabajador resguardar estos equipos para evitar su daño o perdida. a la vez es responsabilidad del trabajador cambiar las claves entregadas esto para evitar mal uso de los accesos al notebook y los sistemas asociados.

9. Uso de correo electrónico

El uso descuidado del correo electrónico de la Compañía o de Internet pueden tener serias consecuencias. Por esta razón, la Compañía establece límites en cuanto a su uso, ya sea con fines profesionales o Personales. El correo electrónico y los sistemas de correo electrónico de la Compañía deben emplearse exclusivamente para asuntos laborales (y a modo excepcional para fines personales), y deben ajustarse a las políticas y procedimientos de LAP en relación con el comportamiento ético, la seguridad, el cumplimiento de las leyes y las prácticas comerciales aplicables.

Todos los datos e información que contengan los correos electrónicos enviados, por cualquier trabajador, a través de su correo corporativo podrán ser revisados y auditados por LAP, cuando ésta última lo estime adecuado. Esta revisión o auditoría se podrá realizar tanto en el servidor como en el computador personal donde se encuentre alojada la aplicación de correo. LAP se reserva el derecho de supervisar los mensajes sin previo aviso. Esto en particular en procesos de desvinculación, sea ésta por cualquier motivo que genere necesidades de búsqueda de información dentro de las plataformas de correo.

En caso de que se transfiera Información de Identidad Personal por correo electrónico, deben seguirse los siguientes pasos para garantizar una transmisión segura y minimizar el riesgo de infracción:

a) Proteger el documento con contraseña, ya sea PDF, Word o Excel. Si el documento se encuentra en un formato que no se puede proteger fácilmente (como gif o jpeg), debe convertirse en un archivo PDF, protegerlo con contraseña en este formato.

b) Enviar el documento por correo electrónico con la descripción "Confidencial" como etiqueta después del nombre del asunto.

c) Comunicarse con el destinatario por teléfono para confirmar la recepción del correo electrónico y proporcionarle la contraseña.

Asimismo, antes de intentar acceder al correo electrónico de LAP a través de dispositivos móviles Personales, los empleados deben obtener la aprobación previa de su gerente o supervisor.

LAP no asume responsabilidad por la pérdida de datos en caso de que se borre un dispositivo, ya sea debido a un error del usuario o a las características de seguridad implementadas.

Es crucial que los Colaboradores ejerzan extrema precaución al abrir archivos adjuntos de correos electrónicos recibidos de remitentes desconocidos, ya que podrían contener virus o malware, poniendo en riesgo la Seguridad de la Información y los sistemas de la Compañía.

El cumplimiento de esta política es un requisito para todos los dispositivos informáticos portátiles que almacenan datos protegidos de LAP, o que acceden a éstos.

10. Uso de Internet

Internet es una herramienta comercial para la Compañía. Se utilizará para fines comerciales, como comunicarse por correo electrónico con proveedores y socios comerciales, obtener información comercial útil e investigar temas técnicos y comerciales relevantes.

El servicio de Internet no se podrá utilizar para transmitir, recuperar o almacenar comunicaciones de naturaleza discriminatoria o acosadora, o que sean despectivas para cualquier persona o grupo, obscenas o pornográficas, o de naturaleza difamatoria o amenazante, para "cartas en cadena" o con cualquier otro propósito que sea ilegal o para beneficio Personal.

Al igual que el acceso a las redes, la Compañía se reserva el derecho a restringir en cualquier momento por medio de su red o de los dispositivos asignados o mediante el uso de firewall, el acceso a Internet -ya sea de forma general como a sitios específicos-.

La evolución de las tecnologías y riesgos asociados implica que accesos actuales permitidos puedan pasar a categorías de no permitidos sin expresión de causa.

11. Prevención de Delitos Informáticos

Todos los Colaboradores de las Compañías o cualquier persona que realice actividades de dirección y supervisión en ellas, o represente sus intereses ante terceros, tienen prohibido cometer conductas ilícitas a través de medios informáticos o en contra de sistemas informáticos. Dichas conductas se encuentran sancionadas en la Ley N°21.459, que establece normas sobre delitos informáticos, los cuales se describen a continuación:

a) Sabotaje informático:

Implica interferir o impedir el funcionamiento normal, parcial o total, de un sistema informático mediante la inserción, transmisión, daño, deterioro, modificación o eliminación de datos informáticos (art. 1° ley 21.459).

b) Acceso no autorizado:

Consiste en ingresar a un sistema informático sin permiso o excediendo el permiso otorgado, superando barreras técnicas o medidas de seguridad. La sanción es mayor si el acceso tiene como objetivo apropiarse o utilizar la información contenida en el sistema. También se penaliza la divulgación de la información obtenida de manera ilegal (art. 2° ley 21.459).

c) Interceptación no autorizada:

Involucra interceptar, interrumpir o interferir de manera indebida, mediante medios técnicos, la transmisión privada de información en un sistema informático o entre varios de ellos. También incluye la captación no autorizada de datos de sistemas informáticos a través de emisiones electromagnéticas (art. 3° ley 21.459).

d) Sabotaje de datos:

Consiste en alterar, dañar o eliminar de manera indebida datos informáticos, causando un daño significativo al titular de dichos datos (art. 4° ley 21.459).

e) Falsificación informática:

Implica la introducción, modificación, daño o eliminación indebida de datos informáticos con la intención de que sean considerados auténticos o utilizados para crear documentos auténticos (art. 5° ley 21.459).

f) Receptación de datos informáticos:

Se castiga a quien, sabiendo o debiendo saber su origen ilícito, comercialice, transfiera o almacene datos informáticos con fines ilícitos, provenientes de actividades de acceso no autorizado, interceptación no autorizada y falsificación informática (art. 6° ley 21.459).

g) Fraude informático:

Manipular un sistema informático mediante la introducción, modificación, daño o eliminación de datos, o por medio de cualquier interferencia en su funcionamiento, causando perjuicio a otros, con el objetivo de obtener un beneficio económico propio o para un tercero. Se considera también culpable a quien, sabiendo o debiendo saber la ilicitud de la conducta, facilita los medios para cometer el delito (art. 7° ley 21.459).

h) Abuso de dispositivos:

Con el propósito de cometer delitos de ataque a la integridad de un sistema informático, acceso ilícito, interceptación no autorizada, ataque a la integridad de datos informáticos, y fraude con tarjetas de pago y transacciones electrónicas, entregue, obtenga, importe, difunda o ponga a disposición dispositivos, programas informáticos, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la comisión de estos delitos (art. 8° ley 21.459).

12. Incumplimiento

El incumplimiento de las disposiciones de la presente política será considerado como un incumplimiento grave de las obligaciones del contrato de trabajo suscrito con LAP y se abordará su investigación de acuerdo con lo dispuesto en el Modelo de Prevención de Delitos y el Reglamento Interno de Orden, Higiene y Seguridad de la Compañía.

13. Consultas y denuncias

En caso de dudas respecto de las reglas, obligaciones y prohibiciones señaladas y aplicables de conformidad a la presente política, favor contactar al Encargado de Prevención de Delitos de LAP, Personalmente o su correo electrónico francisca.perez@latampower.com previo a la realización de cualquier actuación, operación o transacción que pueda comprometer a la Compañía.

14. Control de cambio

Versión	Elaborado por	Descripción de la modificación	Fecha	Aprobador
1.0	BSVV	Elaboración de la Política	Mayo 2024	

15. Anexos

Anexo N°1. Política y Procedimiento de Respaldo de Información.

Anexo N° 2. Política de Contraseñas & Seguridad de la Información.