POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

APIUX TECNOLOGÍA SPA

Elaborado por:	Aprobado por:	Lugar de Archivo	
CISO	COMITÉ DE SEGURIDAD	Google Drive > ISO27001	**USO INTERNO**

1. OBJETIVO

Establecer directrices que determinen un uso adecuado de los activos de información, en las actividades que se desarrollan en los procesos incluidos en el alcance del SGSI, **de manera de asegurar la Confidencialidad, Integridad y Disponibilidad** de los servicios e información y de esta forma, garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de información

Definir, Establecer, Implementar, Controlar, Mantener y Mejorar los requisitos y condiciones generales de seguridad necesarias para que la operación de APIUX se desarrolle conforme a la ley y las normas y acuerdos contractuales que correspondan.

Administrar adecuadamente, los riesgos a los que están expuestos los Activos de Información de APIUX Tecnología SpA (en adelante APIUX) y los principios y objetivos internos para resguardar sus operaciones.

2. ALCANCE

La Política de Seguridad de la información aplica al ámbito del proceso central de APIUX y expresa claramente la intención de proteger los activos de información incluidos en el alcance del SGSI, considerando aquellos pertenecientes a los usuarios internos y/o externos, como aquellos compartidos, incluyendo sus recursos y procesos, internos y/o externos si los hubiere, vinculados a la empresa mediante contratos o acuerdos con terceros.

La Política de Seguridad de la Información debe formar parte de la cultura organizacional. En ella se establece directrices y soporte en concordancia con los requerimientos de la empresa, las leyes, normas y acuerdos contractuales, los que sirven de guía para definir políticas específicas, que son complementarias para cumplir lo dispuesto en la presente Política.

La gestión de la seguridad de la información es responsabilidad de todos quienes se relacionan con los procesos de APIUX, colaboradores directos y usuarios externos, identificables, que presten servicios o asesorías y que por la naturaleza de sus funciones deban acceder a los Activos de Información de la empresa.

Por ello, las políticas que se establecen en este documento deben ser de conocimiento y cumplimiento obligatorio para todos aquellos a quienes se autorice el acceso a estos activos. Para usuarios externos, la obligación mencionada se establece en contratos y/o acuerdos correspondientes.

3. RESPONSABILIDADES

La responsabilidad de la implementación, cumplimiento y mantenimiento de la presente Política de Seguridad de la Información corresponde a la alta dirección de la empresa, el Comité de Seguridad de la Información, al Oficial de Seguridad de la Información, CISO de la empresa y la gerencia encargada de esta área de la empresa con su correspondiente equipo de trabajo, la que se encuentra en el alcance del SGSI.

Esta Política de Seguridad de la Información es aprobada y puede ser modificada y actualizada por quienes son identificados como sus responsables, siendo de aplicación obligatoria para todo el personal del área APIUX de la empresa, independientemente del nivel de tareas que desempeñe

4. REFERENCIAS

- Norma ISO 27001:2013: Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos
- Norma ISO 27002:2013: Tecnología de la Información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información
- Norma ISO 27005:2008: Tecnologías de la Información – Técnicas de Seguridad – Gestión de Riesgos de Seguridad de la Información
- Norma ISO 31000:2010 Gestión del Riesgo – Principios y Directrices
- Análisis de Contexto Interno y Externo
- Informe de Evaluación de Riesgos
- Matriz de Evaluación de Riesgos (Inventario de Activos)
- Procedimiento de Gestión de Incidentes de Seguridad

5. DESCRIPCIÓN DE LA POLÍTICA

5.1 DECLARACIÓN DE LA ORGANIZACIÓN

El principal foco de APIUX es el desarrollo e implementación de soluciones informáticas, para ello, APIUX cuenta con la más alta especialización profesional para desarrollar todo tipo de proyectos informáticos abarcando todos los aspectos involucrados:

- Consultoría
- Desarrollo e Implementación de soluciones
- Outsourcing de Procesos
- Gestión de la Calidad
- Reingeniería
- Provisión de hardware y software
- Instalación y Puesta en marcha
- Mantenimiento preventivo/correctivo de aplicaciones.
- Monitoreo de ambientes informáticos o aplicaciones críticas.
- Ingeniería de Sistemas para la administración de infraestructura computacional.
- Capacitación

APIUX también cuenta con acuerdos de “partnership”, representación y/o distribución de productos de los principales proveedores de software del mercado.

Adicionalmente, APIUX ha desarrollado el Servicio de Outsourcing como una alternativa eficaz de subcontratación para aquellas compañías que no desean mantener recursos internos especializados y costosos o que no cuentan con las habilidades requeridas por los productos de última generación que se utilizan en el mercado.

El sistema informático que sobre el cual reside el SGSI, combina la instalación de un sistema de seguridad basado en firewall, IDS, Antivirus y test de vulnerabilidades que cuenta con el soporte y mantenimiento continuo desde las

oficinas de APIUX y a través de Internet se monitorean la accesibilidad, los registros de operaciones y las alertas de seguridad; tomando medidas proactivas y reactivas de defensa y, en algunos casos, medidas contra ataque.

Se gestionará la seguridad de la información para proteger los activos contra amenazas y permitir la continuidad de las operaciones y del negocio, minimizando el riesgo de daño a la empresa y maximizando la eficiencia y oportunidades de mejora.

Apiux protegerá la información que manipula en papel, digital, en correos, en medios electrónicos, en videos o en conversación, y los dispositivos mediante los cuales se comparte esta información.

Para APIUX es muy importante proteger la información y los procesos asociados de TIC, que brinden la tríada de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad, de la cual todo el personal que integra los procesos de APIUX es responsable.

5.2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Considerando que:

- La Alta Dirección de APIUX se hace un deber procurar una correcta administración de la información de la organización y velar por su adecuado uso, conservación y mantenimiento, conforme a leyes, normas y acuerdos contractuales;

- La empresa debe resguardar los activos de información que son de su propiedad para asegurar la confidencialidad, integridad y disponibilidad de estos,

APIUX, procede a definir, establecer, aprobar, implementar, publicar, comunicar, revisar, monitorear, manejar y mejorar continuamente la Política de Seguridad de la Información, que le permita prevenir, detectar y corregir cualquier amenaza y/o vulnerabilidad asociada a la información de la empresa.

Por ello, APIUX reconoce que la seguridad de la información tiene alta prioridad para cumplir la misión de sus compromisos legales, normativos y contractuales, lo que constituye un alto compromiso de la Alta Dirección y de la totalidad de sus trabajadores.

Los criterios y lineamientos relacionados con la seguridad de la información de la empresa se establecen mediante un marco normativo, con políticas y procedimientos que permitan disponer de estándares para manejar, generar, procesar, intercambiar y almacenar los activos de información, de manera de obtener los niveles de Confidencialidad, Integridad y Disponibilidad que permitan la continuidad de las operaciones.

Para cumplir con lo señalado, se ha establecido el siguiente Compromiso de la Dirección:

La Alta Dirección de APIUX provee evidencia de su compromiso con el desarrollo y la implementación del Sistema de Gestión de Seguridad de la Información –SGSI– conforme a ISO 27001:2013, así como la mejora continua de su efectividad mediante las siguientes acciones:

- La autorización para implementar y aprobar el SGSI en el proceso central de APIUX.
- Estableciendo la política y objetivos del SGSI
- Asignando roles y responsabilidades en seguridad de la información.
- Comunicando a todos los empleados de la organización y a las partes externas pertinentes el grupo de políticas para la seguridad de la información, la importancia de lograr los objetivos de seguridad, cumplir sus responsabilidades y buscar la mejora continua en seguridad.
- Proporcionar recursos necesarios para la correcta implementación del SGSI.
- Asegurar que todo el personal a quien se asigna las responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas. Ofrecer y desarrollar las actividades del proceso central de APIUX con tecnología y servicios de alta calidad a precios competitivos de mercado.
- Mejorar continuamente los procesos, mediante el Sistema de Gestión de la Seguridad de la Información, conforme a las directrices establecidas en la Norma Internacional ISO 27001:2013
- Cumplir las expectativas de sus clientes, satisfaciendo sus requerimientos en temas de seguridad de la información, satisfaciendo sus necesidades, asignando los recursos necesarios para lograr un óptimo desempeño.
- Promover la seguridad de la información, comprometiendo para ello la participación de todo su personal, valorando su participación y aportes.
- Promover la mejora continua del Sistema de Gestión de Seguridad de la Información, para aumentar la competitividad en el mercado, utilizando herramientas de control de procesos, auditorías, análisis de riesgos, capacitaciones

y concienciación de todos los actores involucrados para comprometer su participación.

- Asegurar la actividad constante de la organización, en función de los requerimientos legales, reglamentarios y contractuales de seguridad de la información.
- Mantener a través del tiempo la fortaleza de la tríada fundamental de la seguridad de la información, esto es, Confidencialidad, Integridad y Disponibilidad.
- Revisar la Política de Seguridad de la Información a intervalos planificados de un año, coincidiendo con la realización de la Revisión del SGSI por la Dirección y/o cuando se produzcan cambios significativos, con el fin que se mantenga idoneidad, adecuación y de asegurar su conveniencia, suficiencia y eficacia continuas, dejando registro de estas revisiones.
- Asegurar que la Política de Seguridad de la Información es comunicada, conocida y entendida todos y cada uno de los trabajadores que pertenezcan a la organización, así como también por sus proveedores, clientes y terceras partes.
- Apoyar la definición y establecimiento de políticas, procedimientos, instructivos y planes asociados a seguridad de la información que sean necesarios en la empresa.
- La responsabilidad final con respecto a la seguridad de la información de la implementación del SGSI recae sobre EL Oficial de Seguridad y el CSI, soportados por los responsables de las diferentes áreas de APIUX.
- La revisión de la presente Política de Seguridad de la Información incluye las oportunidades de mejora, como respuesta a los cambios que pudiesen aparecer, como son aquellos normativos, legales, contractuales, tecnológicos, operacionales, administrativos, organizacionales, impactos de eventos e incidentes de seguridad, cambios no planeados, cambio en los costos de los controles aplicados, entre otros factores.
- Aquellas mejoras identificadas deben quedar registradas y ser aprobadas por quienes se identifican como responsables del manejo de la presente Política.

La presente Política de Seguridad de la Información, se aplica a todos quienes se relacionan de alguna manera con los procesos de APIUX que compone el Alcance del SGSI implementado, esto es, directivos y trabajadores de APIUX y terceras partes autorizadas para tener acceso a los activos de información de la empresa, sin considerar el tipo de vínculo que pudiesen tener, que será difundida para fomentar y desarrollar una cultura de seguridad de la información a nivel de la organización.

5.3 QUÉ PROTEGER, DE QUIÉN Y POR QUÉ.

Los activos de información definidos en el alcance del SGSI se deben proteger

de ataques internos y/o externos voluntarios o fortuitos, en todas las áreas del negocio.

Lo que se protege incluye personal, información, reputación, continuidad, entre otros.

5.4 REVISIONES

Esta política está aprobada y publicada por la dirección, razón por la cual el Comité de Seguridad de la Información efectuará una revisión de esta Política al menos una vez al año, sin perjuicio de que pueda ser evaluada en cualquier momento, dependiendo de la necesidad de la organización.

5.5 DIFUSIÓN

Dado a que esta política es de dominio público dentro de la organización, todo el personal de APIUX deberá tomar conocimiento de la presente política y ésta quedará disponible para futuras consultas en la plataforma Intranet.

5.6 REGISTROS

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Informe Revisión de Gestión	Google Drive > ISO27001	CISO	Control de acceso lógico	5 años

6. CONTROL DE CAMBIOS

Versión	Responsable	Cargo	Fecha	Motivo de Cambio	Ítem modificado
01	Francisco Cabezas	CISO	31-07-2017	Creación de Documento	Documento completo