KOMUNIKA LATAM
STRATEGIC CONSULTING

Política de Seguridad y Protección de la Información

Julio 2024 Versión #3

MARCO GENERAL DE LA POLÍTICA

Resumen de la política:

La información debe ser siempre protegida, cualquiera que sea su forma de ser compartida, comunicada o almacenada.

La **seguridad de la información es la protección de la información ante una amplia gama de amenazas** con el fin de garantizar la continuidad del negocio y minimizar los riesgos que impactan la gestión de Komunika Latam de cara a sus clientes, colaboradores, proveedores y otras partes interesadas.

Alcance:

Esta política representa el marco general para la gestión de la seguridad y protección de la información de Komunika Latam.

Es de consideración y obligatorio cumplimiento por parte de todos los miembros de la organización, incluyendo socios, colaboradores y aliados, así como por terceras personas, incluyendo clientes, proveedores y otras partes interesadas.

Abarca la protección de la información en sus diversas formas: impresa o almacenada electrónicamente, transmitida por correo o cualquier otro medio electrónico, mostrada en proyecciones o en forma oral en las conversaciones.

Objetivos de seguridad y protección de la información:

Proteger la confidencialidad de la información relacionada con la gestión de clientes y con los planes de desarrollo de negocio de Komunika Latam.

Conservar la integridad de archivos y documentos en cualquiera de sus formas (física y/o electrónica).

Asegurar que los servicios web de acceso público y las redes internas cumplen con las especificaciones de disponibilidad requeridas.

Entender y dar cobertura a las necesidades de todas las partes interesadas.

Principios de seguridad y protección de la información:

Komunika Latam **protege la información** generada, procesada o resguardada en sus procesos de negocio, así como su infraestructura tecnológica y activos.

Preservamos la **confidencialidad de la información**, especialmente aquella relacionada con los datos de carácter personal de clientes y colaboradores.

Implementamos mecanismos de clasificación y control de acceso a la información, sistemas y recursos de red y garantizamos que la seguridad sea parte integral del ciclo de vida de nuestros sistemas de información.

La **disponibilidad de la información** cumple con los tiempos relevantes para el desarrollo de los procesos críticos de negocio.

Komunika **evalúa riesgos y toma acciones** para su mitigación y control según sea el caso.

Los **colaboradores están debidamente informados y son responsables** de la seguridad de la información que manejan en el proceso de atención a clientes y en el desempeño de sus actividades de trabajo.

Los **riesgos en seguridad de la información serán objeto de seguimiento** y se adoptarán medidas cuando existan cambios que impliquen un nivel de riesgo no aceptable.

Las **situaciones que puedan exponer** a Komunika **a la violación de las leyes y normas** legales **no son toleradas.**

Las **políticas de seguridad** vigentes permanecerán disponibles para los colaboradores en el Sharepoint de la organización y se actualizarán regularmente.

Los **planes de continuidad de negocio** serán mantenidos, probados y **actualizados** al menos con carácter anual.

Los colaboradores reciben anualmente **capacitación en seguridad de la información y** son informados de las actualizaciones que se generen en esta materia. Es responsabilidad de cada colaborador asistir a las actividades programadas y aplicar la seguridad según las políticas y los procedimientos establecidos por la empresa.

Las **visitas y terceras personas** que accedan a nuestras instalaciones deberán cumplir con las disposiciones de la presente política.

CLASIFICACIÓN DE LA INFORMACIÓN

La información debe estar inventariada y los riesgos y exposiciones de seguridad deben estar identificados, con el objetivo de evitar pérdidas financieras, operativas o aquellas que pudiesen impactar la reputación de la compañía.

Komunika Latam clasifica la información de acuerdo a los siguientes criterios:

Confidencial: información que debe mantenerse bajo resguardo de los socios o del consultor designado (ej. información sensible de colaboradores y/o clientes) que bajo ningún concepto puede ser compartida a terceros o expuesta públicamente.

Restringida: información de acceso limitado a socios y/o grupo de consultores y/o responsable del área administrativa, en el manejo de la atención a clientes y gestión de actividades propias de Komunika (ej. documentos desarrollados para clientes como mensajes clave, Q&A, notas de prensa, planes y comunicados, información contable o financiera de la compañía, expediente de colaboradores, contratos y acuerdos con clientes y proveedores).

General: información disponible para todos los colaboradores para el desarrollo de sus actividades diarias (ej. templates, estándares, metodologías, políticas, formatos, artículos e investigaciones).

Pública: información pública propia o de terceros, debidamente validada que puede ser compartida con todos los colaboradores e incluso con terceras partes (ej. información de prensa, notas o material audiovisual publicado, documentos de referencia o contenidos disponibles al público como los one pages).

La información **confidencial y restringida** estará soportada por el **acuerdo de confidencialidad de Komunika con clientes, suscrito por socios y colaboradores.**

CONTROL DE ACCESO A LA INFORMACIÓN

Conforme a la clasificación de activos de información, se implementa medidas de seguridad con el fin de evitar la adulteración, pérdida, fuga, consulta, uso o acceso no autorizado o fraudulento a la información.

Komunika Latam establece los procedimientos formales para controlar la definición de perfiles y la asignación de derechos de acceso a los usuarios. Estos procedimientos cubren todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta la eliminación o desactivación del registro a quienes no necesiten más el acceso.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Todos los colaboradores, consultores y/o proveedores, deben informar oportunamente sobre cualquier riesgo que hayan observado o que sospechen que exista en los sistemas, equipos y/o procesos, y que puedan impactar la seguridad de la información.

La gerencia debe asegurarse de que los eventos y los puntos débiles de seguridad de la información se comunican de forma que sea posible emprender acciones correctivas.

Los colaboradores deben notificar oportunamente los incidentes al equipo de soporte de Tecnología Informática a través de la plataforma Wins Telecom y correo electrónico, copiando a la gerencia y al área de administración.

El equipo de soporte de Tecnología Informática atenderá la solicitud, generará la acción correctiva y comunicará a los socios la línea de acción recomendada.

Los socios aprobarán el curso de acción y gestionarán a través del área de administración la resolución del incidente.

Si una acción contra una persona u organización, después de un incidente de seguridad de la información, implica medidas legales, deberán recopilarse y resguardarse todas las pruebas del caso de acuerdo con lo definido en las leyes que rigen la materia.