Estrategia de Seguridad de la Información

Para América Móvil y sus filiales la visión preventiva en el ámbito de la Seguridad de la información ha resultado clave, nos ha permitido anticiparnos a la materialización de riesgos y la identificación de procesos y controles más eficientes, siempre incorporando una consciencia clara de mejora continua.

Por este motivo y tomando como base el análisis de riesgos respecto a su probabilidad e impacto, creamos nuestra **Estrategia Corporativa de Seguridad de la información**, que es la guía para el corporativo y sus filiales, en el objetivo de mitigar los riesgos presentes y evitar su materialización, todo esto mediante la mejora, creación, implementación y prueba de controles, procesos, servicios o herramientas que cumplan con dicho objetivo; aunado a ello nuestra Estrategia también nos permite tener una visión más profunda para hacer más eficientes las inversiones presupuestales.

Los ataques cibernéticos, el robo de **información sensible**, así como las nuevas formas cada vez más sofisticadas para la ejecución de delitos cibernéticos, son riesgos relevantes para todas las organizaciones a nivel mundial, ya que pueden afectar negativamente la reputación y generar impactos financieros tanto para las empresas, como para sus clientes.

En América Móvil ofrecemos soluciones de conectividad de ciberseguridad que no sólo hacen que las personas se sientan seguras cuando las utilizan, sino que también contribuyen a la seguridad general de la información de las comunidades donde operamos.

América Móvil cuenta con una estrategia de seguridad integral que contempla la ciberseguridad como la privacidad de los datos y las comunicaciones, basada en tres pilares principales:

- **Integridad:** La información personal debe permanecer completa y exacta, para lo cual hemos establecido medidas adecuadas.
- **Disponibilidad:** La información debe estar disponible para sus propietarios o usuarios autorizados en el momento preciso en que la necesiten.
- **Confidencialidad:** Los datos personales serán utilizados exclusivamente por el personal autorizado que tenga la justificación necesaria para su uso.

Estrategia de Seguridad de la Información

A través de nuestra Estrategia de Seguridad de la Información, gestionamos y salvaguardamos la información financiera y confidencial de forma eficiente, al tiempo que minimizamos los riesgos de acceso ilegal o no autorizado.

En América Móvil hemos creado un **Marco Normativo de Seguridad de la Información** compuesto por 12 dominios, estos agrupan políticas y procedimientos mínimos que deben ser considerados en la operación de las filiales, mismos que son supervisados en su cumplimiento y ejecución por los responsables de Seguridad de la Información y los Comités de Seguridad de la Información, tanto a nivel Corporativo como de las filiales, junto con un Centro de Operaciones de Seguridad Global (***SOC*, por sus siglas en inglés)** gestionado por Scitum, una filial de Telmex, que incluye un equipo de ciber inteligencia para identificar amenazas.

El ***SOC*** cumple la doble función de asegurar todas nuestras operaciones, para dar confianza a los clientes sobre nuestros servicios y soluciones, además de ofrecer productos de ciberseguridad y servicios de asesoría a nuestros clientes corporativos para ayudarles a anticiparse a este tipo de retos.

El papel del personal de la empresa es clave para el éxito de nuestra estrategia de seguridad de la información. Por ello, es esencial **brindar constante capacitación** acerca de nuestras políticas y procedimientos de seguridad de la información. Asimismo, frecuentemente implementamos campañas de concientización y ejercicios de *Phishing* simulados para recordar a nuestro personal los controles y las mejores prácticas en cuanto a la consulta y el acceso a los sistemas e información de la Empresa y sus filiales.

Para mantenernos actualizados con las últimas tendencias, al menos una vez al año organizamos el **"Simposio de Ciberseguridad de América Móvil"**, en el que abordamos temas como las tendencias de seguridad de la información, el Internet de las Cosas, los estándares, los retos, las oportunidades, la transformación digital y los controles de acceso, entre otros.

Constantemente, evaluamos y actualizamos nuestra estrategia de seguridad de la información basándonos en la prevención, la mejora continua y el intercambio de buenas prácticas entre todas las empresas del Grupo.

GOBERNANZA DE LA SEGURIDAD DE LA INFORMACIÓN

Nuestros CISO´S (*Chief information Security Officer*), lideran los esfuerzos de seguridad de la información dentro de toda la Compañía para asegurar la correcta implementación de nuestra Estrategia, así como la alineación de la certificación ISO 27001 en todas las operaciones.

También contamos con un **Comité Corporativo de Seguridad de la Información**, que se reúne dos veces al mes y supervisa la implementación de la Estrategia de Seguridad de la Información de América Móvil, con las siguientes funciones:

- Identificar los principales riesgos para el negocio centrados en la operación y nuestros servicios, así como en el entorno tecnológico.
- Desarrollar y gestionar la estrategia de seguridad mediante la creación y el seguimiento del Plan Estratégico de Seguridad de la Información.
- Gestionar y asignar los presupuestos corporativos y locales para la seguridad de la información
- Determinar las acciones prioritarias frente a las amenazas actuales o futuras.

La nueva estructura de gobierno también permite que los equipos de seguridad de la información de nuestras filiales y el personal de Scitum trabajen de manera coordinada en la detección y atención de incidentes, además, mantenemos un mecanismo de comunicación cercano y constante entre las operaciones para enviar alertas de manera oportuna.

Los responsables de seguridad de la información en las subsidiarias también son responsables de:

- Adoptar las políticas y los procedimientos de seguridad de la información.
- Establecer estrategias para cumplir con las pautas que contribuyen a aumentar la confidencialidad, integridad y disponibilidad de los recursos de información.
- Implementar mecanismos que contribuyan a cumplir con las mejores prácticas para proteger los recursos de información.
- Coordinar la evaluación y ejecución de proyectos que apoyen las actividades relacionadas con la seguridad de la información.
- Supervisar los planes de comunicación de los lineamientos de seguridad.
- Analizar los incidentes relacionados con la seguridad para determinar soluciones y acciones preventivas.
- Evaluar la infraestructura nueva y existente que soporta los procesos de negocio críticos.
- Coordinar los comités de cada una de nuestras operaciones.
- Supervisar las medidas de mejora en los incidentes reportados por las operaciones.

- Apoyar a otras áreas en el proceso de cumplir con los lineamientos de seguridad de la información.
- Coordinar y verificar que todos los esfuerzos, recursos, herramientas, controles y monitoreos son consistentes con el aseguramiento de la disponibilidad, integridad y confidencialidad de la información.
- Informar al CEO local, al CISO y al Comité de Seguridad de la Información Corporativa sobre cualquier incidente que pueda comprometer la información crítica, así como el impacto potencial y planes de mitigación.

Además, cada subsidiaria tiene su propio Comité Local de Seguridad de la Información. Estos comités interdisciplinarios están conformados por colaboradores de diferentes áreas (TI, ingeniería, finanzas, operación y mantenimiento, entre otros), y están presididos por los jefes locales de seguridad de la información. Asimismo, cada operación tiene un ejecutivo de alto nivel, responsable de revisar la Estrategia de Ciberseguridad. Asimismo, cada país determina un “Plan Estratégico de Seguridad de la Información”, que es actualizado de forma anual o semestral.