Síntesis Política Seguridad de la Información

Nuestra política de Seguridad de la Información establece las normas para garantizar la confidencialidad, integridad y disponibilidad de la información, además de protegerla contra cualquier amenaza.

La política prevé que la Empresa debe:

a) Apegarse a la estrategia y disposiciones normativas institucionales del área de Seguridad de la Información.
b) Proporcionar los recursos, procesos, capacitación y herramientas para mantener la función de Seguridad de la Información en la Empresa.
c) Contar con los siguientes elementos de Seguridad de la Información:
    i. Evaluaciones de seguridad a la infraestructura.
    ii. Análisis de riesgos de Seguridad de la Información.
    iii. Un esquema de monitoreo de activos críticos de información definidos dentro de la Empresa.
    iv. Un procedimiento para la gestión de incidentes de Seguridad de la Información.

Las disposiciones normativas institucionales del área de Seguridad de la Información deben:

a) Estar formalizadas, difundidas y ser de fácil acceso para los empleados.
b) Mantenerse actualizadas apegándose a la operación.

Las evaluaciones de seguridad a la infraestructura deben:

a) Ser ejecutadas al menos anualmente.
b) Incluir pruebas de penetración, escaneos de vulnerabilidades y revisión de aplicaciones, entre otras.

Los riesgos de Seguridad de la Información detectados en el análisis de riesgos de Seguridad de la Información deben:

a) Estar claramente identificados y actualizados.
b) Ser reportados al dueño de la información.
c) Contar con planes para mitigarlos, transferirlos, aceptarlos o eliminarlos.
d) Ser evaluados basándose en la probabilidad de ocurrencia y de impacto para la Empresa.
e) Ser ajustados de acuerdo a fuentes públicas y monitoreo interno de amenazas a la infraestructura de la Empresa, la industria, y la comunidad tecnológica en general.

Los incidentes de Seguridad de la Información deben contar con un procedimiento para su atención conforme a lo establecido en la política de Gestión de Incidentes de Seguridad de la Información.

El monitoreo de activos críticos de información debe contar con:

a) Un esquema de alertas.
b) Las actividades para atender las alertas de Seguridad de la Información resultado del monitoreo.

El incumplimiento por parte de cualquier empleado a lo establecido en la política de Seguridad de la Información lo hará acreedor a las sanciones administrativas establecidas en el Código de Ética de la Empresa y el Reglamento Interior de Trabajo vigentes.