Síntesis Política Aseguramiento de los Sistemas de Información

Nuestra política de Aseguramiento de los Sistemas de Información norma la seguridad de los Sistemas de Información de la Empresa.

La política prevé que los Sistemas de Información deben:

a) Ser utilizados únicamente para los fines que fueron asignados.
b) Cumplir con los estándares de seguridad establecidos por la Empresa.
c) Contar con:
    i. Un identificador de usuario por cada Sistema de Información.
    ii. Mecanismos de autenticación establecidos por la Empresa.
    iii. Perfiles y privilegios de acceso otorgados de acuerdo a las funciones y responsabilidades del usuario final.
    iv. Un esquema de respaldo y recuperación de información, acorde a los requerimientos y necesidades del negocio.
    v. Llaves criptográficas robustas, en su caso.
    vi. Un control de versiones para desarrollos.
    vii. Un inventario de versiones de software de terceros de código cerrado. Ambientes de pruebas distintos a los productivos.
    viii. Mecanismos que aseguren el soporte y mantenimiento de los mismos, así como de su infraestructura.
d) Tener habilitados mecanismos de rastreo de auditoría.
e) Ser monitoreados conforme a lo establecido por la Empresa.
f) Estar protegidos contra software malicioso.
g) Contar con enlaces de comunicación cifrados para enviar y recibir la información clasificada como restringida y muy restringida.

Los identificadores de usuarios y contraseñas con privilegios de administrador en los Sistemas de Información, como bases de datos, sistemas operativos, aplicaciones e infraestructura de seguridad y de sistemas, deben ser resguardados en una bóveda electrónica de control de acceso.

La información contenida en los Sistemas de Información debe revelarse únicamente y con previa autorización, por alguno de los siguientes motivos:

a) Operatividad y continuidad del negocio.
b) Investigación de posibles incidentes de seguridad de la información.
c) Rescate o preservación de la seguridad de los Sistemas de Información de la Empresa.

La información transmitida en los Sistemas de Información entre diferentes puntos y que requiera un alto nivel de disponibilidad, debe contar con enlaces de comunicación redundantes.

Los riesgos de Seguridad de la Información detectados en los Sistemas de Información deben contar con un plan de remediación para mitigarlos.

Queda estrictamente prohibido:

a) Copiar la información de los Sistemas de Información de un ambiente productivo a otro distinto, sin aplicar previamente procesos de enmascaramiento de datos para desensibilizar la información.
b) Hacer uso de los Sistemas de Información para almacenar, crear, descargar o transmitir información personal o pública de índole obscena, ofensiva, ilegal, abusiva, dañina, vulgar, irrelevante o de naturaleza cuestionable.

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