ECIJA
Pasaje Camilo Campos #129, Edificio ECIJA, Lomas Verdes,
Colonia Escalón, San Salvador, El Salvador
Tel: + 503 2252 1561 · Tel: + 503 2260 2736
www.ecija.com

Seguridad de la Información

El día 30 de noviembre de todos los años se celebra mundialmente a la Seguridad de la Información, quisiéramos como firma especializada en la materia, hacer conciencia sobre la importancia de contar dentro de nuestras organizaciones con políticas claras en relación con la protección del activo más importante del siglo XXI *La información*.

Pensemos en el impacto económico que para el público en general podría significar un ciberataque a un Banco o una institución pública o empresa estatal, instituciones que no solo manejan información delicada de terceros, sino que, en el segundo de los casos (es decir de las empresas estatales) podría significar una interrupción en la prestación de servicios esenciales, como por ejemplo la generación y/o distribución de electricidad, o en el caso de compañías de telecomunicación, la interrupción de sus señales, entre otros.

Esto de la Seguridad de la Información es algo sobre lo cual tenemos que tomar conciencia todos los que nos dedicamos a actividades en las cuales nos relacionamos con información de terceros (clientes, usuarios, empleados, proveedores, etc.) ya que, en nuestro país, a contrario de lo que se pudiera pensar, contamos con un régimen legal que impone cierto tipo de obligaciones relativas a la Seguridad de la Información.

Entre las principales leyes y regulaciones sectoriales que afectan a la empresa desde el punto de vista de la Seguridad de la Información tenemos:

- Ley de Comercio Electrónico.
- Ley de Acceso a la Información Pública.
- Ley de Protección al Consumidor.
- Ley de Firma Electrónica.
- Ley Especial contra los Delitos Informáticos y Conexos.
- Ley reguladora del Teletrabajo.
- Ley de regulación de los servicios de información sobre el historial de crédito de las personas.
- Ley de Prevención de lavado de dinero y activos y financiamiento del terrorismo.
- Normas Técnicas para la Gestión de la Seguridad de la Información (NRP 23); y
- Normas Técnicas para el Sistema de Gestión de la Continuidad del Negocio (NRP24)

Estas últimas dos aplicables únicamente a aquellas entidades reguladas por la Superintendencia del Sistema Financiero.

El cumplimiento a estas normativas se hace más estricto en aquellos casos en los cuales la actividad principal de nuestra organización, es la prestación de servicios o la venta de bienes en entornos digitales, por medio de modelos de negocio en los cuales se trate de implementar el comercio electrónico, por ejemplo, o bien, cuando en búsqueda de la optimización de recursos, las industrias buscan realizar la automatización de sus métodos de producción.

En cualquier caso, lo más saludable es el crear una política interna de Seguridad de la Información, que cumpla con los siguientes objetivos principales:

1. **Disponibilidad**: Nuestras estrategias de Seguridad de la Información deben de ayudarnos a asegurar que los usuarios puedan acceder a los recursos cuando lo necesiten.
2. **Autenticidad:** Nuestras estrategias de Seguridad de la Información deben de ayudarnos a garantizar los procesos de autenticación y control de acceso para que solo las personas autorizadas puedan acceder a la información.
3. **Integridad**: Nuestras estrategias de Seguridad de la Información deben de ayudarnos a proteger la exactitud y estado completo de la información detectando cualquier cambio intencional o no intencional en las comunicaciones.
4. **Confidencialidad:** Nuestras estrategias de Seguridad de la Información deben de ayudarnos a asegurar que los datos almacenados por el usuario o en tránsito en las comunicaciones no puedan ser leídos por partes no autorizadas; y
5. **Trazabilidad:** Nuestras estrategias de Seguridad de la Información deben de ayudarnos a establecer los procedimientos y mecanismos para proporcionar los datos necesarios que permitan llevar a cabo un análisis de seguridad en caso de sufrir un incidente.

El cumplir con estos cinco objetivos pudiera sonar un tanto complejo, pero es algo sumamente alcanzable, bastará en algunos casos, con cultivar dentro de nuestras organizaciones hábitos

sanos tales como no tener apuntados en lugares visibles los códigos de acceso a nuestras cuentas de correo electronico, por ejemplo.

La creación de una pólitica de Seguridad de la Información, es un trabajo en conjunto que debe de ser realizado entre la dirección general de la empresa, el departamento de técnología y recursos humanos con la ayuda de profesionales en Seguridad de la Información y abogados con conocimiento en la materia, ya que esta política debe de contar con elementos técnicos y legales, a fin de poder convertir estas politicas en un verdadero esquema de protección para la empresa y para todas aquellas personas que tienen contacto con ella.

Finalmente, quisiera recalcar el hecho que en la mayoría de los casos, la vulneración de los sistemas de información de una empresa, provienen de acciones humanas, es por ello que, dentro de toda Politica de Seguridad de la Información ***es importante tener*** los mecanismos y procedimientos internos para determinar en el evento de un posible Delito Informático:

1. Que internamente se tomaron las medidas para prevenir el evento;
2. Que internamente se tomaron medidas rápidas para contrarrestar el evento;
3. Que los procedimientos internos, permiten tener trazabilidad del evento para:
    - Individualizar un posible hechor.
    - Individualizar un posible cómplice interno.

Carlos Gil

Socio ECIJA El Salvador