Manual de ciberseguridad para abogados de empresa

Guía para gestionar la ciberseguridad desde la perspectiva legal

Tabla de Contenidos

Presentación

“La ciberseguridad dejó de ser un problema exclusivo del departamento de TI”

La ciberseguridad es uno de los problemas más importantes que enfrentan los abogados internos y sus empresas hoy en día. Dependiendo del sector industrial y la estructura de una organización, la protección de datos y otros activos digitales contra pérdidas, destrucción o acceso no autorizado suele ser responsabilidad del Oficial de Seguridad de la Información (CISO), Departamento de TI, u otros equivalentes.

Sin embargo, desde hace mucho tiempo que la ciberseguridad dejó de ser un problema exclusivo del departamento de TI. Los abogados internos tienen un papel importante que asumir en la protección de sus organizaciones contra ciberataques, violaciones de datos y otros incidentes cibernéticos. Esta Guía aporta cuestiones clave de ciberseguridad que los abogados y abogadas internos deben considerar y los pasos proactivos que ellos y sus organizaciones pueden tomar para minimizar los riesgos y prepararse antes de que ocurra un incidente cibernético.

/01
Introducción

La ciberseguridad es el conjunto de prácticas, procesos y tecnologías diseñadas para proteger redes, dispositivos, programas y datos de ataques, daños o accesos no autorizados. En el contexto legal y corporativo, la ciberseguridad es crucial para salvaguardar información confidencial, mantener la integridad de los datos y garantizar la continuidad del negocio.

La ciberseguridad tiene como objetivo proteger los tres principales atributos de la información: confidencialidad, integridad, y disponibilidad (la triada de la ciberseguridad).

Para los abogados in-house, comprender y aplicar principios de ciberseguridad es esencial para:

- Proteger la información confidencial de clientes y de la empresa.
- Cumplir con regulaciones y normativas de protección de datos.
- Mitigar riesgos legales asociados a violaciones de datos.
- Asesorar a la organización en la implementación de políticas de seguridad digital.

Este manual proporcionará algunas herramientas y conocimientos necesarios para abordar eficazmente los desafíos de ciberseguridad en el entorno legal corporativo.

/02
Algunos Números Relevantes

78%

de organizaciones costarricenses consideran el robo de datos como una amenaza significativa. (LABCIBE-UNA, 2024)

46%

de las organizaciones no tiene medidas implementadas para cumplir con la legislación de protección de datos y ciberseguridad. (LABCIBE-UNA, 2024)

$4.16

millones de dólares: el costo de un incidente cibernético en Latinoamérica. (IBM, 2024)

>9-10

Más de 9 de 10 clientes están preocupados por la seguridad de sus datos. (Arcserve, 2024)

92%

de consumidores cree que las empresas priorizan el lucro sobre la protección de su información (Arcserve, 2024)

/03

Comprendiendo los Activos de Información y Riesgos de la Empresa

Los abogados internos deben comprender cuáles son los activos de información de sus organizaciones para ayudar a protegerlos. Las organizaciones deben inventariar y rastrear sus activos de TI, incluyendo computadoras, elementos de redes, dispositivos de almacenamiento y otros recursos, para permitir una evaluación adecuada de riesgos de ciberseguridad y la gestión de vulnerabilidades.

De manera similar, el mapeo y categorización de datos cataloga la información confidencial de la organización, incluido su propietario comercial, ubicación y usos.

En Costa Rica, tanto el inventario de activos como la categorización y descripción de los datos son acciones mínimas exigidas por la legislación (Artículo 36 del Reglamento a la Ley No. 8968).

/04

Realizar Evaluaciones de Riesgos

Las evaluaciones de riesgo de ciberseguridad son inherentemente actividades operativas. Sin embargo, los abogados internos juegan un papel importante en este proceso, ya que las leyes, regulaciones y obligaciones contractuales de seguridad de datos a menudo utilizan un estándar de razonabilidad y diligencia. Las organizaciones buscan el asesoramiento de sus abogados sobre lo que es una práctica de seguridad razonable. Para proporcionar un asesoramiento eficaz, los abogados internos deben comprender la terminología, los procesos y los estándares comunes de evaluación de riesgos de seguridad de datos, incluyendo cómo:

- Definir y priorizar los riesgos cibernéticos.
- Realizar evaluaciones de riesgos y gestionar los resultados.
- Reconocer las limitaciones de la evaluación de riesgos cibernéticos.
- Proteger los informes confidenciales de evaluación de riesgos.

/05

Identificar las Obligaciones Legales de la Empresa

Las regulaciones y estándares de la industria requieren que las organizaciones aseguren la información personal que almacenan y otros activos de información.

En Costa Rica, estas obligaciones provienen esencialmente de:

- la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (Ley No. 8968) y su Reglamento.
- Código Penal y Ley de Delitos Informáticos (Ley 8148 - 2000 y Ley 9048 - 2012
- Reglamento General de Gobierno y Gestión de la Tecnología de Información (Acuerdo CONASSIF 5-24) (Aplicable solo a entidades financieras y sus proveedores).
- Reglamento sobre medidas de ciberseguridad aplicables a los servicios de telecomunicaciones basados en la tecnología de quinta generación móvil (5G) y superiores, Nº 44196-MSP-MICITT (aplicable a proveedores de servicios de telecomunicaciones y sus proveedores).
- Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001), Ley No. 9452.
- Directrices del Ministerio de Ciencia, Tecnología, Innovación y Telecomunicaciones (MICITT), aplicables especialmente al sector público.

> Los abogados internos deben revisar las prácticas organizacionales e identificar las obligaciones legales que pueden resultar de escenarios comunes, tales como la recopilación y uso de datos personales de clientes, colaboradores u otros; participar en un sector industrial considerado de alto riesgo o infraestructura crítica; poseer secretos comerciales u otra información protegida, entre otros.

/06

Apoyar en la Creación, Implementación y Supervisión de un Programa de Seguridad de la Información

Las regulaciones requieren que algunas organizaciones desarrollen, implementen y mantengan un programa integral de seguridad de la información por escrito.

Este Programa:

- Documenta el compromiso de una organización con la seguridad de la información.
- Asigna la responsabilidad del programa de seguridad de la información.
- Describe los elementos clave del programa, incluyendo:
  - Evaluación de riesgos
  - Políticas y procedimientos de seguridad de la información
  - Controles de seguridad
  - Supervisión de proveedores de servicios
  - Respuesta a incidentes
  - Entre otros

> Incluso cuando no lo exija explícitamente la ley, un programa bien desarrollado y mantenido puede beneficiar legalmentea la organización,porque evidencia que la organización toma medidas proactivas para proteger la información personal y confidencial, especialmente si ocurre un incidente cibernético y resulta en litigios o investigaciones.

/07

Considerar Estándares y Mejores Prácticas de la Industria

Los abogados internos deben familiarizarse y considerar los estándares y las mejores prácticas de la industria cuando ayuden a sus organizaciones a desarrollar, ejecutar y monitorear un programa de seguridad de la información. Algunos de esos estándares son:

a. El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF)
b. ISO 27001:2022, Sistema de Gestión de la Seguridad de la Información
c. CIS Critical Security Controls
d. SOC 2
e. COBIT
f. PCI DSS

Ser capaces de demostrar el cumplimiento de algunos o varios de estos estándares es esencial para mitigar el riesgo de sanciones o multas. Además, los abogados internos pueden exigir algunos de estos estándares a sus proveedores tecnológicos en los contratos que pacten con éstos.

/08

Desarrollar y Hacer Cumplir una Política de Seguridad de la Información

Una política integral de seguridad de la información sienta las bases para un programa eficaz de seguridad de la información. Las políticas ayudan a los colaboradores y otros a comprender los límites de uso y las acciones que deben (o no deben) tomar para proteger los activos de información de la organización. Las personas a menudo se convierten en el eslabón más débil en la ciberseguridad, lo que hace que una orientación clara sea aún más crucial.

Los abogados internos deben ayudar a sus organizaciones a desarrollar y hacer cumplir consistentemente una política de seguridad de la información que se aplique a todos los miembros de la fuerza laboral, incluidos empleados, contratistas, agentes y cualquier otro que acceda o use los activos de información de la organización.

/09

Gestionar los Riesgos de Proveedores

Aún las empresas más cuidadosas pueden sufrir ataques informáticos o filtraciones de información cuando sus proveedores externos no mantienen estándares adecuados de seguridad digital. Esta vulnerabilidad se denomina "riesgo de la cadena de valor" y surge cuando dependemos de terceros que proporcionan servicios tecnológicos. Es responsabilidad de los asesores legales de la empresa supervisar la selección y contratación de proveedores que tengan acceso a la información o plataformas de la organización, así como establecer protocolos específicos para minimizar estos riesgos.

09.1 Realizar la debida diligencia previa al contrato

La debida diligencia previa al contrato ayuda a determinar si los proveedores tienen programas y prácticas razonables de seguridad digital en su lugar antes de acceder a los datos o sistemas de la organización.

Los abogados internos deben considerar varios métodos para evaluar las capacidades de los proveedores y los programas de cumplimiento, tales como: Cuestionarios de evaluación de proveedores, Evaluaciones y certificaciones independiente, o Auditorías.

09.2 Usar modelos preaprobados de contratos

Los abogados internos deben desarrollar e imponer cláusulas contractuales de ciberseguridad para garantizar que los proveedores protejan los datos y sistemas de la organización de una manera que:

- Cumplan o excedan las propias prácticas de la organización.
- Cumpla con las leyes, regulaciones y estándares aplicables.

Es común que los proveedores busquen utilizar sus propios contratos de adhesión. Los abogados internos deben sopesar y evaluar el poder de negociación que posee frente al proveedor, y los riesgos de usar contratos de adhesión del proveedor, en lugar de los propios.

09.3 Realizar supervisión y monitoreo continuos

Los abogados internos también deben ayudar a gestionar los riesgos de los proveedores de manera continua para:

- Evaluar continuamente el trabajo del proveedor.
- Verificar que cumpla o supere lo acordado.
- Anticipar posibles problemas.
- Proteger los datos al terminar la relación comercial.

/10

Desarrollar y Evaluar el Plan de Respuesta a Incidentes Cibernéticos

Cada incidente cibernético presenta hechos y circunstancias únicos, lo que dificulta que las organizaciones se preparen para cada tipo de evento que pueda afectarlas. Sin embargo, un plan de respuesta a incidentes cibernéticos (IRP, por sus siglas en inglés) proporciona un marco estándar que ayuda a las organizaciones a prepararse y manejar efectivamente los ciberataques, violaciones de datos y otros incidentes cibernéticos.

Los abogados internos deben trabajar con los departamentos tecnológicos para desarrollar un IRP robusto que, entre otros temas, incluya: el rol de los abogados internos y externos durante un incidente; la forma y características del reporte del incidente, y las reglas para la preservación de la evidencia digital y para valorar la necesidad de comunicación del incidente a las autoridades judiciales.

/11

Obtener un Seguro Cibernético

Los seguros tradicionales de responsabilidad civil a menudo excluyen de la cobertura las pérdidas sustanciales que pueden resultar de una violación de datos u otro incidente cibernético.

Como resultado, muchas empresas obtienen cobertura de seguro cibernético para mitigar el riesgo de violaciones de datos y otros incidentes cibernéticos. Dependiendo de la póliza, el seguro cibernético puede cubrir los costos asociados a robo, destrucción y restauración de datos, investigaciones forenses, gestión de crisis, interrupción del negocio, multas, daños y perjuicios, entre otros costos relacionados con incidentes.

Antes de comprar un seguro cibernético, los abogados internos deben consultar a varios corredores para garantizar que sus pólizas cubran los tipos de riesgos de violación de datos y otros riesgos cibernéticos que la organización probablemente enfrente.

> Después de obtener la cobertura del seguro cibernético, se recomienda que los abogados internos revisen la póliza de la empresa al menos anualmente, ya que el perfil de riesgo cibernético de la empresa pueden cambiar con el tiempo.

/12

Cooperación con Autoridades de Investigación en Ciberdelitos

Antes de que ocurra un ciberataque u otro incidente cibernético, los abogados internos deben tener un protocolo para la eventual cooperación y comunicación con las autoridades judiciales que investigan los ciberataques; en el caso de Costa Rica, con la Sección Especializada contra el Cibercrimen del OIJ, entre otros.

Antes de que ocurra un ciberataque u otro incidente cibernético, los abogados internos deben tener un protocolo para la eventual cooperación y comunicación con las autoridades judiciales que investigan los ciberataques; en el caso de Costa Rica, con la Sección Especializada contra el Cibercrimen del OIJ, entre otros.

Los abogados internos deben mantener una lista de contactos de las autoridades relevantes como parte de su papel en el equipo de respuesta a incidentes (IRT) de la organización.

Sin embargo, los abogados internos deben consultar con la gerencia y considerar contratar abogados externos antes de notificar a dichas autoridades sobre una violación de datos u otro incidente cibernético para determinar si la notificación es aconsejable o requerida por ley bajo las circunstancias.

Conclusión

“Los abogados pueden desempeñar un papel crucial en la protección de los datos y sistemas de la empresa.”

La ciberseguridad es un desafío en constante evolución que exige la atención y el compromiso de toda la organización, incluidos los abogados internos. Al entender los activos de información y los riesgos asociados, cumplir con las obligaciones legales y adoptar medidas proactivas, los abogados pueden desempeñar un papel crucial en la protección de los datos y sistemas de la empresa. Este manual ofrece herramientas esenciales para abordar los complejos retos legales y técnicos de la ciberseguridad. Al final, una estrategia sólida en ciberseguridad no solo protege a la organización frente a amenazas, sino que también fortalece la confianza de clientes y socios, contribuyendo al éxito y la resiliencia a largo plazo de la empresa.

datalex
cyber law & policy

Contáctenos para asesorarle y capacitarle en cumplimiento y gobernanza digital.

Llámenos

(506) 8714-3598

Síganos:

LinkedIn Instagram

info@datalexlatam.com
www.datalexlatam.com
San José, Costa Rica