WHITE PAPER

CIBERSEGURIDAD: CUÁL ES EL ROL DEL DEPARTAMENTO LEGAL

La ciberseguridad es un tema de urgencia para las empresas de todo el mundo. Según una encuesta de la consultora PWC, para el 49% de los CEOs encuestados, el riesgo cibernético es su principal preocupación.

Los ataques cibernéticos han aumentado en los últimos dos años, ayudados principalmente por la adopción de tecnología en todas las industrias, el aumento del trabajo desde casa y la facilidad de difusión de información durante la pandemia.

Los sistemas empresariales tuvieron un 50% más de ataques por semana en 2021 en comparación con el año anterior, según datos de la firma de inteligencia Check Point Research. Y la expectativa es que las cifras aumenten aún más en los próximos años.

Dada la creciente importancia de la conectividad digital, estos problemas van mucho más allá del alcance y las capacidades técnicas de la industria de la seguridad de la información. Como administradores de cumplimiento corporativo, el departamento legal puede brindar orientación sobre cómo los líderes ejecutivos pueden prepararse y tratar los incidentes cibernéticos.

THOMSON REUTERS®

¿QUÉ ES LA CIBERSEGURIDAD?

La ciberseguridad es el conjunto de medidas y prácticas adoptadas para proteger los equipos, redes, programas o sistemas frente a ciberataques. Los ataques digitales tienen como objetivo acceder, destruir y/o alterar datos confidenciales, interrumpir los flujos de trabajo y extorsionar.

Los ciberdelincuentes implementan una amplia variedad de tipos de ataques contra organizaciones e individuos para comprometer la confidencialidad, integridad y disponibilidad de los datos:

Los **ataques de confidencialidad** están diseñados para robar información confidencial.

Los **ataques a la integridad** tienen como objetivo sabotear las operaciones e infligir daños a la reputación.

Los **ataques de disponibilidad** tienen como objetivo evitar que los usuarios accedan a los datos.

¿POR QUÉ FALLA LA CIBERSEGURIDAD?

La ciberseguridad puede fallar principalmente debido a la falta de un seguimiento adecuado. Ninguna empresa es 100% segura y es muy difícil controlar amenazas o actores maliciosos.

Para decidir dónde, cuándo y cómo invertir en controles de TI y defensa cibernética, el primer paso es evaluar las capacidades de seguridad para las personas, los procesos y la tecnología, identificando las brechas que deben llenarse y las prioridades que deben abordarse.

El elemento humano aparece en los riesgos de ciberseguridad. Según el **Instituto Ponemon, en una investigación realizada en conjunto con IBM**, el 24% de los incidentes de violación de datos son causados por errores humanos.

Los ciberdelincuentes se han convertido en expertos en ingeniería social y utilizan técnicas sofisticadas para engañar a los empleados para que hagan clic en enlaces maliciosos. Asegurarse de que estas personas sepan cómo defenderse contra estos ataques es fundamental.

EL ESCENARIO DE LOS CIBERATAQUES EN MÉXICO

Número de ataques cibernéticos

enero-junio	2021	2022
	60 mil millones	85 mil millones

Número total de ataques cibernéticos

2019	2021	crecimiento
300.3 millones	120 mil millones	casi 400 veces

Lucros del Cibercrime

2021	2025
US$ 6 trillones	US$ 15 trillones

Fuente: El Financiero

LEYES DE PROTECCIÓN DE DATOS Y CIBERSEGURIDAD EN MÉXICO

En México no existe un marco legal específico que regule la ciberseguridad. Si bien existe una Estrategia Nacional de Ciberseguridad, esta es solo un documento que hace referencia a cuáles deben ser los objetivos del Estado a la hora de regular la ciberseguridad.

El documento también menciona que cualquier esfuerzo que se dedique a la ciberseguridad debe ser para el desarrollo social, económico y político, en los sectores público y privado.

En México, la ciberseguridad trabaja más con acciones de prevención de algunos delitos que con la adopción de políticas y principios para el sector público y privado. De esa forma, solo existe una regulación específica respecto a delitos como las violaciones de los sistemas de seguridad de la información.

Desde 2013, el acceso a internet es considerado un derecho fundamental porque forma parte de los derechos constitucionales fundamentales. Esto ha influido en que los organismos reguladores reconozcan el uso de Internet y la protección de la seguridad en el entorno digital.

Existen ciertas disposiciones relacionadas con la ciberseguridad:

- **Ley de Protección de Datos (para entidades públicas y privadas).**
- **Ley Federal de Telecomunicaciones y Radiodifusión y sus lineamientos sobre colaboración en seguridad y justicia.**
- **Ley General de Transparencia y Acceso a la Información Pública.**
- **Código Penal Federal y Código Procesal Penal Nacional.**
- **Ley de Acceso de las Mujeres a una Vida Libre de Violencia.**
- **Acuerdo Estados Unidos-México-Canadá.**

LA IMPORTANCIA DEL DEPARTAMENTO JURÍDICO EN LA CIBERSEGURIDAD

El impacto del riesgo cibernético es capaz de afectar profundamente a un negocio. Y, como se ve a menudo, las brechas en la seguridad de los datos resultan en pérdidas críticas como la propiedad intelectual y la información corporativa, lo que resulta en una pérdida de credibilidad y responsabilidad legal.

Históricamente, la responsabilidad de administrar y mitigar el riesgo de ciberseguridad ha recaído principalmente en el equipo de seguridad de la información.

A menudo, las empresas atacadas tardan días (o incluso semanas) en responder legalmente. La razón es que el departamento legal demora en familiarizarse con el asunto.

Este sector juega un papel clave para asegurar que todos los esfuerzos de la compañía cumplan con las obligaciones regulatorias. Su función es estratégica para establecer la gobernanza y los controles que equilibren la protección de la información crítica y confidencial con la productividad y el cumplimiento normativo. Se necesita una gran implicación lo antes posible.

Expectativas empresariales para la ciberseguridad

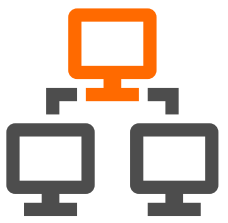
El 50% espera más cumplimiento y participación del consejo general en la evaluación de resiliencia cibernética

El 73% dijo que los altos directivos reciben información sobre seguridad de la información trimestral o anualmente

El 33% dijo que recibe esta información mensualmente.

5 MEDIDAS DE PREVENCIÓN DE CIBERATAQUES

Como dice el dicho, "más vale prevenir que curar". El departamento legal puede ayudar a desarrollar planes de acción estratégicos para mejorar la ciberseguridad.



1. Comprender la diferencia entre compliance y seguridad

Si la empresa recopila información o datos personales de clientes o proveedores, debe tener la obligación ética y legal de administrarlos. No es suficiente usar la frase "no compartiremos su información personal" o instituir informes de auditoría.

El primer paso es saber qué datos se recopilan, dónde se almacenan, quién tiene acceso a ellos y por qué. Esto permite establecer cuál es el uso "normal" de los datos para la organización, lo que facilita saber cuándo alguien intenta sustraerlos.

2. Hacer que la seguridad de los datos sea responsabilidad de todos

Muchas de las brechas de seguridad involucran accesos privilegiados. Esto significa que una persona interna, sin saberlo o con malas intenciones, ha expuesto sus credenciales y datos confidenciales.

Otro pilar de una estrategia debe ser educar a los empleados sobre cómo limitar su exposición. También es importante considerar cuestiones como el control de acceso a los datos.

3. Conoce al enemigo

En el proceso de análisis de 100 filtraciones de datos, **el equipo de investigación de Imperva identificó los cuatro tipos de atacantes de una empresa**. El primer tipo es el interno involuntario o malicioso, que generalmente tiene acceso a los activos o credenciales y es el menos sospechoso.

Los otros son atacantes externos, que toman la información confidencial que quieren. Una estrategia de seguridad debe considerar atacantes internos y externos y contar con mecanismos para descubrir y corregir la extracción de datos anormales.

4. Hacer un PRD

Un PRD (Plan de Recuperación ante Desastres) contiene una lista de infraestructuras de TI críticas, priorizando el OTR (Objetivo de Tiempo de Recuperación). Debe detallar las prioridades y describir los pasos necesarios para reiniciar, reconfigurar y recuperar sistemas y redes.

El Plan también debe tener una lista de responsabilidades, personal clave y debe mantenerse en formato físico. También detalle los sistemas de almacenamiento de datos, que pueden mejorar tu velocidad de recuperación.

5. Documentar la estrategia de ciberseguridad

Otro punto importante es documentar la estrategia de ciberseguridad. Esto incluye redactar o actualizar evaluaciones de riesgos, planes, políticas y directrices. Es fundamental dejar en claro cuáles son las responsabilidades de cada persona.

Asegúrate de que, al redactar y actualizar estos documentos, cuentes con la participación activa y la retroalimentación de las personas involucradas. También llevará tiempo explicar la importancia de los cambios.

¿QUÉ HACER DESPUÉS DE UN CIBERATAQUE?

Contención inmediata

El primer punto es asegurar la red para evitar más daños o robo de datos. El departamento legal debe convocar de inmediato una reunión con todos los involucrados en ciberseguridad. Si las credenciales se indican como comprometidas, solicita cambiar todas las contraseñas y los permisos de acceso hasta que todo termine. Será necesario tomar otras medidas más específicas, dependiendo del tipo de ataque.

Informar a los interesados

Según las circunstancias, puede ser necesario notificar a los clientes, empleados, inversores y otros socios comerciales. El departamento legal debe trabajar para identificar rápidamente qué obligaciones de notificación tiene. Involucrar a los líderes de marketing y comunicaciones para ayudar a elaborar mensajes internos y externos apropiados cuando sea necesario.

Notificar a las autoridades

A quién debe contactar el departamento legal depende de dónde se encuentre la empresa en el mundo. Pero primero, tienes que empezar con la policía local. Luego te informarán dónde más puedes denunciar la infracción, a nivel nacional e internacional. Si la empresa tiene un seguro que cubre el delito cibernético, comunícate también con esa empresa.

PONIENDO EN PRÁCTICA EL PRD

Ahora toca poner en práctica todo lo pensado en PRD. Si tu organización no cuenta con un plan de recuperación ante desastres, es hora de pensar en uno. ¿Qué es lo más importante para las operaciones comerciales? ¿Qué es fundamental para volver a funcionar primero? ¿Qué datos de copia de seguridad se han aislado de forma segura? Junto con el equipo de seguridad, deberás pensar en las prioridades y dependencias.

CONCLUSIÓN

Desarrollar e implementar una estrategia de seguridad cibernética es un proceso continuo y presentará muchos desafíos. Es extremadamente importante monitorear y reevaluar periódicamente las políticas y prácticas de seguridad cibernética de su organización.

Finalmente, es importante prepararte para repensar tu estrategia de seguridad cibernética si surge una nueva amenaza. La velocidad es primordial.