Las leyes 21.459, 21.633 de **CIBERDELITOS/CIBERSEGURIDAD** y la ley 21.719 de **PROTECCIÓN DE DATOS PERSONALES** obligan a las empresas a implementar sistemas de gestión, que permitan prevenir, detectar, responder y demostrar cumplimiento frente a riesgos tecnológicos y de tratamiento de información.

STePconsulting
riesgo corporativo · seguridad pública

¿Qué pasasi ocurre un incidente y la empresa no tiene un modelo de prevención de los delitos que norman ambas leyes?

Un incidente puede ocurrir igual. La diferencia es si la empresa puede demostrar debida diligencia: Prevención, control y respuesta.

Contar con este modelo de prevención de delitos y **operarlo de manera eficiente**, representa un **seguro legal** frente a las graves y altas sanciones a los que se expone cualquier empresa y sus ejecutivos y directores.

STePconsulting
riesgo corporativo . seguridad pública

¿QUIÉN PUEDE SANCIONAR?

- **Autoridad de Ciberseguridad** (según aplique): fiscaliza y puede exigir medidas correctivas.
- **Autoridad de Protección de Datos**: fiscaliza, investiga y sanciona por incumplimientos de privacidad y seguridad.
- **Tribunales civiles**: demandas por daños de clientes/terceros.
- **Reguladores sectoriales / contrapartes** (si aplica): exigencias contractuales, auditorías y restricciones.

¿POR QUÉ SANCIONAN A LA EMPRESA SI FUE "VÍCTIMA"?

No por el ataque en sí, sino por no haber adoptado medidas razonables exigibles: gestión de riesgos, controles, protocolos de incidentes, seguridad de datos, trazabilidad

¿A QUÉ SE EXPONE LA EMPRESA?

- Multas administrativas (especialmente en datos personales).
- Órdenes obligatorias de corrección (implementación de medidas, auditorías, controles).
- Suspensión/limitación de tratamientos o procesos críticos (en datos personales).
- Responsabilidad civil por daños + impacto reputacional y comercial

¿A QUÉ SE EXPONEN DIRECTORES/EJECUTIVOS?

- Cuestionamientos por falta de supervisión y diligencia (deber de cuidado).
- Responsabilidad administrativa y/o civilen casos de negligencia relevante.
- Mayor exposiciónen auditorías, fiscalizaciones y eventuales litigios.

STePconsulting
riesgo corporativo . seguridad pública

¿CÓMO SE CUMPLE LA NORMA Y SE EVITAN LOS RIESGOS?

Diseñamos e implementamos un modelo que permita prevenir y reducir el riesgo de sanciones, y, si ocurre un incidente, acreditar cumplimiento y debida diligencia con evidencia verificable.

Nuestra propuesta es elaborada por un equipo experto en infraestructura, seguridad y cumplimiento TI, mas un equipo legal especializado, lo que permitirá evaluar sistemas, procesos y controles tecnológicos, identificando brechas técnicas que impactan directamente el cumplimiento legal.

¿CÓMO LOS PODEMOS APOYAR?

Elaborando un MPD "llave en mano" operativo

- Revisión técnica de infraestructura, sistemas y procesos TI.
- Entrevistas con personal clave (TI, operaciones, seguridad, legal).
- Análisis de cumplimiento frente a checklist técnico-legal.
- Análisis de cumplimiento técnico-informático.
- Identificación de brechas y riesgos asociados.
- Propuesta de acciones correctivas técnicas infomáticas y legales (priorizadas).
- Informe técnico legal e informático con hallazgos.
- Plan de acción y apoyo en su implentación

STePconsulting
riesgo corporativo . seguridad pública

Han confiado en nosotros empresas del rubro industrial, alimentos, eléctrico, financiero y retail. Complementa lo anterior el trabajo que nuestro equipo desarrolla en prevención y control de delitos para proyectos de Naciones Unidas, Comité Interamericano contra el Terrorismo, Gobiernos de Estados Unidos, Canadá, República Dominicana, Costa Rica y Colombia, entre otros.

¿CÓMO SEGUIMOS?

Si quiere implementar de manera rápida y eficiente las nuevas exigencias legales contáctenos al e-mail compliance@step-c.com o al whatsapp +56978549125

WWW.STEP-C.COM