CYBERGUARD

Cumpliendo con la Ley: Guía para Implementar un Sistema de Gestión de Ciberseguridad en Chile

Ley Marco de Ciberseguridad en Chile (Ley N° 21.663):

¿Qué deben cumplir las empresas?

La Ley Marco de Ciberseguridad en Chile (Ley N° 21.663) representa un hito en la protección de datos y sistemas informáticos en el país. Esta normativa establece una serie de requisitos y obligaciones para las empresas, especialmente aquellas que operan en sectores críticos como el eléctrico, financiero, salud y telecomunicaciones.

¿Qué deben cumplir las empresas afectadas por esta ley?

A grandes rasgos, las empresas deben implementar un **sistema de gestión de ciberseguridad** que les permita:

- **Identificar y evaluar los riesgos:** Realizar un análisis exhaustivo de las amenazas a las que están expuestas y evaluar su impacto potencial.
- **Implementar medidas de seguridad:** Adoptar medidas técnicas y organizativas para proteger sus sistemas y datos, como firewalls, sistemas de detección de intrusiones, encriptación, políticas de acceso y capacitación del personal.
- **Gestionar incidentes de ciberseguridad:** Establecer procedimientos para detectar, responder y contener los incidentes de seguridad de manera oportuna y eficaz.
- **Informar sobre incidentes:** Notificar a las autoridades competentes y a los afectados en caso de sufrir un incidente de ciberseguridad que pueda poner en riesgo la seguridad nacional o los derechos de terceros.
- **Realizar evaluaciones periódicas:** Evaluar de forma regular la efectividad de su sistema de gestión de ciberseguridad y realizar los ajustes necesarios.

Al identificar los riesgos y puntos críticos, será necesario establecer medidas mitigatorias a estos riesgos, como; la instalación de antivirus de nueva generación, implementación de sistemas de detección de intrusos, generar nexos y métodos de comunicación con entidades del estado, sistemas de respuesta ante incidentes, entre otros.

¿Qué sectores están especialmente afectados?

Aunque la ley se aplica a una amplia gama de empresas, existen algunos sectores que son considerados críticos y, por lo tanto, están sujetos a requisitos más exigentes. Entre ellos se encuentran:

- **Red pública del Estado**
- **Energía y suministro**
- **Telecomunicaciones**
- **Transportes**
- **Financieros**
- **Salud**

¿Cuáles son las consecuencias de no cumplir con la ley?

El incumplimiento de la Ley Marco de Ciberseguridad puede acarrear sanciones administrativas, como multas que pueden alcanzar cifras significativas. Además, las empresas podrían enfrentar demandas por parte de terceros afectados por un incidente de seguridad.

¿Cómo pueden las empresas prepararse?

Para cumplir con los requisitos de la ley, las empresas pueden tomar las siguientes medidas:

- **Realizar una auditoría de seguridad:** Identificar las brechas de seguridad existentes y establecer un plan de acción para remediarlas.
- **Implementar un sistema de gestión de identidad y acceso (IAM):** Controlar el acceso a los sistemas y datos de la empresa.
- **Capacitar al personal:** Concientizar a los empleados sobre los riesgos de seguridad y enseñarles a identificar y reportar posibles amenazas.
- **Contratar a un experto en ciberseguridad externo:** Obtener asesoramiento especializado para implementar y mantener un sistema de gestión de ciberseguridad efectivo.
- **Contratar sistemas de detección:** Obtener un servicio que permita la detección y protección proactiva frente a intrusos
- **Instalar Antivirus de nueva generación:** Gestionar la adquisición de un Antivirus de nueva generación, que permita la identificación oportuna de amenazas a los dispositivos finales

¿Por dónde debo partir para cumplir con ley?

Nuestro grupo de expertos recomienda los siguientes pasos para el fiel cumplimiento de la ley:

- **Evaluación inicial:** Comienza por una evaluación exhaustiva de tu infraestructura tecnológica actual. Identificaremos tus activos, sistemas y datos más valiosos.
- **Análisis de riesgos:** Analizaremos los riesgos a los que está expuesta tu empresa, considerando amenazas internas y externas.
- **Diseño de un plan de cumplimiento:** Desarrollaremos un plan personalizado que te guiará paso a paso hacia el cumplimiento de la ley. Este plan incluirá medidas de seguridad, políticas y procedimientos.
- **Implementación de soluciones:** Implementaremos las soluciones tecnológicas y de gestión necesarias para proteger tus sistemas y datos.
- **Capacitación:** Capacitaremos a tu equipo en las mejores prácticas de ciberseguridad para que puedan identificar y responder a posibles amenazas.
- **Monitoreo continuo:** Realizaremos un monitoreo constante de tu infraestructura para detectar y responder a cualquier incidente de seguridad de manera proactiva.

¿Cuáles son los beneficios que me aportaría implementar Ciberseguridad en mi empresa?

- **Protege tu negocio:** La ciberseguridad es una inversión en la protección de tu negocio. Al cumplir con la ley, evitarás costosas multas y protegerás tu reputación.
- **Aumenta la confianza de tus clientes:** Demuestra a tus clientes que tomas en serio la seguridad de sus datos y cumple con las regulaciones vigentes.
- **Optimiza tus operaciones:** Implementaremos soluciones eficientes que te permitirán operar de manera más segura y sin interrupciones.
- **Cumple con la ley:** Asegúrate de estar al día con las últimas regulaciones y evita sanciones legales.

Preguntas frecuentes

- **¿Por dónde empiezo?** La mejor manera de comenzar es realizando una evaluación de riesgos para identificar tus necesidades específicas.
- **¿Qué tan rápido puedo cumplir con la ley?** El tiempo de implementación dependerá del tamaño y complejidad de tu organización.
- **¿Cuánto me costará?** El costo de implementar un sistema de gestión de ciberseguridad variará según tus necesidades específicas.
- **¿Qué pasa si tengo un incidente de seguridad?** Contamos con un plan de respuesta a incidentes para ayudarte a gestionar cualquier situación de crisis.