iSentinel
Protegemos el éxito de su negocio

Ley 21663
LEY MARCO DE CIBERSEGURIDAD

Principales Aspectos

Protección de Datos y Sistemas

Prevención de Ciberataques

Cumplimiento de Normativas

iSentinel
Protegemos el éxito de su negocio

Contenido

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl
www.isentinel.cl

iSentinel
Protegemos el éxito de su negocio

¿Qué es la Ley Marco de Ciberseguridad?

El Senado de Chile aprobó y publicó el pasado 8 de abril de 2024 la nueva Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información como parte de su agenda de seguridad pública.

Esta ley es fundamental para proteger los activos informáticos de las organizaciones estatales y privadas, asegurando la prevención, contención y respuesta efectiva ante incidentes de ciberseguridad.

Su objetivo es fortalecer la seguridad nacional, proteger la privacidad de los ciudadanos y aumentar la resiliencia de nuestras redes y sistemas informáticos frente a amenazas cibernéticas.

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl
www.isentinel.cl

iSentinel
Protegemos el éxito de su negocio

Objetivos de la Ley
Marco de Ciberseguridad

1
Protección
de Datos y Sistemas

2
Prevención
de Ciberataques

3
Cumplimiento
de Normativas

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl
www.isentinel.cl

iSentinel
Protegemos el éxito de su negocio

Importancia de cumplir con la ley

Marco de Ciberseguridad

Seguridad de la Información

Al cumplir con la ley, las empresas protegen sus datos y sistemas críticos, reduciendo el riesgo de brechas y ataques cibernéticos.

Confianza de los Clientes

El cumplimiento mejora la percepción de seguridad y responsabilidad, lo que fortalece la relación con los clientes al brindarles mayor tranquilidad sobre el manejo de sus datos.

Ventajas Competitivas

Las empresas que cumplen con los estándares de ciberseguridad ganan una posición de liderazgo en su sector, ya que demuestran un compromiso con la protección y la innovación.

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl
www.isentinel.cl

Nuevos Organismos

Con la publicación de la nueva ley, se han creado las siguientes instituciones o entidades, que buscan proteger el entorno digital del país:

ANCI

Agencia Nacional de Ciberseguridad

Agencia Nacional de Ciberseguridad (ANCI)

Se crea la Agencia Nacional de Ciberseguridad descrita en la propia ley como “un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, velar por la protección, promoción y respeto del derecho a la seguridad informática, y coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.”

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl
www.isentinel.cl

iSentinel
Protegemos el éxito de su negocio

Nuevos Organismos

CSIRT
Defensa Nacional

Equipo de Respuesta ante Incidentes de Seguridad Informática de la Defensa Nacional (CSIRT)

Se trata del organismo encargado de coordinar, proteger y asegurar las redes y sistemas del Ministerio de Defensa Nacional, así como los servicios esenciales y operadores vitales para la defensa nacional. Asimismo, además de crear un CSIRT Nacional, se habilita la creación de CSIRT sectoriales.

CSIRT
Nacional

Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional)

Dependiente de la ANCI. Entre sus responsabilidades está el responder a ciberataques o incidentes de ciberseguridad de efecto significativo, supervisar incidentes a nivel nacional, coordinar a los CSIRT de los distintos organismos del Estado, difundir alertas y riesgos cibernéticos a la ciudadanía y ser el punto de enlace con CSIRT extranjeros para intercambiar información en la materia.

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl
www.isentinel.cl

Nuevos Organismos

RCSE

Red de Conectividad Segura del Estado

Red de Conectividad Segura del Estado

Esta nueva Red de Conectividad ofrecerá servicios de interconexión y conectividad a internet a los organismos de la Administración del Estado como los Ministerios, las Delegaciones Presidenciales Regionales y Provinciales, las Fuerzas Armadas, la Seguridad Pública, etc.

CMS

Consejo Multisectorial

Consejo Multisectorial

Se crea un Consejo que tiene carácter consultivo y cuya función será asesorar y hacer recomendaciones a la Agencia en el análisis y revisión periódica del estado de la ciberseguridad del país. Adicionalmente, se encargará de analizar las amenazas actuales y potenciales relacionadas con la ciberseguridad y proponer medidas para hacerles frente.

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl
www.isentinel.cl

iSentinel
Protegemos el éxito de su negocio

Ámbito de Aplicación

Como se detalla en el artículo 4 de la Ley Marco de Ciberseguridad, aplicará a aquellas instituciones que presten servicios esenciales, así como las calificadas como operadores de importancia vital.

Servicios Esenciales

Se consideran servicios esenciales los provistos por los organismos de la Administración del Estado y por aquellas entidades privadas que realicen labores relacionadas con las actividades eléctricas (generación, transmisión o distribución), de combustibles (transporte, almacenamiento o distribución), suministros de agua, telecomunicaciones, infraestructuras digitales, transportes, banca, seguridad social, mensajería, servicios de salud, etc. Estos servicios se consideran vitales para el desempeño nacional y bienestar social.

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl
www.isentinel.cl

iSentinel
Protegemos el éxito de su negocio

Ambito de Aplicación

Servicios Esenciales

- ELECTRICIDAD
- BANCA
- TELECOMUNICACIONES
- INFRAESTRUCTURA DIGITAL
- SERVICIOS TI DE TERCEROS
- AGUA POTABLE
- TRANSPORTE
- TRANSPORTE DE COMBUSTIBLE
- SERVICIOS POSTALES Y MENSAJERÍA
- ATENCIÓN DE SALUD
- SEGURIDAD SOCIAL

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl
www.isentinel.cl

iSentinel
Protegemos el éxito de su negocio

Ambito de Aplicación

Importancia Vital (OIV)

Operadores de Importancia Vital (OIV)

La Agencia establecerá mediante resolución dictada por el Director o la Directora Nacional, a los prestadores de servicios esenciales que sean calificados como operadores de importancia vital.

La Agencia deberá, al menos cada tres años, revisar y actualizar la calificación de operadores de importancia vital, mediante una resolución dictada por el director o la directora nacional.

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl
www.isentinel.cl

Ambito de Aplicación

Importancia Vital (OIV)

Como se detalla en el artículo 4 de la Ley Marco de Ciberseguridad, aplicará a aquellas instituciones que sean operadores de importancia vital y que cumplan con los siguientes requisistos:

01.

El servicio que ofrecen depende de redes y sistemas informáticos.

02.

La interrupción del servicio que prestan tiene un impacto significativo en el orden público, la seguridad nacional o el cumplimiento de las funciones del Estado.

03.

El servicio que ofrecen debe ser garantizado por el Estado.

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl
www.isentinel.cl

iSentinel
Protegemos el éxito de su negocio

Obligaciones de ciberseguridad y deberes específicos en Chile

Esta ley determina que quienes estén sujetos a ella deben establecer y aplicar protocolos para prevenir, reportar y resolver incidentes de ciberseguridad. Esto incluye:

01. Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) continuo, capaz de determinar la probabilidad y el impacto de un incidente de ciberseguridad.

02. Mantener un registro de las acciones que componen al SGSI.

03. Crear e implementar planes de continuidad operacional que deben actualizarse, como mínimo, cada 2 años.

04. Realizar operaciones de revisión de forma continua, incluyendo pruebas de penetración o pentesting, para la detección temprana de situaciones que comprometan la seguridad.

05. Tomar de forma oportuna acciones que reduzcan el impacto y la propagación de un incidente de ciberseguridad.

06. Contar con las certificaciones nacionales e internacionales en materia de ciberseguridad.

07. Informar a los potenciales afectados sobre la incidencia de ciberataques que podrían afectar su acceso a redes y sistemas informáticos, así como aquellos que involucren sus datos personales.

08. Contar con programas de capacitación para sus trabajadores y colaboradores de forma continua.

09. Designar un delegado de ciberseguridad interno o subcontratado, encargado de informar a la autoridad competente (según sea el caso) sobre eventualidades en materia de ciberseguridad.

10. Todas las instituciones públicas y privadas alcanzadas por esta ley deben de reportar al Equipo Nacional de Respuesta los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos sobre el funcionamiento del país y sus instituciones.

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl
www.isentinel.cl

iSentinel
Protegemos el éxito de su negocio

Sanciones

Legales y Financieras

1 La ley también establece distintos tipos de infracciones que podrían ser cometidas y las consecuencias del incumplimiento de las obligaciones. Esto incluye multas que van desde 5.000 hasta 40.000 unidades tributarias mensuales (UTM), según la gravedad de la infracción cometida.

Daño a la Reputación

2 Una brecha de seguridad puede afectar gravemente la imagen pública de la empresa, resultando en la pérdida de clientes y socios comerciales.

Perdida de Datos y Posibles Ciberataques

3 El no cumplir con las normativas de seguridad aumenta la vulnerabilidad a ciberataques, lo que puede llevar a la pérdida de datos sensibles y disrupciones operativas.

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl
www.isentinel.cl

iSentinel
Protegemos el éxito de su negocio

Prepara a tu empresa para cumplir con nueva ley de ciberseguridad en Chile

Ante esta nueva política nacional de ciberseguridad, las empresas deben adaptarse para dar cumplimiento a las nuevas normativas. En este proceso de adaptación hay ciertas acciones importantes que las instituciones implicadas deben tomar:

01. Definir si califican como prestadores de servicios esenciales o como operadores de importancia vital.

02. Comprender los aspectos que abarca la ley y sus implicaciones en cuanto a procesos y objetivos empresariales.

03. Analizar su estatus de cumplimiento actual y determinar las acciones a tomar para optimizarlo.

04. Alinear sus protocolos y políticas de seguridad informática con los requerimientos de la ley.

05. Educar a los trabajadores de la empresa para que comprendan el ámbito de aplicación de la ley.

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl
www.isentinel.cl

iSentinel
Protegemos el éxito de su negocio

Contáctenos

Podemos ayudarlo a cumplir con esta nueva ley

NUESTRAS **SOLUCIONES**

01 SERVICIOS GESTIONADOS

02 HARDWARE

03 SOFTWARE Y LICENCIAS

04 SERVICIOS PROFESIONALES

Estos sencillos lineamientos pueden funcionar como una base sobre la cual su empresa puede construir una estrategia que le permita dar cumplimiento a la ley, protegiendo sus sistemas y redes informáticas, y evitando sanciones.

En iSentinel contamos con el equipo de prpfesionales y las soluciones que pueden adaptarse a las necesidades particulares de su empresa para ayudarle a cumplir con las obligaciones de esta nueva ley.

DIRECCIÓN: Av La Divisa 340. San Bernardo.
Santiago, Chile
FONO: +56 2 2488 6550
CORREO: ventas@isentinel.cl

+56 9 5316 7879

Protegemos el éxito de su negocio

Protegemos el éxito de su negocio