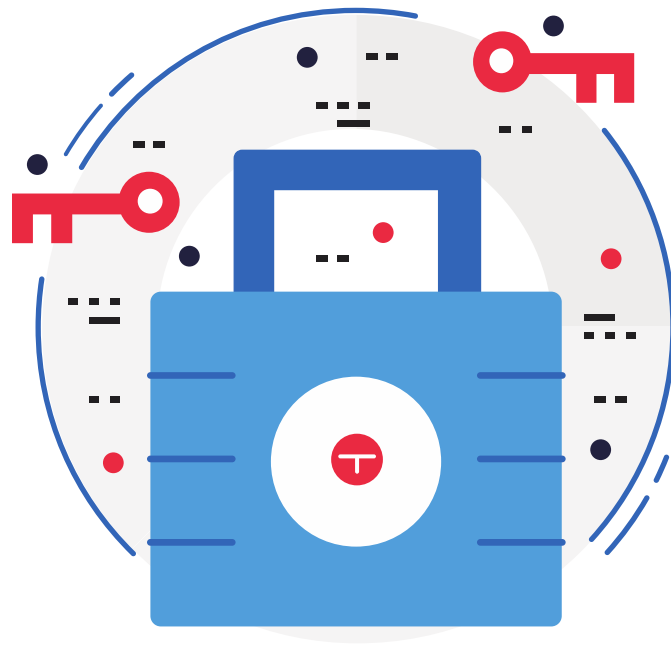


Política de Ciberseguridad

Ministerio del Interior y
Seguridad Pública



CONFIANZA

La CLAVE de la economía DIGITAL

ANTECEDENTES GENERALES

Los hechos recientes de seguridad informática **crearon un ambiente donde Chile es percibido como un país altamente vulnerable a delitos informáticos** o hackeos masivos.

El desarrollo tecnológico y la digitalización de los procesos **ha superado la velocidad de actualización de las normativas o leyes, por lo que se está trabajando en iniciativas** para subir estándares y establecer normas de Ciberseguridad.

Los datos personales, su privacidad y cuidado **son responsabilidad de cada persona**. Solo si el Estado los solicita, es responsabilidad de las Instituciones resguardar dichos datos personales y las transacciones asociadas a ellos.

Debe quedar claro que la responsabilidad de la seguridad informática es de cada sector, de las autoridades **fiscalizadoras y de los Ministerios respectivos**.

La problemática de **ciberseguridad no siempre tiene la relevancia** en la mapa de riesgos de las Instituciones o Empresas.

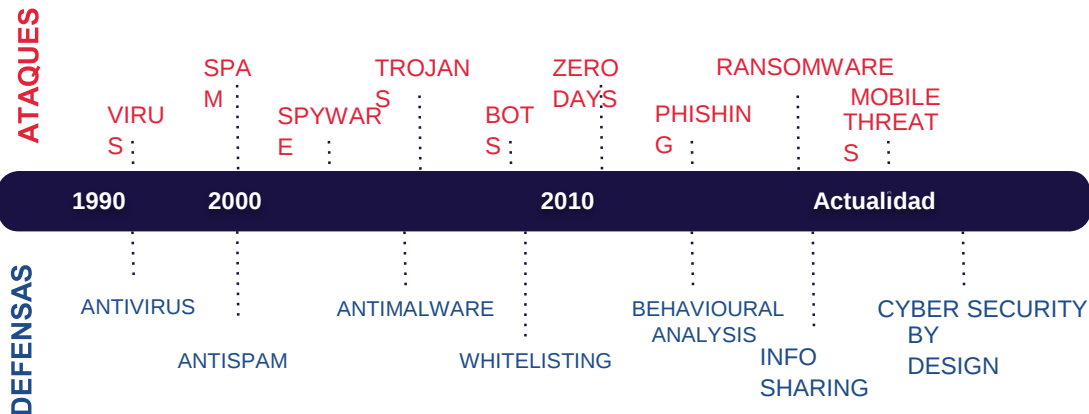


CONTEXTO ACTUAL

Ciberseguridad

Las tecnologías digitales mejoran los negocios tradicionales y exploran nuevos espacios de mercado. De esta forma, **LA DIGITALIZACION**, se convierte en un pilar fundamental para el crecimiento y eficiencia de la Sociedad.

Los mecanismos de seguridad informática deben evolucionar a la par con el desarrollo digital.



Innovación Digital y Modernización

La CIBERSEGURIDAD es un elemento clave para la digitalización. Su principal tarea es digitalizar y proteger las infraestructuras críticas para los Sistemas de Información.

POLITICA NACIONAL DE CIBERSEGURIDAD



Es un lineamiento político del Estado de Chile en materia de Ciberseguridad.



El objetivo principal es tener un Ciberespacio libre, abierto, seguro y resiliente a través de acciones que permitan identificar y gestionar riesgos.



Establece 5 ejes estratégicos: Infraestructura, Legislación, Difusión, Colaboración Internacional y Desarrollo de Industria.



Establece proyectos de ley tales como: Nueva Ley de Delitos Informáticos ; Ley Marco de Ciberseguridad ;Ley de Infraestructura Crítica para Ciberseguridad.



Debe definir un modelo de gobernanza que determine las relaciones interministeriales y el rol específico de los organismos al implementar esas funciones.

PRÓXIMOS PASOS

DEBE EXISTIR una Gobernanza responsable de coordinar la administración de la seguridad informática o Ciberseguridad, actualizar y/o realizar normas o leyes.

Respecto a Ciberseguridad se deben distinguir **TRES AREAS** claramente identificadas:

- 1 Instituciones del Gobierno:** Responsable de la Seguridad Informática en Ministerios y/o empresas públicas del Estado, definidas como estratégicas para los sistemas de información dependiente del **Ministerio del Interior**.
- 2 Infraestructuras Críticas:** Responsable de coordinar las políticas de Seguridad Informática en los sectores regulados estratégicos del sector privado, dependiente del **Ministerio de Economía**.
- 3 Ciberdefensa:** bajo la coordinación y responsabilidad del **Ministerio de Defensa**.

Los responsables de esas áreas deben implementar los estándares informáticos y crear los **Centros de Respuesta ante Incidencias Informáticas** (Centros de Coordinación de Seguridad Informática).



La responsabilidad de la seguridad informática y cumplimiento de los estándares que dicte Gobierno Digital es **de cada sector, de las autoridades fiscalizadoras y de los Ministerios respectivos.**

GOBERNANZA DE CIBERSEGURIDAD NACIONAL

Bajo la dependencia de un **Coordinador Nacional de Ciberseguridad** (Ministerio del Interior) deberá implementar los tres Centros de Respuestas a Incidencias Informáticas y las macro-tareas que se proponen a continuación;

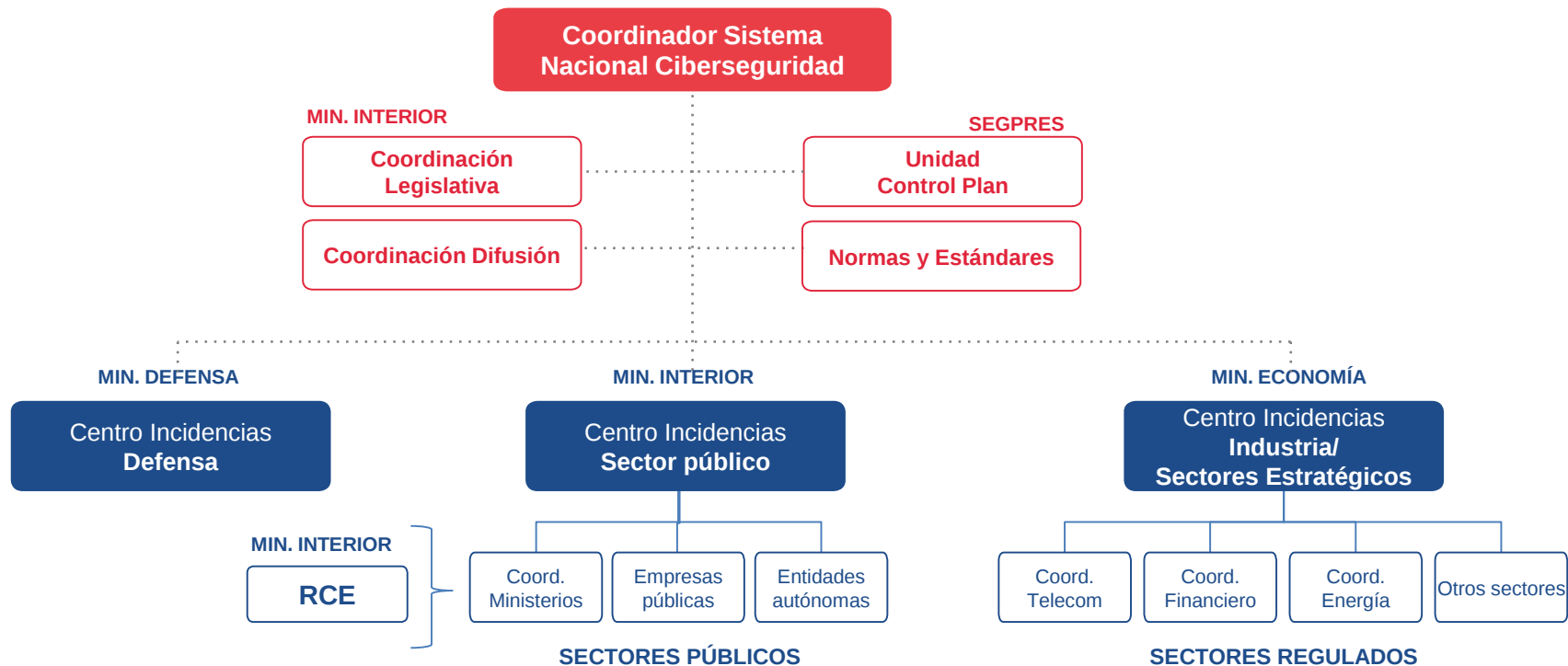
- **Centro de Gobierno y Nacional** (Ministerio Interior)
- **Centro de Infraestructuras Críticas** (Ministerio de Economía)
- **Centro Incidencias Ciberdefensa** (Ministerio de Defensa)

MACRO TAREAS

- Normativa y Estándares Ciberseguridad (Gobierno Digital Segpres)
- Reformulación Red de Conectividad del Estado (Ministerio del Interior)



GOBERNANZA PROVISORIA DE CIBERSEGURIDAD



METAS Y COMPROMISOS (1/2)

I.

Actualización Decretos de Conectividad y Ciberseguridad del Estado AÑO 2018

- Incorporación de **estándares de Seguridad Informática** a las Redes de Telecomunicaciones.
- Incorporación de **nuevos estándares** de Ciberseguridad a las *instituciones del Estado* y *actualización de la RED de Conectividad del Estado*.
- **Instructivo Presidencial** con Gobernanza Transitoria y normas mínimas de Ciberseguridad para el Estado
- **Exigencias de Ciberseguridad** a *proveedores del Estado*.
- Coordinación y mecanismos de **intercambio de experiencias y de información** con Gobiernos y Entidades Internacionales.

METAS Y COMPROMISOS (2/2)

II.

Infraestructura Crítica Para Sistemas de Información AÑO 2019

- Implementación del **Centro de Respuesta a Incidencias Informáticas** y de Ciberseguridad del Estado.
- Estándares y *exigencias mínimas de **seguridad informática** a sectores estratégicos Sector Privado.*
- Implementar en sectores de servicios básicos y servicios financieros o de retail más relevantes, **Centros de Respuesta ante Incidentes Informáticos.**
- **Capacitación y difusión de buenas prácticas** en los organismo del Estado.
- Incentivar **campañas de Información y Difusión**, en los sectores más sensibles para la población, al resguardo y cuidado de su información personal

AGENDA LEGISLATIVA

Proyecto de Ley General de Banco (LGB)

- Proyecto de Ley en trámite.
- Ley Corta para incorporar exigencias de Ciberseguridad mercado financiero.

Proyecto Ley Registro de Celulares Prepago

- Presentar proyecto ley para el registro de teléfonos de prepago. Este tema tiene beneficios para prevención del delito, disminuir el fraude en Portabilidad y minimizar los delitos de Ciberseguridad.

Proyecto Ley de Datos Personales

- En trámite. Una buena protección de los datos personales es clave.

Nueva Ley de Delitos Informáticos

- Tipificación de Nuevos Delitos.
- (Convención de Budapest)
- Mejora procesal de la prueba del delito.

Ley de Infraestructura crítica para Sistemas de Información

- Definición de Instituciones Públicas y Empresas Privadas estratégicas para los sistemas de Información.
- Regulación de ellas para evitar y mejorar incidentes de emergencias Informáticas.

Ley Marco de Ciberseguridad

- Definiciones y responsabilidades sobre Ciberseguridad.
- Creación de Centros de Respuesta ante Incidencias/Emergencias Informáticas en sectores público y privado.

MUCHAS GRACIAS



Política de Ciberseguridad

Ministerio del Interior y
Seguridad Pública