

SUBSECRETARÍA DE DEFENSA

Amenazas de Ciberseguridad que afectan a la Sociedad Civil y la Defensa



Subsecretaría de
Defensa

Gobierno de Chile

Subsecretario de Defensa
Fernando Ayala González

Junio, 2022

Agenda

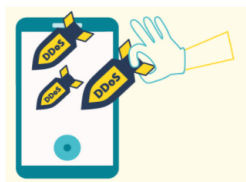
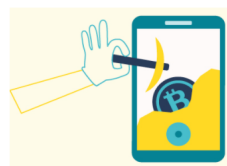
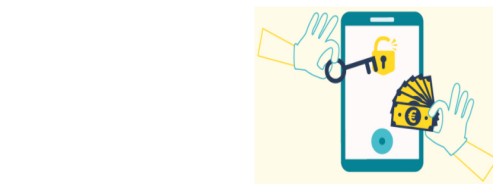
- Amenazas Cibernéticas
- Tendencias en Ciberseguridad
- Política Nacional de Ciberseguridad
- Gobernanza de Ciberseguridad Sector Defensa
- Conclusiones



Amenazas Cibernéticas

Unión Europea – Dic. 2021

- Programas de Secuestro Ransomware
- Criptominería no autorizada
- Programas malignos
- Violaciones o fugas de datos
- Ataques por email y captura de credenciales
- Amenazas por errores humanos
- Ataques de denegación de servicio
- Campañas de Desinformación
- Amenaza a Cadena de Suministros



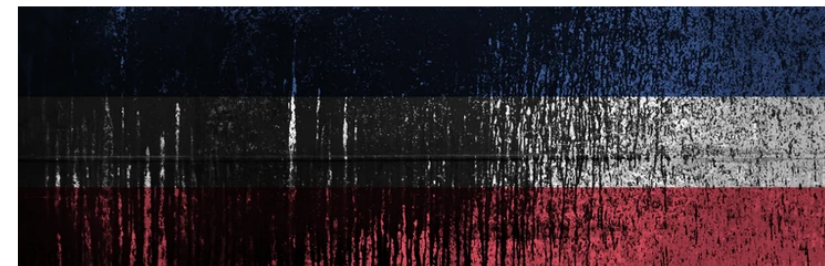
internationalIT

ES

HOME SOLUCIONES

Conti Ransomware: Costa Rica declara estado de emergencia

El presidente de Costa Rica, Rodrigo Chaves, declaró el estado de emergencia nacional luego de los ataques cibernéticos del grupo de ransomware Conti en varias agencias gubernamentales.



<https://www.internationalit.com/>

Tendencias en Ciberseguridad

- **Zero Trust - Confianza Cero**

Modelo basado en el principio de «*no confiar nunca y verificar siempre*» cada conexión de los dispositivos.

- **Ciberseguridad impulsada por Inteligencia Artificial – IA**

La IA mediante la orquestación y automatización de procesos, permite identificar amenazas y responder a ataques en menor tiempo, además de la protección proactiva de los datos y sistemas.

- **Dispositivos móviles, nuevos vectores de ataque**

Dispositivos conectados permanente con plataformas y servicios, exponiendo inconscientemente, información personal o de la organización a ciberdelincuentes.

- **Concienciación y Capacitación**

El factor humano suele ser un facilitador de ingreso de malware a la organización o captura de credenciales (phishing), es clave la formación y el desarrollo de una cultura de ciberseguridad.

Política Nacional de Ciberseguridad - PNCS

A. Pilares

1. Resguardar la seguridad de las personas en el ciberespacio
2. Proteger la seguridad del país, (ej. Costa Rica)
3. Promover la colaboración y coordinación entre instituciones
4. Gestionar los riesgos del ciberespacio

B. Objetivos

- ✓ ... Infraestructura de la información robusta y resiliente ...
- ✓ El Estado velará por los derechos de las personas en el ciberespacio
- ✓ ... Cultura de la ciberseguridad ...
- ✓ ... Cooperación en ciberseguridad con otros actores ...
- ✓ El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos

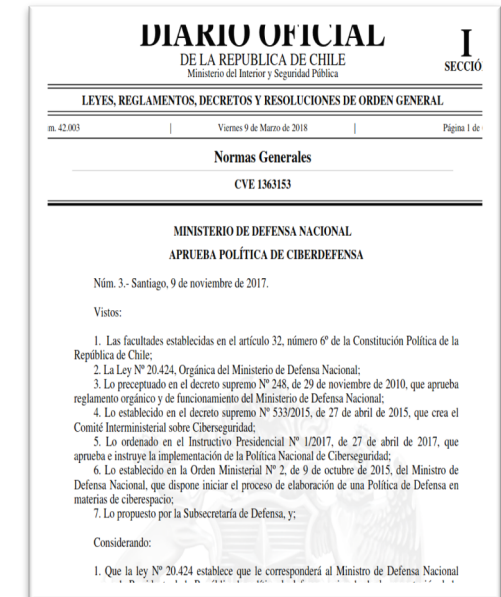
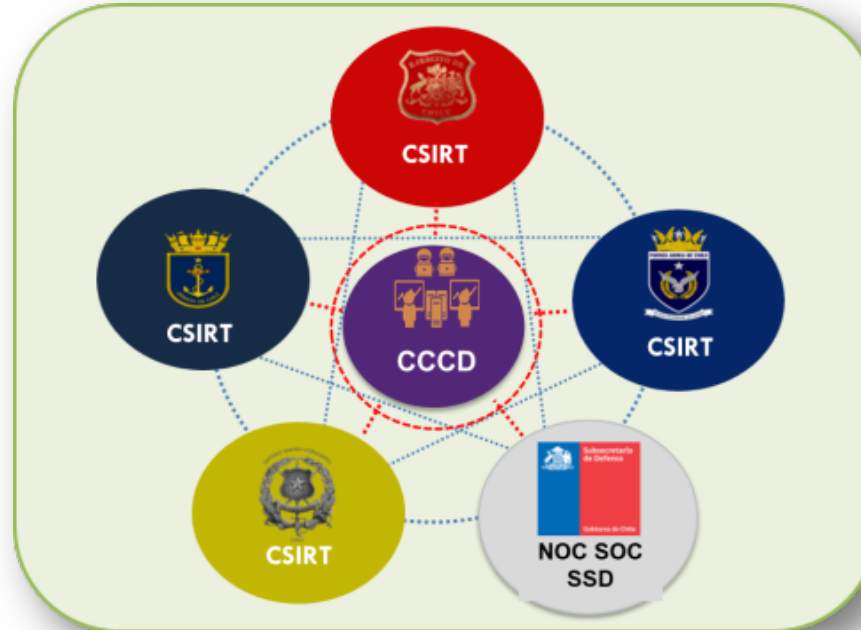


Gobernanza de Ciberseguridad en el Sector Defensa

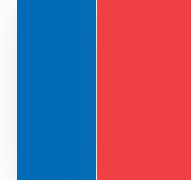
Política de Ciberdefensa, aspectos considerados:

1. Empleo de los medios de ciberdefensa
2. Cooperación internacional y promoción de la transparencia y la confianza entre los Estados
3. Desarrollo de capacidades

Organización e interacción



Gobernanza de Ciberseguridad en el Sector Defensa



Colaboración y cooperación internacional

Acuerdos para facilitar el intercambio de información de amenazas en el ciberespacio y de ciberincidentes. Acceso a formación y ejercicios en Ciberseguridad



Argentina



Brasil



Colombia



Ecuador



España



EE.UU.



Estonia



Israel



OEA



UK.



Uruguay



México

Colaboración con la Academia

Acuerdos para fomentar la investigación y desarrollo de tecnologías aplicadas y herramientas de Ciberseguridad.



Instancias de Colaboración Nacional - sector público, privado, academia y sociedad civil.

- ✓ "Hoja de Ruta en Ciberseguridad" - PUC y Microsoft
- ✓ "Mesa de Ciberseguridad de la Comisión Futuro del Senado de Chile" - Senado.



Conclusiones

A. Desafíos

Fomentar una cultura digital segura.

Incentivar la inversión, investigación y el trabajo conjunto sector público, privado, academia y ciudadanía.

B. Normas y regulaciones

Continuar avanzando en la Gobernanza de Ciberseguridad p.ej. "*Ley Marco sobre Ciberseguridad e Infraestructuras Críticas de la Información*", institucionalidad para un ciberespacio libre, abierto, seguro y resiliente.

C. Colaboración nacional e internacional

Potenciar el círculo virtuoso, donde se avanza hacia una mayor madurez, conciencia y mitigación de los riesgos en el ciberespacio de manera colaborativa, a través de formación, innovación, prevención y respuesta, para un mayor beneficio y desarrollo económico social.

SUBSECRETARÍA DE DEFENSA

Amenazas de Ciberseguridad que afectan a la Sociedad Civil y la Defensa



Subsecretaría de
Defensa

Gobierno de Chile

Subsecretario de Defensa
Fernando Ayala González

Junio, 2022