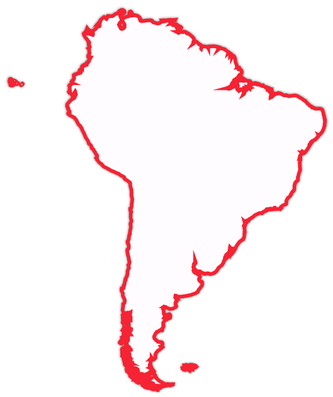
Gobierno de Chile

Avances en Ley de Infraestructura Crítica

Ciberseguridad en Chile



En Chile el gasto en ciberseguridad en 2017 totalizó US$195,7 millones*.

↑ 4,1 % 2017/2016

El 82,9% de los accesos a internet en Chile son móviles.

La navegación vía smartphones, tuvo un 1 9,8% de crecimiento en 2017

El desarrollo Digital en Chile ha alcanzado un 65,71% y un 38,96% de desarrollo en ciberseguridad (Brecha de 26,75%)

Los ciber-délitos crecieron en un 74% entre 2016 y 2017

0.07% Inversión del PIB nacional por debajo del 0,12% promedio mundial

*Fuente : *Boston Consulting Group/ SUBTEL - PDI

Se define como Infraestructura Crítica (IC) a las instalaciones, sistema o parte de éste, que es esencial para el mantenimiento de las funciones sociales básicas, y cuya perturbación o destrucción, afectaría gravemente la salud, la integridad física, la seguridad y el bienestar social y económico de la población*.

En el caso chileno, mientras se adopta una medida especifica para IC, la infraestructura de la información de los siguientes sectores será considerada como crítica (tentativa):

Aguas

Telecomunicaciones

Transporte

Servicios Financieros

Defensa

Energía

Seguridad Pública

Salud

Administración Pública

Protección Civil

Espacio

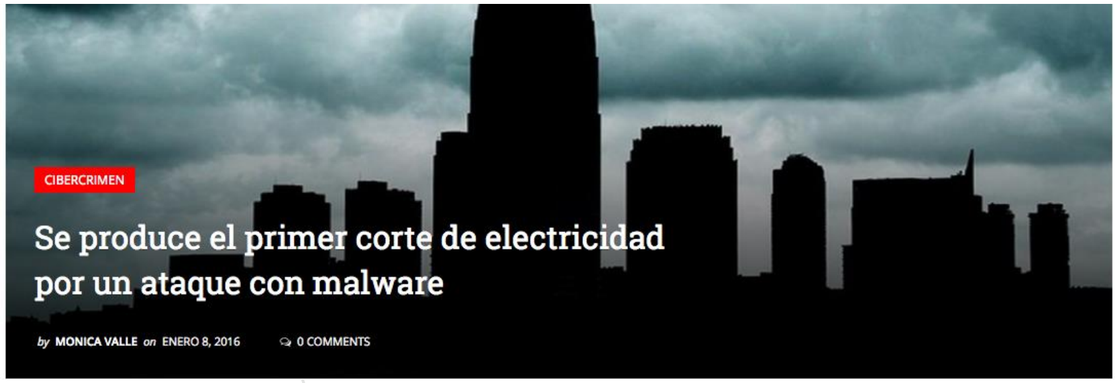
Algunos ciber-ataques a Infraestructura Crítica

Miles de hogares perdieron en pleno invierno, su suministro de servicio eléctrico por varias horas, en distintas zonas de Ucrania a causa de el troyano Industroyer.

La noche en la que Ucrania se quedó sin luz

Tecnología

Ucrania sufre una ola de ciberataques a sus compañías eléctricas



Corte de electricidad en Ucrania fue un ciberataque

BBC 11-Ene-2017

Tweet Compartir **Un corte de energía que afectó a parte de la capital ucraniana, Kiev, en diciembre de 2016, ha sido catalogado como un ataque cibernético por investigadores que analizan el incidente.**

El apagón duró poco más de una hora y comenzó poco antes de la medianoche del 17 de diciembre.

La compañía de seguridad informática Security Systems Security Partners (ISSP) ha vinculado el incidente a un ataque y apagón en 2015 que afectó a 225,000 personas.

También dijo que otra serie de ataques recientes en Ucrania estaban relacionados.

El corte de energía de 2016 ocasionó una pérdida aproximada de un quinto del consumo de energía de Kiev a esa hora de la noche, informó la compañía energética nacional Ukrenergo en ese momento.

Se confirma que un ciberataque causó los cortes de luz en Ucrania

El Departamento de Seguridad Nacional de los Estados Unidos emitió un reporte que confirma la causa de los cortes de luz, que afectaron a 225.000 personas.

Algunos ciber-ataques a Infraestructura Crítica

En enero de 2017 Las cámaras de seguridad de Washington fueron infectadas por 2 ransomware, días antes de asumir Donald Trump, dejando sin vigilancia a la ciudad durante unas 48 horas.

Durante cuatro días en enero pasado, tuvieron acceso a más de 120 cámaras controladas por la policía.

por RAÚL ESTRADA

Romanian hackers infiltrated 65% of DC's outdoor surveillance cameras

Public Safety

Romanian hackers took over D.C. surveillance cameras just before presidential inauguration, federal prosecutors say

UN RANSOMWARE ATACA EL CIRCUITO CERRADO DE CÁMARAS DE VÍDEO DE LA POLICÍA DE WASHINGTON D.C.

Noticias Seguridad | January 30, 2017 | Incidentes, Malware - Virus | No Comments

Share this...

US says Romanians hacked Washington DC police cameras

29 December 2017 Share

Algunos ciber-ataques a Infraestructura Crítica

En mayo del 2017 más de 16 hospitales del Reino Unido se vieron afectados por un ransomware, interrumpiendo atenciones a pacientes de emergencia.

TECH | CYBERSECURITY | CRYPTOCURRENCY

UK hospitals hit with massive ransomware attack

Sixteen hospitals shut down as a result of the attack

By Russell Brandom | @russellbrandom | May 12, 2017, 11:36am EDT

Health

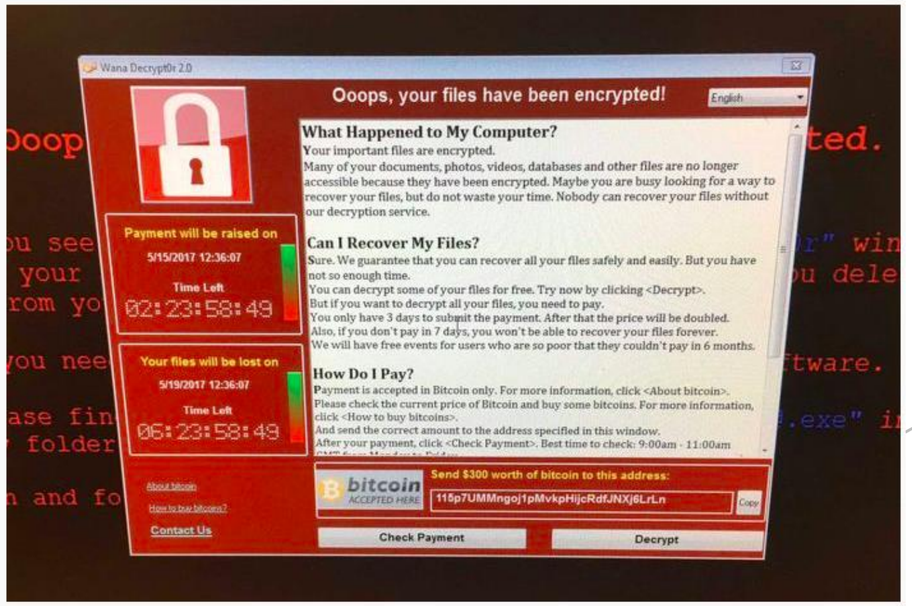
NHS cyber-attack: GPs and hospitals hit by ransomware

13 May 2017 Share

'Ransomware' cyberattack cripples hospitals across England

Ransomware cyberattack: UK's health system recovered from hacking, interior minister says

Updated 13 May 2017, 5:24pm



Algunos ciber-ataques a Infraestructura Crítica

En mayo de 2018 en Banco de Chile, un virus entro a la red anulando sus discos de arranque y obligó a la suspensión de más de 9 mil sucursales a nivel nacional.

Hackers roban 10 mdd de un banco en Chile

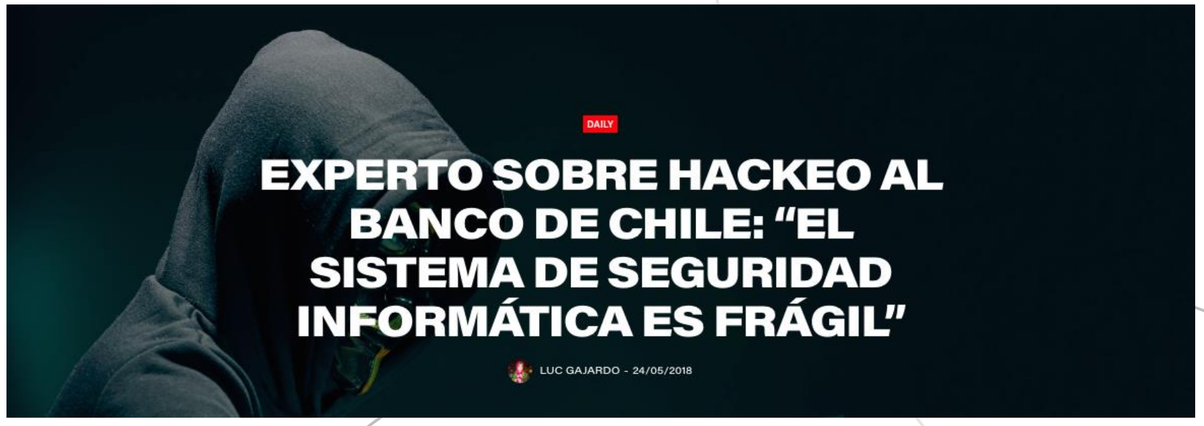
El gerente general del Banco de Chile anuncia que una banda de hackers robó 10 millones de dólares a través de un ataque informático el pasado 24 de mayo

BUSINESS NEWS JUNE 11, 2018 / 3:48 PM / 2 MONTHS AGO

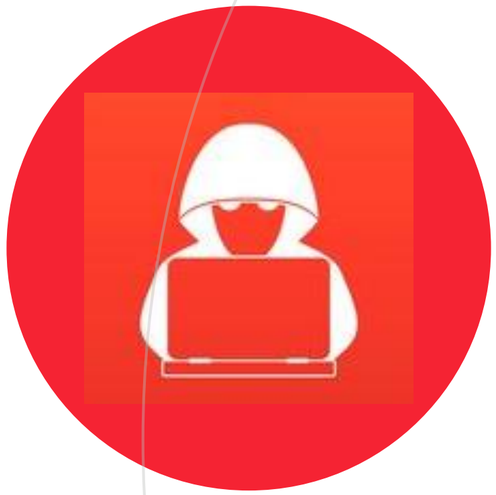
Bank of Chile trading down after hackers rob millions in cyberattack

Caída del sistema informático del Banco de Chile lo obligó a cerrar todas las sucursales del país

lo



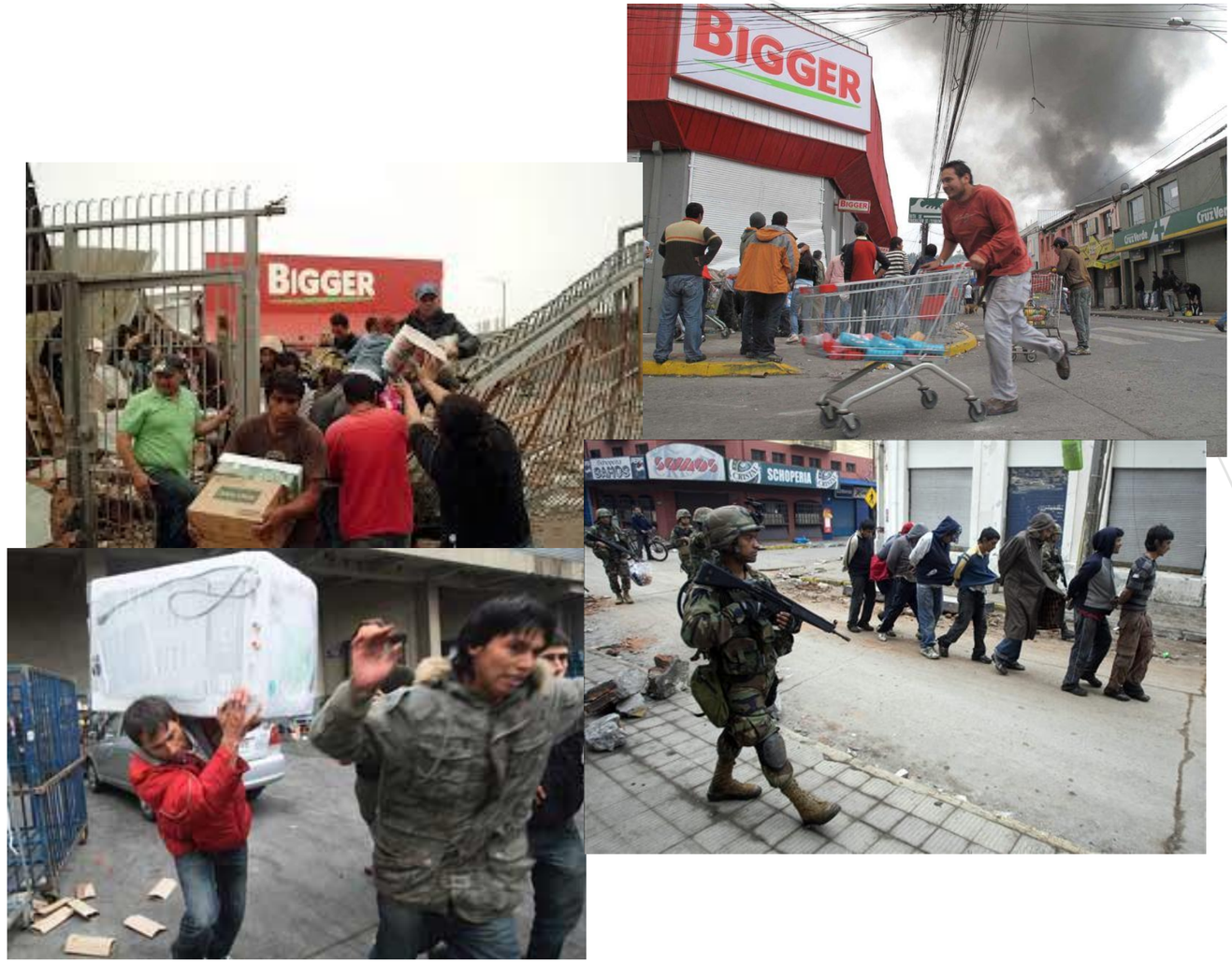
¿Qué podría ocurrir si un día en Chile no funcionase nada? no hubiese luz, no se pudiera sacar dinero del cajero, pagar con tarjeta, o no funcionaran las redes de comunicaciones…



La “incomunicación” se convierte en un desastre progresivo que desencadena accidentes, agresividad, saqueos y, en definitiva, un estado de terror generalizado .

"El impacto —se simula lo que sucedería si se tratase de un ciberataque que cortase la electricidad—, se propaga en progresión geométrica, y acaba siendo similar al que podría producir un desastre natural como un gran terremoto o un huracán o un atentado brutal…"

Un ejemplo, similar a nivel país, sería lo que ocurrió en la Ciudad de Concepción después del Terremoto del 2010, un caos generalizado….



La OEA junto a Microsoft realizaron el primer reporte de "Protección a infraestructura crítica en Latinoamérica y el Caribe", donde encuestaron a más de 500 dueños y operadores del sector en la región. Del estudio se extrae que, entre 2016 y 2017, el 73% de las organizaciones y empresas ligadas a este tipo de infraestructuras recibieron ataques de terceros. Sólo en España, los ataques a la Infraestructura Crítica los dos primeros meses del 2018, duplicaron a todos los del 2017.

Ejemplos de amenazas a la Infraestructura Crítica

✓Compromiso de información: Señales de interferencia e interceptación que comprometen, Espionaje remoto, Escucha secreta, Robo de medios o documentos, Robo de equipos, Recuperación de medios reciclados o descartados, Divulgación, Datos de fuentes poco fiables, Manipulación con hardware, Manipulación con software, Detección de posición.

✓Fallas técnicas: Saturación del sistemas críticos de información, Mal funcionamiento del software, Brecha/fisura de mantenimiento del sistema de información.

✓Acciones no autorizadas: Uso no autorizado del equipo, Copia fraudulenta de software, Uso de software falsificado o copiado, Corrupción de datos, Procesamiento ilegal de datos.

✓Compromiso de funciones: Error de uso, Abuso de derechos, Falsificación de derechos, Negación de acciones, Brecha de disponibilidad de personal.

✓Fuentes de amenazas humanas: Hackers, Delitos Informáticos, Terrorismo, Espionaje Industrial.

Referencia: ISO27005

Cuales son los objetivos de una Ley de Infraestructura Crítica

- ✓Establecer mecanismos apropiados para facilitar el desarrollo y el intercambio de mejores prácticas sobre la protección de sitios vulnerables, espacios públicos o infraestructura crítica.
- ✓Fortalecer la capacidad de los sectores público / privado y aumentar el desarrollo de alianzas para la protección de la infraestructura crítica, incluida la seguridad en Internet, cibernética y turística, responsables de la respuesta a incidentes, a fin de prevenir y reaccionar de manera eficiente a los riesgos y amenazas potenciales.
- ✓Mejorar la capacidad de respuesta y la resiliencia promoviendo métodos de planificación, prevención, gestión de crisis y recuperación.
- ✓Utilizar los mecanismos de colaboración existentes para cooperar en identificar y mitigar las intrusiones o diseminación de actos maliciosos que afecten al ciberespacio nacional.

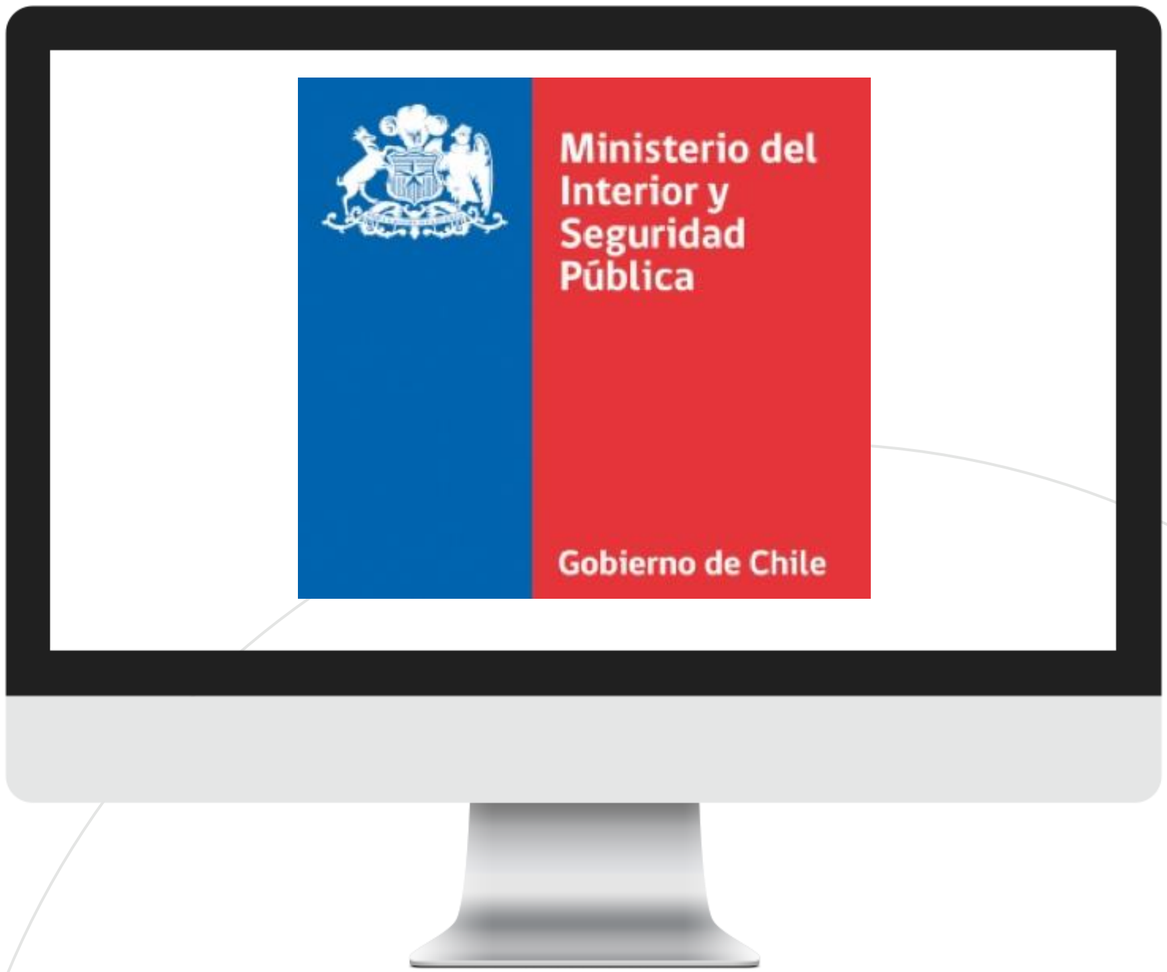
Avances en Ley de Infraestructura Crítica

Considerando los elementos entregados por la Política Nacional de Ciberseguridad, se están definiendo los términos de Infraestructura Crítica General e Infraestructura Crítica de la Información, centrándose en un set de riesgos de **infraestructuras críticas de la información.** Para ello, se están analizando, diversos modelos internacionales de complejidad, alta o media.

- Es esencial identificar y jerarquizar cuáles son los sectores que se considerarán críticos y establecer equipos de respuesta de incidentes de Ciberseguridad por cada uno, tanto desde la perspectiva pública como privada.
- Un papel relevante es el que tiene el CSIRT Gubernamental como organismo central en la Administración del Estado en el proceso de manejo, respuesta y coordinación frente a incidentes de seguridad en aquellos sectores definidos como críticos.
- Se esta trabajando en la creación de un CSIRT Nacional.
- Mesas de trabajo a nivel de distintos ministerios: Interior y Seguridad Pública, Defensa, Segpres, Obras Públicas, Hacienda, Transporte y Telecomunicaciones y ANI, cuyo resultado será un proyecto de ley en esta materia y algunas medidas sectoriales a implementar.

MUCHAS GRACIAS

www.ciberseguridad.gob.cl



CARLOS LANDEROS CARTES
Director del programa Red de Conectividad del Estado
Ministerio del Interior y Seguridad Publica