Alamys

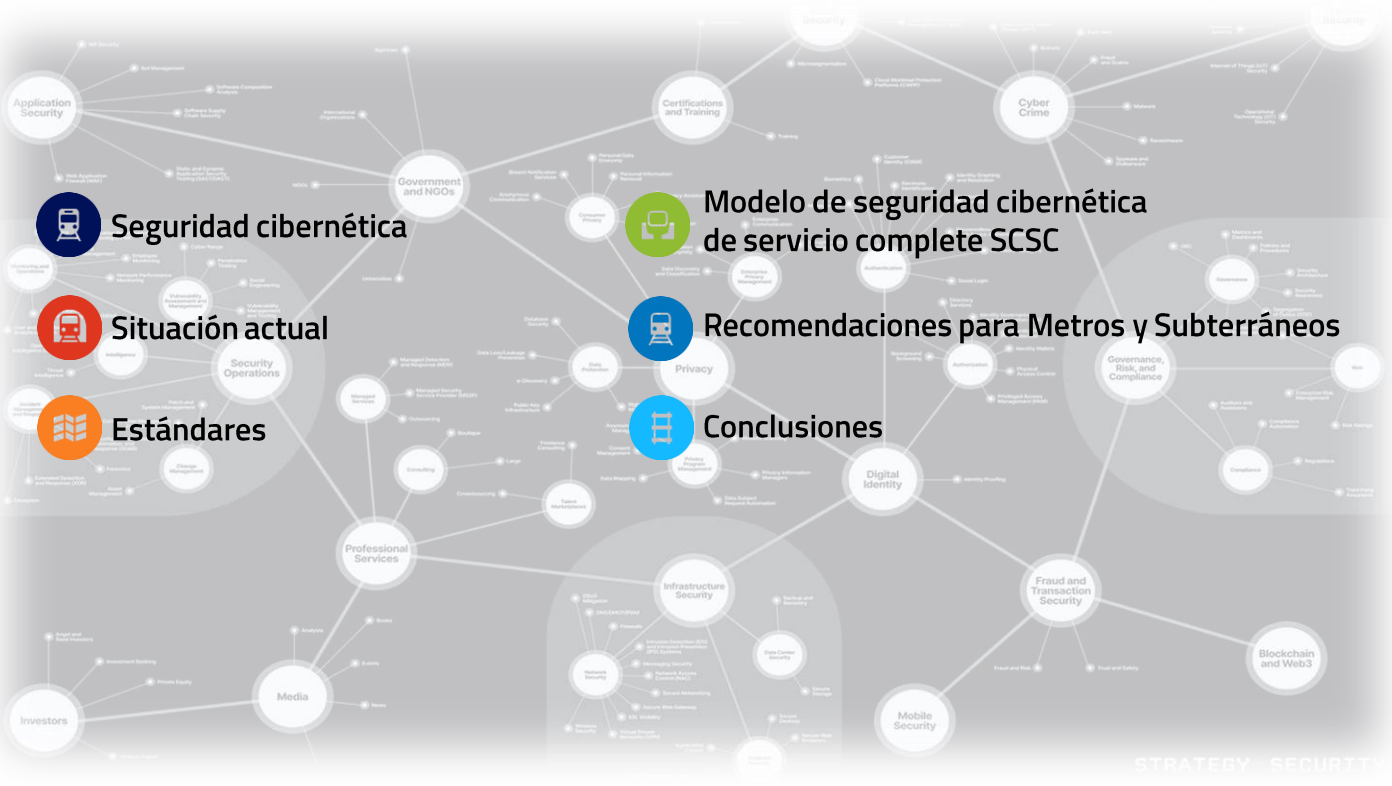
Asociación Latinoamericana de Metros y Subterráneos

Implementación Tecnológica en beneficio de la seguridad Pública y Privada

Seguridad cibernética en el transporte

DB

Índice



Seguridad cibernética

Alamys | Uniendo Destinos

"Se necesitan 20 años para construir una reputación y pocos minutos de incidente cibernético para arruinarla."

Stéphane Nappo
Global Head Information Security for Société Générale International Banking

El área de transporte ocupa el 3° puesto en objetivos de ataque!*

* Fuente: IBM Security 2021

DB

Ataque cibernético / Seguridad cibernética

Los ataques cibernéticos contra los sistemas ferroviarios han aumentado un 173% en los últimos cinco años.*

Los ataques cibernéticos son intentos maliciosos de acceder o dañar sistemas informáticos, redes y/o equipos de operación o control. Los ataques cibernéticos pueden ocasionar accidentes, pérdidas de dinero, robo de información personal o financiera.

Tácticas de ataque en 2021:#

Otros 42%

Phishing 24,8%

URL 16,2%

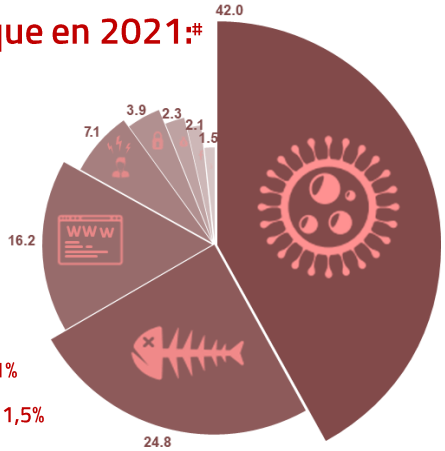
Chantaje 7,1%

Ejecutable en archivo/imagen de disco 3,9%

Fraude avanzado 2,3%

Suplantación de marcas 2,1%

Maldoc (adjunto malicioso) 1,5%



La seguridad cibernética trata de prevenir, detectar y responder los ataques cibernéticos que podrían afectar ampliamente a las personas, las organizaciones, la comunidad y la nación.

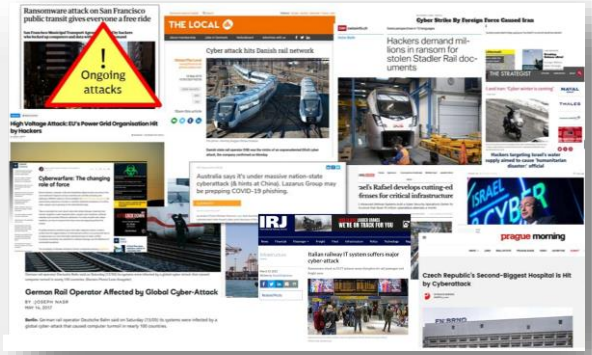
No podemos obtener un 100% de seguridad, pero se puede lograr un gran nivel de protección.
La seguridad cibernética es una tarea operativa y continua.

Hay tres etapas para evitar, reconocer y combatir ataques:

*Fuente: Reporte Cylus 2022 #Fuente: Hornetsecurity report 2022

Situación actual

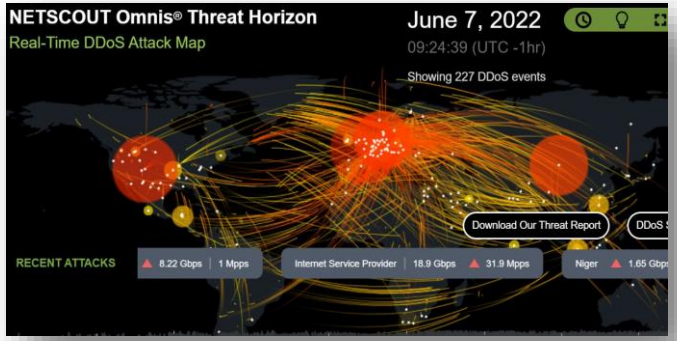
Los ataques cibernéticos fueron aumentando drásticamente desde 2017.



Daños causados por la ciberdelincuencia en empresas según Bitkom

6 Áreas problemáticas actuales:

- Demasiados puntos débiles en softwares.
- Protección insuficiente contra malwares.
- Redes inseguras.
- Peligros por el uso de dispositivos móviles.
- Los usuarios de Internet tienen muy poca competencia en Internet y su seguridad.
- Tecnologías informáticas y de seguridad manipuladas.



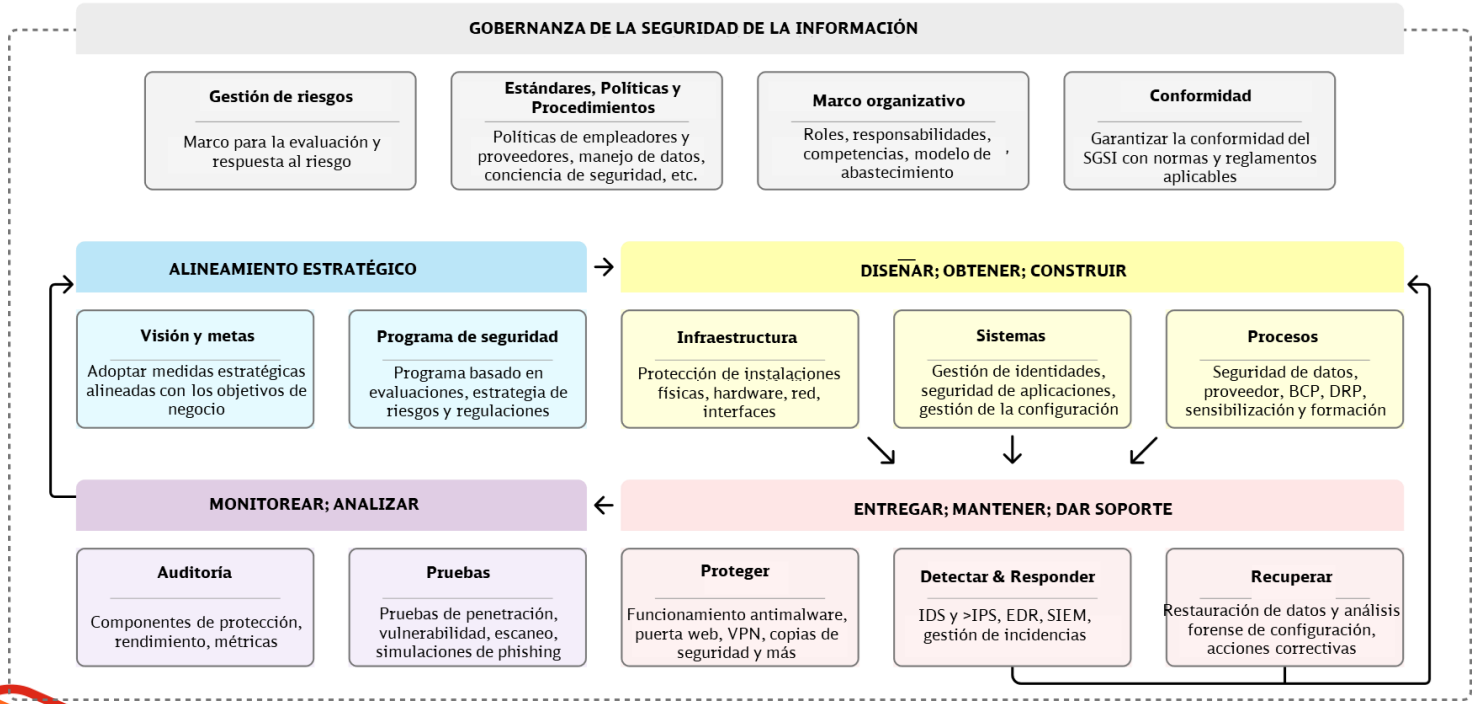
Un ataque de denegación de servicio distribuido (DDoS) es un intento malicioso de interferir en el tráfico normal de un sitio web.

Estándares en seguridad cibernética

Ejemplo del marco de implementación de un sistema de seguridad bajo la norma **NIST**

El sistema de seguridad a implementar tiene que conectarse con la organización:

Modelo de SC de servicio completo



Recomendaciones para Metros y Subterráneos

- Proporcionar directrices, procedimientos, medidas y plataformas con las que se pueda controlar, optimizar y garantizar la seguridad de la información.
- Concientizar a todos los colaboradores.
- Establecer normas uniformes para los proveedores de servicios y comprobar su cumplimiento.
- Crear un equipo de respuesta a Incidentes de seguridad cibernética.
- Revisar el riesgo global de las vulnerabilidades y evaluarlas sistemáticamente. Escenarios con cisnes negros.
- Actualización periódica del catálogo de activos.
- Tener en foco la totalidad de la red con monitoreo permanente.
- En caso de daños, tener un plan B y permitir así que el negocio de pueda continuar.

Para trabajar con seguridad cibernética debemos:

a) Posicionar a la seguridad cibrenética desde la gobernanza corporative dentro de un modelo de servicio complete.

b) Implementar un sistema de seguridad considerando a la organización, los procesos y la tecnología:

I. Organización de la protección por medio de un Centro Operativo en Seguridad.
II. Control de acceso a la red.
III. Seguridad en IOT.
IV. Conformidad de los dispositivos.
V. Inventario de activos en tiempo real.

c) Responder a las necesidades de seguridad convergentes de IT-OT de manera integral:

I. Plataforma convergente capaz de supervisar redes de IT y OT desde una sola pantalla
II. Visibilidad de dispositivos en profundidad.
III. Supervisión pasiva continua para agilizar la detección y la respuesta ante amenazas.


Muchas Gracias