Evaluaciones de Seguridad en las Infraestructuras Criticas y Vulnerables de Latino América

ARTICULO DE OPINION N.4

Viernes 24 de Julio 2020.

James Sutton

Diofanor Rodriguez

Dr. Norberto Emmerich

CEEYPP

CENTRO DE ESTUDIOS EN ESTRATEGIA Y POLITICAS PUBLICAS

Dr.Norberto Emmerich
Presidente del CEEYPP

Introducción

El futuro desarrollo de Latinoamérica depende de la calidad y resiliencia de su infraestructura física sin la cual el continente no puede avanzar hacia la modernidad. El CEEYPP va a desarrollar un proyecto de clase mundial que incluirá a profesionales, funcionarios gubernamentales y académicos latinoamericanos, también a organizaciones públicas, privadas y corporativas interesadas en invertir en la región en temas de sustentabilidad de la infraestructura crítica.

La infraestructura nacional y regional va a jugar un papel crítico en la futura recuperación económica de América Latina. La conferencia identificará infraestructuras críticas, evaluará sus vulnerabilidades, recomendará una política nacional integral y una estrategia de implementación para proteger esas infraestructuras de las amenazas físicas y cibernéticas y propondrá medidas legales o legislativas que implementen los remedios recomendados.

Ejemplos de infraestructuras críticas son las telecomunicaciones, la energía eléctrica, la banca y finanzas y los sistemas de transporte. Los tipos de amenazas cibernéticas de interés son los ataques electrónicos, de radiofrecuencia o basados en computadoras dirigidos a los componentes de información o comunicaciones que controlan las infraestructuras críticas.

Al final de la conferencia se publicarán recomendaciones para el Desarrollo de una política nacional para proteger y garantizar la operación de infraestructuras nacionales críticas. En este proceso los participantes pueden representar los intereses de sus respectivos países.

Mgs. James Sutton
Analista de Inteligencia. Director General del North American Intelligence Exchange, Pensilvania.

Los problemas de infraestructura crítica en América Latina. Diagnóstico general y vulnerabilidades.

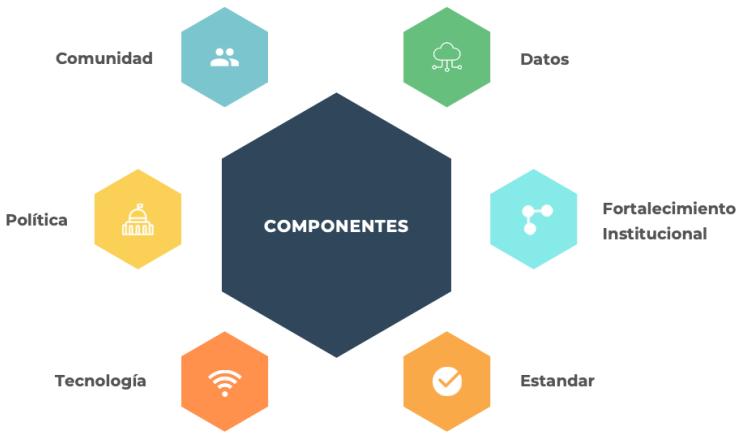
La Protección de Infraestructuras Críticas (PIC) es la necesidad de proteger los recursos vitales de una nación, como la alimentación, la agricultura o el transporte. Sin la infraestructura un país puede fallar. Sería como un cuerpo, sin huesos, cerebro o sistema circulatorio.

Todos los gobiernos Latino americanos tienen la responsabilidad moral y política de proteger su infraestructura crítica contra desastres naturales, actividades criminales al presente amenazas cibernéticas. Particularmente ahora que pasamos por un período de gran inestabilidad social, económica y multinacional. La infraestructura crítica describe los sistemas, activos físicos y cibernéticos que son vitales para un país – en los que su incapacidad o destrucción tendría un impacto debilitante para la seguridad económica y la salud pública. La infraestructura crítica juega un papel clave para proporcionar los servicios esenciales que sustentan la sociedad del país.

En Colombia, la ICDE* se entiende como un ecosistema que permite la construcción e implementación colectiva de políticas y facilita los procesos de gestión de los recursos geográficos, que incluyen datos, información y conocimiento, para armonizarlos, disponerlos y utilizarlos por el país y la Sociedad, como sustento de la Gobernanza y la toma de decisiones.

El ICDE incluye:

- Datos e Información geográfica.
- Gobierno geoespacial.
- Min – TIC (Tecnologías de Información y Comunicación).
- Conocimiento geoespacial.
- Sociedad geoespacial.



Con variaciones nacionales, los sectores críticos de los países avanzados o en desarrollo son:

1. Sector Químico.
2. Sector de Instalaciones Comerciales.
3. Sector de Comunicaciones.
4. Sector de Fabricación Esencial.
5. Sector de Presas.
6. Sector Base Industrial de Defensa.
7. Sector de Servicios de Emergencia.
8. Sector Energético.
9. Sector de Servicios Financieros.
10. Sector de Alimentación y Agricultura.
11. Sector de Instalaciones Gubernamentales.
12. Sector de Salud y Salud Pública.
13. Identificación de infraestructura crítica durante COVID-19
14. Sector de Tecnologías de Información.
15. Reactores Nucleares, Materiales y Residuos Radioactivos.
16. Agencias Sectoriales Específicas.
17. Sector de Sistemas de Transporte.
18. Sector de Sistemas de Agua y Aguas Residuales.

Algunos de estos sectores están acoplados y altamente dependientes de otros y el fracaso de uno puede afectar a todos.

Los riesgos para la infraestructura crítica son el resultado de un número finito de factores:

- **Catástrofes naturales** (inundaciones, terremotos, erupciones volcánicasimpactos de meteoritos, cualquier incidente causado por eventos naturales.)
- **Fallas del sistema** (sistemas complejos, buques, aviones, edificios, ciudades y otros componentes de infraestructura son propensos a fallas debido a la complejidad del propio sistema).
- **Errores humanos.**
- **Actividades delictivas, como el terrorismo, insurgencias y sabotaje.**

Amenaza	Descripción
Grupos Criminales	Hay un notable aumento de intrusiones cibernéticas por grupos criminales que atacan los sistemas con fines de ganancia monetaria.
Servicios de Inteligencia Extranjera	Los servicios de inteligencia extranjera utilizan herramientas cibernéticas como parte de sus actividades de recopilación de información, espionaje y sabotaje.
Hakers	Los Hakers atacan a las redes de internet por el desafío o para presumir de sus hazañas. Mientras que las herramientas de ataque se han vuelto más sofisticadas, tambien se han vuelto mas fáciles de usar. Una agresión remota requiere habilidades informáticas de fondo, mientras que los hackers pueden inyectar scripts y protocolos contra víctimas/sitios distantes.
Hakers	El hacktivismo se refiere a ataques políticamente motivados en páginas web o servidores de correo electrónico públicos. Estos grupos o individuos sobrecargan los servidores hacken el sitio web para enviar mensajes políticamente motivados, estafadores, sobotear actividades normales.
Ofensiva de Información	Varias naciones están trabajando agresivamente para desarrollar la doctrina, los programas para fines bélicos. Estas capacidades permiten que una sola entidad tenfa un impacto significativo y grave al interrumpor el suministro, y grave al interrumpir el suministro, las comunicaciones y la infraestructura económicas que apoyan el poder militar del país.
Amenaza interna (Amenaza de información privilegiada)	Esto se refiere a un empleado de confianza dentro de la organización que motivado por insatisfacción o problemas emocionales está dispuesto a traicionarla. Estos individuos son la fuente principal de delitos informáticos. Los internos no necesitan una gran cantidad de intrusiones informáticas porque su conocimiento de sistema interno de la organización les permite obtener acceso sin restricciones para causar daños al sistema o para robar datos o amenazar la distribución información privilegiada/ comprometedora.

Amenaza	Descripción
Diseñadores de Virus	Los autores de virus están planteando una amenaza cada vez más grave. Varios virus y ¨gusanos de computadoras destructivas: han dañado archivos y discos duros. Incluyendo el Virus Macro Melissa, Stuxnet, el gusano postal Explorar, el virus CiH (Chernóbil), Nimda, y Código rojo,

Recomendaciones para el desarrollo de una política nacional

La necesidad de una respuesta conjunta no es nueva. Los hallazgos y lecciones identificados por las investigaciones públicas han puesto de relieve los casos en que los servicios de emergencia podrían haber funcionado mejor juntos y han mostrado niveles mucho mayores de comunicación, cooperación y coordinación.Además de mejorar el trabajo conjunto entre los servicios de emergencia, este documento hace hincapié en la necesidad de que todas las organizaciones que responden trabajen en un enfoque conjunto y coordinado.

Co - ubicación

De esta manera los comandantes pueden realizar las funciones de comando, control y coordinación cara a cara. Deben reunirse tan pronto como sea posible, en un lugar acordado conjuntamente en la escena se conoce como el Puesto de Mando Delantero (PMD).

Comunicación

La comunicación eficaz entre los organizamos de respuesta inmediata respalda el trabajo conjunto eficaz. Compartir y comprender la información ayuda al desarrollo de una conciencia situacional compartida, que sustenta los mejores resultados posibles de un incidente.

Coordinación

Para una coordinación eficaz, una agencia generalmente necesita asumir un papel de liderazgo. Para decidir quién debe ser la agencia principal, se deben considerar factores como la fase del incidente, la necesidad de capacidades especializadas e investigación, tanto durant las fases de respuesta como de recuperación. Hay orientación específica para algunos tipos de incidentes, destacando qué agencia debe asumir el papel principal. La decision sobre quién toma el papel pricipal debe ser documentada - la agencia principal puede cambiar a medida que se desarrolla el incidente.

Terminología común

Los servicios de emergencia y los organismos de respuesta deben hacer referencias cruzadas de definiciones en los documentos de su propia organización y adoptar las definiciones comunes contenidas en el léxico. Acordar y usar terminología comín es un elemento básico para la interoperabilidad. Si hay alguna duda sobre lo que se entiende por un termino especifico, las personas deben verificar y confirmar si se ha establecido un entendimiento común.

Comprensión conjunta del riesgo

Cada organismo debe llevar a cabo sus propias ¨Evaluaciones dinámicas de riesgos¨ , pero luego compartir los resultados para que puedan planificar las medidas de control y las contingencias juntas de manera más eficaz.

Conciencia situacional compartida

La ¨conciencia situacional compartida¨ CSC es una comprensión comun de las circunstancias, las consecuencias inmediatas y las implicaciónes de las emergencias, cunto con una apreciacion de las capacidades disponibles y las prioridades de los servicios de emergencia y los organismos de respuesta. El CSC es esencial para una nteroperabilidad eficaz e importante para un entendimiento común en todos los niveles de mando, entre los comandantes de incidentes y entre las salas de control.

Observaciones Finales

Las organizaciones a menudo no consideran la importancia de su sistema de seguridad hasta que ocurre un incidente mayor que causa gran daño, resultando en pérdidas, recursos, tiempo, operaciones y servicios esenciales. Evaluaciones de seguridad utilizando protocolos profesionales establecidos y auditables refuerzan la seguridad organizacional y notablemente descubren vulnerabilidades desconocidas. Análisis a fondo de la causa de origen/fundamental (root-cause analysis), seguido por remediación de estas ofrece protección lógica a posible incidentes y minimiza la magnitud de daños futuros.

Aparte de presentar una perspectiva táctica y estratégica del tema, nuestro objetivo es identificar infraestructuras críticas, evaluar sus vulnerabilidades, recomendar una política nacional integral y una estrategia de implementación para proteger esas infraestructuras de las amenazas físicas y cibernéticas. Con investigación adicional y su colaboración para proponer medidas legales o legislativas que implementen los remedios recomendados.
Una evaluación anual y exhaustiva de riesgos y amenazas es lo más importante que la dirección ejecutiva pueden hacer para mejorar la seguridad de su organización anticipando y documentando riesgos y amenazas, posibles y probables.

Mgs. Diofanor Rodríguez
Especialista en Seguridad Privada, Seguridad Empresarial, Seguridad en los Procesos Administrativos, Análisis de Riesgos, Manejo de Personal.

Protección de Infraestructura Critica

La infraestructura crítica y cómo la protegemos se está convirtiendo en un tema destacado en todo el mundo. Mucha atención ha acaparado debido al papel que ofrece la infraestructura crítica para el bienestar de la sociedad, especialmente debido al impacto social si ocurriera una pérdida catastrófica de infraestructura crítica, ya sea debido a desastres, terrorismo o actos de guerra.

¿Qué es?

La Infraestructura Crítica (CI) está definida por el Departamento de Seguridad Nacional (DHS) en los Estados Unidos como "...los activos, sistemas y redes, ya sean físicos o virtuales, tan vitales para los Estados Unidos que su incapacitación o destrucción tendría un efecto debilitante en la seguridad, la seguridad económica nacional, la seguridad pública, salud o seguridad, o cualquier combinación de los mismos ".

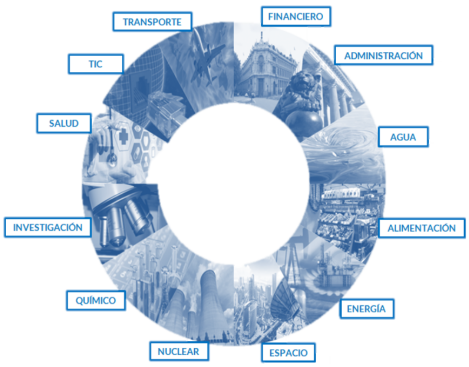
Infraestructura:

- Instalaciones
- Redes
- Sistemas
- Equipos físicos
- Equipos informáticos

Críticas

- Sobre ellas descansa el funcionamiento de los servicios esenciales.
- Su funcionamiento es indispensable y no permite soluciones alternativas.
- Su perturbación o destrucción tendrá un grave impacto en los servicios esenciales.

SECTORES ESTRATÉGICOS



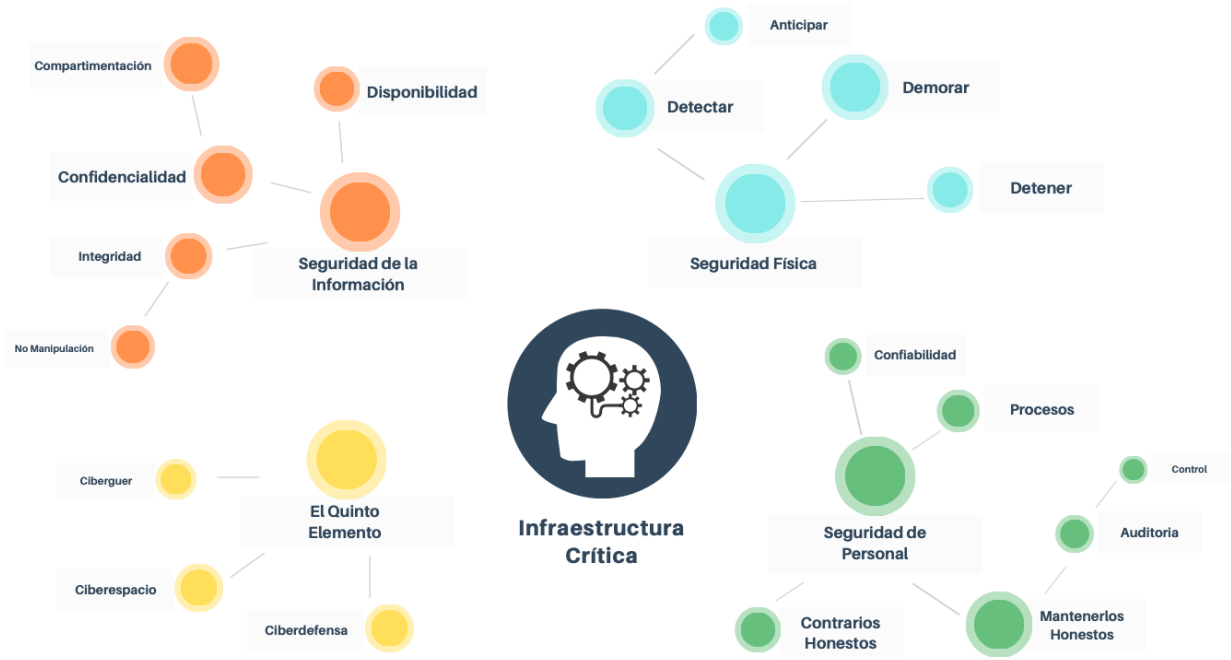
PRINCIPALES RESPONSABLES DE LA PROTECCIÓN DE LA INFRAESTRUCTURA CRÍTICA

Operadores críticos

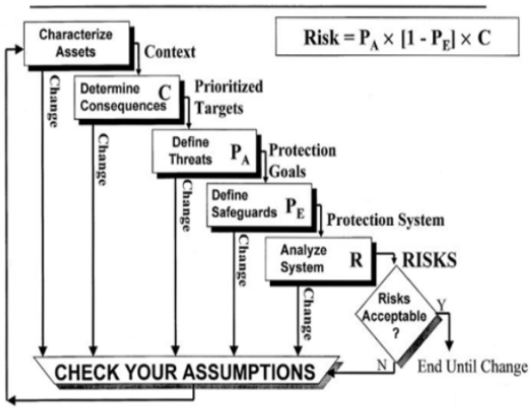
Entidad u organismo responsable de las inversiones o del funcionamiento diario de una infraestructura critica.

Tipologías

- Públicos/Privados.
- Titulares/Gestores.
- Diferencias por sector.



Riesgo



Caracterizar activos

Determinar Secuencias C

Definir Salvaguardias P_A

Analizar Sistema P_E

Costo Beneficio R

- Contexto.
- Objetivos Priorizados.
- Objetivos de Protección.
- Sistemas de Protección.
- Riesgos.
- Definir Riesgos.

Compruebe sus suposiciones

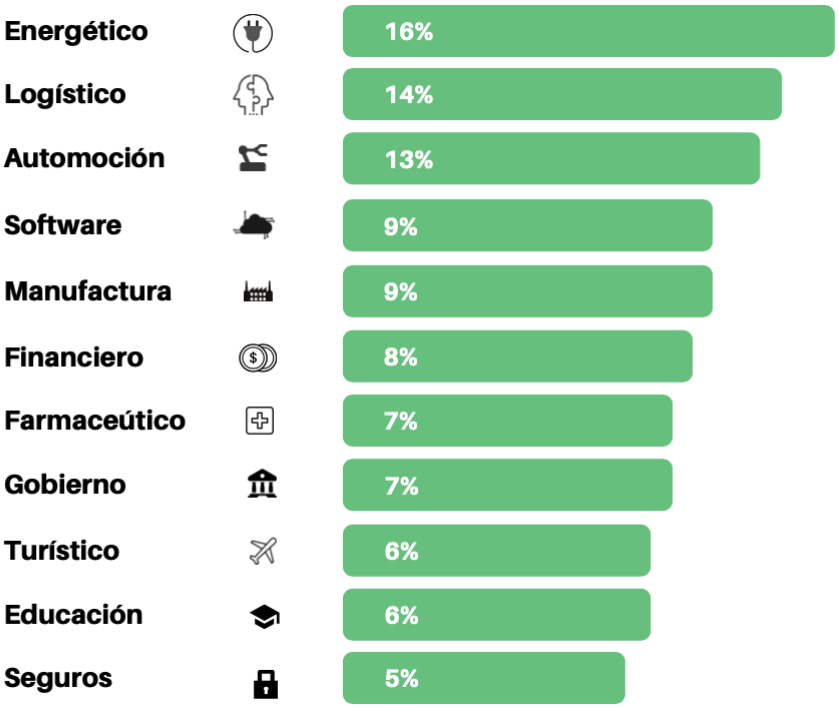
RIESGO = $P_A \times (1 - P_E) \times C$

Ciberseguridad en infraestructura crítica

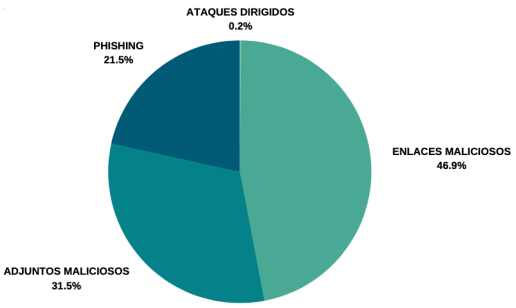
1. **El ataque en 2010 a la planta nuclear de Natanz, en Irán.**
2. **Cinco años después,** en diciembre de 2015, Ucrania experimentó un asalto sin precedentes en su red eléctrica.
3. **El tercer y más alarmante ataque que conocemos tuvo lugar en 2017.** Los ciberterroristas asumieron el control remoto de una estación de trabajo ampliamente conocida que estaba en Arabia Saudita.

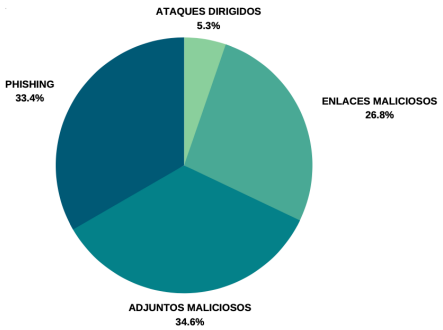
La seguridad en estos sistemas en estos últimos años en un tema de excepcional relevancia desde que aparecieron una serie de incidentes en los cuales estaban implicados Stuxnet, Dragonfly y Sandworm.
Estos ataques mostraban que es posible para los ciberterroristas, empresas competidoras y servicios secretos de otros países, sacar provecho cuando no se le da alta prioridad a la seguridad de la información de las infraestructuras críticas .

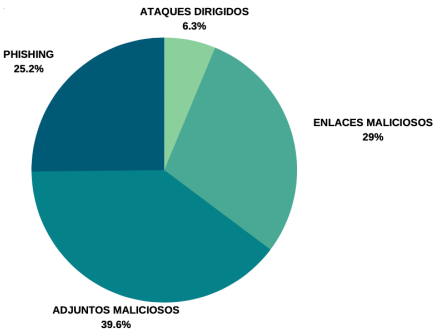
PRINCIPALES SECTORES DE ATAQUE



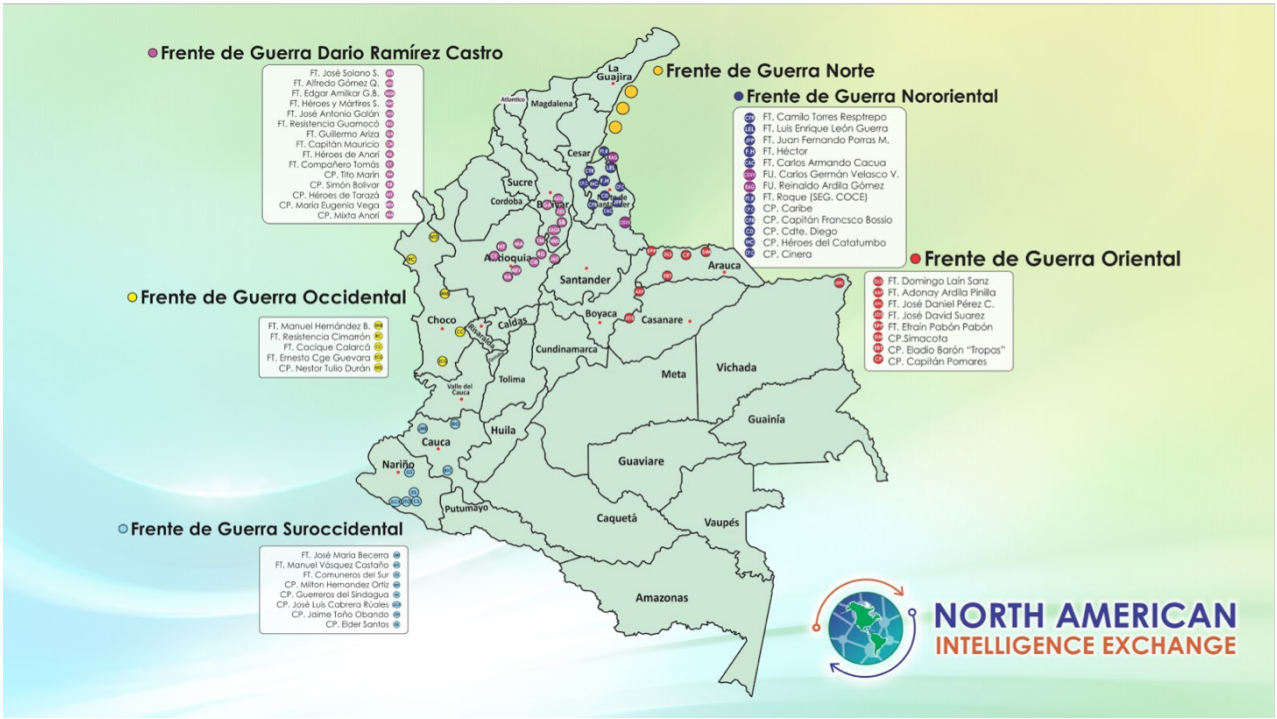
TIPOS DE ATAQUE EN INFRAESTRUCTURA CRÍTICA







CASO COLOMBIA



Conclusiones

1. Las brechas relacionadas con la protección de CI no parecen estar relacionadas con los esfuerzos de planificación o la colaboración del grupo de trabajo.
2. Las brechas en la planificación de la protección de CI generalmente se encuentran en el financiamiento gubernamental, las disputas entre agencias sobre liderazgo en varios aspectos de la planificación de protección de CI.
3. Lo relacionado con la promoción y participación de grupos de intereses especiales en lo que respecta a los derechos individuales, la privacidad, la sociedad y el medio ambiente