infosecurity MEXICO

Ciberseguridad en Infraestructuras Críticas

Ing. Omar Alfonso Castañon Sanchez

Global IT Security Senior

Compliance, Risk & Incident Response Manager

Mexichem

Definición de Infraestructuras Críticas

Se denominan **infraestructuras críticas** a aquellos sistemas y servicios que soportan infraestructuras esenciales para el desarrollo de la sociedad tal y como las conocemos actualmente, y que garantizan el normal funcionamiento de los servicios prestados por los países. De acuerdo con esta definición, existen sectores que por sus características son especialmente sensibles, como, por ejemplo:

- Alimentación
- Energía
- Agua
- Gas
- Nuclear
- Transporte
- Químico
- Comunicaciones
- Sistema Financiero y Tributario
- Salud

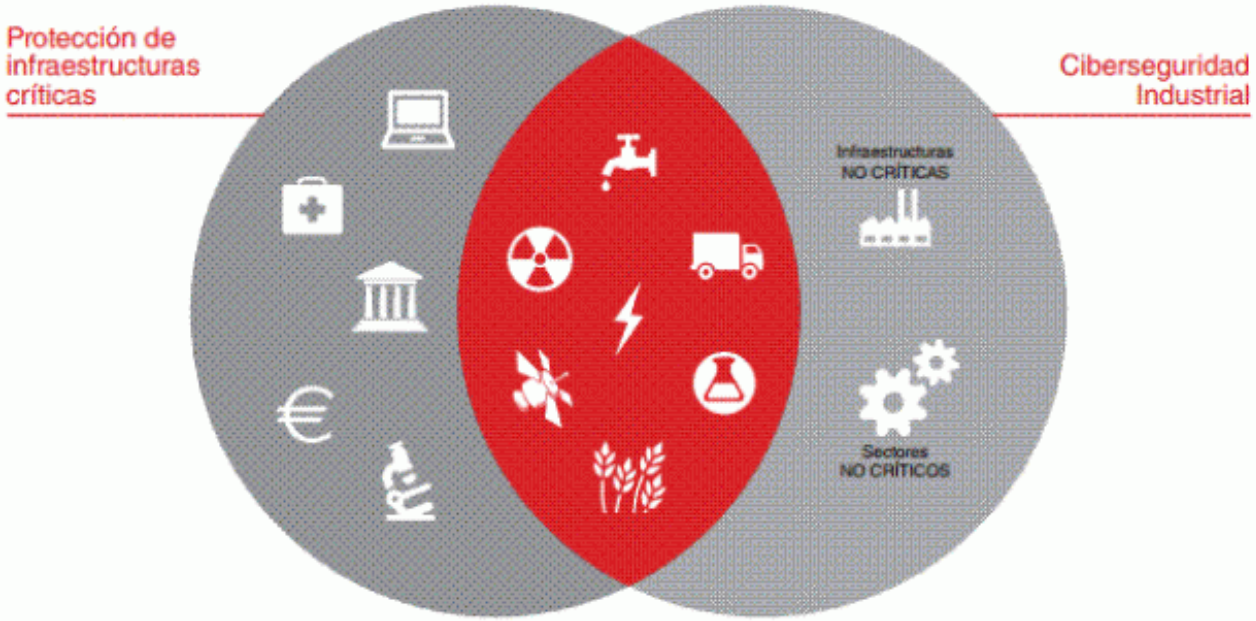


Imagen: Centro de Ciberseguridad Industrial

Actualidad de las amenazas en Infraestructuras Críticas

infosecurity MEXICO

Más interconectados que nunca

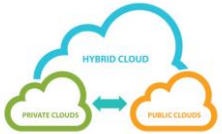
Superficie de ataque extendida

Operaciones continuas

Mantener el negocio funcionando

Usuarios conectándose de todas partes

Pérdida de control



Realidad Multi-Nube

Un mundo definido por el Software

Amenazas automatizadas y sofisticadas

Alta probabilidad de una brecha de seguridad

Los ataques están en constante evolución

infosecurity MEXICO

Advanced Persistent Threat

Unpatched Software

Spyware/Malware

Phishing

Wiper Attacks

Man in the Middle

DDoS

Cryptomining

Supply Chain Attacks

Ransomware

Data/IP Theft

Malvertising

Drive by Download

Botnets

Credential compromise

Cronograma de los principales ataques a IC

infosecurity MEXICO

2009 — NIGHT DRAGON
- Servidores de acceso público comprometidos vía inyección de SQL
- Spear-phishing
- Vulnerabilidades en Windows

2010 — STUXNET
- USB infectado
- Vulnerabilidad 0-day
- Propagación en LAN/SMB vía 0-days en Windows
- Alteración de Código Siemens

2011 — DUQU
- E-mail Spear-phishing
- Documento office explota el 0-day
- Propagación vía red interna y USB

2012 — FLAME
- E-mail Spear-phishing
- Watering Hole (webs comprometidas)
- USB infectado
- Propagación vía red interna y USB
- Ciber-Espionaje industrial

2012 — SHAMOON
- E-mail Spear-phishing
- Vulnerabilidades 0-day
- Detección de sistemas vulnerables en la red
- Wipe (Borrado de disco)

2013 — DRAGON FLY
- Ataque Spear-phishing (PDF + Havex)
- Watering Hole (webs de confianza comprometidas)
- Webs legítimas con aplicaciones comprometidas (VPN cliente, eWon, ...)

2015 — BLACK ENERGY, CRASHOVERRRIDE
- E-mail Spear-phishing (Docs Office)
- Kill-Disk
- Wipe (borrado de disco)
- DDoS (denegación servicio)
- Malware para protocolos industriales y SIEMENS Siprotec

2017 — TRITON
- USB como vía de infección
- Fallo en dispositivos Triconex SIS
- Objetivo: redes SCADA
- Cambio de la lógica programada

2018

Ciberataque al aplicativo paralelo de algunos bancos

2019

Un ransomware sacude a la productora de aluminio Hydro

CyberInsurance

3 Preguntas de Empoderamiento

¨3 preguntas para ayudar a los líderes de seguridad y gestión de riesgos a adaptarse, transformarse y escalar en el mundo digital¨

Fuente: Gartner 2018

Abordar el riesgo operacional a partir del núcleo del negocio de la empresa

- Desarrollar un programa para evaluar los riesgos y vulnerabilidades de las infraestructuras críticas

- Aprovechar los resultados de la evaluación de riesgo cibernético para crear una estrategia holística de reducción de riesgo y evitar la reparación en silos.

- A “Alto Nivel”

    - Crear un marco de seguridad cibernética para infraestructuras críticas
    - Identificar posibles vectores de ataque y riesgos cibernéticos
    - Asignar criticidad
    - Determinar acciones de remediación inmediata para reducir riesgos.
    - Proponer un enfoque estratégico para reducir los riesgos de seguridad cibernética en las Infraestructuras.

Amenazas vs Riesgos

Amenazas vs Riesgos

infosecurity MEXICO

Contramedidas

1. Gestión de Activos y Vulnerabilidades
2. Tecnologías de Protección
3. Control/Gestión de Accesos, Identidades y Cuentas Privilegiadas
4. Governance
5. Concientización y Entrenamiento
6. Evaluación de Riesgos
7. Seguridad de los Datos
8. Procesos y Procedimientos para la Protección de la Información
9. Estrategia de Gestión de Riesgos
10. Entendimiento del Negocio
11. Mantenimientos

Identificación y Medidas de Respuesta

1. Eventos y Anomalías
2. Monitoreo Continuo de Seguridad
3. Procesos de Detección
4. Planes de Respuesta
5. Comunicaciones
6. Análisis
7. Mitigación
8. Mejora Continua
9. Planes de Recuperación
10. Mejora en la Estrategia de Seguridad

Proceso de Evaluación

infosecurity MEXICO

Evaluación de Riesgo Corporativo

Evaluación de Riesgo a Alto Nivel

1. Entender la Gestión de Riesgo Corporativa
2. Entender el Apetito de Riesgo
3. Entender incidentes previos y el impacto
4. Revisar evaluaciones previas y aprovechar la información

Estado Actual de la Tecnología

1. Entender la Arquitectura de Red
2. Entender el Flujo de Datos
3. Entender el Acceso Lógico
4. Entender los Servicios Compartidos Corporativos

Alcance en los SCI

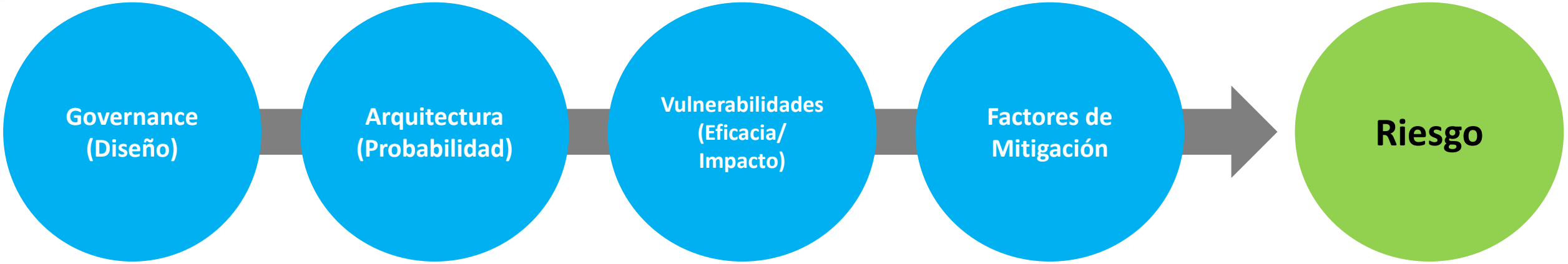
Activos

1. Entender los tipos de Activos para los SCI
2. Entender los procesos soportados del negocio actual por activo
3. Entender el riesgo de cada activo
4. Conocer a los proveedores y terceras partes involucradas

Arquitectura y Regulaciones

1. Entender la arquitectura de red desde la perspectiva de los SCI
2. Entender el Acceso Lógico de los SCI
3. Entender el entorno regulatoria y sus requerimientos

Riesgos en Infraestructuras Críticas

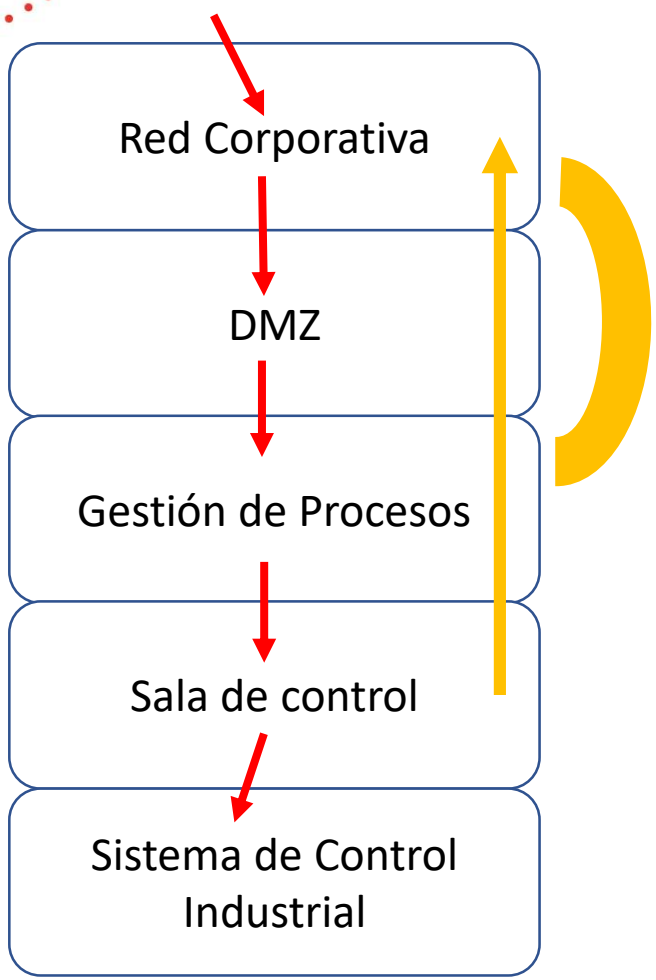


Políticas y Procedimientos

Controles Implementados

Gestión de Acceso	Gestión de Activos	Gestión de Cambios	Gestión de Configuraciones	Gestión de Vulnerabilidades y Parches
Log y Monitoreo	Recuperación y Respuesta a Incidentes	Plan de Continuidad del Negocio	Concientización y Entrenamiento	Seguridad Ambiental y Física

Por qué alinear IT y OT es tan importante



Adopción de Tecnología

- Machine Learning
- Inteligencia Artificial
- Automatización Orquestación

Objetivo: Encontrar los caminos adecuados para orquestar y automatizar la respuesta a las amenazas a través de herramientas de detección a un proceso de respuesta a incidentes más rápido y eficaz

Proceso de Cyber-Defensa IT/OT

infosecurity MEXICO

Predecir

Vulnerabilidades

Conocer nuestras vulnerabilidades y entender el riesgo resultante

Análisis de Riesgo

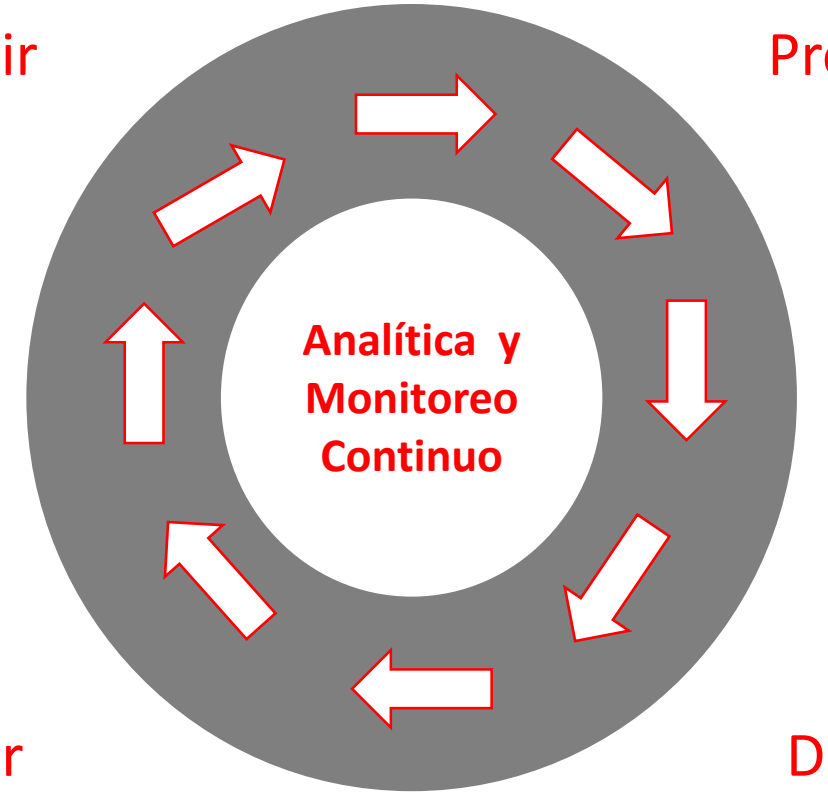
Prevenir

Segmentación

Acceso Remoto

Minimizar el escenario de ataque, evitar incidentes, limitar el impacto.

Endpoint Security



Responder

SOC

Responder de manera efectiva, aislar al atacante, limitar el daño y aprender!

Respuesta a Incidentes

Detectar

Monitoreo

Detectar rápidamente el ataque, recolectar inteligencia para contrarrestarlo

Orquestación

"El enfoque debería cambiar en 2019 de la cantidad a la calidad de las funciones y capas de seguridad"

Colaboración continua entre el Negocio, Infraestructura y Seguridad

Security is a Journey, NOT a Destination

infosecurity MEXICO