Gestión de la seguridad en la cadena de suministro

1 de octubre de 2019

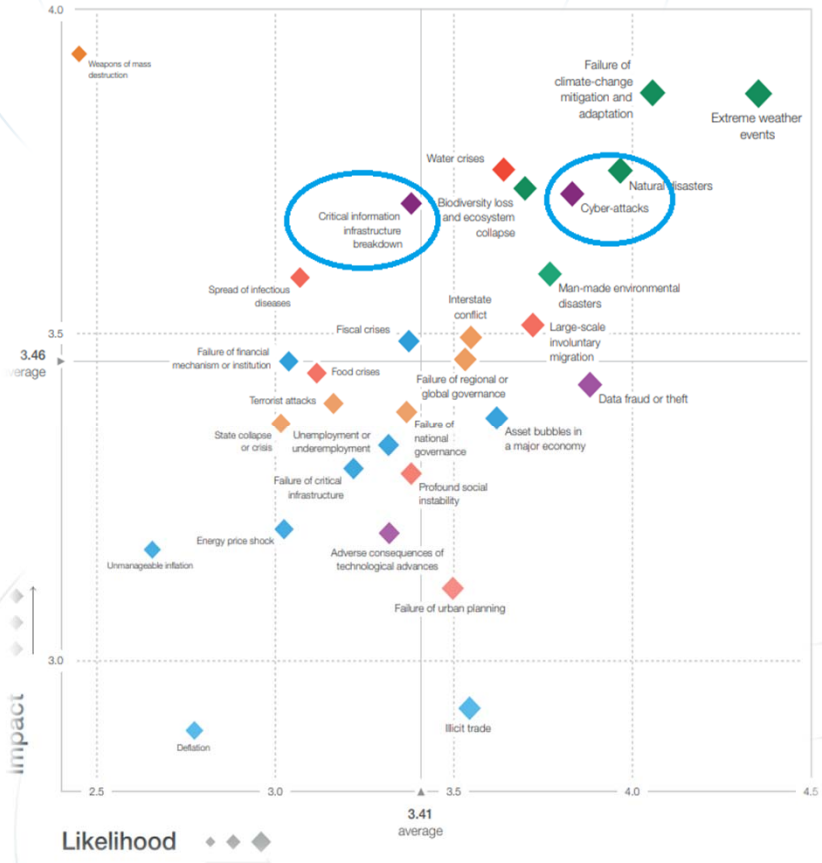
GRUPO RED ELÉCTRICA

Índice

Gestión de la seguridad en la cadena de suministro – Grupo RE

El entorno de seguridad para el Grupo RE

Condiciones del entorno que son tenidas en cuenta para la estrategia de seguridad



- Las organizaciones demandan un enfoque integral de la gestión de la seguridad para responder a las amenazas físicas y cibernéticas de manera global.
- Preocupación creciente por la seguridad: los ciber-riesgos alcanzan las posiciones más altas en los mapas de riesgos globales (WEF – Global Risk report 2019).
- Las infraestructuras críticas son objetivos de ataques dirigidos: impacto amplio sobre la sociedad, repercusión para el atacante. Las IICC se enfrentan a amenazas muy complejas.
- Múltiples actores (motivaciones) tras los ataques: terrorismo, hacktivismo, ciber-delincuencia, competencia, estados.
- Las nuevas regulaciones internacionales persiguen el comportamiento proactivo del operador en materia de seguridad (responsabilidad activa): marcos de control, gestión de riesgos, debida diligencia.

Marco normativo

Operador de infraestructuras críticas y proveedor de servicios esenciales

Protección de infraestructuras críticas (PIC)

- **Ley 8/2011** para la protección de Infraestructuras críticas.
- **RD 704/2011** por el que se aprueba el Reglamento de protección de las Infraestructuras críticas.
- Ley 36/205 de Seguridad Nacional.
- **RD 3/2010**: Esquema Nacional de Seguridad
- 12 Sectores esenciales. De todos ellos, se determina al energético como el más crítico y dentro de éste, el eléctrico como más importante.
- **Red Eléctrica de España: designación como operador crítico (2014).**

Seguridad de las redes y sistemas de información (NIS)

- **RD 12/2018** transposición de la Directiva (UE) 2016/1148 NIS (Directive on Security of Network and Information Systems).
- **Red Eléctrica de España: designación como proveedor de servicios esenciales (2018).**

Protección de Datos

- **Reglamento (UE) 2016/679**: Reglamento general de protección de datos (RGPD).

Modelo de seguridad integral del Grupo RE

Modelo de mejora de madurez en capacidades de seguridad

Antecedentes

- Inspirado en el modelo ES-C2M2 Cybersecurity Capability Maturity Model) del Electricity Subsector - DOE (Department of Energy, USA), pero añadiendo un enfoque holístico de Seguridad integral.

Objetivo

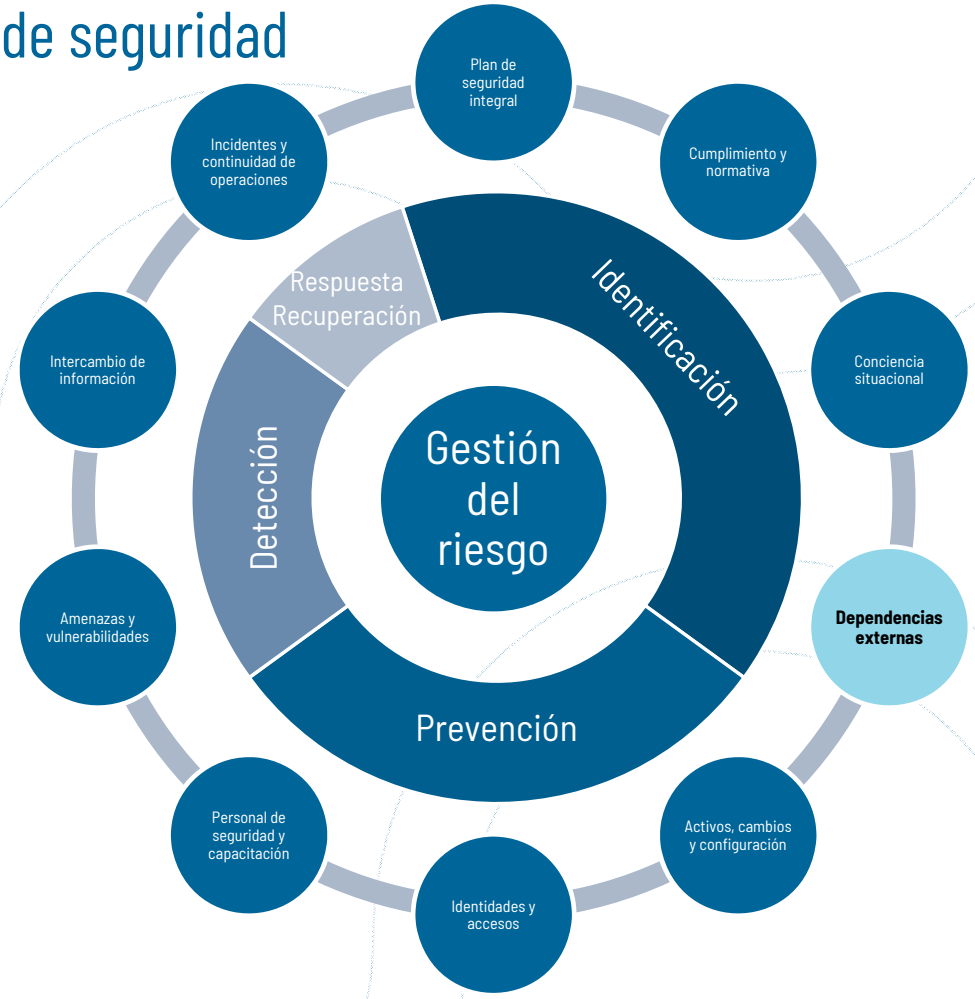
- Capacidades que debe desarrollar una organización con el objetivo de promover la protección y la resiliencia en Seguridad mediante un proceso iterativo de mejora continua de la madurez.

Modelo

- Estas capacidades se despliegan en torno a la Gestión del riesgo en seguridad.

Actividades

- Tienen una correspondencia con las actividades del marco de referencia NIST (National Institute of Standards and Technology): **Identificación, Prevención, Detección, Recuperación y Respuesta**.



La capacidad de Dependencias externas

Dependencias externas: aprovisionamiento

Objetivos

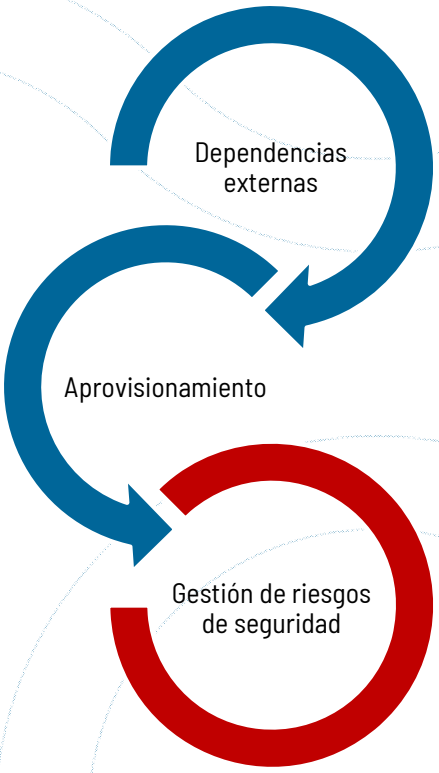
- Establecer y mantener controles para gestionar los riesgos de seguridad asociados a los servicios y activos que dependen de entidades externas, acorde con el riesgo para la infraestructura crítica y los objetivos de la organización.

Motivación

- Los proveedores son una pieza clave para el desarrollo de las funciones de los negocios del Grupo RE: deben tratarse como una entrada al proceso de Gestión de riesgos.

Aplicable a

- Proveedores de equipos, aplicaciones o sistemas que se conectan a las redes de comunicaciones del Grupo RE.
- Proveedores que tienen acceso físico o lógico a la información, a los activos que la contienen o a las redes de comunicaciones.
- Proveedores de servicios de seguridad.
- Proveedores que tratan datos de carácter personal.



Gestión de riesgos de seguridad en la cadena de suministro

El objetivo del modelo es gestionar los riesgos de seguridad en el ciclo completo de aprovisionamiento: homologación de proveedores, licitaciones, gestión y finalización de contratos.

Determinación del riesgo inherente al suministro	Establecimiento del marco de control	Aplicación y evaluación de los controles	Procedimiento para intercambio de información

• Identificación de los perfiles de proveedor (grupos de artículos) y determinar su riesgo inherente para seguridad.	• Establecer un marco de controles a aplicar en las diferentes fases del aprovisionamiento, para que sirvan como contramedidas que reduzcan los riesgos a niveles aceptables (riesgo residual).	• Aplicar y evaluar los controles como medidas para reducir el riesgo.	• Establecer procedimientos para el intercambio de información con los proveedores:
			  • Reporte de incidentes.
			  • Comunicación de vulnerabilidades y brechas de seguridad.
			  • Aplicación de medidas de seguridad.

Gestión de riesgos de seguridad

Debate

Buenas prácticas

- ¿Utilizan algún código de buenas prácticas para la gestión de la seguridad?

Certificaciones

- ¿De qué certificaciones relativas al ámbito de la seguridad disponen?

Homologación, Scoring, Rating

- ¿Están presentes en algún esquema de scoring de proveedores que plantee cuestiones específicas de cumplimiento, privacidad y seguridad?

Contratos con operadores IICC

- ¿Qué certificaciones de seguridad les son exigidas habitualmente en contratos con operadores de IICC / proveedores de servicios esenciales?
- ¿Aplican algún modelo en lo relativo a interlocutor único en materia de seguridad, marco de controles, evaluación de los controles en el ciclo de vida del contrato, comunicación de incidentes / brechas de seguridad, devolución del contrato?

GRUPO RED
ELÉCTRICA

Comprometidos con la **energía inteligente**

Gracias por su atención

www.ree.es