MÓDULO 2

Tema 2: Ciberseguridad en Sistemas de Control Industrial en Infraestructuras críticas

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme.
European Commission - Directorate-General Home Affair

Índice:

Módulo 2 – Tema 2: ciberseguridad en Sistemas de control industrial en Infraestructuras críticas

1.- INTRODUCCIÓN A LAS INFRAESTRUCTURAS CRÍTICAS

1. Introducción
2. Antecedentes históricos
3. Definiciones de la Directiva del Consejo 2008/114/EC
4. Critical Infrastructure Warning Information Network (CIWIN)

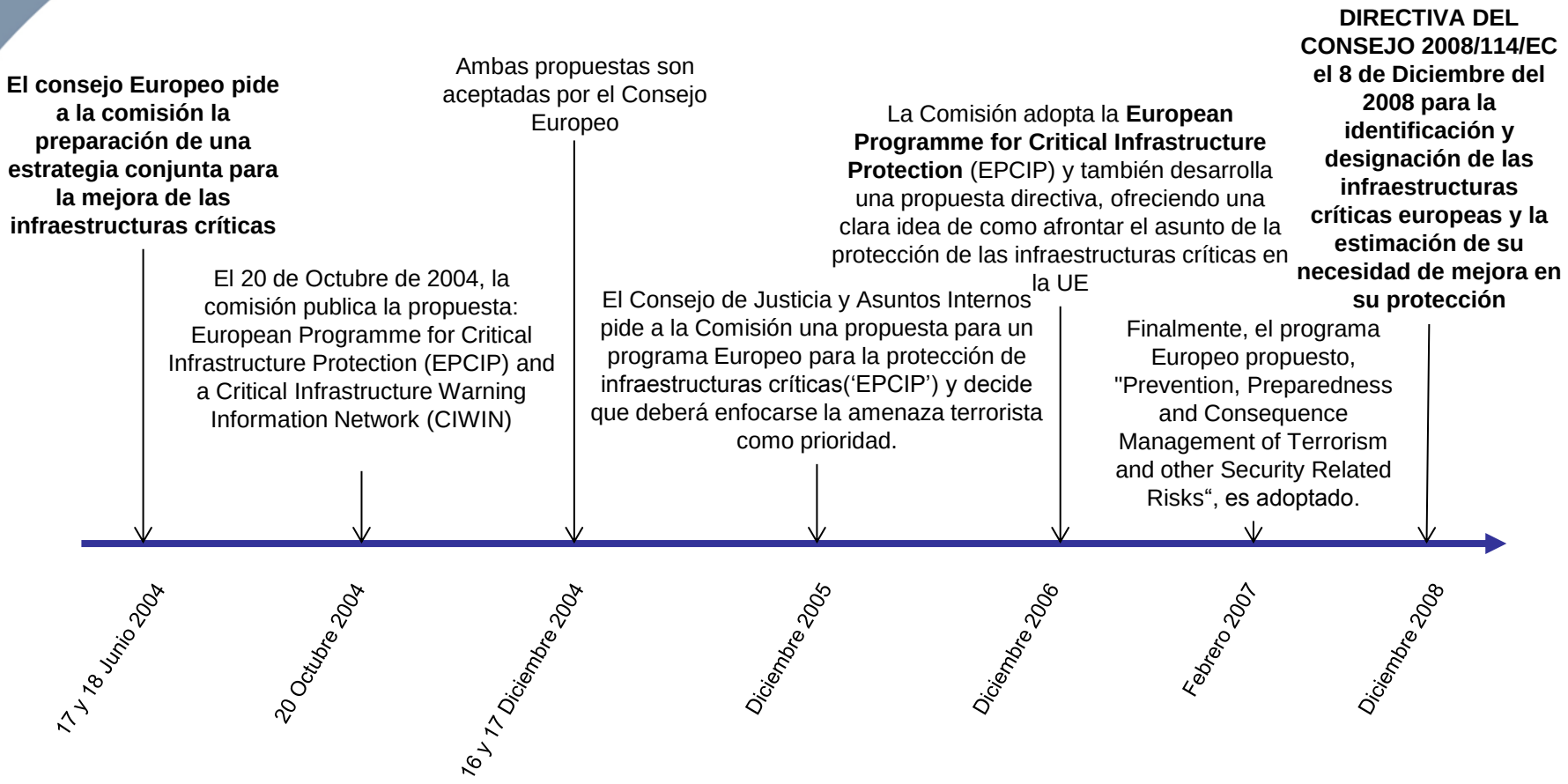
Introducción

La **sociedad del bienestar** está basada en el acceso a determinados bienes y **servicios esenciales** útiles para nuestra vida personal y profesional. Piensa por un momento que pasaría si el suministro de energía de tu ciudad se cortara durante un día. Se presentaría ante nosotros un escenario catastrófico donde una de las consecuencias posibles es la pérdida de vidas.

En la última década ha surgido una nueva oleada de amenazas internacionales que ha ido realizando ataques complejos con serias consecuencias a lo largo del mundo, incluyendo zonas Europeas. Velando por el bienestar de los ciudadanos, las instituciones Europeas han afrontado este reto mediante regulaciones específicas con el propósito de proteger los servicios esenciales para los Estados Miembros

La Comisión Europea , en representación de los intereses de la Unión Europea, ha desarrollado una legislación específica a la espera de ser aprobada por el Parlamento Europeo y el consejo de la Unión Europea.

Precedentes Históricos



Definiciones de la DIRECTIVA DEL CONSEJO 2008/114/EC (I)

Esta directiva establece las bases de la implementación para todos los estados miembros. Para una buena compresión, es esencial tener una idea de los conceptos usados.

Infraestructura Crítica (CI)

Activo, sistema o parte del mismo que se encuentra en un estado miembro y que **es esencial para el mantenimiento de las funciones vitales de la sociedad como: salud, seguridad, economía o bienestar de la población**. La interrupción o destrucción del mismo tendría un impacto significativo en el estado miembro como consecuencia de la falta o reducción de las funciones mencionadas

Solo un estado miembro es afectado

Infraestructura Europea Crítica (ECI)

Infraestructura crítica situada en un estado miembro cuya interrupción o destrucción **tendría un impacto significativo en al menos dos estados miembros.**

La importancia del impacto ha de evaluarse en función de criterios transversales. Se debe incluir los efectos debidos a las dependencias intrasectoriales en otros tipos de infraestructuras.

Dos o más estados miembros son afectados

Definiciones de la DIRECTIVA DEL CONSEJO 2008/114/EC (II)

Otros conceptos clave:

Análisis de riesgo	Protección de la información de una CI	Protección	Propietarios/Operadores ECIs
• Consideración de escenarios relevantes para evaluar las vulnerabilidades y el impacto potencial de la interrupción o destrucción de una infraestructura crítica	• Datos sobre la infraestructura crítica que, en caso de ser revelados, podrían ser usados para para causar una interrupción o destrucción de las instalaciones de la infraestructura crítica.	• Todas las actividades dirigidas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas para disuadir, mitigar y neutralizar una amenaza, riesgo o vulnerabilidad.	• Entidades responsables de la inversión u operación del día a día de un particular bien, sistema o parte del mismo designado como ICE en la presente directiva.

Critical Infrastructure Warning Information Network (CIWIN)

CIWIN es una iniciativa de la Dirección General de la Comisión Europea de Justicia y Asuntos Internos para la **divulgación de las mejores prácticas** y **proporcionar a su vez una plataforma optativa para la divulgación de alertas rápidas** vinculadas al sistema ARGUS de la Comisión.

Es un pilar clave en el Programa Europeo de Protección de las Infraestructuras Críticas (EPCIP) que busca mejorar la protección de las Infraestructuras Críticas.

Esta red está disponible exclusivamente para funcionarios, empleados o miembro del personal de las instituciones nacionales o europeas con actividades CIP relacionadas.

Módulo 2 – Tema 2: ciberseguridad en Sistemas de control industrial en Infraestructuras críticas

2.- SECTORES INCLUIDOS EN LAS ECIS

1. Sectores ECI acorde al comunicado de 2004.
2. Ejemplos de sectores ECI por Estado Miembro.
3. Entendiendo las relaciones entre sectores .

Sectores ECI acorde al comunicado de 2004

Comunicado de la Comisión al Consejo y el Parlamento Europeo, 20 Octubre 2004 – Critical Infrastructure Protection in the fight against terrorism [COM(2004) 702 final –No publicado en el boletín oficial.]

- Instalaciones y redes energéticas
- Comunicaciones y tecnologías de la información
- Finanzas (banca, seguros e inversión)
- Sanidad
- Alimentación
- Agua (presas, almacenamiento, tratamiento y distribución)
- Transporte (aeropuertos, puertos, estaciones de tren, redes masivas de transporte y sistemas de control del tráfico)
- Producción, almacenamiento y transporte de materiales peligrosos (como químicos, biológicos, radioactivos)
- Gobiernos (servicios críticos, instalaciones, redes de información, lugares nacionales clave y monumentos)

Sectores ECI según la directiva 2008/114/EC (I)

La directiva 2008/114/EC establece dos sectores que deben de implementar dicha directiva:

Sector	Subsector	
I Energía	• Electricidad	• Infraestructuras para la generación y transmisión de electricidad respecto al abastecimiento de esta.
	• Petróleo	• Producción de petróleo, refinería, tratamiento, almacenamiento y transmisión por oleoductos.
	• Gas	• Producción de gas, refinería, tratamiento, almacenado y transmisión por gaseoductos. • Terminales de gas natural licuado (LNG)
II Transporte	• Transporte en carretera • Transporte ferroviario • Transporte aéreo • Transporte fluvial • Transporte transoceánico, marítimo y portuario.	

El resto de sectores implicados en la implantación de la directiva deben de ser identificados por cada estado miembro. La prioridad debe de ser asignada según el ICT del sector.

Sectores ECI según la directiva 2008/114/EC (II)

Cada estado miembro, junto con la Comisión, debe continuar el proceso de identificar potenciales ECIs. Este proceso consiste en el análisis mediante criterios transversales y sectoriales. Ambos criterios deben satisfacerse para considerar una estructura como ECI.

Los criterios transversales deben de comprender:
(a) Criterio cuantitativo (valorada según el número potencial de víctimas o instalaciones perjudicadas).
(b) Criterio de esfuerzo económico (valorada según la importancia de la pérdida económica o degradación de productos o servicios, incluyendo efectos medioambientales potenciales).
(c) Criterio de efectos públicos (valorada según el impacto en la confianza pública, sufrimiento físico e interrupción de la vida diaria, incluyendo la pérdida de servicios esenciales).
El criterio sectorial debe considerar las características de cada sector ECI individual.

La comisión, junto con los estados miembros deben de desarrollar las directrices para la aplicación de los criterios transversales y sectoriales y aproximar los umbrales de decisión usados para identificar ECIs.

Ejemplos de sectores ECI por Estado Miembro (I)

Reino Unido
Comunicaciones
Servicios de emergencia
Energía
Servicios financieros
Alimentación
Gobierno
Sanidad
Transporte
Agua

España
Administración pública
Industria espacial
Industria nuclear
Industria química
Centros de investigación
Agua
Energía
Sanidad
ICT
Transporte
Alimentación
Servicios financieros y tributarios

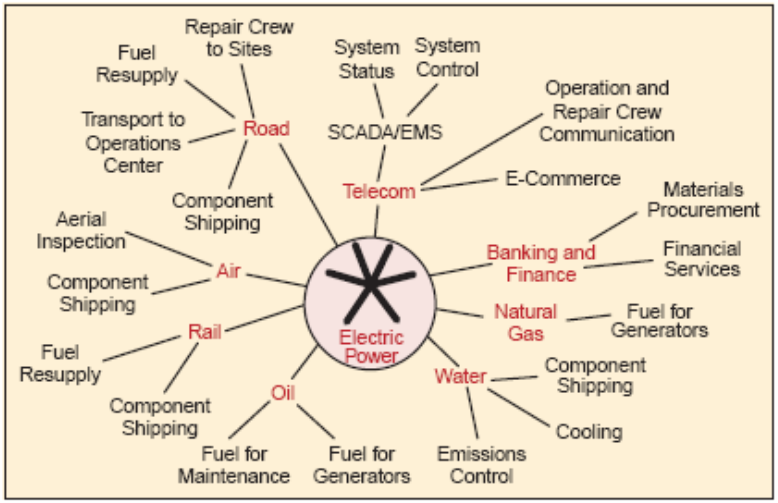
Francia
Autoridades públicas
Energía
Residuos
Servicios financieros
Sanidad
Industria
Comunicación e información
Alimentación
Seguridad pública
Transporte

Ejemplos de sectores ECI por Estado Miembro (II)

ALEMANIA	
Infraestructuras tecnológicas básicas	**Infraestructuras de servicios socio-económicos**
Fuentes de alimentación	Sanidad pública, alimentación
Tecnologías de la información y comunicación	Servicios de rescate y emergencias; control y gestión de desastres
Transporte	Parlamento; gobierno; administración pública; fuerzas del orden
Abastecimiento de agua; eliminación de aguas residuales	Financieros; negocios de seguros
	Medios de comunicación; objetos culturales (patrimonio cultural)

Entendiendo las relaciones entre sectores (I)

La interdependencia sectorial es una cuestión clave en la evaluación del riesgo en los servicios esenciales.



Brussels, 28.8.2013
SWD(2013) 318 final
COMMISSION STAFF WORKING DOCUMENT
on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure

Por ejemplo, el sector energético. Existen fuertes interdependencias con otros servicios esenciales: si hay un corte en el servicio eléctrico durante la etapa de distribución, entonces los servicios de transporte, energía, telecomunicaciones y banca se ven en serio peligro.

Entendiendo las relaciones entre sectores (II)

Posibles dependencias entre el sector energético y otros sectores críticos (*):

Comunicaciones generales

- Datos;
- Sistemas de control (SCADA);
- Control operacional;
- Aumento de interfaces con sistemas financieros

Servicios financieros

- Precios relacionados del gas y el petróleo
- Financiación de instalaciones – inversiones a largo plazo que afectan al abastecimiento sostenible

Futuros avances técnicos / no técnicos

- Redes distribuidas
- Aumento del número de interconexiones entre estados miembros
- Cambios en la tecnología ICT (desarrollo de software, mejora de la defensa, aumento de la sofisticación de los virus, etc)

Coordinación activa de apagados, mantenimiento o inesperados cortes de suministro

- Salas de control – usuarios mayoristas y suministradores de gas

Interfaces entre países

- Autopistas de información para la red UE (private secure system)
- Back-up vía Internet.

Interfaces con ICT

- Dependencias con el abastecimiento eléctrico.
- Back-ups de baterías (duración no definida)
- Problemas de fiabilidad

(*) Source: Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector (http://ec.europa.eu/energy/infrastructure/studies/doc/2009_10_risk_governance_report.pdf)

Módulo 2 - Capítulo 2: Ciberseguridad en Sistemas de Control Industrial en Infraestructuras críticas

3.- MARCO DE TRABAJO DE CIBERSEGURIDAD

1. Introducción
2. Resumen del marco de trabajo
3. Elementos del marco de trabajo
4. Flujos de información y decisión
5. Implementando el marco de trabajo

Introducción

Debido al incremento de amenazas internas y externas, las organizaciones responsables de infraestructuras críticas deben tener un enfoque consistente e iterativo en identificar, evaluar y gestionar los riesgos de ciberseguridad.

NIST (National Institute of Standards and Technology) ha desarrollado, en colaboración con la industria, un marco de trabajo con el objetivo de proveer orientación en la gestión de riesgos de ciberseguridad en las infraestructuras críticas. (*)

El marco de trabajo provee de una taxonomía común y unos mecanismo que permiten a las organizaciones:

- Describir su postura de ciberseguridad actual
- Describir su objetivo de ciberseguridad
- Identificar y priorizar oportunidades de mejora
- Evaluar el progreso en el avance hacia el alcance del nivel de ciberseguridad deseado
- Intercambio de información relativa a riesgos de ciberseguridad entre proveedores internos y externos

(*) NIST Cybersecurity Framework: http://www.nist.gov/cyberframework/

Resumen del marco de trabajo

El marco de trabajo del NIST tiene un enfoque basado en el riesgo para gestionar la seguridad. La gestión del riesgo es el proceso continuo basado en: identificar, evaluar y responder a los riesgos. Con la comprensión de los riesgos, las organizaciones pueden informar y dar prioridad a las decisiones relativas a la seguridad ciberseguridad.

El marco de trabajo del NIST se compone de **tres elementos**:

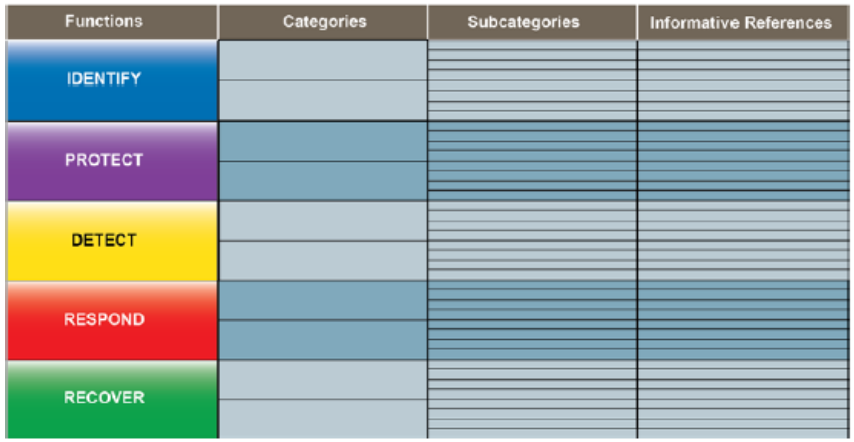
1.- Núcleo (Core)	•Es un conjunto de actividades de ciberseguridad, resultados esperados y referencias a documentos específicos con información relativa a infraestructuras críticas. •Se divide en cinco funciones: Identificar, Proteger, Detectar, Responder y Recuperar.
2.- Grados (Tiers)	•Representa cómo una organización trata los riesgos de ciberseguridad y qué madurez tienen los procesos aplicados para gestionar ese riesgo. •Describen el grado en el cual una organización realiza la gestión de la ciberseguridad plasmada en el marco de trabajo.
3.- Perfil	•Representa el objetivo de ciberseguridad basado en las necesidades de negocio. •Puede ser usado para identificar oportunidades de mejoras comprando el "Perfil actual" con el "Perfil objetivo"

Elementos del marco de trabajo (I)

1.- Núcleo del marco de trabajo

El núcleo del marco de trabajo está organizado en:

- **Funciones**: organiza las actividades en el nivel más alto. Se dividen en: identificar, proteger, detectar, responder y recuperar.
- **Categorías**: son las subdivisiones de las funciones. Algunos ejemplos son: Control de Acceso, Procesos de detección, etc..
- **Subcategorías**: provee de un conjunto de acciones que ayudan a lograr el objetivo de cada categoría.
- **Referencias informativas**: son secciones específicas de estándares, guías y buenas prácticas que ilustran un método para lograr el objetivo buscado en cada subcategoría.



El núcleo del marco de trabajo puede ser descargado desde la siguiente URL: http://www.nist.gov/cyberframework/upload/framework-for-improving-critical-infrastructure-cybersecurity-core.xlsx

Elementos del marco de trabajo (II)

1.- Núcleo del marco de trabajo

Las cinco funciones del núcleo del marco de trabajo son:

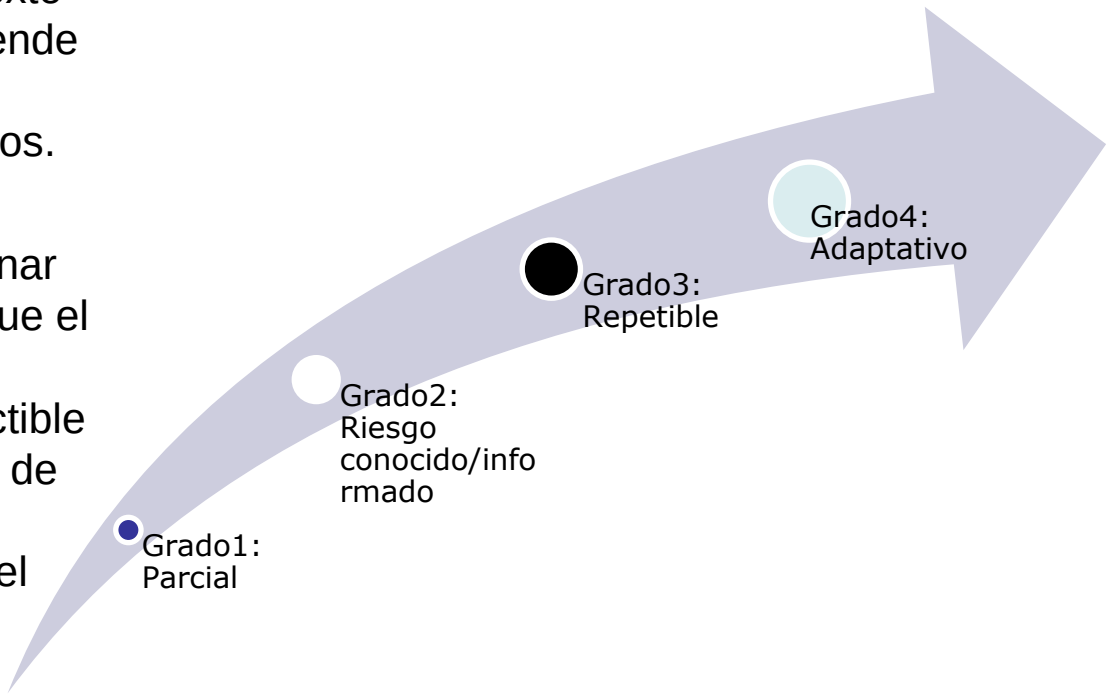
- **Identificar**
  - Desarrollar la comprensión de la organización para gestionar el riesgo de ciberseguridad aplicados a los sistemas, activos, datos y capacidades.
- **Proteger**
  - Desarrollar y poner en práctica las salvaguardias adecuadas para garantizar la prestación de servicios de infraestructura crítica.
- **Detectar**
  - Desarrollar y poner en práctica las actividades pertinentes para detectar la ocurrencia de un evento de ciberseguridad.
- **Responder**
  - Desarrollar e implementar las actividades necesarias para adoptar medidas respecto a la sucesión de un evento de ciberseguridad detectado.
- **Recuperar**
  - Desarrollar e implementar las actividades necesarias para mantener los planes para la resiliencia y para restaurar los servicios que fueron perjudicados debido a un evento de ciberseguridad.

Elementos del marco de trabajo (III)

2.- Grados de implementación

Proporcionan información de contexto sobre cómo una organización entiende los riesgos de ciberseguridad y los procesos para gestionar gestionarlos.

Las organizaciones deben determinar el “Grado” deseado, asegurando que el nivel seleccionado cumple con los objetivos de la organización, es factible de implementar, y reduce el riesgo de la seguridad cibernética para los activos críticos y recursos a un nivel aceptable para la organización.

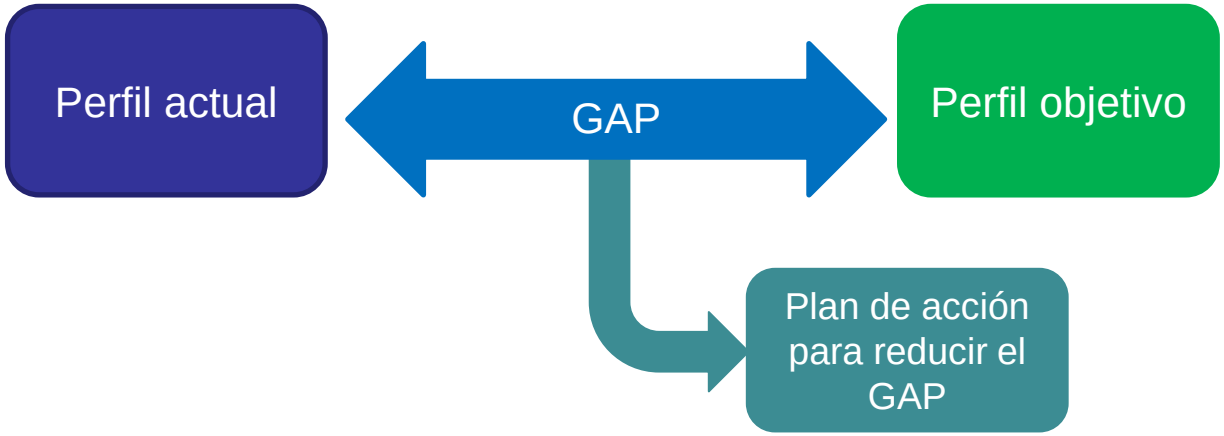


Elementos del marco de trabajo (IV)

3.- Perfil del marco de trabajo:

Los perfiles del marco de trabajo pueden ser usados para describir el estado de madurez actual y el estado de madurez objetivo en las distintas actividades del marco.

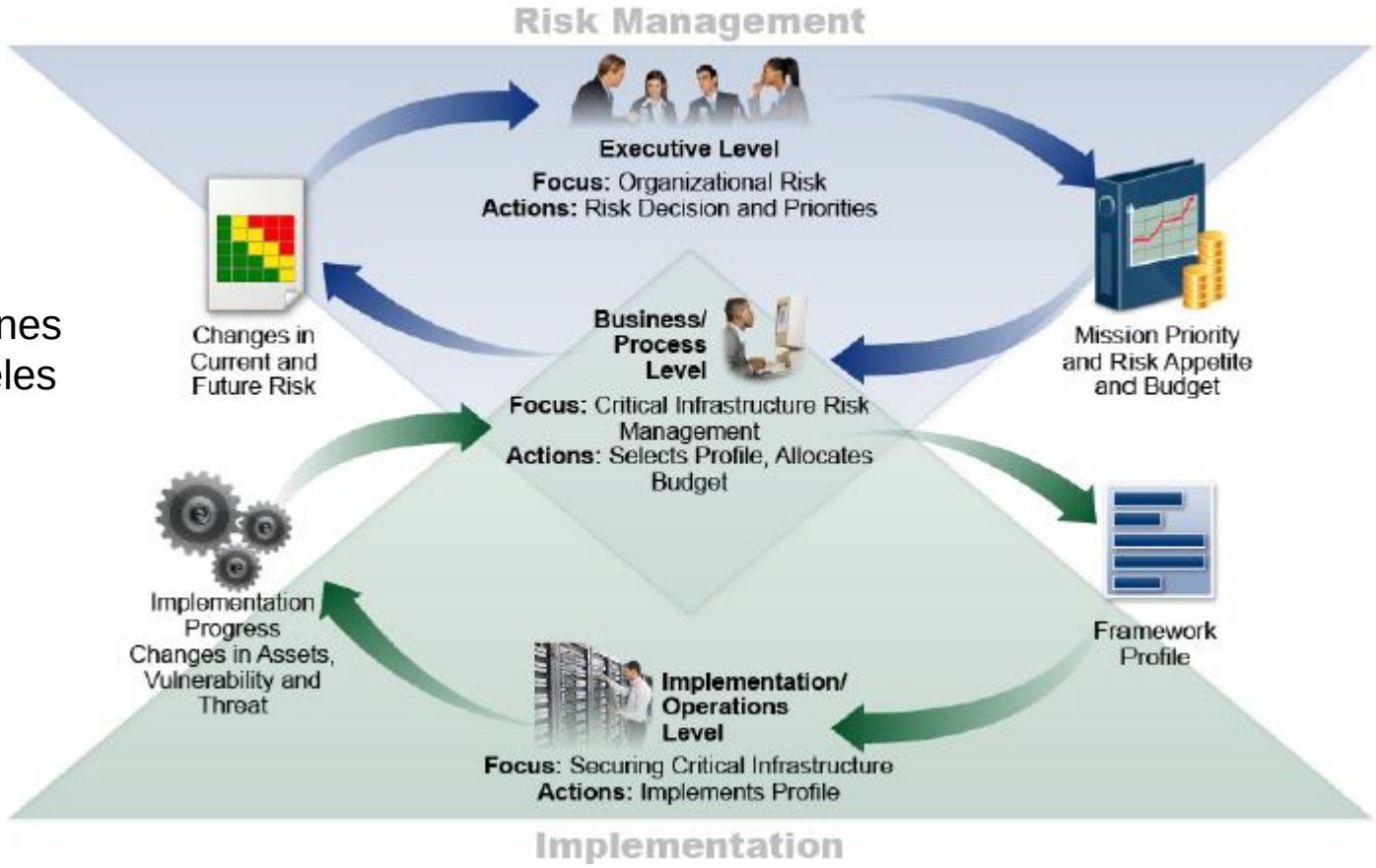
La comparación entre perfiles (perfil actual y perfil objetivo) revelan lagunas que deben abordarse para para lograr los objetivos de gestión de riesgos de seguridad cibernética.



Flujos de información y decisión (IV)

La siguiente figura describe un flujo de información y decisiones en los siguientes niveles dentro de una organización:

- Ejecutivo
- Negocios / Proceso
- Implementación / Operaciones



Fuente de la figura: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Implementando el marco de trabajo

Los pasos siguientes ilustran cómo una organización puede implementar el marco de trabajo:

Paso 1: Priorización y alcance
La organización identifica sus objetivos de negocio y las prioridades de la organización a alto nivel

Paso 2: Orientación
Consiste en la identificación de los sistemas y de los activos, los requisitos regulatorios y del riesgo global

Paso 3: Crear un perfil actual
La organización identifica qué funciones del marco se están ya llevando a cabo

Paso 4: Realizar un análisis de riesgos
La organización realiza un análisis de riesgos

Paso 5: Crear un perfil objetivo
La organización define el nivel de ciberseguridad deseado.

Paso 6: Determinar, analizar y priorizar el GAP
La organización analiza las diferencias entre el perfil actual y el objetivo y define el GAP.

Paso 7: Implementar el plan de acción
La organización decide qué opciones tomar para reducir el GAP

Thank you!

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme.
European Commission - Directorate-General Justice, Freedom and Security