

**enise**



**inteco**



Instituto Nacional  
de Tecnologías  
de la Comunicación

# **Visión del PIC desde un marco de calidad en IT**

## ***Las Tecnologías de la Información en la Protección de las Infraestructuras Críticas***

Eva Rodríguez

Consultora Senior

**SATEC**



1. Introducción
2. Problemática
3. Y el PIC, ¿es nuevo?
4. Cambiar el enfoque
5. Conclusiones
6. Bibliografía

## ¿Que es la seguridad?

Libre y exento de todo peligro, daño o riesgo.

RAE

## ¿Porque es difícil la seguridad?

Porque sólo se sabe que existe cuando falla

Porque es difícil “vender” un concepto negativo

El caso de la enfermedad asiática mortal

Grupo 1: A: se salvará 1/3 de la población.

B: hay un 50% de que mueran la mitad de la población.

Grupo 2: A: morirán 2/3 de la población

B: hay un 50% de que se salve la mitad de la población

Porque no podemos saber cuánta seguridad hace falta

Si en un disco duro no cabe lo que necesito, pongo más

¿Cuánta seguridad hace falta? ¿Cuánto pongo?

## ¿Porque es difícil la seguridad?

Porque es una guerra asimétrica

El atacante sabe qué va a atacar: un objetivo.  
El defensor no: debe defender todo.

El atacante sabe cómo va a atacar: un método.  
El defensor no: debe defender contra todo.

No importa cómo elija concentrar mis esfuerzos,  
el ataque vendrá de otra forma, y en otro sitio.

## La Protección de Infraestructuras Críticas



Objetivo:

Prevenir y proteger las infraestructuras críticas de las amenazas y actos intencionados.

La dependencia a las Tecnologías de la Información de las organizaciones a aumentado drásticamente y por lo tanto la dependencia de los servicios esenciales.

Por otra parte, debido a la clasificación de la documentación relacionada con la Protección de Infraestructuras Críticas, es necesario garantizar la seguridad de los sistemas de información involucrados.

## La Protección de Infraestructuras Críticas

El Operador Crítico:

- Elabora el Plan de Seguridad del Operador (PSO)
- Elabora un Plan de Protección Especifica para cada una de las Infraestructuras Críticas.
- Designa el Responsable de Seguridad y Enlace.

La finalidad del PSO es garantizar la seguridad del conjunto de instalaciones mediante la definición de políticas generales.

Los PPEs son documentos operativos donde se definan medidas concretas adoptadas o que se vayan a adoptar para una seguridad integral.

## Problemática

- No podemos ser vulnerables.
- Recursos limitados.
- Recortes de presupuesto.
- Necesidad de especialización.
- Múltiples exigencias.

## Dudas que surgen

Existen medidas tecnológicas, pero...

¿Cómo priorizar?

¿Cuánto invertir?

¿Cómo estar al día?

También metodológicas, pero...

¿Sabemos si son las adecuadas?

¿Sabemos si se cumplen?

¿Podemos medir su efectividad?

¿Lo estamos haciendo bien?

¿Podemos saberlo?



## Las Tecnologías de la Información frente a exigencias múltiples



### Que esta pasando

Iniciativa del departamento de Tecnología

No es una función transversal

Tiende a centrarse más en la seguridad informática

Responsabilidades redundas e incomunicadas

Visión por islotes

Auditorías múltiples



## Aspectos clave en la protección de las infraestructuras críticas

Política de seguridad

Definir la política de seguridad.

Análisis de riesgos

Analizar los riesgos de la infraestructura crítica para identificar las medidas a implantar.

Continuidad del negocio

Garantizar la continuidad de los servicios esenciales.

Mejora continua

Revisar lo planes periódicamente para mantenerlos actualizados .

## No es tan nuevo

Gobierno TI	Gestión de la seguridad	Continuidad del Negocio
ISO/IEC 20000	ISO/IEC 27001	BS25999-2
	ISO/IEC 27002	BS25999-1
ITIL		
COBIT	Guías CCN-CERT	Guías BCI
Lean IT	Guías NIST	Guías NIST

## El análisis de riesgos

Proceso sistemático para identificar los riesgos y estimar su magnitud

Permite identificar las áreas que requieren medidas de seguridad.

Algunas metodologías:

- ISO 27005
- MAGERIT
- NIST
- OCTAVE
- MEHARI
- EBIOS

## Continuidad de negocio

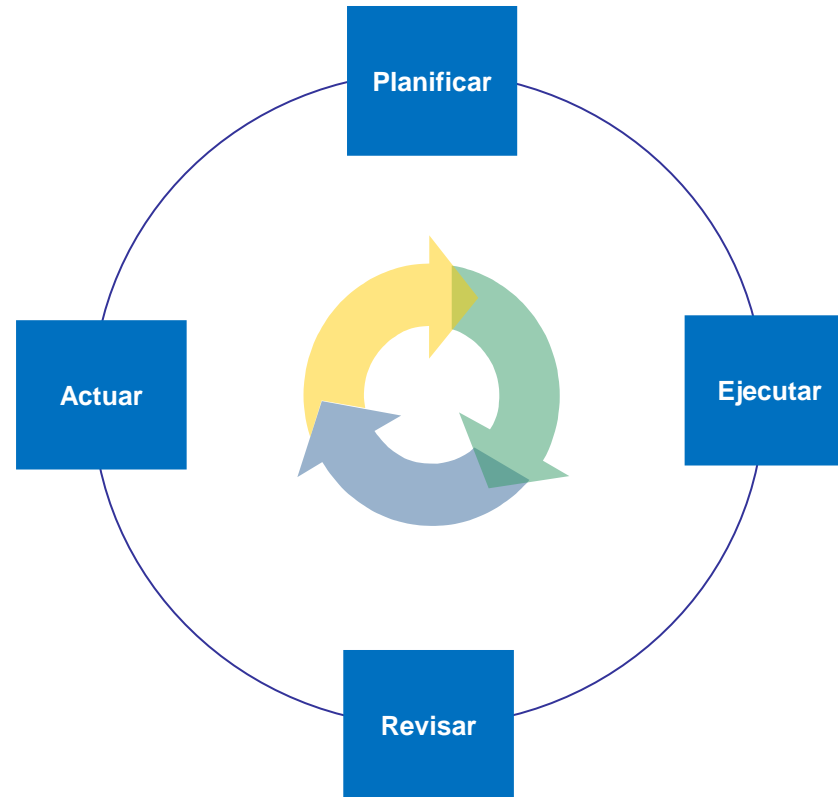
- Responsabilidades
- Gestión de incidentes
- Gestión de crisis
- Planes de continuidad
- Plan de recuperación ante desastre
- Pruebas de los planes

## Medidas de seguridad

- Políticas de Seguridad
- Procedimientos
- Controles, Infraestructuras, Herramientas
- Instrucciones técnicas



## El ciclo de Deming - PDCA



## Hacia el cambio

Cambiar la cultura de seguridad para optimizar los recursos y ahorrar... y también para ser más eficientes .



## Cambiar nuestra visión

- Visión global de seguridad
- Abrir horizontes/Colaborar
- Lanzar un mensaje único



# 4 – Cambiar el enfoque

	RLOPD	ENS	PIC
Política de seguridad	-	Org.1	Política de seguridad PSO y PPE
Análisis de riesgos	-	Principio básico op-.pl.1	Análisis de riesgos de las infraestructuras críticas. Plan de tratamiento
Seguridad física	Control de acceso	Control de acceso Condiciones ambientales Medidas para mitigar el riesgo	Medidas para mitigar el riesgo
Continuidad de Negocio	-	Op.cont Análisis de impacto Plan de continuidad Pruebas periódicas	Revisión PSO y PPE cada 2 años
Auditorías/ Revisiones	Auditoría bienal seguridad Art. 96	Auditoría bienal seguridad Art. 34	Revisión PSO y PPE cada 2 años

## Reutilizar, unificar, interrelacionar y optimizar...

- Políticas de seguridad
- Responsables de seguridad
- Procedimientos
- Normas
- Mediciones



## El buen gobierno y gestión de la seguridad

Gestionar la seguridad es:

Gestionar el nivel de riesgo.

Usar medidas adecuadas, efectivas y proporcionadas.

Tener control sobre su funcionamiento y eficacia.

Y recordemos:

Justificar las inversiones.

Medir los resultados.

Prever el impacto.

Y como todo cambia:

Reevaluar continuamente.

Corregir las desviaciones.



## Revisión, seguimiento y control

Unificar las distintas auditorías.

Unificar los cuadros de mando.

Sistemas/ procesos de gestión.

Mejora continua.

## Factores de éxito

- ❖ **Compromiso** de la Dirección.
- ❖ Seguridad **Integral**.
- ❖ Medidas de seguridad **adaptadas**.
- ❖ Seguimiento y revisión periódica.
- ❖ **Formación** y concienciación.



## 3 ideas

Las organizaciones primero adquieren productos, luego implantan procesos y finalmente forman personas.

*Mejor al revés.*

Más seguridad de la necesaria es derroche.

Menos, es irresponsabilidad.

Si no sabes cuánto debes gastar...

*...tal vez la mejor inversión sea averiguarlo.*

Mejor que prepararse para un riesgo concreto es estar dispuesto para lo imprevisto.

## Y recordemos

“La seguridad es tan fuerte como el más débil de sus eslabones”.

“La máxima seguridad obtenible es la del elemento más débil del sistema”



# Muchas gracias

