Grupo Estudios Técnicos

Seminario

"Tecnologías aplicadas a la protección IC"

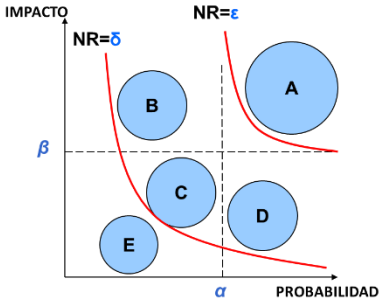
Proceso para el tratamiento de Riesgos en Infraestructuras Críticas

ÍNDICE

1. FUNDAMENTOS DEL ANÁLISIS DE RIESGOS

1. FUNDAMENTOS DEL ANÁLISIS DE RIESGOS

Introducción



El Análisis de Riesgos permite evaluar el nivel de exposición que están soportando determinados activos frente a diversas amenazas.

Aunque existen múltiples metodologías de Análisis de Riesgos, casi todas coinciden en recoger, de un modo u otro, la relación entre **amenazas y activos**

Casi todas las metodologías tienen en cuenta:

- Factibilidad de ocurrencia (si es posible, con qué probabilidad, con qué frecuencia, cómo de vulnerable sería, etc.)
- Las consecuencias o impacto de esta materialización.

La Ley PIC considera la Probabilidad y el Impacto

Objetivos del Análisis de Riesgos

- Permite conocer frente a qué riesgos debe protegerse cada activo.
- Permite justificar la disposición de medidas de Seguridad, que serán adecuadas y proporcionadas a los riesgos analizados.
- Es una herramienta fundamental para el establecimiento de una estrategia de Seguridad.
- Es una pieza clave de cualquier ciclo de mejora continua en la gestión de riesgos.
- Todo sistema de Seguridad debe partir de unos criterios de diseño que necesariamente emanan de un análisis de riesgos.
- Toda medida que se implante debe tener como fin disminuir alguno de los riesgos analizados. De lo contrario, dicha medida no tiene sentido.
- Permite cumplir con requisitos legislativos.

1. FUNDAMENTOS DEL ANÁLISIS DE RIESGOS

"Apellidos" de la Seguridad

Seguridad Laboral

	Bienes	Personas	Medio-ambiente	Información
Naturales		X		
Técnicos		X		
Deliberados				

Seguridad Industrial

	Bienes	Personas	Medio-ambiente	Información
Naturales	X	X	X	
Técnicos	X	X	X	
Deliberados				

Seguridad de la información Ciberseguridad

	Bienes	Personas	Medio-ambiente	Información
Naturales				X
Técnicos				X
Deliberados				X

Seguridad Física (Security)

	Bienes	Personas	Medio-ambiente	Información
Naturales				
Técnicos				
Deliberados	X	X	X	X

1. FUNDAMENTOS DEL ANÁLISIS DE RIESGOS

Dos "Apellidos" próximos: Security

Seguridad Física, Seguridad de la información y Ciberseguridad

	Bienes	Personas	Medio-ambiente	Información
Naturales				X
Técnicos				X
Deliberados	X	X	X	X

1. FUNDAMENTOS DEL ANÁLISIS DE RIESGOS

El enfoque de Seguridad del CNPIC

Seguridad integral frente a ataques terroristas o grupos organizados

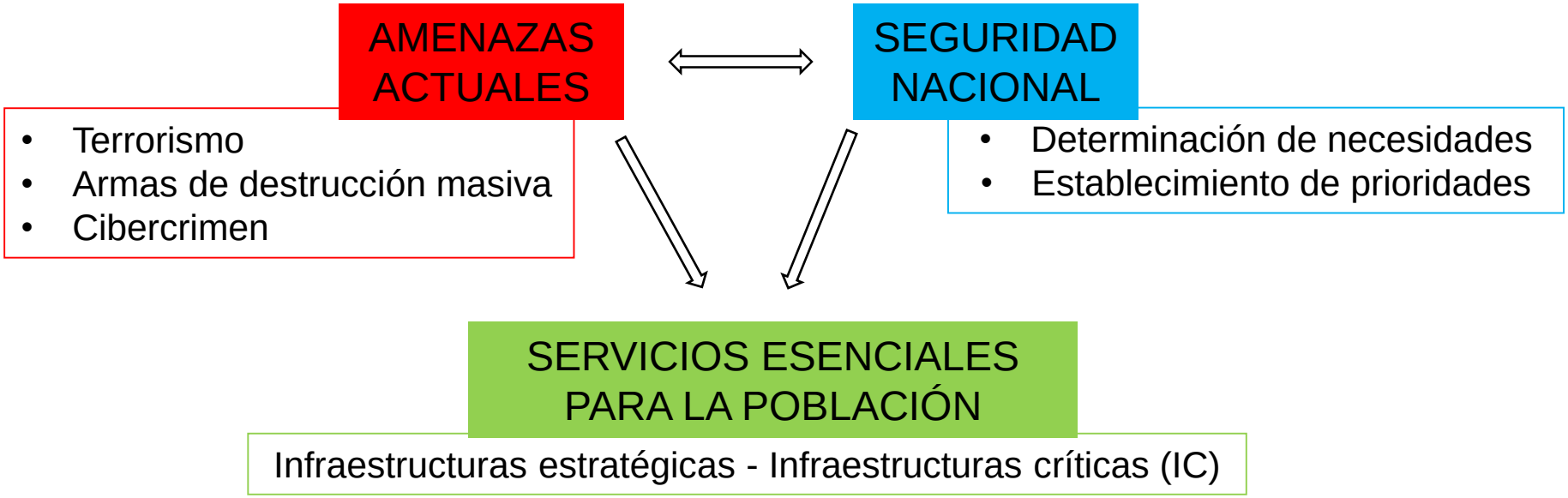
Tipo de Amenaza \ Criterios horizontales	Economía Nacional	Personas	Medio-ambiente	Servicios esenciales
Naturales				
Técnicos				
Deliberados				
Deliberados de origen terrorista o crimen organizado	X	X	X	X

En este caso, los apellidos se centran en el tipo de consecuencias (criterios horizontales) y no en los tipos de activos afectados

Aunque de acuerdo al alcance estricto de la misión del CNPIC deberían atenderse exclusivamente los riesgos indicados, suelen considerarse amenazas de otra naturaleza

1. FUNDAMENTOS DEL ANÁLISIS DE RIESGOS

El enfoque de Seguridad del CNPIC



Frente a otros enfoques de Análisis de Riesgos, la primera aproximación al riesgo no considera el valor de los activos o de la información de los mismos, sino la criticidad de los servicios esenciales.

1. FUNDAMENTOS DEL ANÁLISIS DE RIESGOS

El enfoque de Seguridad del CNPIC

Nivel de alerta en infraestructuras críticas (NAIC)

A falta de otras fuentes de inteligencia, el NAIC es un factor que no debe ignorarse en los análisis de riesgos de los OC

2. ANÁLISIS DE RIESGOS EN PROCESOS DE SEGURIDAD

2. ANÁLISIS DE RIESGOS EN PROCESOS DE SEGURIDAD

La Seguridad en las Empresas

La seguridad como función dentro de una empresa se entiende habitualmente como el área encargada de la prevención y protección frente a ciertas amenazas o riesgos.

Como se ha indicado, existen diversos apellidos para definir las diferentes Seguridades.

- Riesgos laborales
- Seguridad industrial

} Safety

- Seguridad de la información (CISO)
- Seguridad física (Director de Seguridad)

} Seguridad Corporativa (CSO)

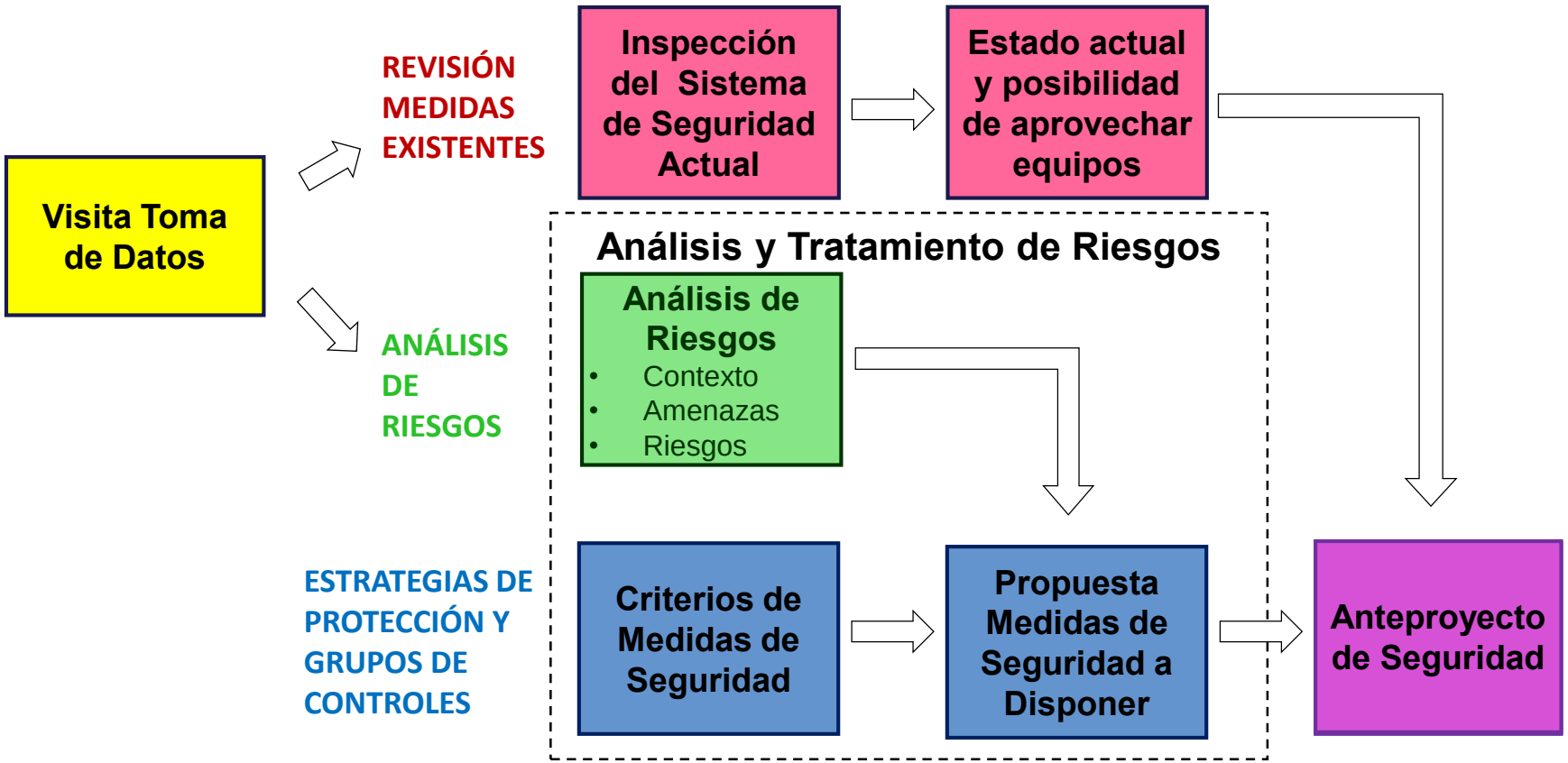
Para la alta dirección, el/las área/s de Seguridad se encargan de la gestión de ciertos riesgos operativos

2. ANÁLISIS DE RIESGOS EN PROCESOS DE SEGURIDAD

Análisis de Riesgos Macro como apoyo a los Planes de Seguridad

2. ANÁLISIS DE RIESGOS EN PROCESOS DE SEGURIDAD

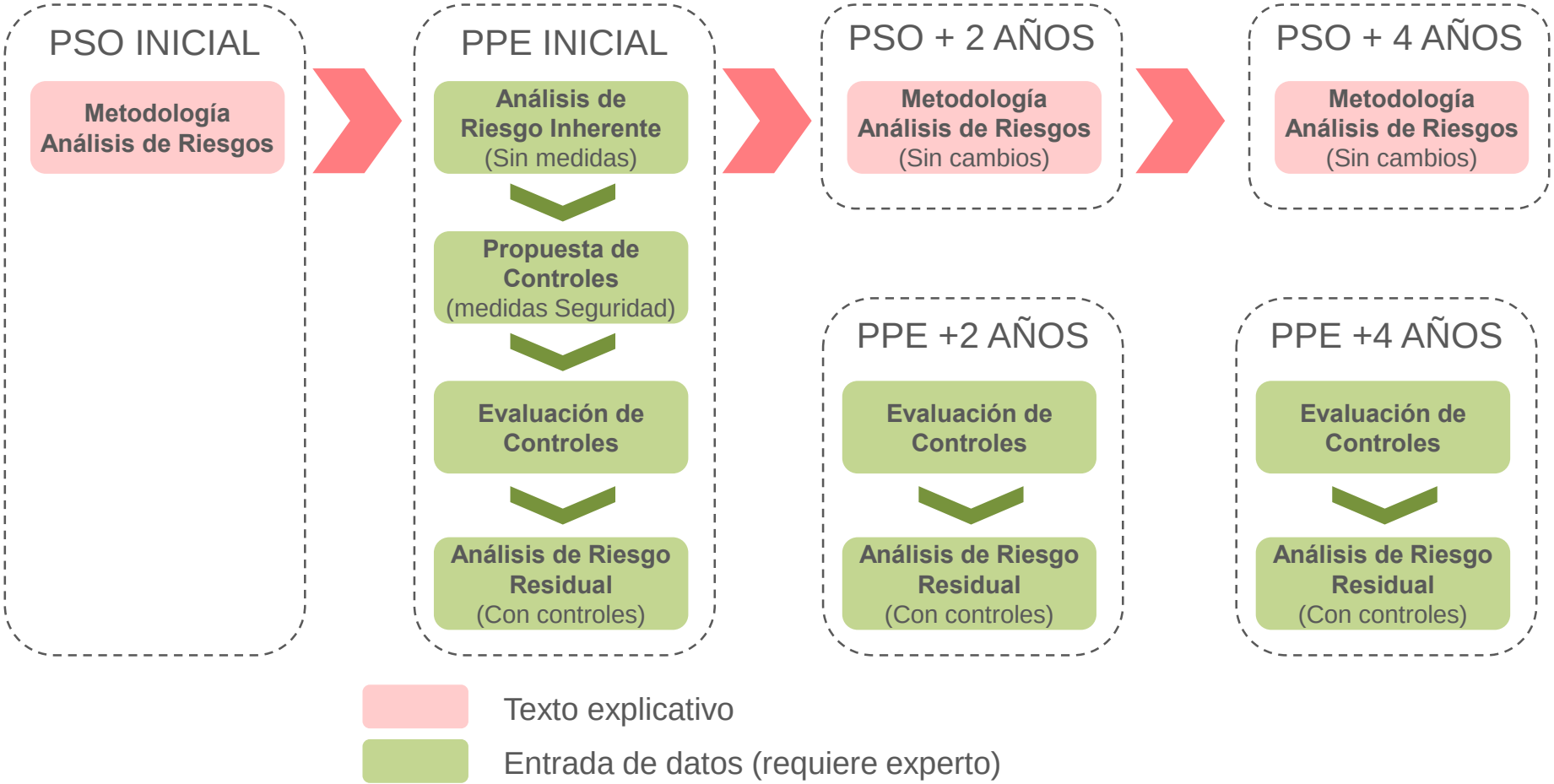
Análisis de Riesgos Micro como apoyo a Auditorías y Anteproyectos



Proceso para el tratamiento de Riesgos en Infraestructuras Críticas

2. ANÁLISIS DE RIESGOS EN PROCESOS DE SEGURIDAD

Análisis de Riesgos en PSO y PPEs

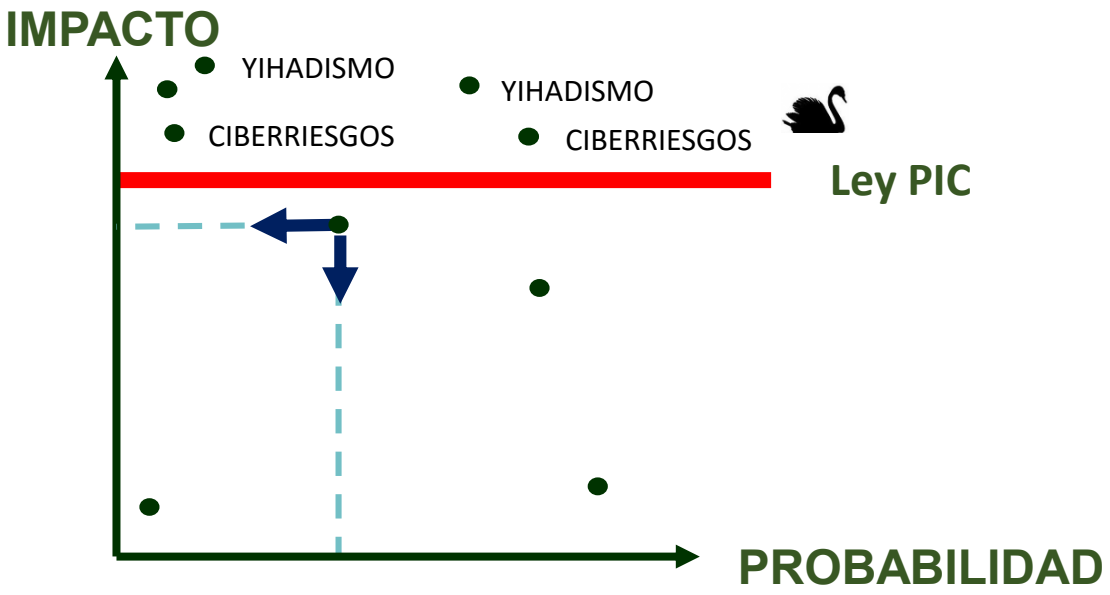


Proceso para el tratamiento de Riesgos en Infraestructuras Críticas

3. DECISIONES DE GESTIÓN DE RIESGOS

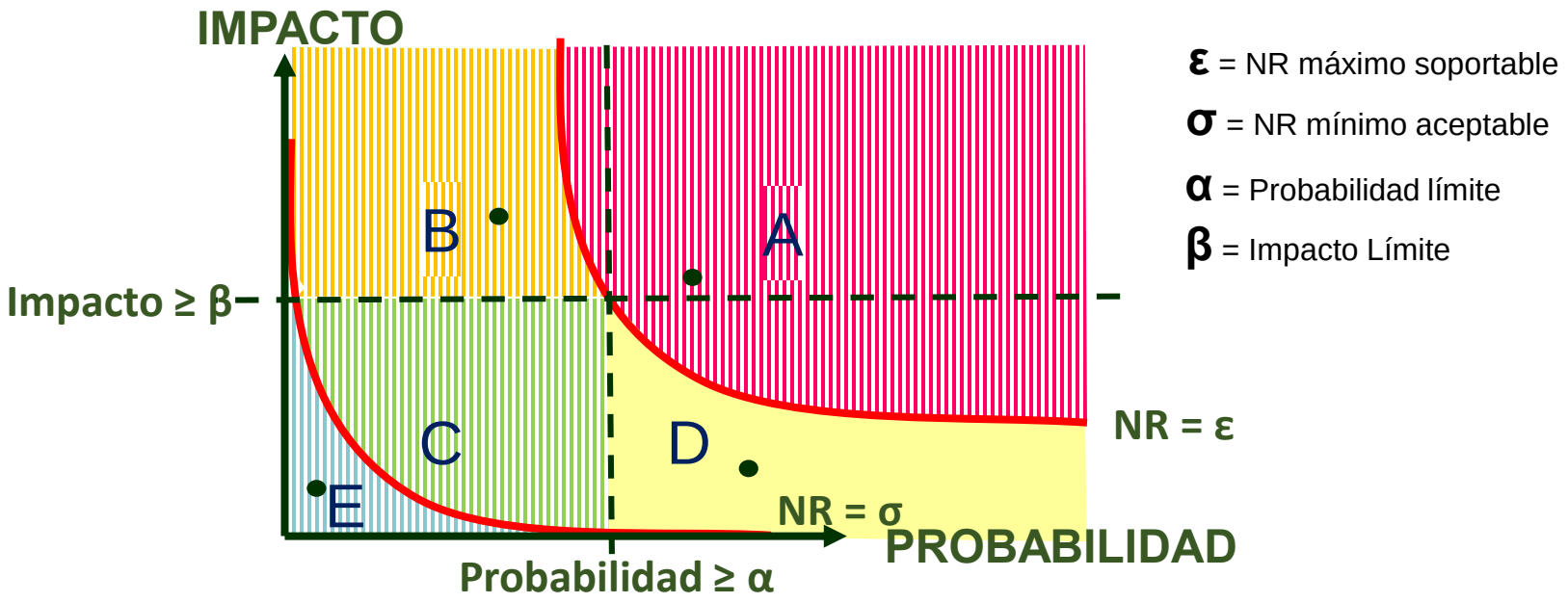
3. DECISIONES DE GESTIÓN DE RIESGOS

Ubicación de riesgos en Plano Probabilidad/Impacto



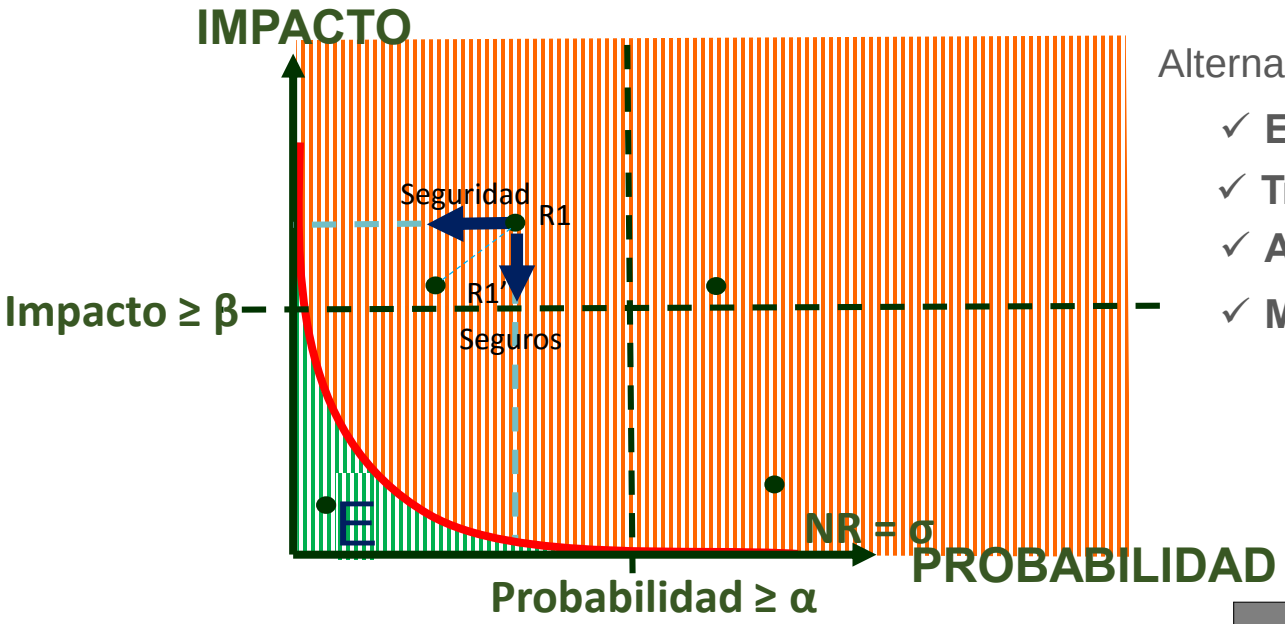
3. DECISIONES DE GESTIÓN DE RIESGOS

Agrupación de Riesgos



3. DECISIONES DE GESTIÓN DE RIESGOS

Alternativas de Gestión de Riesgos



Alternativas posibles de gestión:

- ✓ **Evitar o eliminar el Riesgo**
- ✓ **Transferir el Riesgo**
- ✓ **Aceptar el Riesgo**
- ✓ **Mitigar el Riesgo**

GESTIÓN DE RIESGOS	
GRUPO A	MITIGAR
GRUPO B	MITIGAR/ASEGURAR
GRUPO C	MITIGAR
GRUPO D	MITIGAR
GRUPO E	ACEPTAR

4. ANÁLISIS DE RIESGOS FÍSICO Y LÓGICO

4. ANÁLISIS DE RIESGOS FÍSICOS Y LÓGICOS

Análisis de Riesgos Físico

1. Activos analizados: áreas físicas (escenarios/instalaciones) y personas
2. Catálogos de amenazas muy variados
3. Habitualmente se realiza considerando las medidas de Seguridad existentes, las cuales se evalúan o auditan como parte del análisis
4. En ocasiones, se analizan diversas franjas temporales (se analizan amenazas sobre activos en un tiempo determinado)
5. Poco implantado a través de herramientas
6. Hasta aparición de ISO 31000, no asociado a normativa
7. Realización obligatoria para realizar proyectos de sistemas de Seguridad y como parte de los PPEs
8. Metodologías más extendidas: Penta/Mosler y Cuantitativo-Mixto

4. ANÁLISIS DE RIESGOS FÍSICOS Y LÓGICOS

Análisis de Riesgos Lógico

1. Activos analizados: Servicios, Comunicaciones, HW, SW, Personas…
2. Catálogos de amenazas estandarizados. Incluyen muchas físicas
3. Suelen analizarse amenazas, activos y dimensiones afectadas
4. Evaluación de probabilidad habitualmente basada en datos estadísticos
5. Dos fases: nivel de riesgo inherente (sin controles) y residual (con controles). Se suele evaluar la madurez de los controles según CMMI.
6. Implantado frecuentemente a través de herramientas, permitiendo PDCA
7. Asociado a normativas y legislación: ISO 2700X, ENS…
8. Salvo la administración, realización no obligatoria, pero sí extendida
9. Metodologías más extendidas: Magerit en administración en España

4. ANÁLISIS DE RIESGOS FÍSICOS Y LÓGICOS

Procesos típicos comparados

Proceso de Análisis de Riesgos Físico

AUDITORÍA
- Análisis de Contexto
- Valoración de las medidas de Seguridad

EVALUACIÓN DE RIESGOS
- Requiere expertos
- Subjetividad al interpretarse medidas

EMPLEO DE RESULTADOS
- Justificar Inversiones
- Justificar miedos transmitidos

Proceso de Análisis de Riesgos Lógico

BIA
- Cada dueño valora sus activos
- Valoración de impacto

EVALUACIÓN DE RIESGOS
- Tablas con probabilidad por amenaza
- Valoración de madurez de controles

EMPLEO DE RESULTADOS
- Justificar Inversiones
- Proceso de mejora continua

5. ANÁLISIS DE RIESGOS DE OPERADORES CRÍTICOS

5. ANÁLISIS DE RIESGOS DE OPERADORES CRÍTICOS

Plan de Seguridad del Operador

Índice PSO

1. Introducción.
1.1 Base Legal.
1.2 Objetivo de este Documento.
1.3 Finalidad y Contenido del PSO.
1.4 Método de Revisión y Actualización.
1.5 Protección y Gestión de la Información y Documentación

2. Política General de Seguridad del Operador y Marco de Gobierno.
2.1 Política General de Seguridad del Operador Crítico.
2.2 Marco de Gobierno de Seguridad.
2.2.1 Organización de la Seguridad y Comunicación.
2.2.2 Formación y Concienciación.
2.2.3 Modelo de Gestión Aplicado.
2.2.4 Comunicación.

3. Relación de Servicios Esenciales prestados por el Operador Crítico.
3.1 Identificación de los Servicios Esenciales.
3.2 Mantenimiento del Inventario de Servicios Esenciales.
3.3 Estudio de las Consecuencias de la Interrupción del Servicio Esencial.
3.4 Interdependencias

4. Metodología de Análisis de Riesgos.
4.1 Descripción de la Metodología de Análisis.
4.2 Tipologías de Activos que Soportan los Servicios Esenciales.
4.3 Identificación y Evaluación de Amenazas.
4.4 Valoración y Gestión de Riesgos.

5. Criterios de aplicación de medidas de seguridad integral.

6. Documentación complementaria.
6.1 Normativa, Buenas Prácticas y Regulatoria.
6.2 Coordinación con Otros Planes.

5. ANÁLISIS DE RIESGOS DE OPERADORES CRÍTICOS

Plan de Protección Específico

Índice PPE

1. Introducción.
1.1 Base Legal.
1.2 Objetivo de este Documento.
1.3 Finalidad y Contenido del PPE
1.4 Método de Revisión y Actualización.
1.5 Protección y Gestión de la Información y Documentación

2. Aspectos Organizativos.
2.1 Organigrama de Seguridad.
2.2 Delegados de Seguridad de las Infraestructuras Críticas.
2.3 Mecanismos de Coordinación.
2.4 Mecanismos y Responsables de Aprobación.

3. Descripción de la Infraestructura Crítica.
3.1 Datos Generales de la infraestructura crítica.
3.2 Activos/Elementos de la infraestructura crítica.
3.3 Interdependencias.

4. Resultados del Análisis de Riesgos.
4.1 Amenazas Consideradas.
4.2 Medidas de Seguridad Integral existentes.
4.2.1 Organizativas o de Gestión.
4.2.2 Operacionales o Procedimentales.
4.2.3 De Protección o Técnicas.
4.3 Valoración de Riesgos.

5. Plan de Acción propuesto (por activo).

6. Documentación complementaria.

5. ANÁLISIS DE RIESGOS DE OPERADORES CRÍTICOS

Principales escollos del AR en OC

Algunas de las dificultades más habitualmente encontradas son:

- Existencia de análisis de riesgos previos con otro objeto:
  - Considerando impacto al negocio y no a la Sociedad
  - Con metodologías dispares de Seguridad Física y Lógica
  - Centrado en activos, no en servicios esenciales
  - Escalas de impacto incompatibles con consecuencias analizadas por CNPIC
- Función de Seguridad integral no desarrollada en la compañía:
  - Falta de concienciación de Seguridad, dificultades para obtener información de los servicios, procesos y activos
  - Responsables sin capacidad de toma de decisiones
  - Áreas de Seguridad física y de información muy distantes

5. ANÁLISIS DE RIESGOS DE OPERADORES CRÍTICOS

Principales herramientas disponibles

Para solventar los problemas indicados, se dispone de ciertas herramientas al alcance de los Operadores Críticos:

- Concienciación de la Dirección, mediante carta recibida por el más alto representante de cada empresa desde el Ministerio del Interior. Deben involucrarse en una política de Seguridad integral.
- Obligaciones legales:
  - De presentación de PSO y PPE, incluyendo información sobre análisis de riesgos
  - De designar interlocutores únicos de Seguridad
    - ✓ Responsable de Seguridad y Enlace en general
    - ✓ Responsable de Seguridad de la información (CISO)
    - ✓ Delegados de Seguridad en cada IC
- Soporte del CNPIC en el proceso

6. UNA METODOLOGÍA CÓMÚN:

6. UNA METODOLOGÍA COMÚN: GR2SEC

Metodología propia de Cuevavaliente

MAGERIT + ISO 27000

- Esquema general de Magerit.
- Propuesta de controles de ambos.
- Identificación de activos según Magerit.
- Lista de amenazas según Magerit.

ISO 31000 + AS/NZS 4360

- Esquema general de ISO 31000.
- Análisis de Riesgos según AS/NZS 4360.
- Lista de amenazas y de Medidas de Seguridad según GRSec31000.

- Tratamiento unificado de todo tipo de Riesgos
- Propuesta de controles automática para todos los riesgos deliberados
- Análisis de madurez de controles para riesgos deliberados
- Permite generar un proceso de mejora continua en gestión de riesgos

6. UNA METODOLOGÍA COMÚN: GR2SEC

Etapas de la metodología

Las etapas que componen la metodología GR2sec forman parte de un ciclo de mejora continua, ubicándose en las fases de:

- Planificación:
  - ✓ Permitiendo definir el contexto (activos, amenazas y tiempos)
  - ✓ Obteniendo el riesgo inherente tras analizar sus componentes
- Implantación:
  - Proponiendo los controles (medidas) paliativos
  - Evaluando su estado actual y obteniendo con ello el riesgo residual

Proceso para el tratamiento de Riesgos en Infraestructuras Críticas

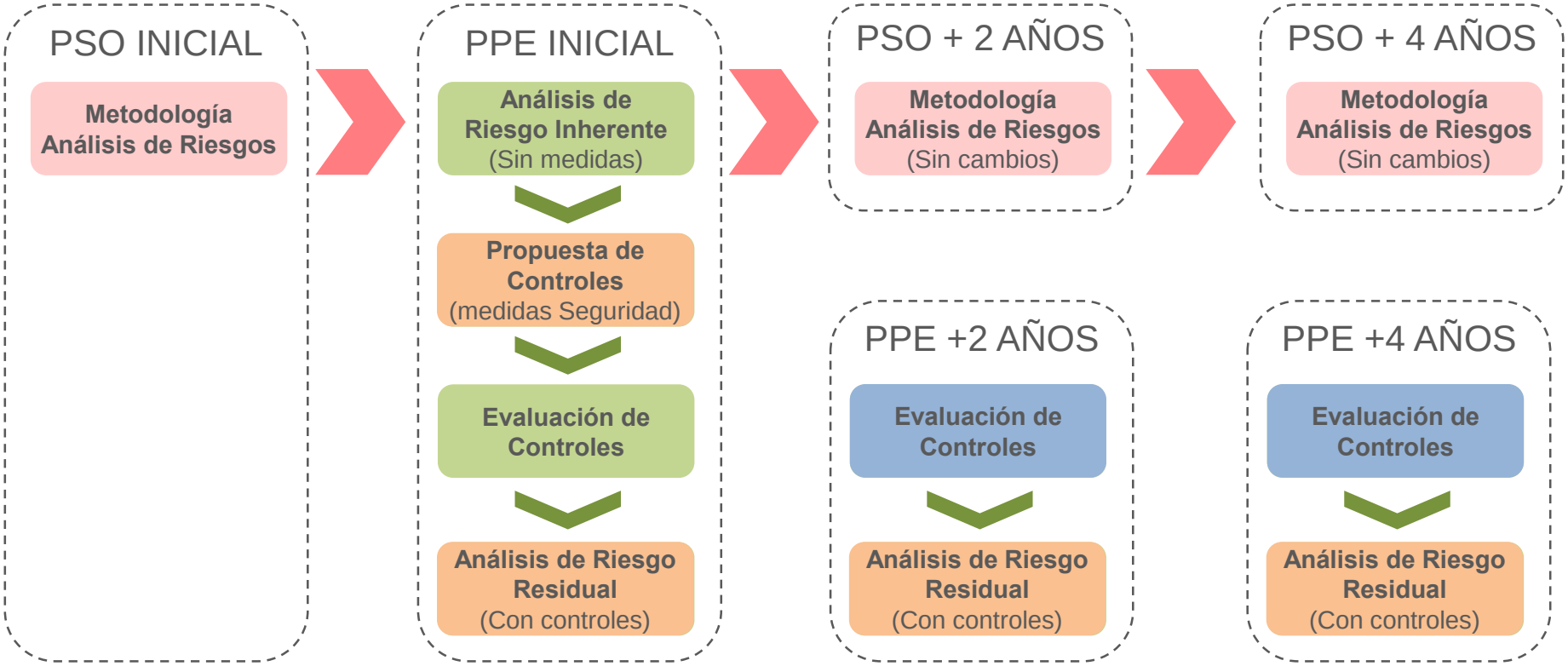
6. UNA METODOLOGÍA COMÚN: GR2SEC

Esquema de la metodología

Proceso para el tratamiento de Riesgos en Infraestructuras Críticas

6. UNA METODOLOGÍA COMÚN: GR2SEC

Análisis de Riesgos en PSO y PPEs con GR2sec

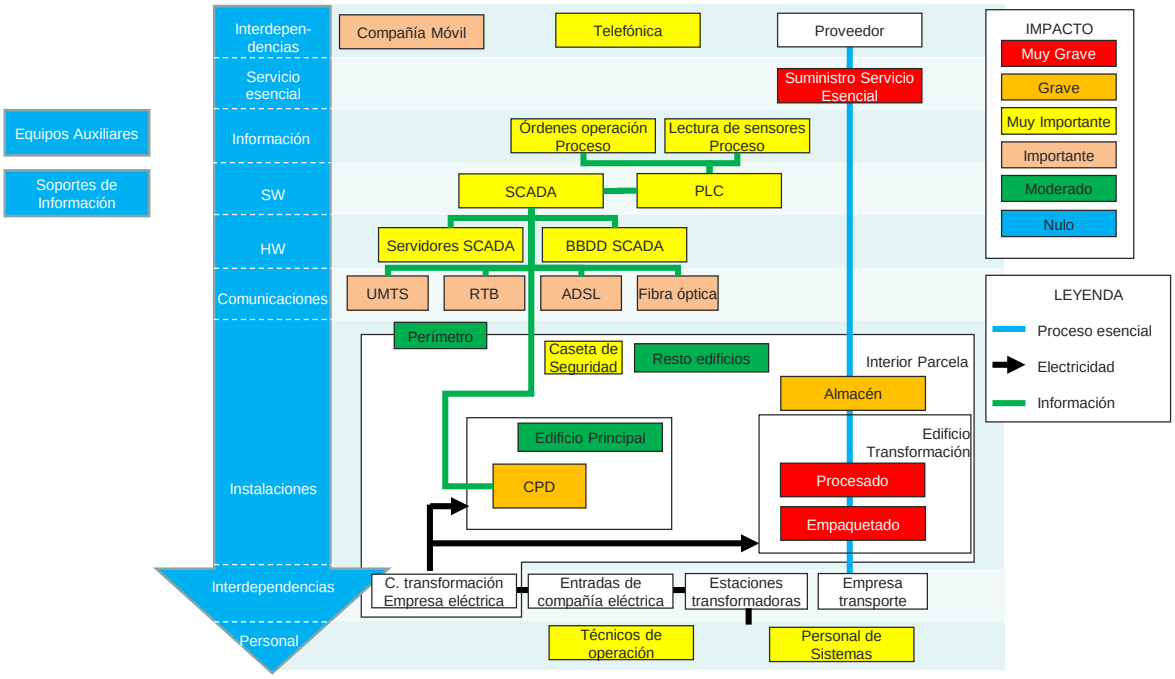


Texto explicativo
Entrada de datos (requiere experto)
Entrada de datos periódica (cliente con formación mínima)
Resultados generados automáticamente

6. UNA METODOLOGÍA COMÚN: GR2SEC

Herramientas del proceso unificado

Árbol de Activos



Proceso de Análisis de Riesgos

6. UNA METODOLOGÍA COMÚN: GR2SEC

Implantación mediante herramientas informáticas

1. Información muy compleja requiere quedar registrada y ser visualizada o modificada según responsabilidades
2. Los procesos de mejora continua requieren repetir los análisis y valorar la mejora
3. La homogenización requiere catálogos estandarizados y automatización en la propuesta de medidas (controles de Seguridad)
4. El análisis de riesgos no es un fin en sí mismo. Es también una herramienta de venta y justificación interna de las áreas que gestionan riesgo
5. Cuevavaliente Ingenierosofrece:
   - Herramienta GR2sec (www.gr2sec.com) diseñada para OC
   - Implantación de la metodología en otras herramientas existentes