Ingenia

INGENIERÍA E INTEGRACIÓN AVANZADAS

POWERING IT FOR YOUR BUSINESS

Ingenia
INGENIERÍA E INTEGRACIÓN AVANZADAS

SEGURIDAD, NUEVOS RETOS

APROSIP

Profesionales de la Seguridad

Medidas de seguridad en infraestructuras críticas y certificaciones normativas

Sevilla, 26 de noviembre de 2015

Universidad Pablo de Olavide

Ingenia
INGENIERÍA E INTEGRACIÓN AVANZADAS

INDICE

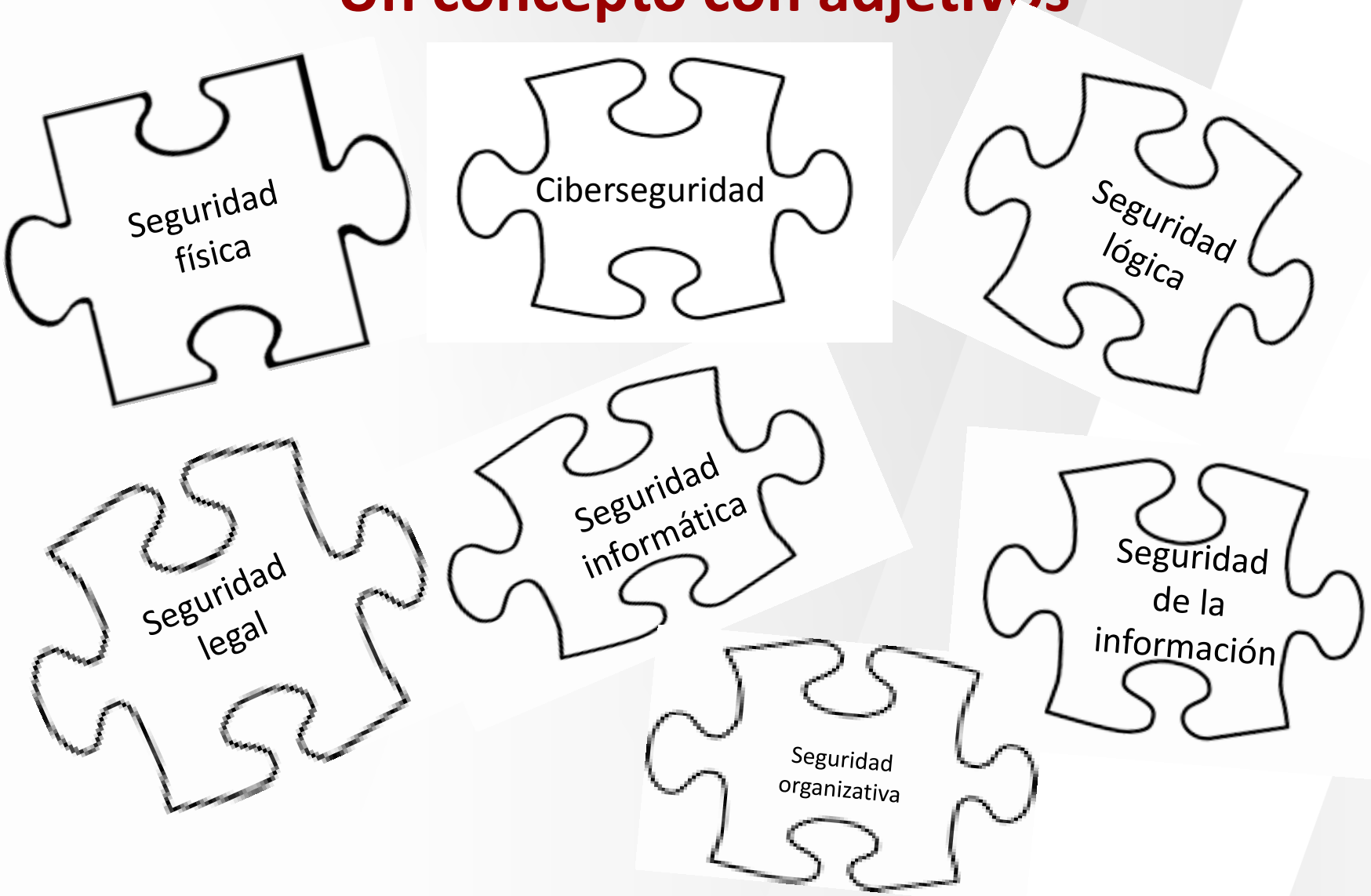
1. Seguridad: un concepto “amplio”.
2. Las medidas de seguridad en IC.
3. Las certificaciones de seguridad.
4. Conclusiones.

Ingenia
INGENIERÍA E INTEGRACIÓN AVANZADAS

INDICE

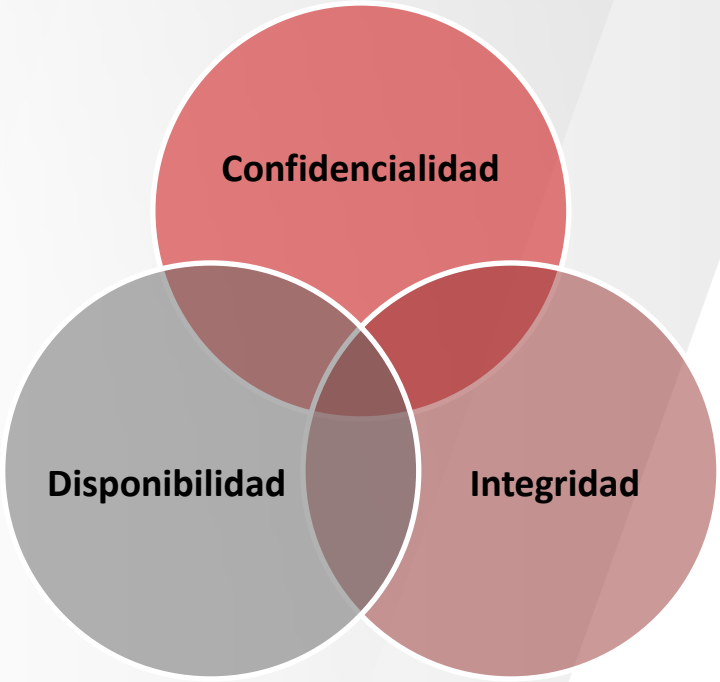
1. **Seguridad: un concepto “amplio”.**
2. Las medidas de seguridad en IC.
3. Las certificaciones de seguridad.
4. Conclusiones.

1. Seguridad: un concepto “amplio”. Un concepto con adjetivos



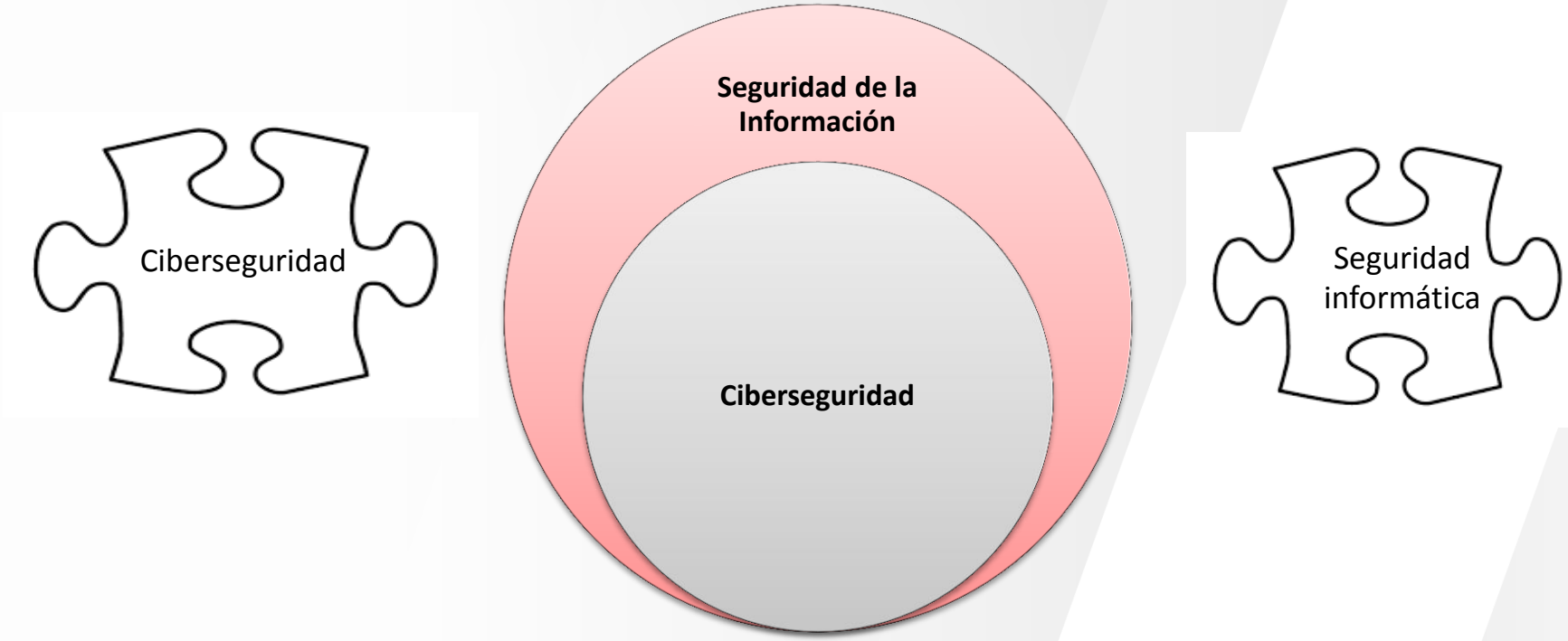
1. Seguridad: un concepto “amplio”. Seguridad de la información

- Se relaciona con la **protección de la información tanto en soporte físico como electrónico**, incluyendo la infraestructura que la almacena, procesa o transporta.
- Se orienta a proteger las diferentes dimensiones de seguridad de la información: al menos en la Confidencialidad, Integridad y Disponibilidad.



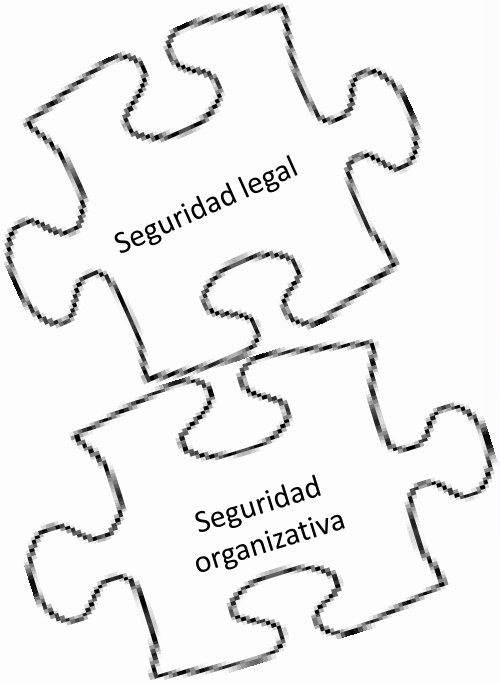
1. Seguridad: un concepto “amplio”. Ciberseguridad

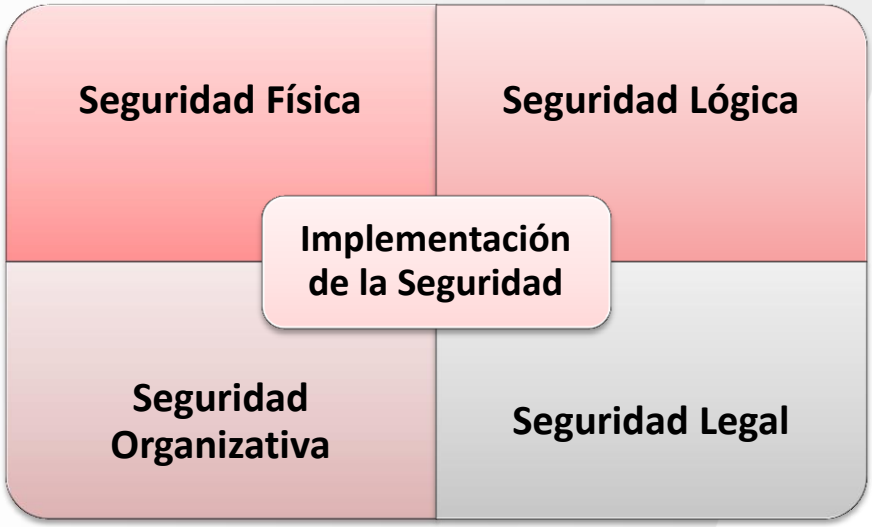
- Es aquella parte de la seguridad de la información centrada en la información procesada, almacenada y transportada por **sistemas de información interconectados**.



1. Seguridad: un concepto “amplio”. Seguridad física, lógica, legal…

- La información no es lo único que hay que proteger ni la única razón por la cual proteger, si bien en una infraestructura crítica es crucial, ya que una importante parte de la misma funciona mediante sistemas de información.
- **La seguridad en general,** y la seguridad de la información en particular, tienen varias **vertientes: lógica, física, legal, organizativa.**





1. Seguridad: un concepto “amplio”. Proteger los activos

- El fin de la seguridad es **la protección de los activos/elementos que soportan la infraestructura crítica**.
- Las medidas de seguridad físicas y lógicas a las que hace mención la legislación de IC protegerán los activos de las amenazas a las que están expuestos, conforme a un previo **análisis de riesgos**.

Amenazas

Riesgo

Medidas de Seguridad

=

1. Seguridad: un concepto “amplio”. Qué activos proteger

- Las **instalaciones** o componentes de la IC que son necesarios y por lo tanto vitales para la prestación del **servicio esencial**.
- Los **sistemas informáticos** (hardware y software) utilizado.
- Las redes de **comunicaciones** que permiten intercambiar datos y que se utilicen para dicha IC.
- Las **personas** o grupos de personas que explotan u operan todos los elementos anteriormente citados.
- Los **proveedores** críticos que son necesarios para el funcionamiento de dicha IC (emergencias, abastecimiento, etc.).
- Otras **terceras partes**: otras IICC del propio operador o de otro, usuarios finales.

1. Seguridad: un concepto “amplio”. normativa de seguridad de IC

- La normativa de IC contempla esta **visión holística de la seguridad**, en la cual se requiere la identificación de los servicios esenciales, los activos que los soportan, los riesgos asociados y las medidas de seguridad básicas.
- Plan de Seguridad del Operador (**PSO**) y Plan de Protección Específico (**PPE**) son los instrumentos para establecer las estrategias de implementación de las medidas de seguridad.

1. Seguridad: un concepto “amplio”. El PSO y los PPEs

- Son los documentos donde se plasma la estrategia e implementación de las medidas de seguridad de la IC.

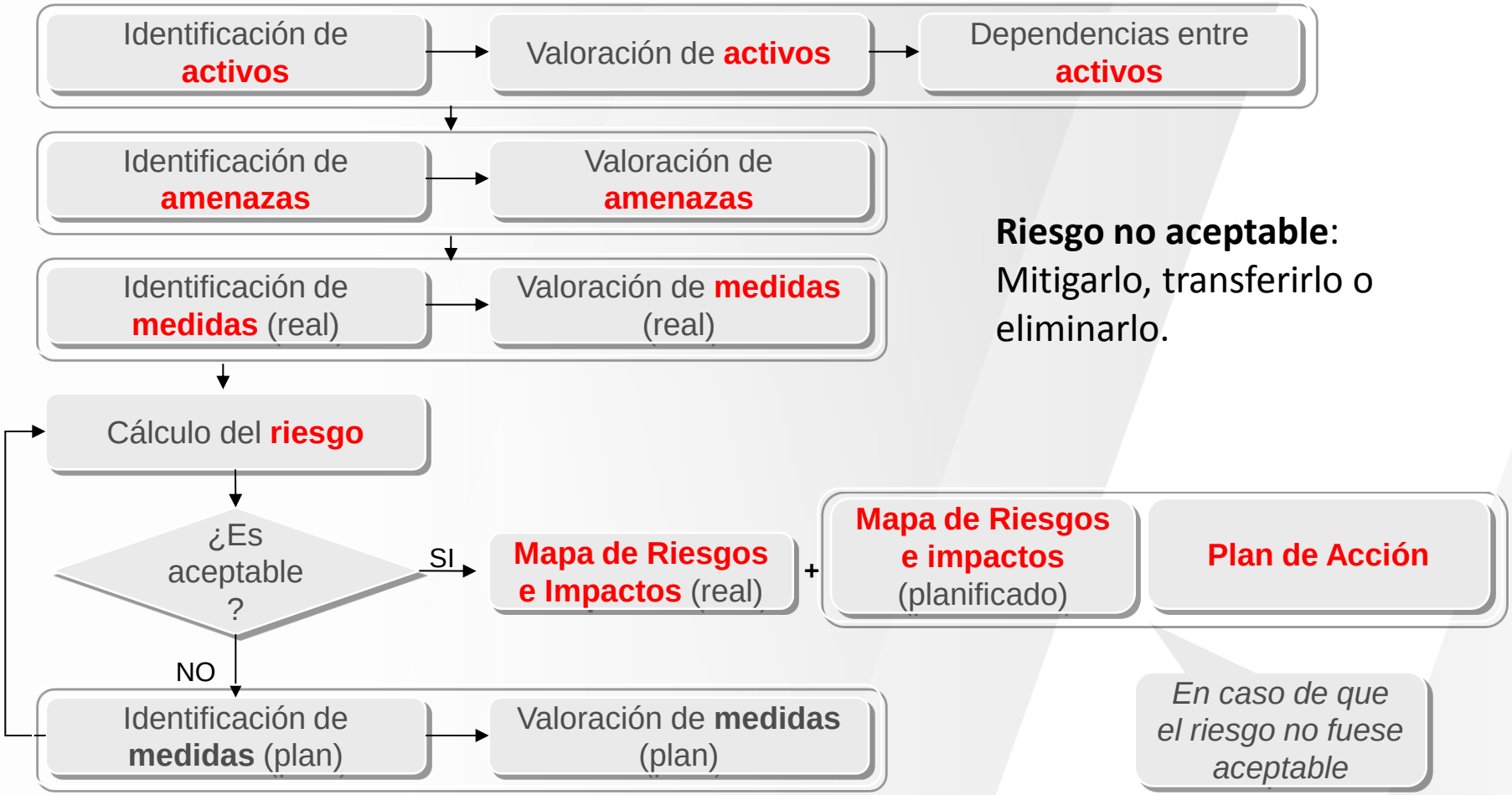
Plan de Seguridad del Operador (PSO)	Plan de Protección Específico por cada IC (PPEs)
Política general de seguridad del operador y marco de gobierno	Organización de la seguridad
Relación de Servicios Esenciales prestados por el Operador Crítico	Descripción de la infraestructura
Metodología de análisis de riesgo (amenazas físicas y lógicas)	Resultado del análisis de riesgos
Criterios de aplicación de **Medidas de seguridad**	**Medidas de seguridad y Plan de Acción propuesto (por activo)**
Documentación complementaria	Documentación complementaria

Ingenia
INGENIERÍA E INTEGRACIÓN AVANZADAS

INDICE

1. Seguridad: un concepto “amplio”.
2. **Las medidas de seguridad en IC.**
3. Las certificaciones de seguridad.
4. Conclusiones.

2. Las medidas de seguridad. Analicemos el riesgo: el proceso



Riesgo no aceptable: Mitigarlo, transferirlo o eliminarlo.

En caso de que el riesgo no fuese aceptable

2. Las medidas de seguridad. Analicemos el riesgo: amenazas y medidas

Identificación de **activos**

- Los **servicios** esenciales
- Las **instalaciones**
- Los sistemas informáticos (**hardware y software**).
- Las **comunicaciones**.
- Las **personas** que explotan/ operan.
- Los proveedores críticos
- Otras terceras partes: otras IICC del propio operador o de otro, usuarios finales.

Identificación de **amenazas**

Se podrían tomar como punto de partida diferentes tipologías de amenazas que están definidas en diferentes **catálogos existentes o referentes a nivel nacional o internacional** y que pudieran afectar a los activos tanto de tipo lógico como de tipo físico

Identificación de **medidas**

Las guía de Buenas Prácticas para el PPE proporciona **recomendaciones y ejemplos generales** que puede servir de punto de partida (Anexo I).
Podrán ser permanentes, temporales y graduales.
Deberán estar acordes con la **legislación vigente** y aplicable.

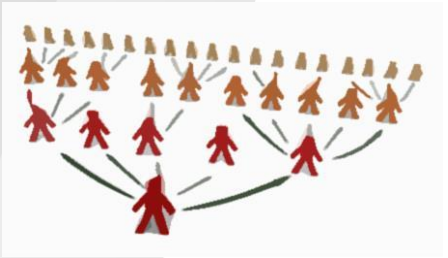
✓ Los OC y resto de agentes con un interés legítimo podrán dirigirse al CNPIC para obtener una **modelización típica de activos, amenazas y salvaguardas** que podrá ser utilizada a modo de guía para la realización del análisis de riesgos.

2. Las medidas de seguridad. Clasificación de medidas de seguridad

En la resolución de contenidos mínimos del PPE se determina que deben describirse las medidas conforme a los siguientes **niveles**:

Tipo de medida de seguridad	Descripción
Organizativas o de gestión	Medidas relacionadas con la gestión del proceso de seguridad. Embebidas en los procesos y estructuras organizativas, dan respuesta a los **riesgos**, condicionantes **normativos y regulatorio**s del entorno.
Operacionales o procedimentales	Derivados del cuerpo normativo establecido en la organización, engloban **Los procedimientos operacionales** o procedimentales que permiten realizar una gestión integral del proceso de seguridad y de **los controles implantados**.
De protección o técnicas	Controles de **carácter técnico** (preferiblemente automatizadas, que permitan crear registros de evidencias fiables)

2. Las medidas de seguridad. Medidas organizativas



- [2.4.2] Medidas existentes
  - [2.4.2.1] Medidas organizativas o de gestión
    - [2.4.2.1.1] ¿Se dispone de medidas permanentes para este nivel?
    - [2.4.2.1.2] ¿Se dispone de medidas temporales y graduales para este nivel?
    - [2.4.2.1.3] ¿Se dispone de un Análisis de Riesgos?
      - [RM.1] Se dispone de normativa en materia de gestión de riesgos
    - [2.4.2.1.4] ¿Se tienen definidos los roles y las responsabilidades?
      - [G.1.3] Roles identificados
      - [G.1.4] Asignación de responsabilidades para la seguridad de la información
      - [G.3.1.5] Se han identificado los roles y responsabilidades requeridas
      - [G.3.4.4] Se detalla quién es responsable de cada actividad
    - [2.4.2.1.5] ¿Se tiene definido el cuerpo normativo (políticas, procedimientos y estándares de seguridad)?
      - [G.3.2] Política de Seguridad de la Organización
      - [G.3.4] Procedimientos operativos de seguridad (POS)
    - [2.4.2.1.6] ¿Se dispone de las normas y/o regulaciones de aplicación a la infraestructura crítica así como su nivel de
      - [G.3.3] Normas de seguridad
    - [2.4.2.1.7] ¿Se tienen certificaciones, acreditaciones y evaluaciones de seguridad de la IC?
      - [G.exam.5] Certificación o acreditación del sistema
  - [2.4.2.2] Medidas operacionales o procedimentales
  - [2.4.2.3] Medidas de protección o técnicas

2. Las medidas de seguridad. Medidas operacionales o procedimentales

- [2.4.2] Medidas existentes
  - [2.4.2.1] Medidas organizativas o de gestión
  - [2.4.2.2] Medidas operacionales o procedimentales
    - [2.4.2.2.1] ¿Se dispone de medidas permanentes para este nivel?
    - [2.4.2.2.2] ¿Se dispone de medidas temporales y graduales para este nivel?
    - [2.4.2.2.3] ¿Se dispone de procedimientos para la realización, gestión y mantenimiento de activos?
      - [2.4.2.2.3.1] ¿Se dispone de un procedimiento de inventariado (Identificación/Catalogación/etc.) de activos físicos y lógicos?
      - [2.4.2.2.3.2] ¿Se dispone de un procedimiento de gestión continua de activos físicos y lógicos (Alta/Baja/Modificación)?
    - [2.4.2.2.4] ¿Se dispone de procedimientos de formación y concienciación?
      - [2.4.2.2.4.1] ¿De carácter tanto general como específica para empleados/operarios?
      - [2.4.2.2.4.2] ¿De carácter tanto general como específica para personal de seguridad?
      - [PS.AT] Formación y concienciación
    - [2.4.2.2.5] ¿Se dispone de procedimientos de contingencia/recuperación según los escenarios definidos?
    - [2.4.2.2.6] ¿Se dispone de procedimientos para supervisión/evaluación/auditoría?
      - [2.4.2.2.6.1] ¿De activos físicos de la infraestructura (Alcance / Operación / Seguimiento)?
      - [2.4.2.2.6.2] ¿De activos lógicos o de sistemas de operación (Alcance / Operación / Seguimiento)?
    - [2.4.2.2.7] ¿Se dispone de procedimientos para la gestión de acceso?
      - [2.4.2.2.7.1] ¿Para gestión de usuarios (altas, bajas, modificaciones, procesos de selección, régimen interno, procedimientos de cese, etc)?
      - [2.4.2.2.7.2] ¿Para control de accesos temporales?
      - [2.4.2.2.7.3] ¿Para control de entradas y salidas?
    - [2.4.2.2.8] ¿Se dispone de procedimientos operacionales del personal de seguridad (funciones, horarios, dotaciones, etc.)?
    - [2.4.2.2.9] ¿Se dispone de procedimientos de gestión y respuesta de incidentes?
  - [2.4.2.3] Medidas de protección o técnicas

2. Las medidas de seguridad. Medidas de protección o técnicas

- [2.4.2] Medidas existentes
  - [2.4.2.1] Medidas organizativas o de gestión
  - [2.4.2.2] Medidas operacionales o procedimentales
  - [2.4.2.3] Medidas de protección o técnicas
    - [2.4.2.3.1] ¿Se dispone de medidas permanentes para este nivel?
    - [2.4.2.3.2] ¿Se dispone de medidas temporales y graduales para este nivel?
    - [2.4.2.3.3] ¿Se dispone de medidas de prevención y detección?
      - [2.4.2.3.3.1] ¿Se dispone de elementos de seguridad física y electrónica para la protección del perímetro y control de accesos?
        - [L.AC.2.b] Sistema automático de control de accesos
        - [L.AC.c.2] Las áreas de seguridad disponen de algún tipo de llave, combinación o dispositivo de seguridad para acceder a las mismas
        - [L.AC.2.c] Se dispone de un sistema de cámaras de vigilancia
        - [L.8] Protección del perímetro
        - [L.a] Iluminación de seguridad
      - [2.4.2.3.3.2] ¿Se dispone de elementos de seguridad lógica?
    - [2.4.2.3.7] ¿Se dispone de medidas de coordinación y monitorización?
      - [2.4.2.3.7.1] ¿Se dispone de Centro de Control de Seguridad (control de alarmas, recepción y visionado de imágenes, etc.)?
        - [L.9.3] La vigilancia se realiza desde un centro de control en el que se centralizan todos los sistemas de seguridad
        - [L.8.3.4.2] Conectado con central receptora de alarmas fuera de las horas de trabajo
      - [2.4.2.3.7.2] ¿Se dispone de equipos de vigilancia (turnos, rondas, volumen, etc.)?
        - [L.9] Vigilancia
      - [2.4.2.3.7.3] ¿Se dispone de sistemas de comunicación?

2. Las medidas de seguridad. Medidas complementarias

- Se podrán contemplar otras medidas **físicas o lógicas** además de las establecidas en la resolución de contenidos mínimos del PPE y conforme a los criterios que se hayan establecido en el PPO.
- En el ámbito de **la seguridad lógica** se establece como buena práctica, realizar la selección de los controles de seguridad a implementar y gestionar de la **ISO 27002 (guía de buenas prácticas para implantar el Anexo I de la norma ISO 27001).**
- En el ámbito de la **seguridad física** se deberá seguir lo especificado por la legislación de Seguridad Privada, especialmente lo recogido en la **Orden Ministerial 316/2011** del Ministerio del Interior y su referencia a la normativa UNE-EN y UNE-CLC/TS (sistemas de alarmas, grados de seguridad).
- Y todo ello sin olvidar cualquier **otra legislación vigente aplicable** al ámbito en materia de seguridad:
  - Esquema Nacional de Seguridad (RD 3/2010 y RD 951/2015)
  - Ley Orgánica de Protección de Datos (Ley 15/1999 y RD 1720/2007).
  - Seguridad ambiental y de las personas (PRL, sectoriales…)

2. Las medidas de seguridad. El plan de acción

- Si las medidas establecidas en la resolución de contenidos mínimos y complementarias no fuesen suficientes para mitigar el riesgo, preciso establecer acciones.
- La guía de buenas practicas establece que sea a 3 años y que presente la siguiente estructura

IDENTIFICADOR DE LA ACCIÓN:		
CÓDIGO ÚNICO NOMBRE DESCRIPTIVO		
OBJETIVO:		
ESPECIFICACIÓN DE LA FINALIDAD DE LA ACCIÓN.		
DESCRIPCIÓN:		
DESCRIPCIÓN DE LA ACCIÓN.		
RESPONSABLE:		
RESPONSABLE DE LA ACCIÓN.		
DEPENDENCIAS CON OTRAS ACCIONES:		
ACCIONES CON LAS QUE ÉSTA GUARDA RELACIÓN.		
Activos		
Identificador:	Responsable:	Tipología:
Identificador del Activo 1 (Código y Nombre Descriptivo)	Responsable del Activo 1	INS / SI / RED / PER / PRO
Identificador del Activo 2	Responsable del Activo 2	INS / SI / RED / PER / PRO
Medidas de Seguridad		
Identificador:	Responsable:	Tipología y Carácter
Medida de seguridad 1.	Responsable de la medida de seguridad 1.	Organizativa / Operacional / Técnica Permanente / Gradual
Medida de seguridad 2.	Responsable de la medida de seguridad 2.	Organizativa / Operacional / Técnica Permanente / Gradual
MECANISMOS DE COORDINACIÓN Y SEGUIMIENTO:		
MECANISMOS PARA LA ACCIÓN.		
INVERSIÓN:	ESTIMACIÓN TEMPORAL:	
ESTIMACIÓN DEL COSTE DE LA ACCIÓN.		

2. Las medidas de seguridad. El plan de acción

- Las medidas de seguridad pueden segmentarse en tareas atómicas.

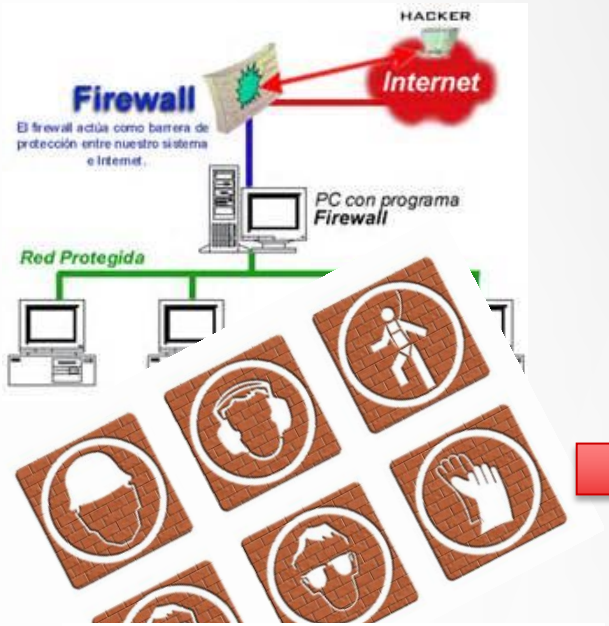
IDENTIFICADOR DE LA MEDIDA DE SEGURIDAD:		
CÓDIGO ÚNICO NOMBRE DESCRIPTIVO		
DESCRIPCIÓN:		
DESCRIPCIÓN DE LA MEDIDA DE SEGURIDAD.		
RESPONSABLE		
RESPONSABLE DE LA MEDIDA DE SEGURIDAD.		
ACCIÓN:		
IDENTIFICADOR DE LA ACCIÓN QUE ENGLOBA ESTA MEDIDA DE SEGURIDAD.		
CRITICIDAD:	CARÁCTER:	TIPOLOGÍA:
NIVEL DE CRITICIDAD.	☐PERMANENTE ☐ TEMPORAL / GRADUAL NIVEL DE AMENAZA INDICA EL NIVEL DE AMENAZA O CIRCUNSTANCIA PARA LA ACTIVACIÓN DE LA MEDIDA TEMPORAL O GRADUAL.	ORGANIZATIVA O DE GESTIÓN / OPERACIONAL O PROCEDIMENTAL / DE PROTECCIÓN O TÉCNICA.
Activos		
Identificador:	Responsable:	Tipología:
Identificador del Activo 1 (Código y Nombre Descriptivo)	Responsable del Activo 1	INS / SI / RED / PER / PRO
Identificador del Activo 2	Responsable del Activo 2	INS / SI / RED / PER / PRO

Ingenia
INGENIERÍA E INTEGRACIÓN AVANZADAS

INDICE

1. Seguridad: un concepto “amplio”.
2. Las medidas de seguridad en IC.
3. **Las certificaciones de seguridad.**
4. Conclusiones.

3. Las certificaciones de seguridad. La necesidad de gestionar



Es necesario un proceso de organización y gestión, ya que la seguridad sin un control y mantenimiento perderá su eficacia en el tiempo.

Además deberán contemplarse otros aspectos de seguridad corporativos más allá de la IC.

Las seguridad debe gestionarse como un proceso de negocio mas.

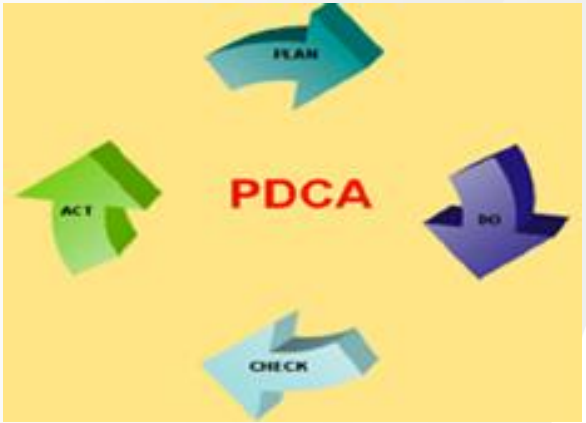
3. Las certificaciones de seguridad. La obligatoriedad de gestionar

PSO apartado 2.2.3 Modelo de Gestión Aplicado.

*La **seguridad integral** depende de un proceso de gestión integral que debe aportar el control organizativo y técnico necesario para determinar en todo momento el nivel de exposición a las amenazas y el nivel de protección y respuesta que es capaz de proporcionar la organización para la protección y seguridad de sus servicios esenciales e Infraestructuras Críticas.*

[…] el Operador Crítico deberá recoger dentro del PSO su modelo de gestión, que deberá contemplar al menos, los siguientes aspectos:

- *Una implementación de controles de seguridad acorde con las prioridades y necesidades evaluadas.*
- *Una evaluación y monitorización periódica de seguridad*



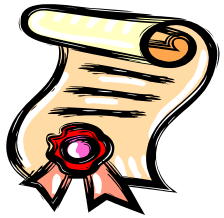
3. Las certificaciones de seguridad. Modelos de Gestión posibles

- **ISO 27001: 2013 – SGSI** – **S**istema de **G**estión de la **S**eguridad de la **I**nformación.
- **ISO 22301: 2012 – SGCN** - **S**istema de **G**estión de la **C**ontinuidad del **N**egocio.
- **ISO 22320:2013 – S**istema de **G**estión de **E**mergencias y Respuesta ante incidentes

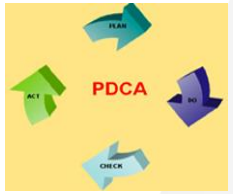
3. Las certificaciones de seguridad. Implantación y mantenimiento de un Sistema de Gestión

- Análisis de Riesgos
- Plan (Seguridad, Continuidad)
- Manual del Sistema
- Definición de Indicadores
- Ejecución del Plan y Formación
- Auditoría Interna

- Gestión de la Certificación
- Auditoría Externa
- Plan de Acciones Correctivas



- Revisiones Periódicas – Nuevos Planes de Seguridad
- Seguimiento y Control (Oficina Técnica)



3. Las certificaciones de seguridad. Beneficios

Para la Organización

- Tener la confianza de que la gestión de la seguridad se adecua a las mejores prácticas **reconocidas internacionalmente**.
- Garantía de continuidad del negocio y reducción de riesgos.
- Garantía del **cumplimiento** con la legislación vigente. Cumplimiento de las **actualizaciones bienales PSO y PPEs**

Para el Negocio

- Una **entidad externa a la organización certifica** que el sistema está correctamente implantado internacionalmente.
- Aumento del **valor comercial** y mejora de la imagen frente a **clientes, instituciones y proveedores**.
- Diferenciación con respecto a la **competencia**.

Ingenia
INGENIERÍA E INTEGRACIÓN AVANZADAS

INDICE

1. Seguridad: un concepto “amplio”.
2. Las medidas de seguridad en IC.
3. Las certificaciones de seguridad.
4. **Conclusiones.**

Ingenia
INGENIERÍA E INTEGRACIÓN AVANZADAS

3. Conclusiones

- **La seguridad integral**. Contemplar un modelo holístico de seguridad en la protección de la IC, abarcando ciberseguridad, seguridad de las personas, de las instalaciones, etc.
- **El análisis de riesgos** como patrón para determinar qué proteger y qué medidas aplicar.
- **Medidas de seguridad** de naturaleza física y lógica, clasificadas en medidas organizativas, operacionales y técnicas.
- La **certificación en estándares ISO** como garantía de cumplimiento en el tiempo.

Ingenia

INGENIERÍA E INTEGRACIÓN AVANZADAS

POWERING IT FOR YOUR BUSINESS

Gracias por su atención

Elisa García Martin. egmartin@ingenia.es
Consultora de Seguridad Estratégica y Consultoría TI