Telecom for energy

PULLNET
Telecom for energy

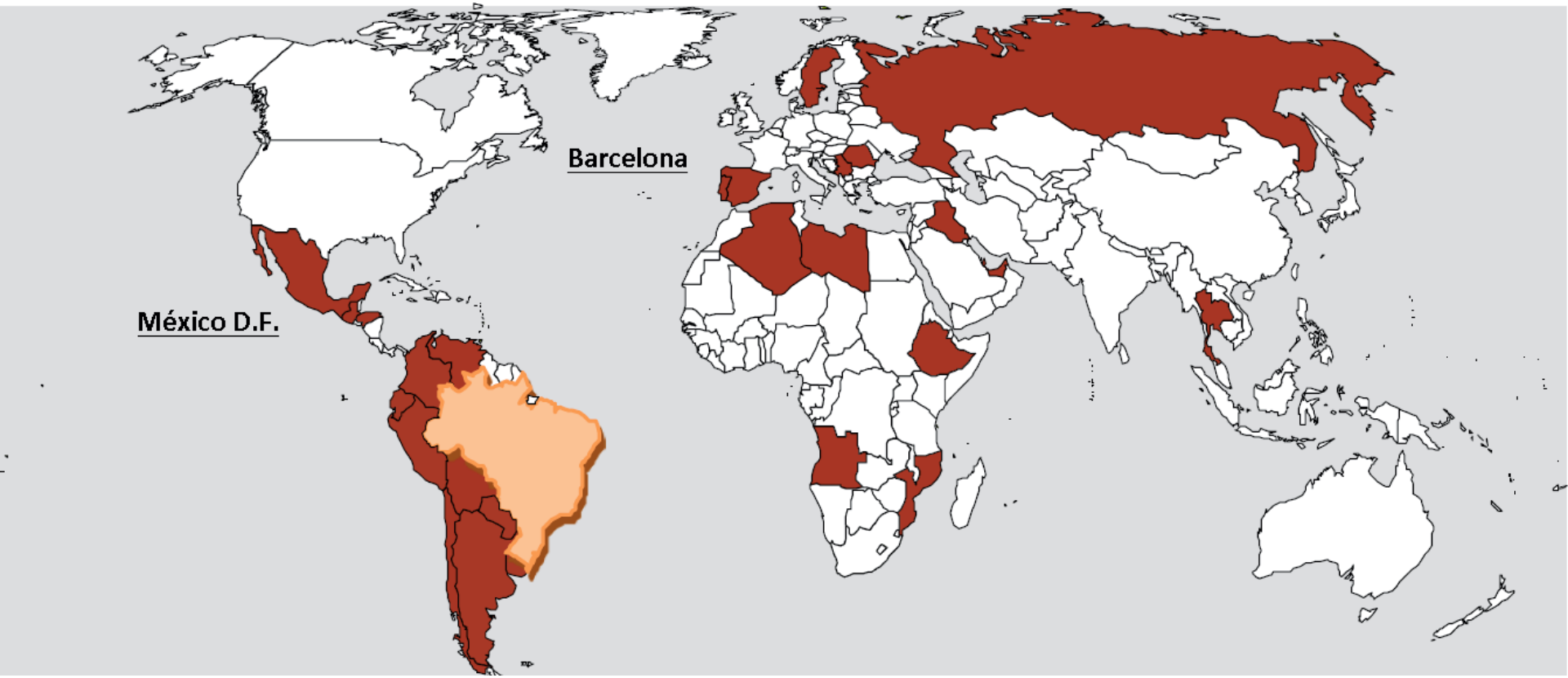
Principios de diseño de la Seguridad Informática de los Sistemas de Operación

INTRODUCCIÓN

Pullnet Technology

- Soluciones ICT para la automatización del sector eléctrico
  - IEC 61850
  - Seguridad informática
- Servicios profesionales
  - Capacitación especializada
  - Consultoría de estrategia tecnológica
- Liderazgo internacional

Presencia Internacional

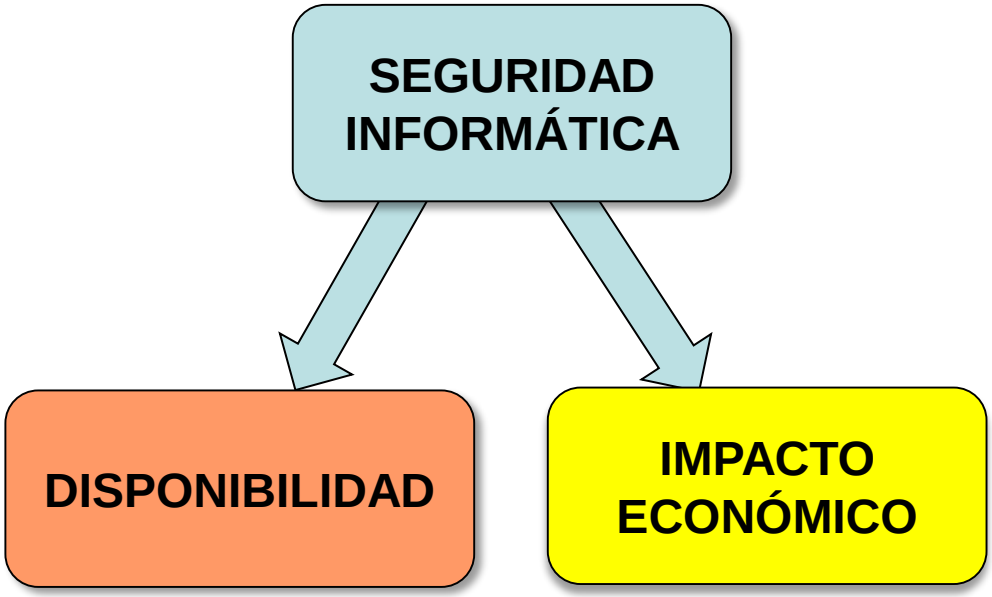


Dificultades

Un cambio de Paradigma

- No se trata de defender los IEDs
- El objetivo es defender las funciones del SAS
  - Una función puede estar implementada por varios IEDs
  - Una función puede requerir comunicaciones entre IEDs
- La configuración de seguridad requiere conocer la implementación de las funciones
  - Los criterios deben ser homogéneos e independientes de la implementación
    - Especificación del dominio de seguridad
  - La configuración de seguridad depende de la implementación

Factores determinantes

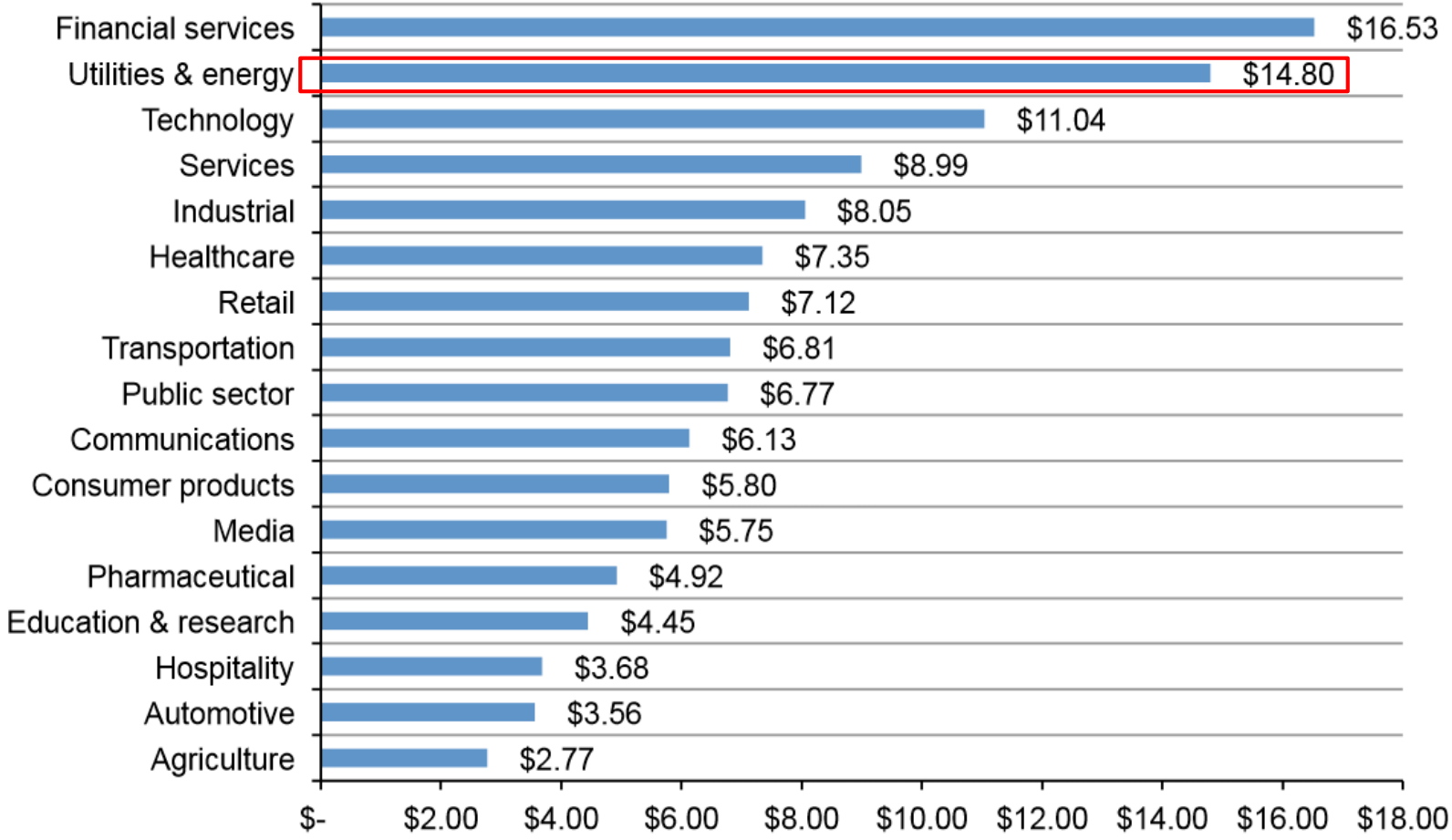


Comparativa IT Vs OT

Área de Interés	Sistemas IT	P&C
Objetivo Básico	Información	Maximizar la disponibilidad del proceso
Impacto del Riesgo Primario	Acceso no autorizado a la Información	Disponibilidad de la Operación
Foco de la Seguridad	Centralizada. Seguridad de los servidores, acceso a Internet	Descentralizada. Seguridad de las funciones de P&C. Bloquear o minimizar el uso de Internet
Disponibilidad	95 – 99%	99.9 – 99.999%
Robustez	Se toleran Interrupciones del servicio	Tolerante a Fallos, Redundancia, No se aceptan interrupciones
Modo de Operación	Interactivo, transaccional	Interactivo, tiempo real, respuesta espontánea
Fiabilidad	Depende del personal	Indirecta, depende de los IEDs

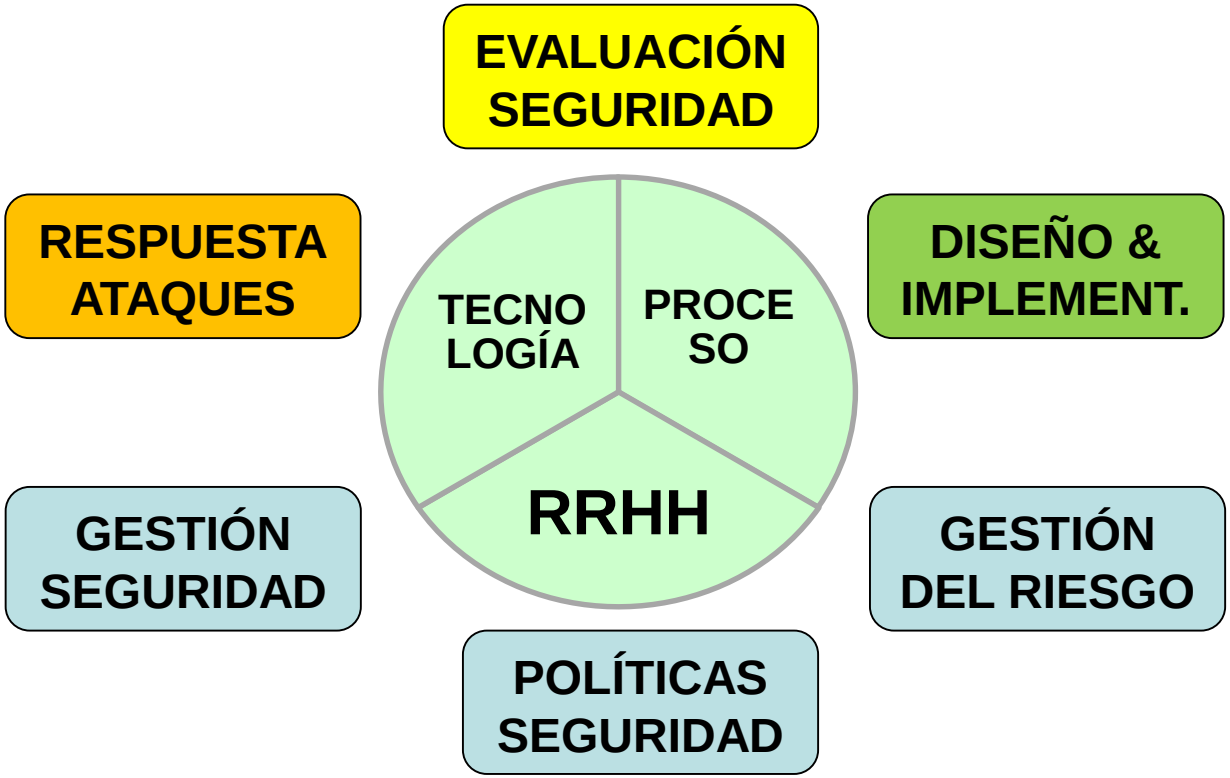
Impacto económico

Coste medio anualizado de 252 empresas agrupadas por sectores



Ponemon Institute "2015 Cost of Cyber Crime Study: Global"

Componentes de la seguridad

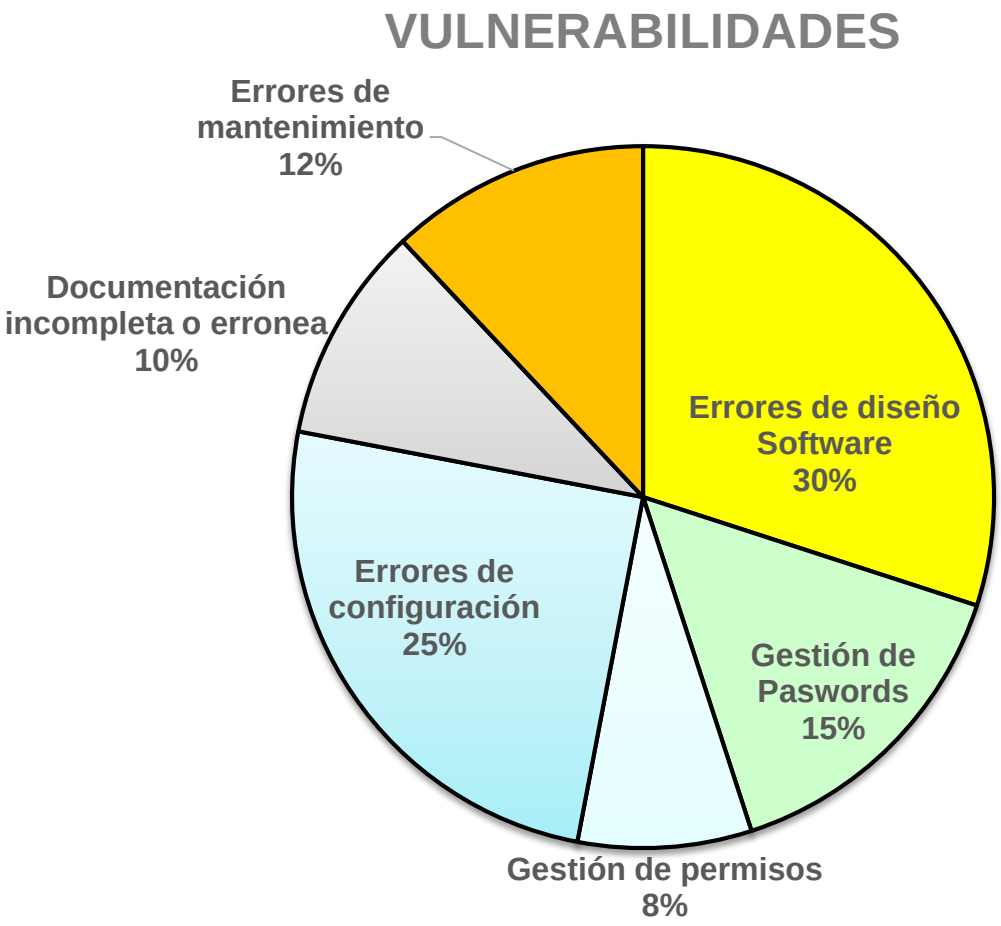


PRINCIPIOS DE DISEÑO

Retos de la Seguridad

- Diseñar un sistema de automatización efectivo en coste
  - Aplicar las medidas necesarias
    - Proporcionales al riesgo y al valor protegido
- Aplicar criterios de seguridad dinámicos
  - Las amenazas evolucionan constantemente
- No afectar al desempeño
  - La seguridad mejora la disponibilidad pero puede afectar al desempeño
    - Equilibrio disponibilidad/desempeño

Desglose de Vulnerabilidades

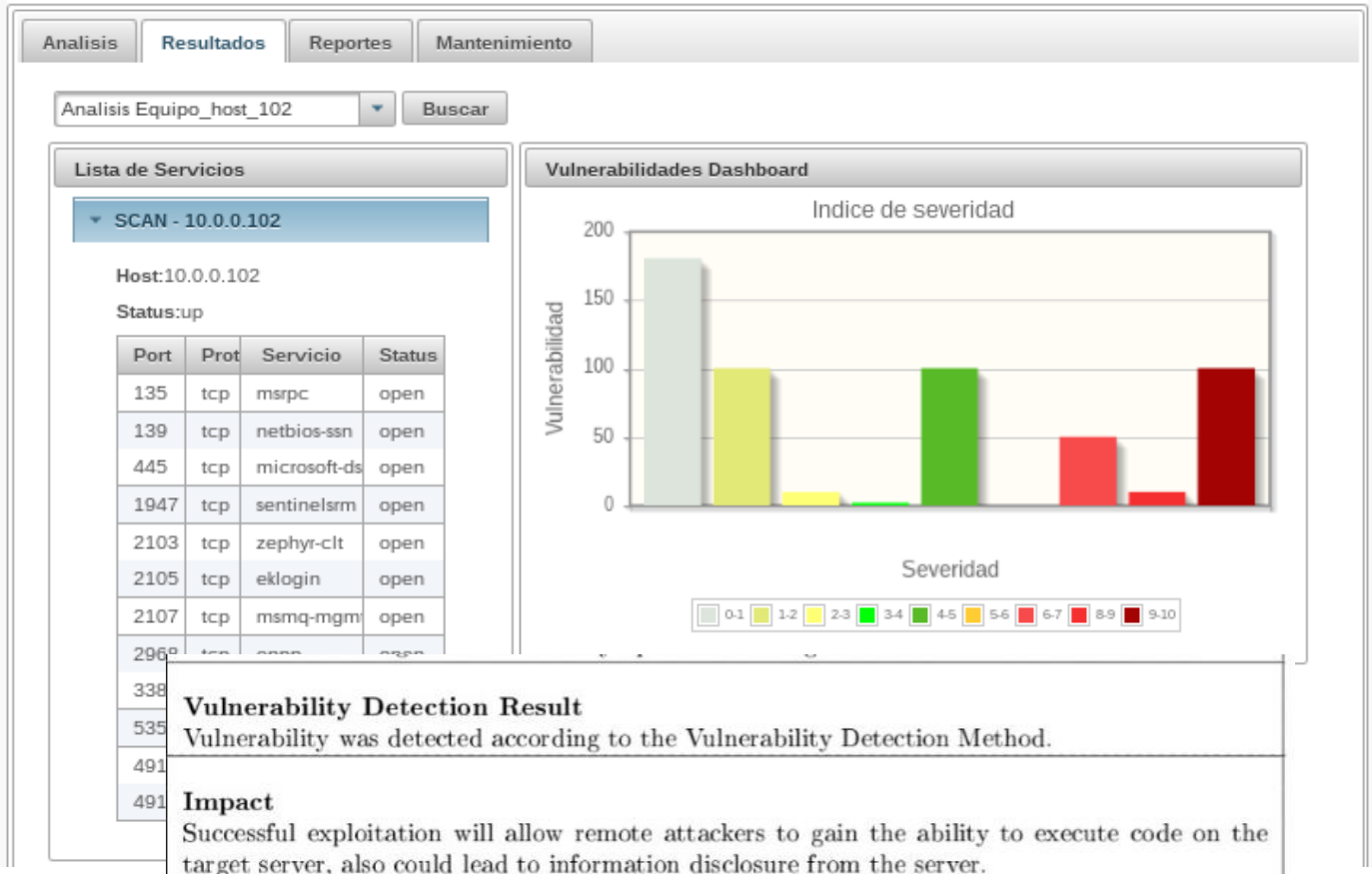


Análisis de Vulnerabilidades

Es el proceso de identificar, cuantificar y priorizar las vulnerabilidades del sistema

- Incluye todos los aspectos relacionados con la seguridad
  - Aplicaciones, equipos, servicios auxiliares, comunicaciones, etc.
- Proceso de análisis
  - Catalogar los equipos y aplicaciones
  - Asignar un peso en función de la importancia del equipo
  - Identificar las vulnerabilidades de cada equipo
  - Mitigar o eliminar las vulnerabilidades más importantes

Ejemplo de herramienta. VSA-7

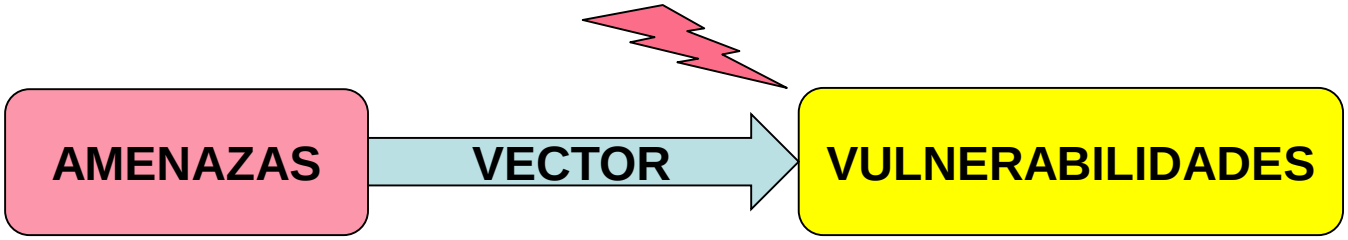


Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.
Impact Level: System

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS17-010

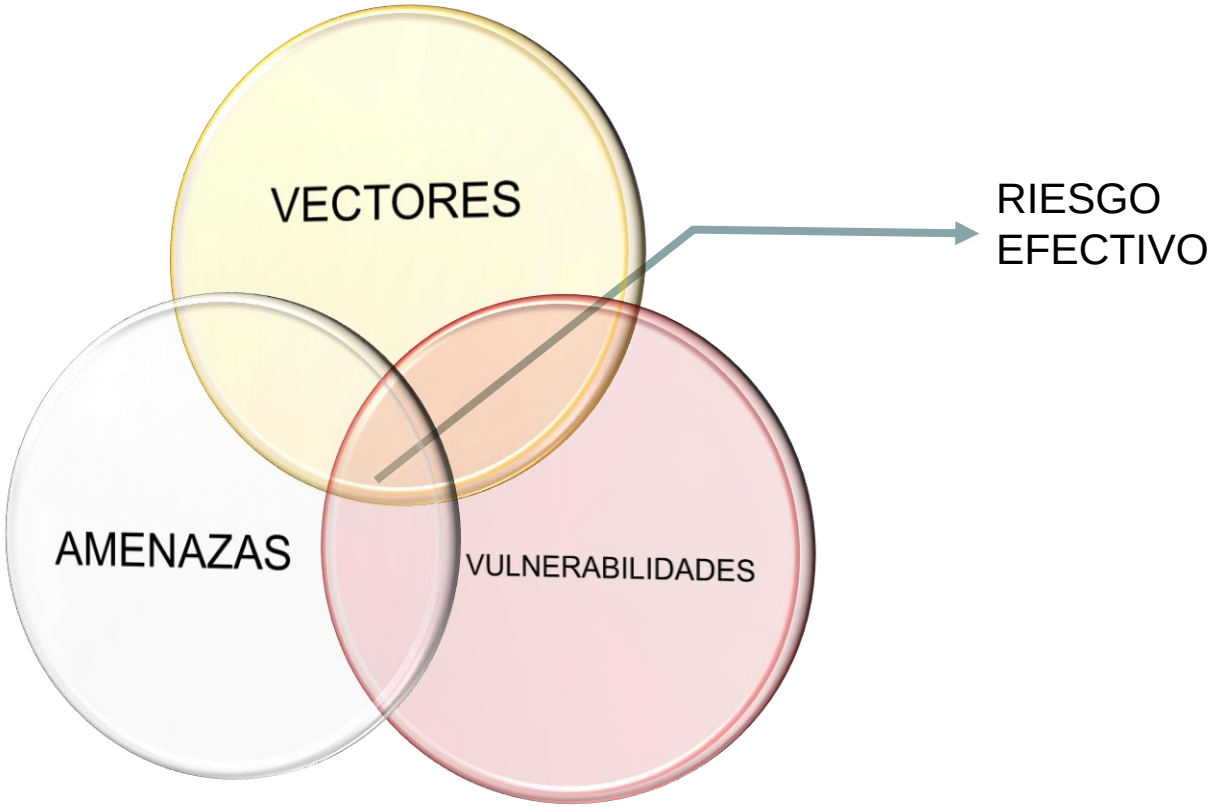
Vectores de ataque



Un Vector de ataque es el medio utilizado por un atacante para explotar una vulnerabilidad

- Las amenazas necesitan un “Vector” de ataque para explotar las vulnerabilidades
- Es importante conocer los posibles vectores para proteger adecuadamente las vulnerabilidades
  - Si no existe el vector no se puede realizar el ataque

Riesgo a considerar



Principales Riesgos

- Acceso remoto
  - Establece conexiones con otras redes
    - Puede abrir una puerta a amenazas no contempladas
- Gestión y configuración de equipos
  - El acceso no autorizado a la gestión de un IED puede modificar su configuración
    - Inhibir funciones, alterar su funcionamiento, etc.
  - Los equipos más críticos son:
    - Firewall
    - Switches LAN P&C y Router
- BYOD

Otras vulnerabilidades

- La mayoría de equipos son antiguos sin mantenimiento de Firmware
  - No han sido diseñados considerando la seguridad
  - No se pueden solucionar las vulnerabilidades conocidas
- No disponen de seguridad en las funciones de mantenimiento
  - Acceso sin password
  - Acceso sin autentificación
- No se verifica la configuración de los Sistemas Operativos
  - Puertas traseras abiertas, passwords no configurados, etc.

Facilitadores de ataques

- Actores
  - Política de seguridad mal aplicada
  - Confianza infundada
    - Confiar en medidas de seguridad que deberían ser implementadas en otras zonas de seguridad por otros departamentos
  - Capacitación inadecuada
  - Auditorías incompletas o poco frecuentes
- Especificación
  - No considerar la seguridad como un aspecto de la especificación puede introducir vulnerabilidades
- Diseño
  - Configuraciones incompletas o no definidas
- FAT/SAT
  - Pruebas de rutina que no validan el diseño
  - IEDs cuya seguridad nunca ha sido evaluada

EVALUACIÓN DE RIESGOS

Definición de riesgo

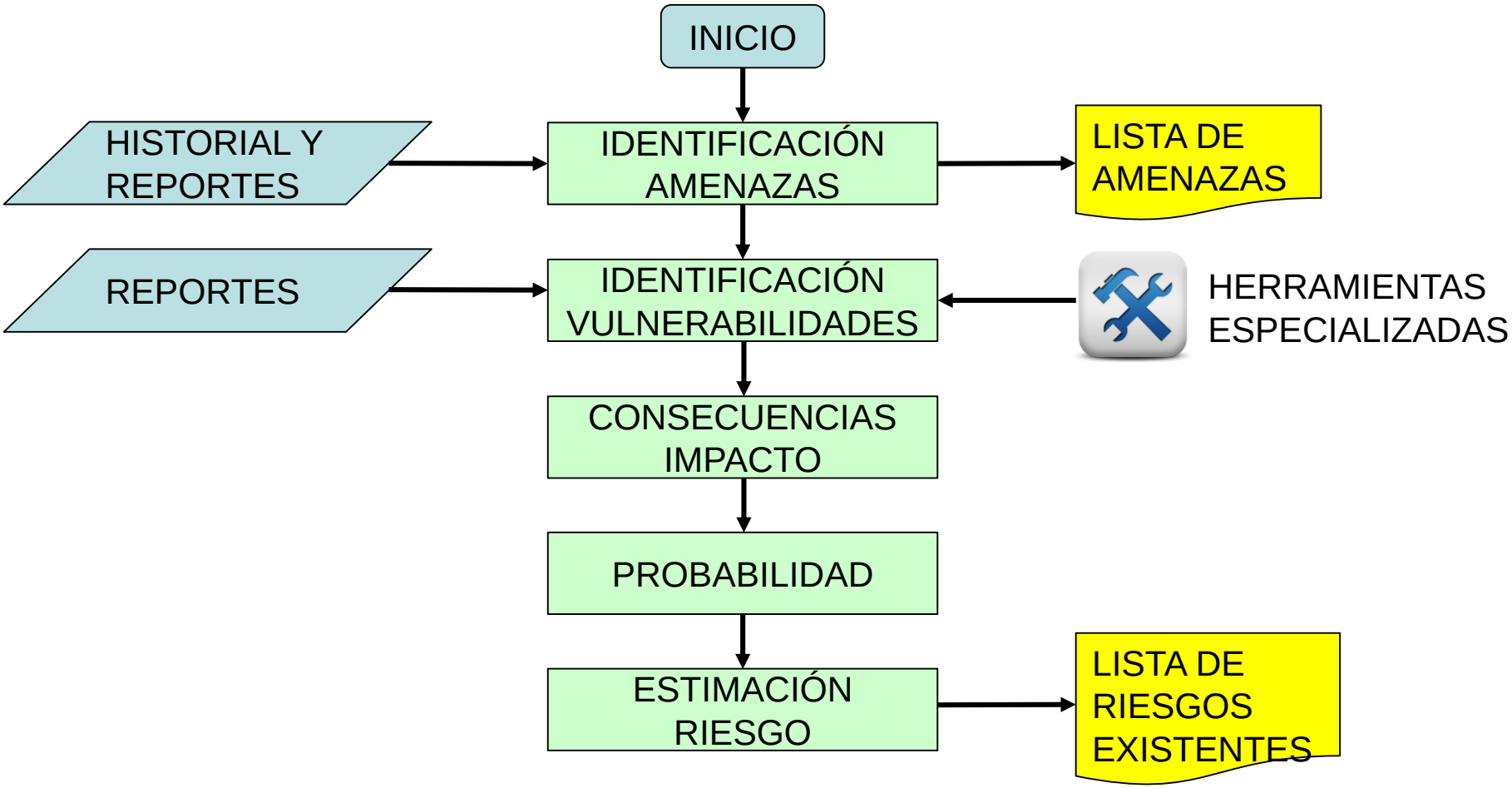
En el contexto de seguridad informática, Riesgo es la posibilidad de que una amenaza explote la vulnerabilidad de uno o varios activos y cause daño a la organización

- Se mide como combinación de la probabilidad de ocurrencia y de sus consecuencias

Evaluación de riesgos

- Identificar amenazas y vulnerabilidades
- Determinar consecuencias e impacto
  - Realizar la matriz de “Impacto – Probabilidad”
  - Se debe considerar el impacto sobre la red eléctrica
    - No se debe limitar al SAS
- Determinar objetivos de seguridad
- Identificar y evaluar protecciones existentes
- Calcular error residual
  - Si no es aceptable incrementar las medidas de seguridad
- Utilizar la normativa relacionada
  - IEC 62443
  - ANSI X9.69

Proceso Análisis de Riesgos



EVALUAR SI SE CUMPLEN LOS OBJETIVOS EN FUNCIÓN DE LAS MEDIDAS DE PROTECCIÓN

Tipos de Riesgos

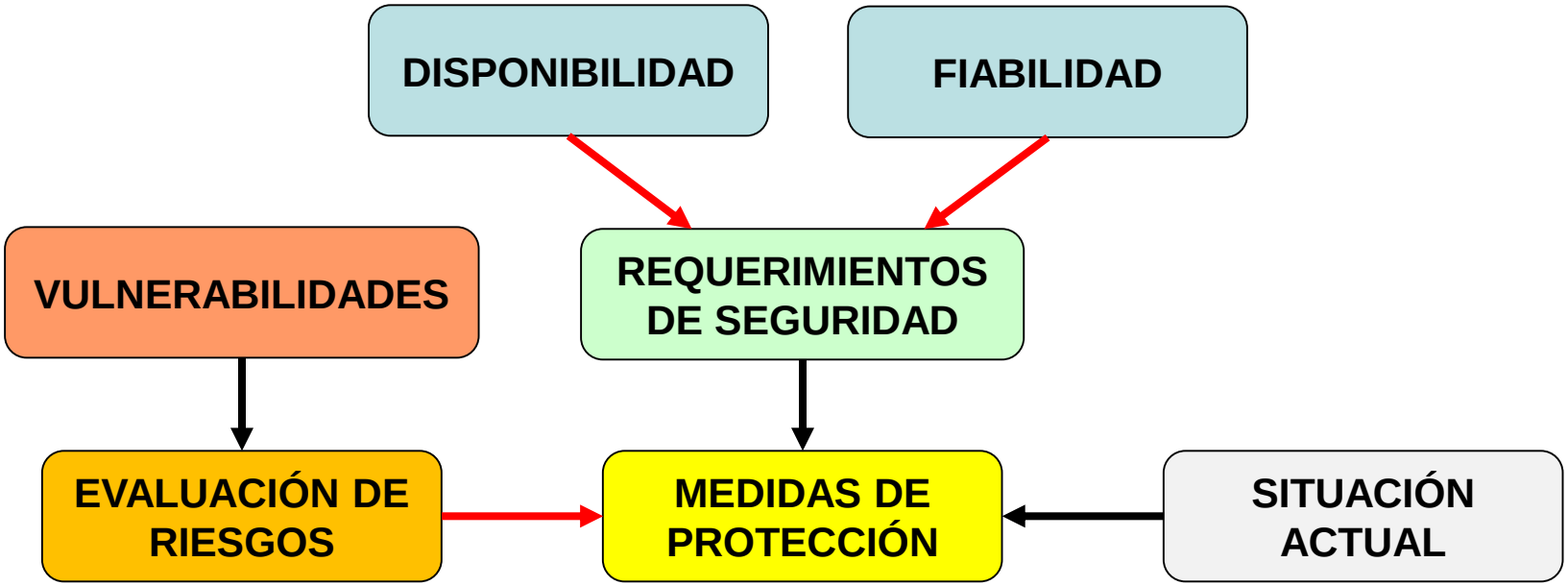
- Pérdidas económicas
  - Equipos destruidos, penalidades y multas.
- Pérdidas de productividad
  - Producción interrumpida, personal ocioso
- Reputación
  - Impacto en medios de comunicación, etc.

Matriz de Riesgos IEC 62443-3-2

		Likelihood				
		1 Remote	2 Unlikely	3 Possible	4 Likely	5 Certain
Impact	1 Trivial	1	2	3	4	5
	2 Minor	2	4	6	8	10
	3 Moderate	3	6	9	12	15
	4 Major	4	8	12	16	20
	5 Critical	5	10	15	20	25

Perfil de Seguridad

- Paso previo a la implementación
- Permite optimizar los recursos
  - *Protección Eficaz y Eficiente*



Objetivos del Perfil

- Concretar los requerimiento de seguridad
- Identificar los medios actuales de protección
- Identificar vulnerabilidades y estimar riesgos
  - Evitar la percepción de falsa protección
  - Enfocar y concretar las acciones de protección
- Proponer acciones y medidas para alcanzar el objetivo de seguridad

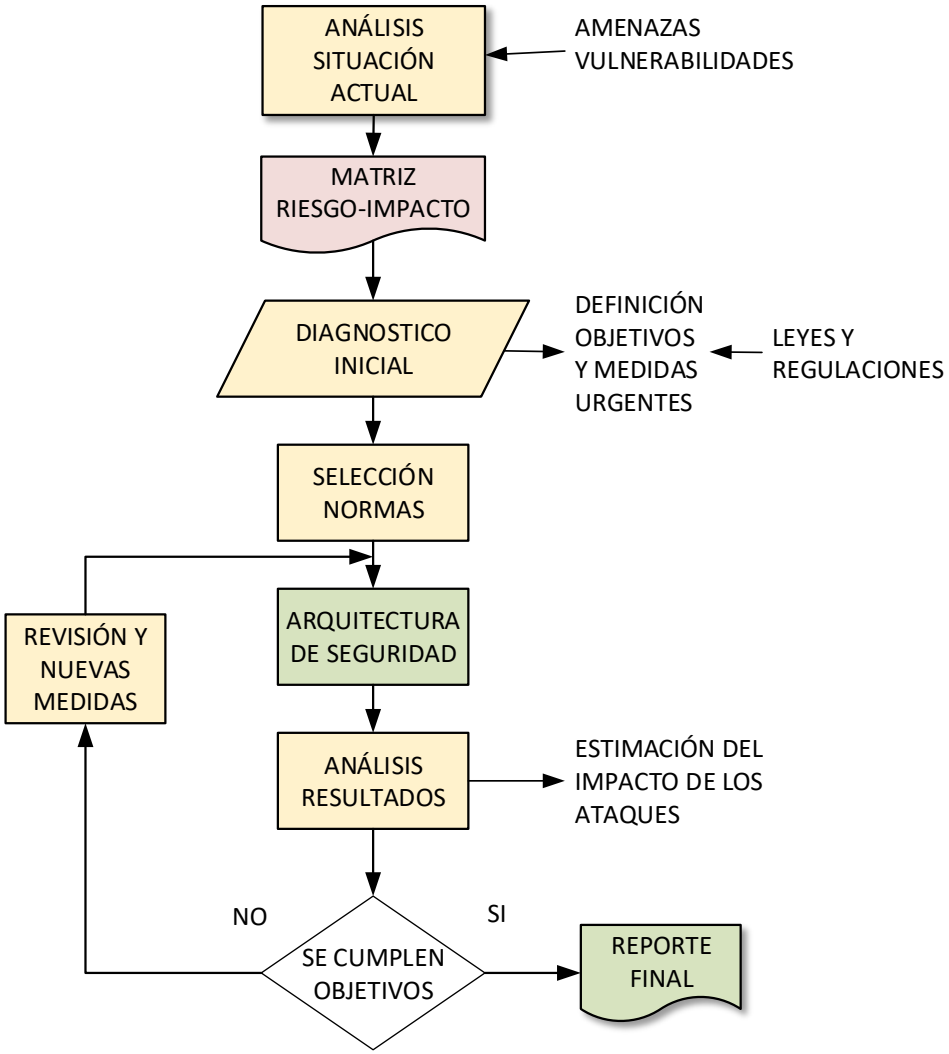
Perfil de seguridad

- Define como utilizar cada una de las herramientas y funciones de seguridad
  - Aplicabilidad de las medidas de seguridad en el entorno del SAS
  - Define criterios de diseño, operación y mantenimiento
- Define como utilizar las normas aplicables
  - IEC 62448, IEC 62351
  - Elimina ambigüedades
  - Asegura el nivel de protección adecuado

Perfil de seguridad

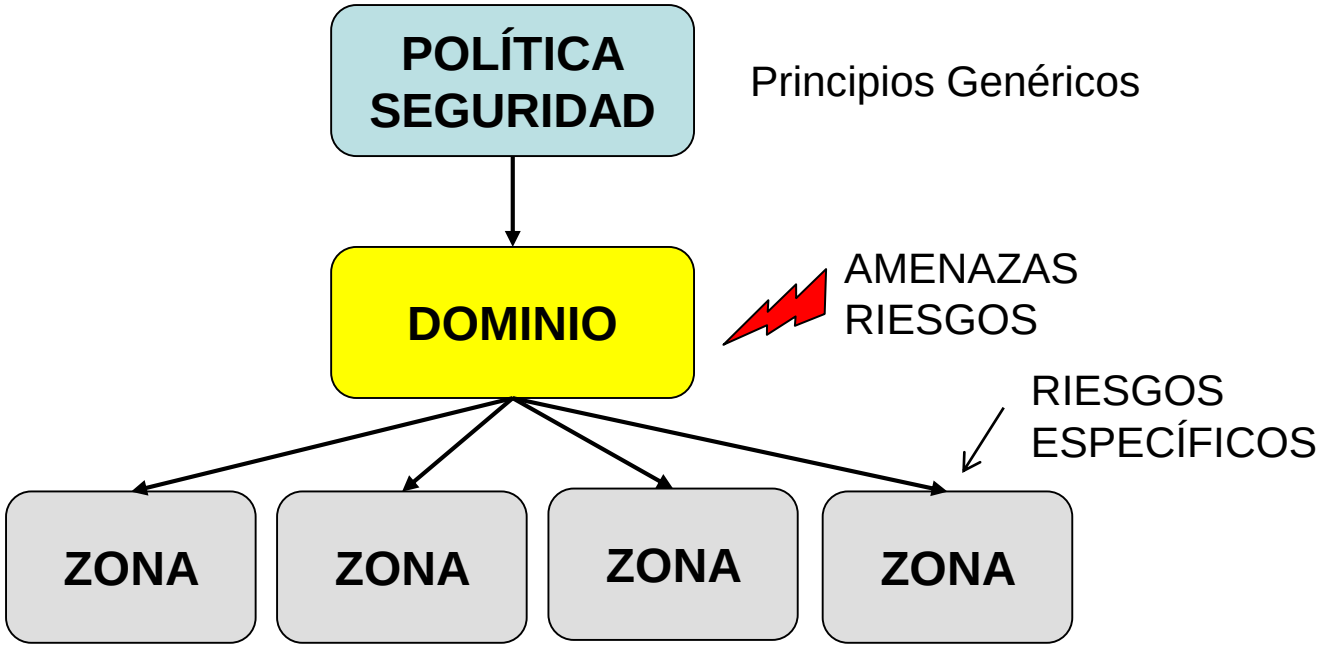
- Define acciones a realizar en el ciclo de vida del SAS
  - Arquitectura de seguridad
  - Requerimientos específicos de compra
  - Guía de configuración del SAS
  - Pruebas específicas de seguridad para FAT/SAT
  - Criterios de mantenimiento y reciclaje
- Especificaciones de equipos y herramientas de seguridad
  - Firewall, aplicaciones, centro gestor, etc.
  - Especificaciones de compra
  - Criterios de configuración

Proceso perfil seguridad



ARQUITECTURA DE SEGURIDAD

Estructura del sistema



- Agrupación de funciones
- Mismo nivel de seguridad
- Zona de confianza
- Objetivo de desempeño común
- Nivel de riesgo aceptable

Definición de Dominios

- Definir el perímetro del Dominio corporativo
- Identificar subdominios y sus perímetros
- Identificar dominios externos con los que hay comunicación
- Definir “inter” y “intra” Dominios
  - Debe haber una autoridad que defina los criterios de seguridad de las conexiones “inter” dominios
- Se deben definir los criterios de seguridad de cada dominio

Zonas de Seguridad

Los Dominios de seguridad se dividen en Zonas

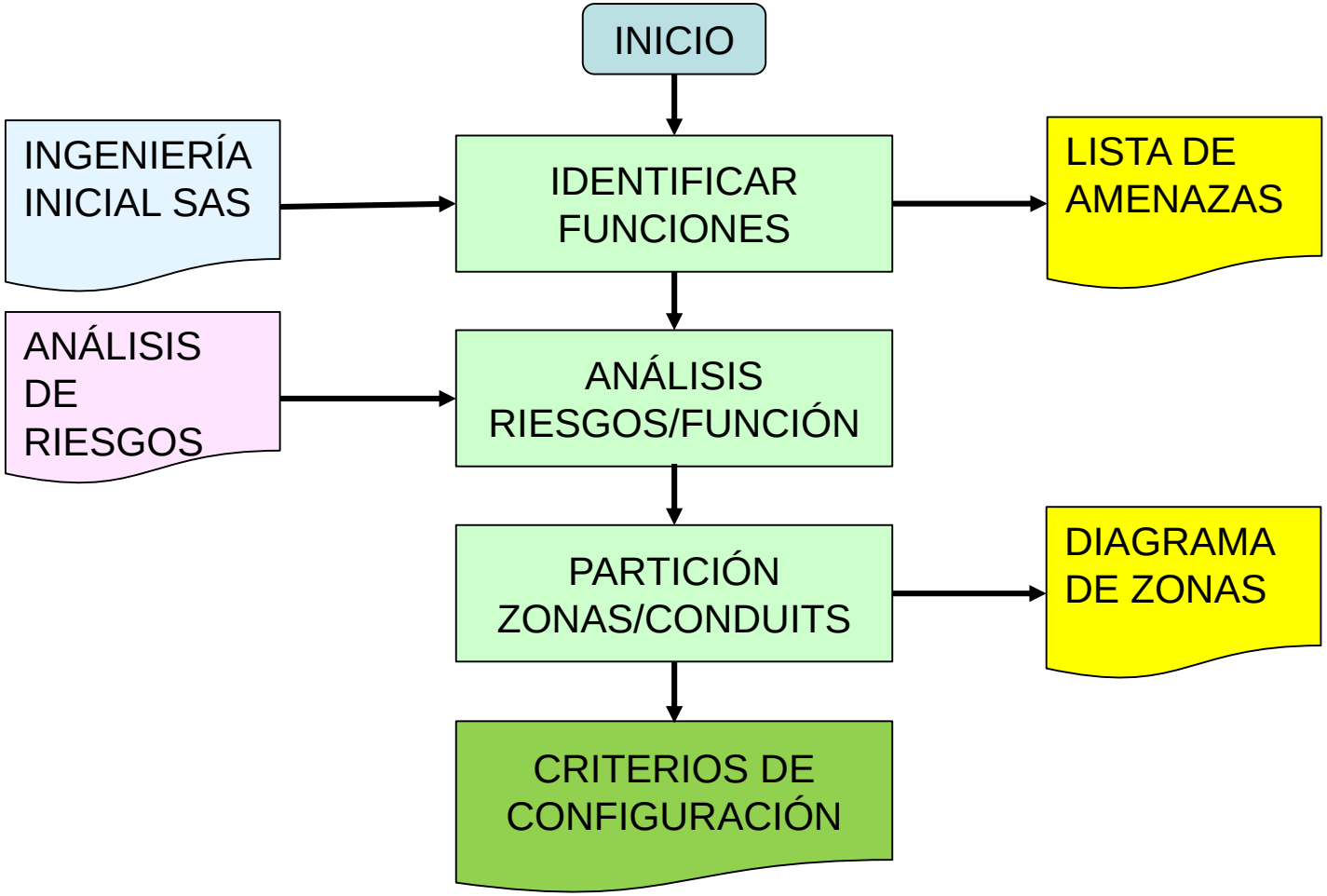
- Las Zonas están formadas por
  - Tecnología
    - Equipos y aplicaciones
  - Reglas de seguridad
    - Configuración
  - Guía de implementación
    - Criterios de diseño
    - Disponibilidad, Desempeño, etc.

Diseño de las Zonas y Conexiones

Un diseño que no analice las Zonas de Seguridad y sus conexiones de forma concienzuda no provee un buen nivel de seguridad independientemente de las medidas de seguridad utilizadas

- Es fundamental entender el funcionamiento del sistema y su aplicación para poder segmentar las zonas
- La protección de las conexiones es tan importante como la de las zonas
  - Son la puerta de entrada de las Zonas
  - Requiere otro tipo de protección
  - Es importante entender los servicios que soporta

Diseño Zonas y Conexiones



VERIFICAR EL CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD

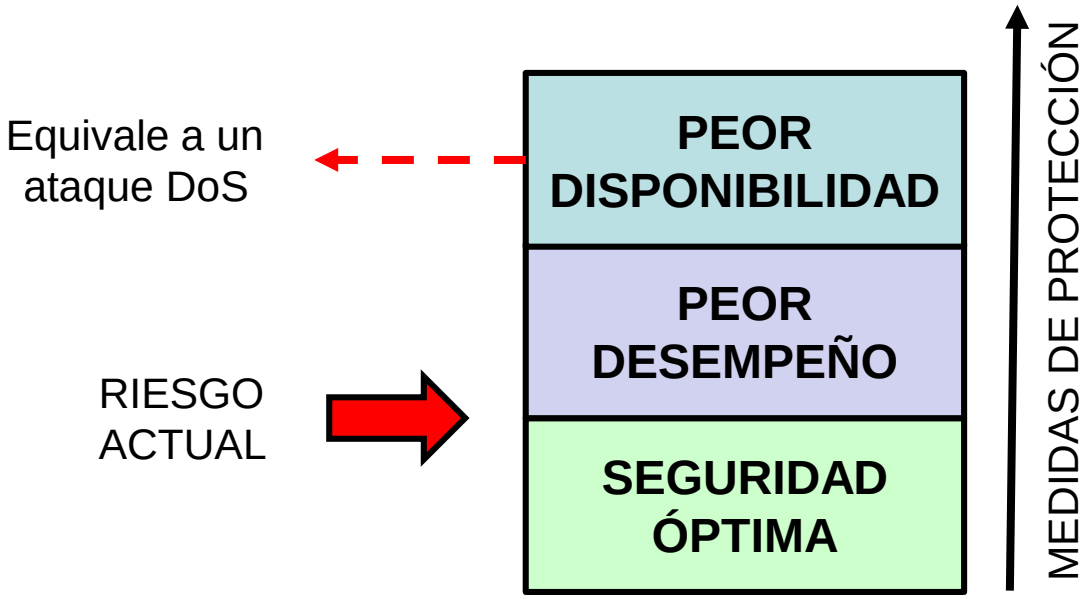
Alternativas de Implementación

- Defense-in-Depth
  - Consiste en aplicar múltiples medidas de seguridad independientes y complementarias
    - Es una aproximación de “Fuerza Bruta”
    - Puede afectar al desempeño del sistema protegido
- Graded Security Approach
  - Consiste en aplicar a cada sistema el nivel y tipo de protección que requiere
  - Se utiliza para proteger sistemas con funciones que requieren un nivel de protección muy diferente
  - Reduce el impacto de la las medidas de seguridad sobre el desempeño

Seguridad Gradual

- Evolución de la defensa en Profundidad
- Objetivos
  - Optimizar costes
  - Disminuir/eliminar el impacto de la seguridad en el desempeño
  - Desplegar medidas de protección proporcionales al riesgo y al valor del elemento protegido

Alcance de la seguridad

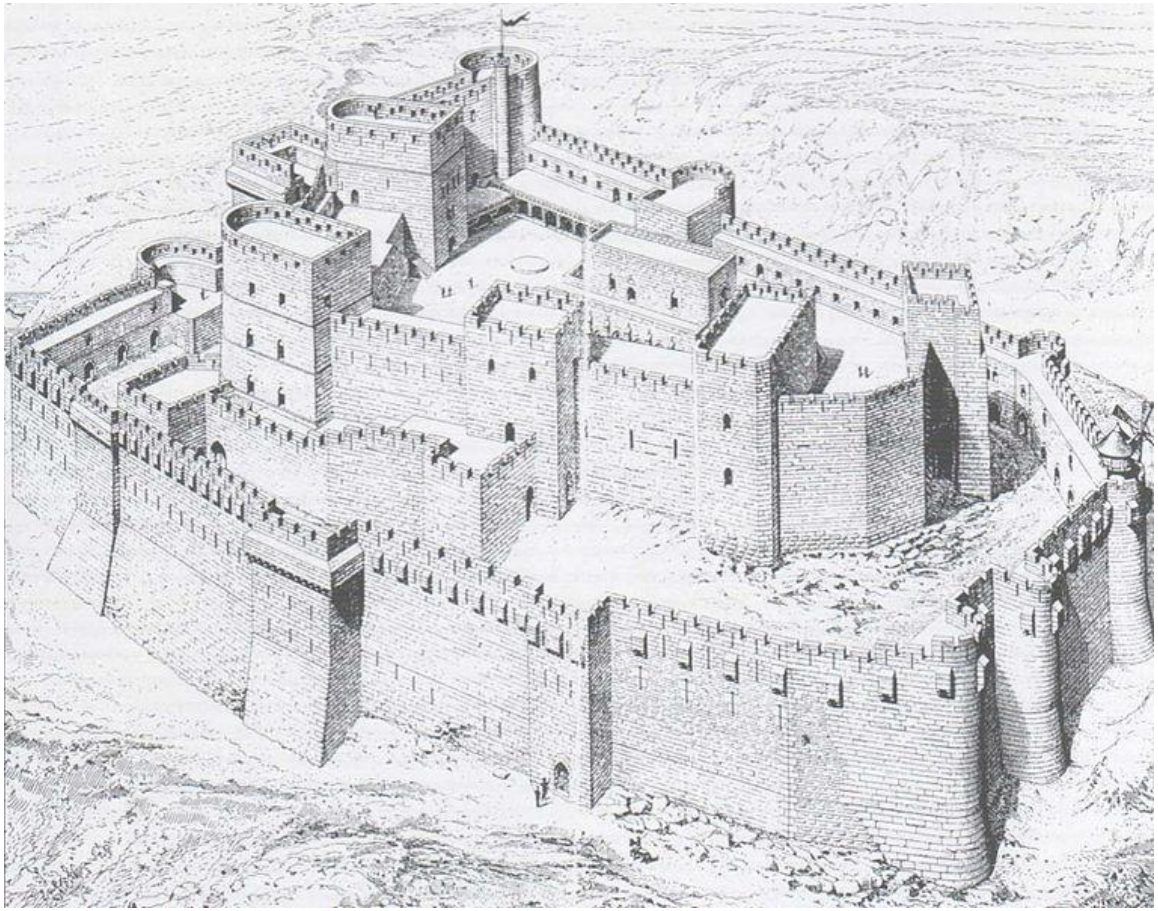


La optimización se consigue con un diseño adecuado de las zonas de seguridad y con las medidas adecuadas para cada zona

Seguridad Gradual

- Es una metodología efectiva de implementación de la seguridad de la infraestructura de operación de las empresas eléctricas
- Surge de las normas internacionales, reportes, mejores practicas y de guías de aplicación.
- Permite alinear los requerimientos de seguridad con principios genéricos de diseño evitando incongruencias y contradicciones
- Se puede utilizar en el diseño de áreas concretas lo cual simplifica su utilización y facilita la integración del sistema
- La metodología de diseño de Seguridad Gradual permite optimizar coste y desempeño

Modelo de Seguridad Gradual



Elementos de protección

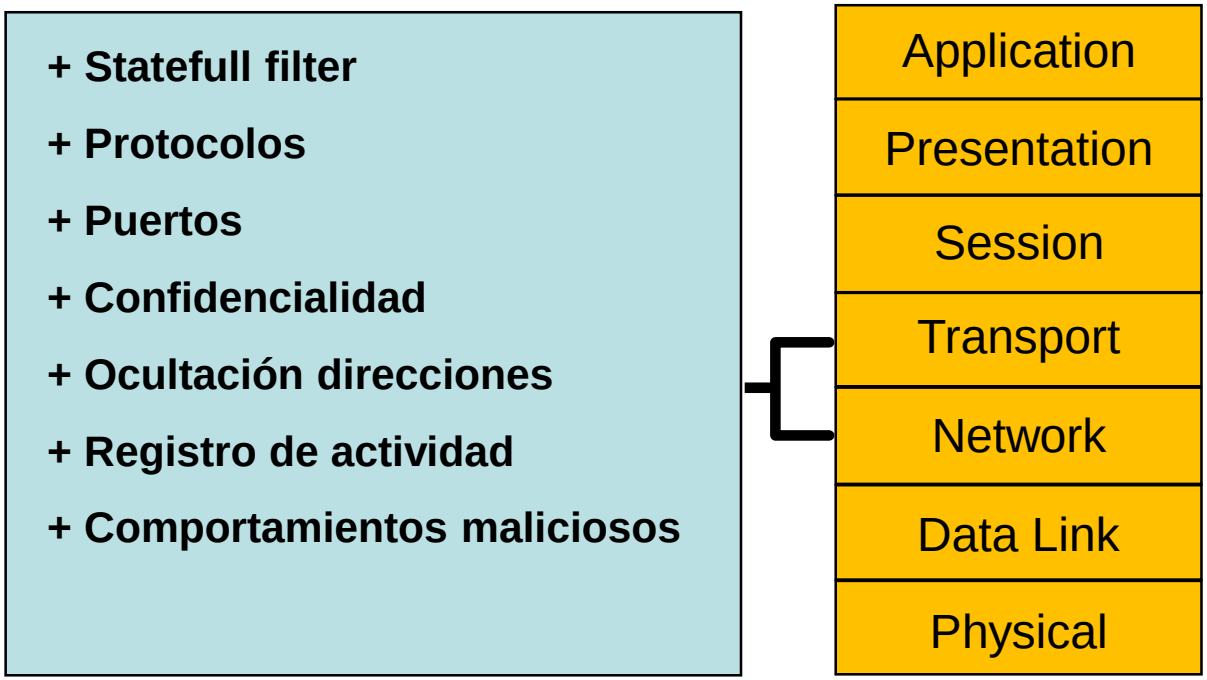
La seguridad de una subestación no puede depender exclusivamente de los elementos de protección, debe ser una propiedad intrínseca del SAS

- Los elementos de protección son imprescindibles para definir las fronteras de las zonas
- Proveen las principales medidas de seguridad
- Principales elementos
  - Firewall
  - Proxy server
  - Mecanismos de comunicación VLAN, VPN, etc.

Características del Firewalls

"Es imprescindible pero No Infalible"

- El nivel de protección depende de su funcionalidad y de la configuración
  - Mayores prestaciones no garantiza mejor protección



Vulnerabilidades del Firewall

- Configuración incompleta o errónea
  - Se debe trabajar en base a “Listas blancas”
    - Por defecto todo está prohibido
- Interfaz de Consola
  - Interfaz físico serial
    - No debe autorizarse su uso
    - No dispone de autentificación ni de control de acceso
  - Interfaz lógico
    - Solo debe usarse con autentificación y control de acceso basado en RBAC

Vulnerabilidades del Firewall

- Interfaz de configuración y mantenimiento
  - No es suficiente los métodos Web seguros
    - No autentifican el servidor. Se puede conectar a un Firewall equivocado
    - Se puede sufrir un ataque de suplantación
  - Es necesario un sistema de autentificación simétrico de mayor nivel
  - Es preferible utilizar aplicaciones propietarias si tienen autentificación simétrica basada en sistemas normalizados
- Interfaz USB
  - Debe estar prohibido
  - No se debe autorizar su uso
    - No es posible controlar la procedencia de la memoria ni verificar su contenido
    - No dispone de autentificación y control de acceso

Características Firewalls

- Compatibilidad electromagnética y ambientales
  - Según IEC 61850-3
- Cumplir con IEC 62351
  - Normativa de seguridad informática para sistemas de operación
- Implementar gestión segura
  - Control de acceso al firewall por Roles según IEC 62351-8 (RBAC)

Ejemplo de Firewall

Familia AGENT-7 FW

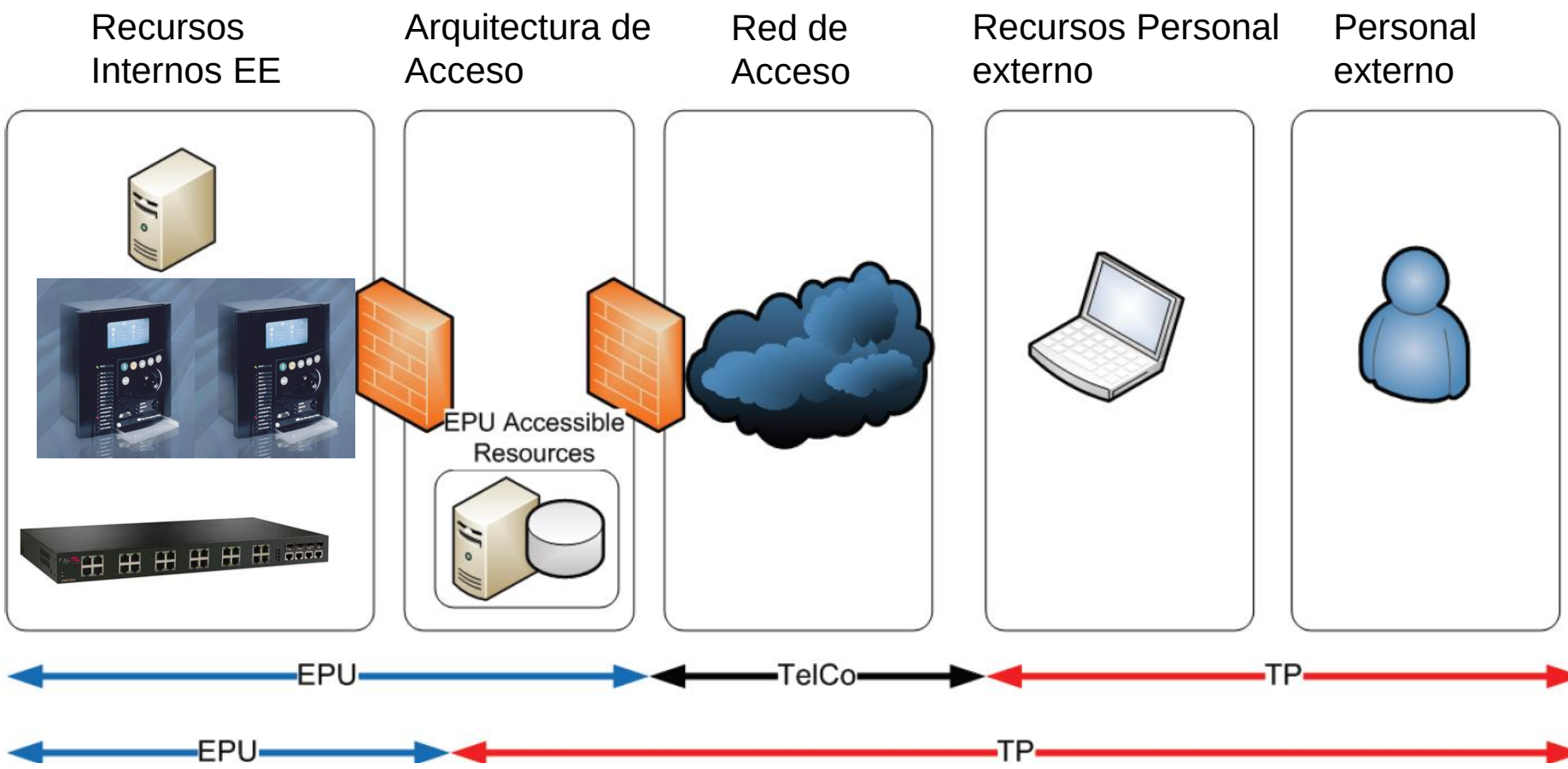
- IEC 61850 e IEC 62351
- Gestión segura con RBAC
- Filtrado e IDS hasta capa 7
- VPNs con autentificación y cifrado
- NAT en IP y MAC
- Protecciones específicas para SAS
- Funciones de router MPLS

ASPECTOS CLAVE

Acceso Remoto

- Es una de las principales fuentes de amenazas
- Su diseño debe asegurar la usabilidad a la vez que garantiza un nivel de protección de acuerdo a nuestros niveles de riesgo aceptables
- Además de implementar las políticas de seguridad se debe considerar la disponibilidad del servicio
  - Evitar punto simples de fallo, fallos en modo común, etc.

Arquitectura de Acceso Remoto



Objetivos de la Arquitectura

- Control de acceso estricto a todos los niveles
- Prevenir la explotación de vulnerabilidades o puertas traseras en el mantenimiento de IEDs
- Mantener confidencialidad e integridad de los datos
- Requerir el Loggin para cualquier acción realizada por un usuario externo
- Asegurar que el mantenimiento remoto no afectará al resto del sistema
  - Especialmente la disponibilidad de funciones críticas
- Prevenir la difusión de datos confidenciales

Segmentación de red

- La segmentación es una práctica fundamental para la implementación de la seguridad
- La segmentación facilita un buen diseño de seguridad permitiendo establecer una jerarquía de controles
  - Zonas de seguridad
  - Firewalls
  - Sistema IDS/IPS
  - Segmentación de redes IP
  - Segmentación de redes con VLANs

Objetivo Auditoría

- Identificar amenazas aplicables al SAS
  - Vectores de ataque
- Analizar factores de vulnerabilidad
  - Arquitectura SAS
  - Configuración
    - Uso Passwords, configuración LAN, etc.
  - Criterios y funciones de operación
  - Operaciones de mantenimiento
- Determinar riesgos
  - Matriz Riesgo – Impacto
- Trabajo de campo (opcional)
  - Visita subestaciones tipo y análisis in-situ

Objetivo Auditoría

- Diagnóstico
  - Principales riesgos y su impacto en el SAS
  - Nivel de seguridad actual
    - Grado de cumplimiento con los objetivos
    - Cumplimiento legislación vigente
- Proponer mejoras
  - Nuevos procedimientos
  - Normativa internacional aplicable
  - Modificación en la arquitectura del SAS
    - Equipamiento necesario
  - Modificaciones en configuraciones
  - Facilidades de mantenimiento
  - Criterios de auditorías periódicas

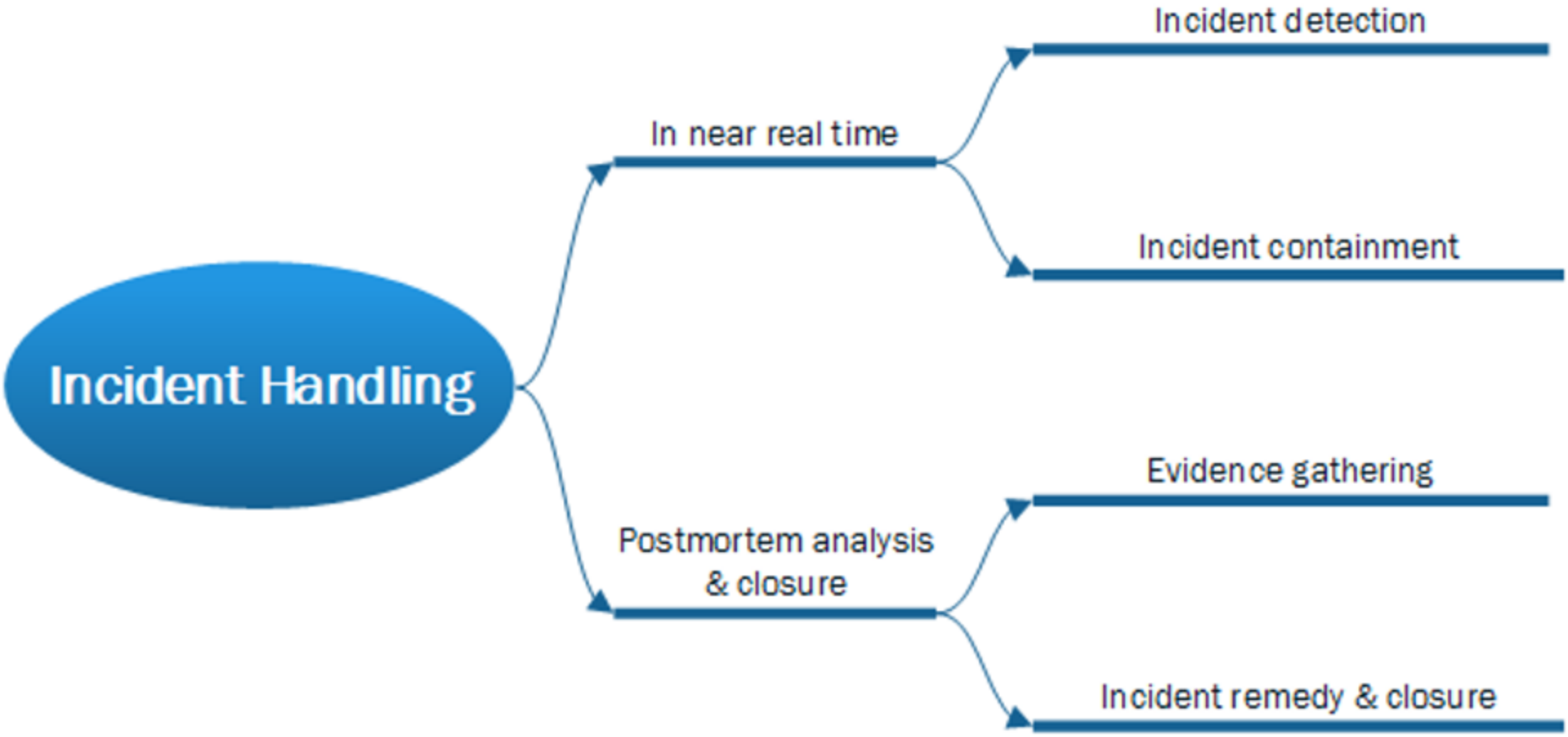
Tipos de Auditorías

- Inicial
  - Se aplica sobre los sistemas existentes
  - Determinar las amenazas
  - Identifica las vulnerabilidades y estima el nivel de riesgo
  - Analizar medidas de protección aplicadas
  - Analizar procedimientos existentes
  - Proponer nuevas medidas y procedimientos
- Rutinaria
  - Analizar registros para:
    - Identificar errores de configuración, incumplimientos, ataques, etc.
    - Revisar configuraciones y/o procedimientos si procede

Las auditorías juegan un papel fundamental durante el ciclo de vida de un ataque

RESPUESTA A LOS ATAQUES

Manejo de Incidentes



Planes de Recuperación

Un plan de Recuperación es un documento que especifica las estrategias y los medios necesarios para recuperar el funcionamiento del sistema

- Un plan de recuperación debe incluir
  - Requerimientos de funcionamiento del sistema incluyendo SLAs
  - Contacto del responsable del Plan
  - Equipo de trabajo que ejecutará el plan
  - Procedimientos del plan
  - Comunicaciones de emergencia. No deben utilizar los recursos del sistema a recuperar
  - Plan de comunicación. A quién hay que comunicar las incidencias
  - Medios de recuperación. Medios y herramientas específicas dedicadas a la ejecución del plan
- Se debe definir en qué circunstancias debe aplicarse el Plan


PULLNET
Telecom for energy