AUDITORIA INFORMATICA

Qué es

- Una auditoría de seguridad informática es un procedimiento que evalúa el nivel de seguridad de una empresa o entidad, analizando sus procesos y comprobando si sus políticas de seguridad se cumplen.
- El principal objetivo de una auditoría de seguridad es el de detectar las vulnerabilidades y debilidades de seguridad que pueden ser utilizadas por terceros malintencionados para robar información, impedir el funcionamiento de sistemas, o en general, causar daños a la empresa.

Beneficios

- Mejora los controles internos de seguridad de la empresa.
- Detecta debilidades en los sistemas de seguridad como errores, omisiones o fallos.
- Identifica posibles actuaciones fraudulentas (acceso a datos no autorizados o robos a nivel interno).
- Ayuda a eliminar los puntos débiles de la empresa en cuestión de seguridad (webs, correo electrónico o accesos remotos, por ejemplo).
- Permite controlar los accesos, tanto físicos como virtuales (revisión de privilegios de acceso).
- Permite mantener sistemas y herramientas actualizadas.

tipos de auditorías de seguridad

- **Auditorías internas y externas**
- Dependiendo de quién realice la auditoría se denominan internas, cuando son realizadas por personal de la propia empresa (aunque pueden tener apoyo o asesoramiento externo) o externas, cuando se realizan por empresas externas que son independientes de la empresa.

- **Auditorías técnicas**
- Son aquellas auditorías cuyo objetivo se centra en una parte concreta o acotada de un sistema informático. Entre estas auditorías podemos encontrar las de cumplimiento de normativas que tienen como objetivo verificar si algún estándar de seguridad se cumple (como la validación de sistemas informatizados en la industria regulada), o si las políticas y protocolos de seguridad se están realizando de forma apropiada.

- **Auditorías por objetivo**
- Se trata de auditorías de seguridad técnicas que se diferencia según el objetivo que persigan. Las más comunes son:
- Sitios web. Son auditorías que tienen como objetivo evaluar la seguridad de las páginas web y eCommerce para descubrir posibles vulnerabilidades que pueden ser utilizadas por terceros.
- Forense. Son auditorías que se realizan tras haberse producido un ataque o incidente de seguridad y que persiguen descubrir las causas por las que se ha producido, el alcance del mismo, por qué no se ha evitado, etc.

- **Auditorías por objetivo**
- Redes. El objetivo es evaluar el funcionamiento y la seguridad de las redes empresariales, como VPN, wifi, firewalls, antivirus, etc.
- Control de acceso. Son auditorías centradas en los controles de acceso y que están vinculadas a dispositivos tecnológicos físicos como cámaras de seguridad, mecanismos de apertura de barreras y puertas y software específico para el control de accesos.
- Hacking ético. Son auditorías que se realizan para medir el nivel de seguridad de una empresa realizando una simulación de ataque externo (como si se tratase de un ataque real) para evaluar los sistemas y medidas de protección, identificando sus vulnerabilidades y debilidades.

Servicios de la auditoria informática

- Análisis de riesgos y fallos de seguridad
- Control de programas y sistemas instalados
- Seguridad de información, datos y programas
- Elementos y amenazas de la seguridad en la entrada y salida de datos e información
- Identificación y localización de amenazas y seguridad en Internet
- Protocolo de seguridad, riesgos, seguros, programas instalados

Servicios de la auditoria informática

- Análisis y evolución de impacto de posibles amenazas
- Plan de seguridad
- Políticas de seguridad
- Protocolo de seguridad y actuación ante ciberataques, fraudes y perdidas
- Plan de contingencia y recuperación de información
- Mejora e implantación de medidas de seguridad preventivas, directivas y correctivas

Fases (I)

- **Objetivos y planificación**
- En primer lugar, hay que fijar cuáles son los objetivos que se persiguen con una auditoría de seguridad. No es lo mismo diseñar una auditoría con el objetivo de validar una normativa de seguridad, que una auditoría técnica para comprobar si la política de seguridad se está cumpliendo.

Fases (I)

- **Objetivos y planificación**

- Una vez se han fijado los objetivos hay que realizar una planificación de los pasos a seguir, de las herramientas a utilizar, elaboración de un calendario de actuaciones, y de las áreas a analizar para poder alcanzar esos objetivos

Fases (II)

- **Recopilación de información**
- En esta fase se recopiló toda la información posible para poder evaluar el funcionamiento de los sistemas informáticos, tecnologías, políticas y protocolos objetivos de la auditoría.

Fases (II)

- Los principales **canales** que se utilizarán para objetar esta información son:
- Entrevistas con el personal de la empresa.
- Revisión de documentación (políticas y protocolos).
- Análisis de especificaciones de hardware y software.
- Realizar test y utilizar herramientas para medir la seguridad de los sistemas.

Fases (III)

- **Análisis de los datos**
- Con toda la información y documentación recabada, así como el resultado de los distintos test y pruebas realizadas se realizará un análisis con el objetivo de encontrar fallos, vulnerabilidades y debilidades en los sistemas.

Fases (IV)

- **Realizar un informe de la auditoría**
- La auditoría se cierra realizando un informe detallado de los resultados obtenidos durante la fase de análisis. Estos resultados deben presentar los problemas de seguridad encontrados, proponiendo soluciones y recomendaciones sobre cómo solventarlos.
- El informe de una auditoría de seguridad debe presentar de forma clara y concisa el propósito y objetivo de la misma, los resultados obtenidos y las medidas correctoras necesarias en ciberseguridad a aplicar.

Regulación internacional sobre Auditoría de Sistemas de Información

- **ISACA (COBIT)**
- **COSO**
- **AICPA (SAS)**
- **IFAC (NIA)**
- **SAC**
- **MARGERIT**
- **EDP**

ISACA-COBIT

- The **Information Systems Audit and Control Foundation, ISACA** (http://www.isaca.org). Es la asociación lider en Auditoría de Sistemas, con 23.000 miembros en 100 países.
- ISACA propone la metodología **COBIT** ® (Control Objectives for Information and related Technology). Es un documento realizado en el año de 1996 y revisado posteriormente, dirigido a auditores, administradores y usuarios de sistemas de información, que tiene como objetivos de control la efectividad y la eficiencia de las operaciones; confidencialidad e integridad de la información financiera y el cumplimiento de las leyes y regulaciones.

Esquema Nacional de Seguridad o ENS

- El **Esquema Nacional de Seguridad o ENS** es una normativa que tiene como objetivo establecer los principios que regulan y aseguran el acceso, integridad, disponibilidad y veracidad de la información empleada en medios electrónicos en o relacionados con las Administraciones Públicas (estatales, autonómicas y locales).

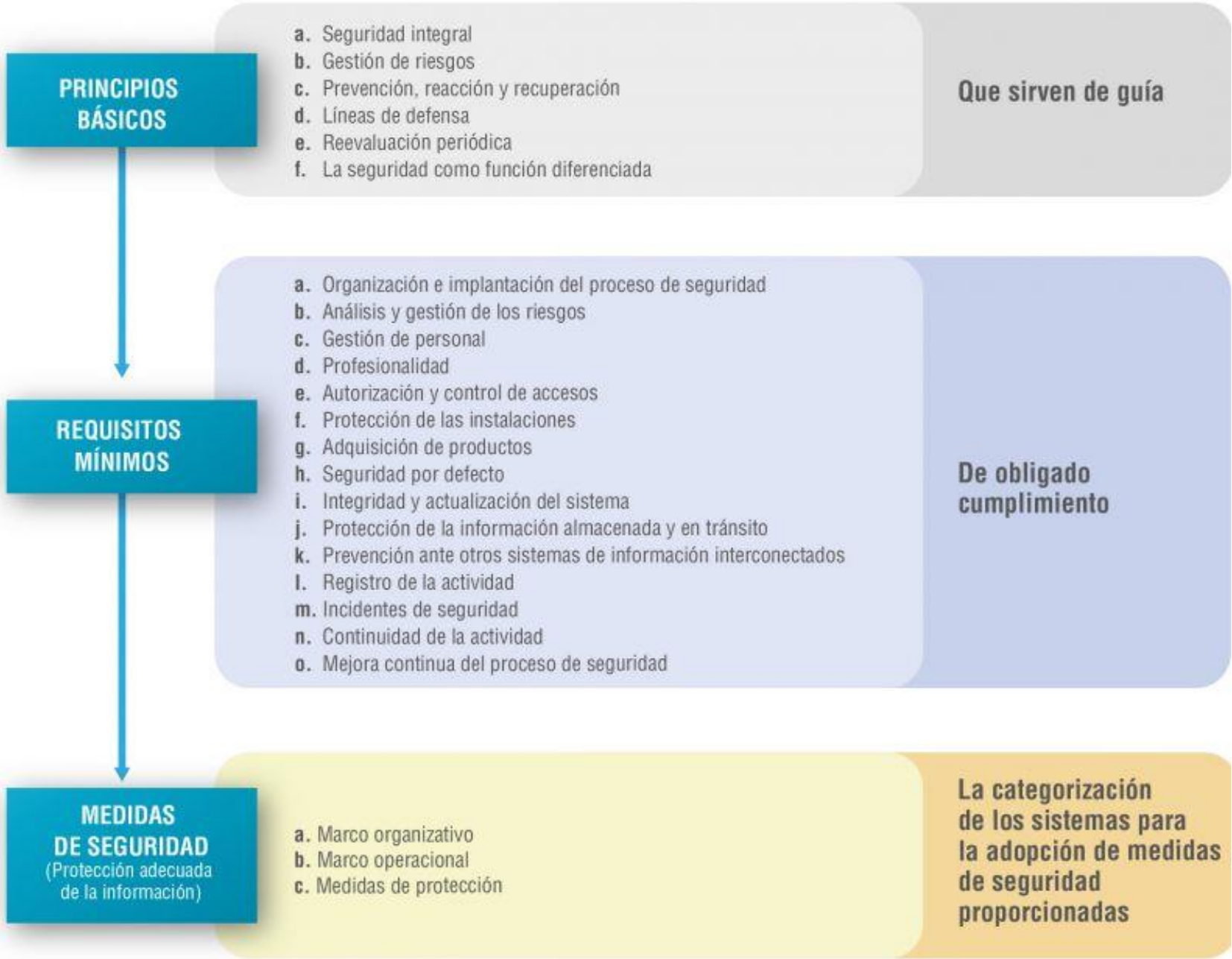
- Recogido en el Real Decreto 3/2010, el ENS se crea con la necesidad de establecer aspectos y metodologías comunes relativas a la segurita en la implantación y utilización de los medios electrónicos por las Administraciones Públicas, con el fin de crear las condiciones de confianza necesarias para que los ciudadanos usen estos medios en el cumplimiento y ejercicio de sus deberes y derechos.

- El ENS surgió como el resultado del trabajo coordinado por Ministerio de la Presidencia y posteriormente por el Ministerio de Política Territorial y Administración Pública, contando con el apoyo del **Centro Criptológico Nacional (CNN)** y la participación de todas las Administraciones Públicas, incluidas universidades públicas y los órganos colegiados con competencias en materia de administración electrónica.

ENS

SEGURIDAD DE LA INFORMACIÓN **EL MARCO ISO27001 COMO PARADIGMA ENS**

Concepto	ISO/IEC 27001:2013	ENS
Tipo de norma	Norma de adscripción **voluntaria**	Norma jurídica de **obligado cumplimiento** (RD 3/2010) para AAPP
Alcance	**Elegible por la organización**: Geográfico, departamental, procesos de negocio, servicios… (+ exclusiones).	**Predefinido**: Todos los servicios prestados a la ciudadanía que se apoyen en medios electrónicos.
Categorización	**NO** **3** dimensiones de la seguridad	**SI**, de los sistemas : BASICA, MEDIA y ALTA. **5** dimensiones de la seguridad
"Risk Approach"	**SI** Cláusulas 6.1 (Acciones para tratar los riesgos y oportunidades)	**SI** Medida de seguridad op.pl.1 (Análisis de riesgos)
Sistema de Gestión	**SI** explícito en la cláusula 4.4	**SI** según op.pl.2 (Arquitectura de seguridad) para categorías MEDIA y ALTA.
Controles	**114** controles de seguridad Anexo A	**75** medidas de seguridad Anexo II


PRINCIPIOS BÁSICOS
a. Seguridad integral
b. Gestión de riesgos
c. Prevención, reacción y recuperación
d. Líneas de defensa
e. Reevaluación periódica
f. La seguridad como función diferenciada
Que sirven de guía
REQUISITOS MÍNIMOS
a. Organización e implantación del proceso de seguridad
b. Análisis y gestión de los riesgos
c. Gestión de personal
d. Profesionalidad
e. Autorización y control de accesos
f. Protección de las instalaciones
g. Adquisición de productos
h. Seguridad por defecto
i. Integridad y actualización del sistema
j. Protección de la información almacenada y en tránsito
k. Prevención ante otros sistemas de información interconectados
l. Registro de la actividad
m. Incidentes de seguridad
n. Continuidad de la actividad
o. Mejora continua del proceso de seguridad
De obligado cumplimiento
MEDIDAS DE SEGURIDAD
(Protección adecuada de la información)
a. Marco organizativo
b. Marco operacional
c. Medidas de protección
La categorización de los sistemas para la adopción de medidas de seguridad proporcionadas

ENS 2010

- **Principios básicos:** prevención, reacción y recuperación.
- No existía el principio básico de **Vigilancia continua**.
- Menor visibilidad al **componente certificado** de hardware y software.
- **Requisitos**: seguridad por defecto.
- No existía el servicio en la nube en las medidas del marco operacional.
- **4** marcos organizativos.
- **31** marcos operacionales.
- **40** medidas de protección.
- **Refuerzos** en los mecanismos de autenticación.

ENS 2022

- **Principios básicos:** prevención, detección, respuesta y conservación.
- Se introduce el principio básico de **Vigilancia continua** (auditoría obligatoria anualmente).
- Máxima importancia **componente certificado** de hardware y software.
- **Requisitos**: mínimo privilegio (modificación de terminología).
- Nueva familia de medidas del marco operacional: **servicio en la nube.**
- **4** marcos organizativos (se mantiene el número).
- **33** marcos operacionales (aumentan 2 marcos).
- **36** medidas de protección (se reducen 4 marcos).
- Mayores **refuerzos** en los mecanismos de autenticación.

Hacking Etico Marco legal Hacking Etico

- **Delitos informáticos según código penal español:**
- **Art. 197 bis**

El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

- **Art 197 ter**

El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

TIPOS DE PENTESTING

CAJA NEGRA

- **No se entrega ningún tipo de información**
- **Hay que descubrir (fingerprint) equipos e infraestructura, sistemas, servicios y puertos, tecnologías sitios web, etc.**

CAJA BLANCA

- **Se entrega información interna de la empresa**
- **Existe mapa de red, firewalls, sistemas operativos, autenticación, usuarios, tecnología de sitios web, etc.**
- **No se invierte tiempo en la fase de descubrimiento (figerprint)**

CAJA GRIS

- **Mezcla características de las 2 anteriores.**
- **Se da a conocer alguna información.**
- **Útil para ataques que puede llegar a hacer un usuario interno con x privilegios a nivel interno.**

¿Con que herramientas lo hacen?

curl://

OpenVAS
Open Vulnerability Assessment System

Nessus®
vulnerability scanner

OWASP
ZAP

metasploit®

ALIEN VAULT

Nikto

EeEF

BURPSUITE PROFESSIONAL

SPARTA
Network Infrastructure Penetration Testing Tool

sqlmap®

John the Ripper

netcat

FASE 1:

DEFINIR EL ALCANCE DEL ANÁLISIS DE RIESGOS, es decir, dónde vamos a analizar los riesgos. Pueden ser todos los servicios, departamentos y actividades o centrarse en algunos en concreto.

FASE 2:

IDENTIFICAR Y VALORAR LOS ACTIVOS DE INFORMACIÓN del departamento, proceso o sistema objeto del estudio.

FASE 3:

IDENTIFICAR LAS AMENAZAS a las que están expuestos estos activos.

FASE 4:

ESTUDIO Y ANÁLISIS DE LAS CARACTERÍSTICAS DE NUESTROS ACTIVOS para identificar los puntos débiles o vulnerabilidades y las salvaguardas existentes.

FASE 5:

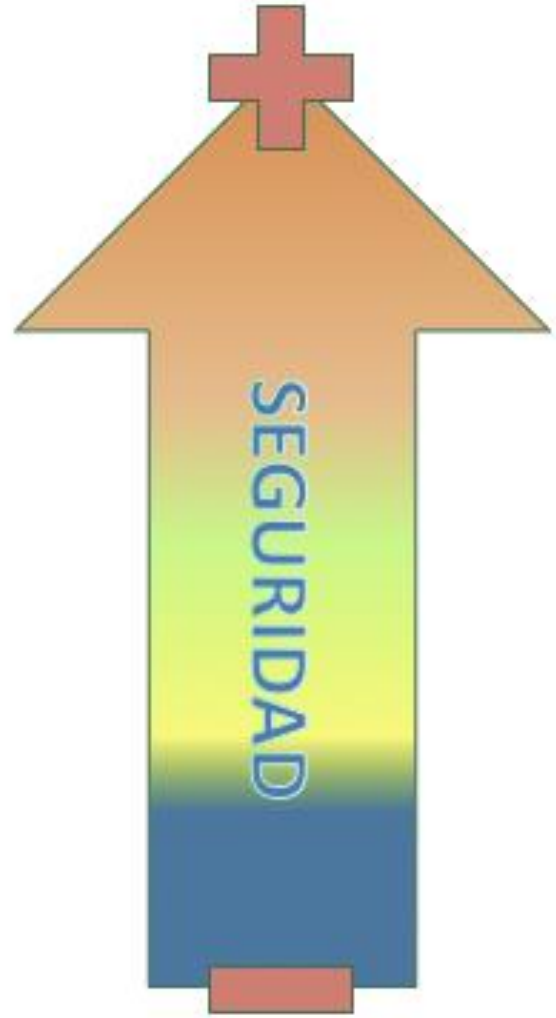
PARA CADA PAR ACTIVO-AMENAZA, estimaremos la **PROBABILIDAD** de que la amenaza se materialice y el **IMPACTO** sobre el negocio que esto produciría.

FASE 6:

Una vez calculado el riesgo, debemos **TRATAR AQUELLOS RIESGOS QUE SUPEREN UN LÍMITE** que nosotros mismos hayamos establecido.

MEDIDAS GLOBALES PARA LA EMPRESA:

- FORMACION/COMUNICACION
- PLANES DE CONTINGENCIA/CONTINUIDAD
- POLITICAS DE SEGURIDAD
- HARDENING
- ACTUALIZACIONES SEGURIDAD
- AUDITORIAS DE SEGURIDAD
- COPIAS DE SEGURIDAD- BACKUP
- MEDIDAS DE SEGURIDAD FISICAS



Política de seguridad

- Debe definir los conjuntos de requisitos para la operación general de los sistemas., mediante normas, reglamentos y protocolos a seguir y debe ser conocida por todos los empleados o colaboradores.

❑ Se deben contemplar la Integridad, Disponibilidad y privacidad de la información y aplicadas a todos los sistemas y personas de una organización.

❑ Se debe definir que se desea proteger y el porque.

❑ Debe ser atemporal, sin afectar eficacia y eficiencia

❑ Adecuarse a necesidades y recursos reales de una empresa.

❑ Se definen estrategias y criterios generales a adoptar según funciones y actividades.

- Ejemplo de documentos incluidos en Política de Seguridad:
- GESTION DE CONTRASEÑAS
- GESTION DE USUARIOS
- GESTION DE EQUIPOS EN RED

❖ APLICAR ISO 27001 a la empresa como guía para garantizar la Seguridad.