Ingeniería de Software II

Auditoría Informática

Auditoría Informática - Concepto

»Permite definir estrategias para prevenir delitos, problemas legales, etc..

»Es una actividad preventiva, el auditor sugiere.

»Los procedimientos de auditoría en informática varían de acuerdo con la filosofía y técnica de cada organización y departamento de auditoría en particular.

»La auditoría en informática debe evaluar todo: informática, organización del centro de cómputo, computadoras, comunicación y programas.

Fuente: Echenique García 2da. Ed. Cap. 1

Auditoría Informática - Objetivos

- Salvaguardar los activos.
- Integridad de datos.
- Efectividad de sistemas.
- Eficiencia de los sistemas.
- Seguridad y confidencialidad.

Fuente: Echenique García 2da. Ed. Cap. 1

Auditoría Informática - Concepto

»Auditoría

Es un examen crítico que se realiza con el objeto de evaluar la eficiencia y la eficacia de una sección o de un organismo y determinar cursos alternativos de acción para mejorar la organización y lograr los objetivos propuestos.

No es una actividad meramente mecánica

Puede ser interna, externa o una combinación de ambas.

Fuente: Echenique García 2da. Ed. Cap. 1

Auditoría Informática - Definiciones

"Es una función que ha sido desarrollada para asegurar la salvaguarda de los activos de los sistemas de computadoras, mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficiente". **Ron Weber.**

"Es la verificación de los controles en las siguientes tres áreas de la organización (informática): Aplicaciones, Desarrollo de sistemas, Instalación del centro de cómputos". **William Mair.**

Fuente: Echenique García 2da. Ed. Cap. 1

Auditoría Informática - Concepto

»Por lo tanto, es la revisión y evaluación de:

- los controles, sistemas y procedimientos de la informática;
- los equipos de cómputo;
- la organización que participa en el procesamiento de la información.

Fuente: Echenique García 2da. Ed. Cap. 1

Influencia de la auditoría en informática

Factores que pueden influir en la organización a través del control y la auditoría en informática:

- Controlar el uso de la computadora.
- Pérdida de capacidades de procesamiento de datos.
- Necesidad de mantener la privacidad individual.
- Posibilidad de pérdida de información o mal uso de la misma.
- Toma de decisiones incorrectas.
- Necesidad de mantener la privacidad de la organización.
- ...

Fuente: Echenique García 2da. Ed. Cap. 1

Auditoría Informática – Campo de acción

1. Evaluación administrativa del área de informática.
2. Evaluación de los sistemas y procedimientos, y de la eficiencia que se tiene en el uso de la información.
3. Evaluación del proceso de datos, de los sistemas y de los equipos de cómputo (software, hardware, redes, bases de datos, comunicaciones).
4. Seguridad y confidencialidad.
5. Aspectos legales de los sistemas y de la información.

Fuente: Echenique García 2da. Ed. Cap. 1

¿Qué hace un auditor informático?

- Es responsable de evaluar los sistemas informáticos y los procesos relacionados con la tecnología de una empresa, lo que incluye la infraestructura tecnológica.
- El objetivo de dicha evaluación es asegurarse de que los sistemas y procesos son los que la empresa verdaderamente necesita, al mismo tiempo que ofrece soluciones viables para cualquier problema que se haya detectado durante la evaluación.

Fuente: Piattini, M., & del Peso CAP 5

Funciones de un Auditor Informático

- Identificar el potencial de optimización de procesos informáticos a partir de un análisis de debilidades y errores.
- Seguir los estándares de auditoría establecidos por cada empresa y la normativa vigente.
- Analizar la situación actual de los sistemas informáticos y procesos de la empresa.
- Elaborar informes detallados que incluyan los resultados de cada auditoría realizada.

Fuente: Piattini, M., & del Peso CAP 5

Funciones de un Auditor Informático

- Controlar y verificar el funcionamiento de los sistemas informáticos internos y de cualquier otro servicio que dependa de la infraestructura tecnológica de la empresa.
- Detectar riesgos del entorno informático para prevenir posibles ciberataques y desvíos de datos.
- Diseñar soluciones para los problemas o errores detectados en la auditoría.
- Proponer estrategias para mejorar los sistemas informáticos.

Fuente: Piattini, M., & del Peso Cap. 5

¿Dónde trabaja un auditor informático?

- Este profesional encuentra oportunidades laborales en grandes empresas que cuentan con su propio departamento de informática y ciberseguridad.
- Por otro lado, puede ser contratado de forma externa por las compañías que requieran de las funciones de un auditor informático, o bien, puede ejercer de forma independiente.

Fuente: Piattini, M., & del Peso CAP 5

Etapas genéricas de la Auditoria Informática

2. Se recopilan datos a partir de entrevistas, revisión de documentos y del uso de herramientas tecnológicas.

3. Se evalúan los controles internos y procesos de los sistemas para determinar su eficacia y eficiencia, así como su alineación con los objetivos de la empresa.
Se analizan e identifican posibles deficiencias o riesgos en los sistemas.

1.En esta etapa se identifican los objetivos específicos de la auditoría y se define su alcance, considerando los recursos disponibles y las áreas clave a examinar.
Se elabora un plan detallado donde se incluyen los métodos y herramientas que se van a utilizar, así como un cronograma de las actividades.

4. Una vez recopilados y analizados los datos, se redacta un informe detallado que incluye las conclusiones de la auditoría, las áreas de mejora, y las recomendaciones. Este documento es crucial para la toma de decisiones a futuro y se presenta a la dirección y otros interesados de la organización

Fuente: Piattini, M., & del Peso CAP 3

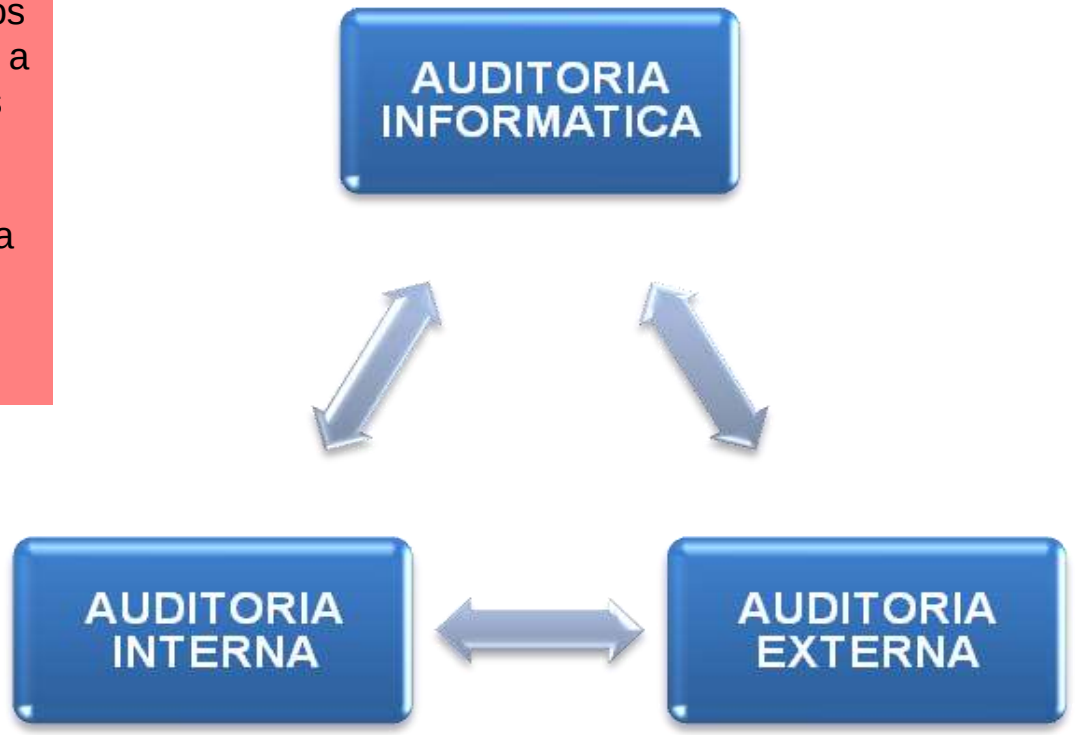
Finalización de la auditoría

- Al finalizar la auditoría se deben implementar las mejoras recomendadas para fortalecer los sistemas de información de la empresa.
- Además, es esencial realizar un seguimiento continuo para asegurar que las mejoras sean efectivas, así como para adaptarse a cualquier cambio en el entorno tecnológico y empresarial.
- Aunque la frecuencia con la que debe hacerse una auditoría informática depende de varios factores, incluyendo el tamaño de la organización y la naturaleza de sus actividades, se recomienda hacerla anualmente.

Fuente: Piattini, M., & del Peso CAP 5

Tipos de auditoria

INTERNA: Es la realizada con recursos materiales y personas que pertenecen a la empresa auditada. Los empleados que realizan esta tarea son remunerados económicamente.
La auditoría interna existe por expresa decisión de la Empresa, o sea, que puede optar por su disolución en cualquier momento



EXTERNA: Es realizada por personas afines a la empresa auditada; es siempre remunerada. Se presupone una mayor objetividad que en la auditoría Interna, debido al mayor distanciamiento entre auditores y auditados.

Fuente: Echenique García 2da. Ed. Cap. 5

Principios aplicados al Auditor Informático

» **PRINCIPIO DE BENEFICIO DE AUDITADO**

En este principio el auditor debe conseguir la máxima eficacia y rentabilidad de los medios informáticos de la empresa auditada, no debe de ningún modo obtener beneficio propio.

» **PRINCIPIO DE CALIDAD**

En el auditor deberá prestar sus servicios conforme las posibilidades de la ciencia y medios a su alcance con absoluta libertad respecto a la utilización de dichos medios y en unas condiciones técnicas adecuadas para el idóneo cumplimiento de su labor.

» **PRINCIPIO DE CONFIANZA**

El auditor deberá facilitar e incrementar la confianza del auditor en base a una actuación de transparencia en su actividad profesional sin alardes científicos-técnicos.

Fuente: Piattini, M., & del Peso CAP 7

Principios aplicados al Auditor Informático

» **PRINCIPIO DE CAPACIDAD**

El auditor debe estar plenamente capacitado para la realización de la auditoría encomendada, máxime teniendo en cuenta que, a los auditados en algunos casos les puede ser extremadamente difícil verificar sus recomendaciones y evaluar correctamente la precisión de las mismas.

» **PRINCIPIO DE COMPORTAMIENTO PROFESIONAL**

El auditor, tanto en sus relaciones con el auditado como con terceras personas, deberá, en todo momento, actuar conforma a las normas, implícitas o explícitas, de dignidad de la profesión y de corrección en el trato personal.

» **PRINCIPIO DE CRITERIO PROPIO**

El auditor durante la ejecución deberá actuar con criterio propio y no permitir que esté subordinado al de otros profesionales, aun de reconocido prestigio, que no coincidan con el mismo.

Fuente: Piattini, M., & del Peso CAP 7

Principios aplicados al Auditor Informático

» **PRINCIPIO DE CONCENTRACION EN EL TRABAJO**

El auditor deberá evitar que un exceso de trabajo supere sus posibilidades de concentración y precisión en cada una de las tareas a él encomendadas, y a que la estructuración y dispersión de trabajos suele, a menudo, si no está debidamente controlada, provocar la conclusión de los mismos sin las debidas garantías de seguridad.

» **PRINCIPIO DE DISCRECIÓN**

El auditor deberá en todo momento mantener una cierta discreción en la divulgación de datos, aparentemente inocuos, que se le hayan puesto de manifiesto durante la ejecución de la auditoria.

» **PRINCIPIO DE ECONOMÍA**

El auditor deberá proteger, en la medida de sus conocimientos, los derechos económicos del auditado evitando generar gastos innecesarios en el ejercicio de su actividad.

Fuente: Piattini, M., & del Peso CAP 7

Principios aplicados al Auditor Informático

» **PRINCIPIO DE FORMACIÓN CONTINUADA**

Este principio impone a los auditores el deber y la responsabilidad de mantener una permanente actualización de sus conocimientos y métodos a fin de adecuarlos a las necesidades de la demanda y a las exigencias de la competencia de la oferta.

» **PRINCIPIO DE FORTALECIMIENTO Y RESPETO DE LA PROFESIÓN**

La defensa de los auditados pasa por el fortalecimiento de la profesión de los auditores informáticos, lo que exige un respeto por el ejercicio, globalmente considerado, de la actividad desarrollada por los mismos y un comportamiento acorde con los requisitos exigibles para el idóneo cumplimiento de la finalidad de las auditorias.

» **PRINCIPIO DE INDEPENDENCIA**

Está relacionado con el principio de criterio propio, obliga al auditor, tanto si actúa como profesional externo o con dependencia laboral respecto a la empresa en la que deba realizar la auditoria informática, a exigir una total autonomía e independencia en su trabajo.

Fuente: Piattini, M., & del Peso CAP 7

Principios aplicados al Auditor Informático

» **PRINCIPIO DE INFORMACIÓN SUFICIENTE**

Este principio obliga al auditor a aportar, en forma pormenorizada, clara, precisa e inteligible para el auditado, información de los puntos y conclusiones relacionados con la auditoria.

» **PRINCIPIO DE INTEGRIDAD MORAL**

Este principio, inherentemente ligado a la dignidad de la persona, obliga al auditor a ser honesto, leal y diligente en el desempeño de su misión, a ajustarse a las normas morales de justicia y prioridad.

» **PRINCIPIO DE LEGALIDAD**

La primacía de esta obligación exige del auditor un comportamiento activo de oposición a todo intento, por parte del auditado o de terceras personas, tendente a infringir cualquier precepto integrado en el derecho positivo.

Fuente: Piattini, M., & del Peso CAP 7

Principios aplicados al Auditor Informático

» **PRINCIPIO DE LIBRE COMPETENCIA**

La actual economía de mercado exige que el ejercicio de la profesión se realice en el marco de la libre competencia siendo rechazables, por tanto, las prácticas colusorias tendentes a impedir o limitar la legítima competencia de otros profesionales.

» **PRINCIPIO DE NO DISCRIMINACIÓN**

El auditor en su actuación previa, durante y posterior a la auditoria deberá evitar cualquier tipo de condicionantes personalizados y actuar en todos los casos con similar diligencia.

» **PRINCIPIO DE NO INJERENCIA**

El auditor, deberá evitar injerencias en los trabajos de otros profesionales, respetar su labor y eludir hacer comentarios que pudieran interpretarse como despreciativos de la misma, deberá igualmente evitar aprovechar los datos.

Fuente: Piattini, M., & del Peso CAP 7

Principios aplicados al Auditor Informático

» **PRINCIPIO DE PRECISIÓN**

Este principio exige del auditor la no conclusión de su trabajo hasta estar convencido, en la medida de lo posible, de la viabilidad de sus propuestas.

» **PRINCIPIO DE PUBLICIDAD ADECUADA**

La oferta y promoción de los servicios de auditoria deberán en todo momento ajustarse a las características, condiciones y finalidad perseguidas.

» **PRINCIPIO DE RESPONSABILIDAD**

El auditor deberá, como elemento intrínseco de todo comportamiento profesional, responsabilizarse de lo que haga, diga o aconseje.

Fuente: Piattini, M., & del Peso CAP 7

Principios aplicados al Auditor Informático

» **PRINCIPIO DE SECRETO PROFESIONAL**

La confidencia y confianza entre el auditor y el auditado e imponen al primero la obligación de guardar en secreto los hechos e informaciones que conozca en el ejercicio de su actividad profesional.

» **PRINCIPIO DE SERVICIO PÚBLICO**

La aplicación de este principio debe incitar al auditor a hacer lo que este en su mano y sin perjuicio de los intereses de su cliente, para evitar daños sociales.

» **PRINCIPIO DE VERACIDAD**

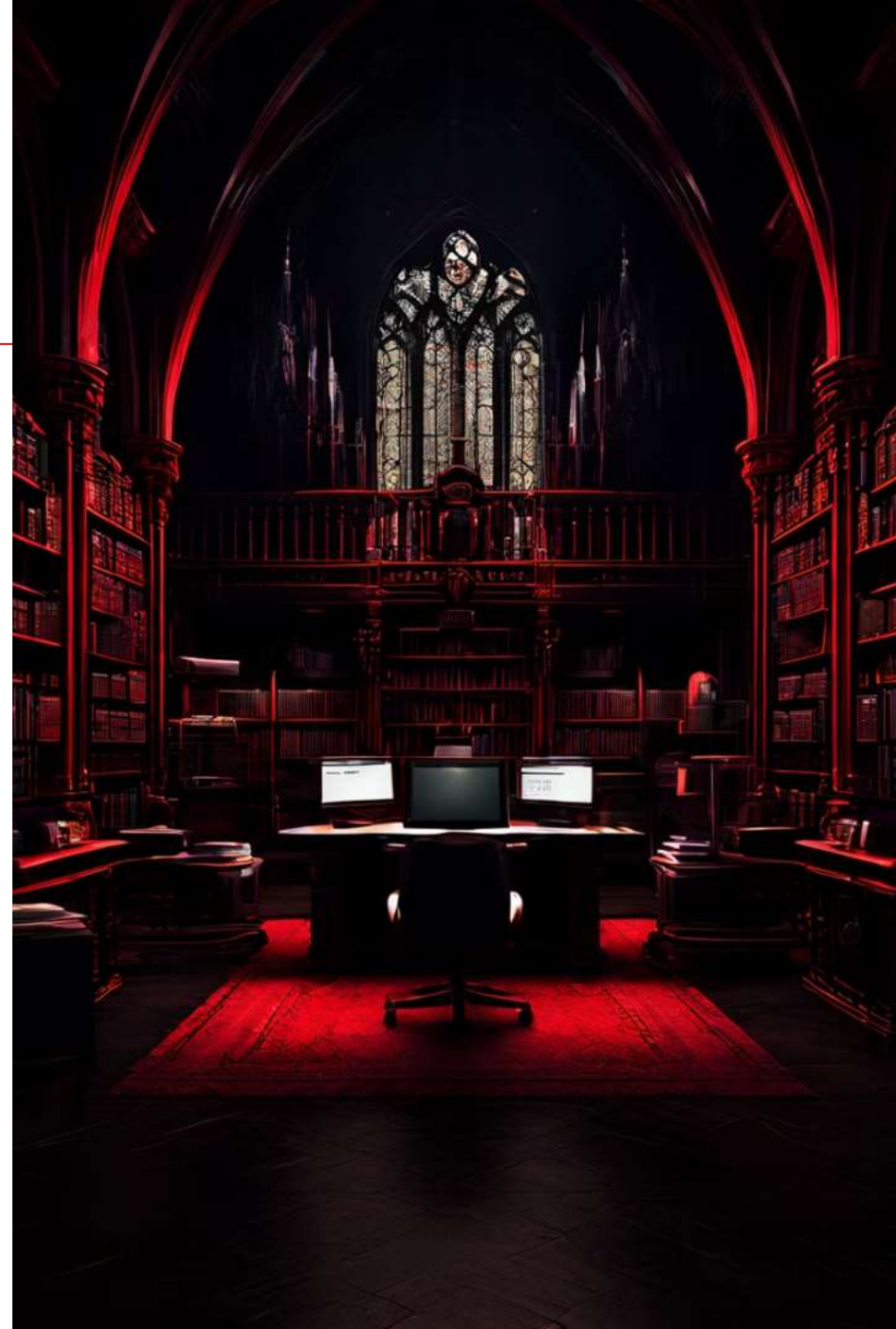
El Auditor en sus comunicaciones con el auditado deberá tener siempre presente la obligación de asegurar la veracidad de sus manifestaciones con los límites impuestos por los deberes de respeto, corrección, y secreto profesional.

Fuente: Piattini, M., & del Peso CAP 7

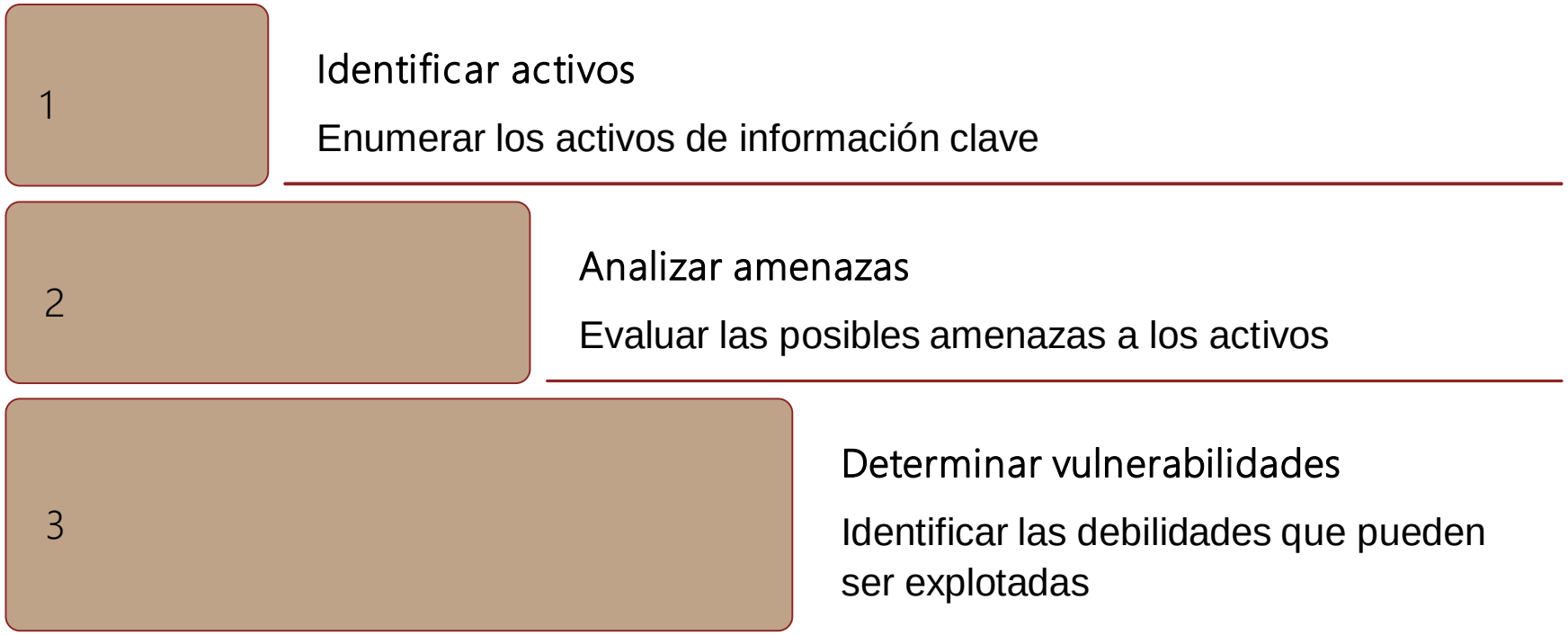
Herramientas para realizar auditorías informáticas

Las auditorías informáticas requieren de un conjunto de herramientas especializadas para examinar y evaluar los sistemas, procesos y controles de una organización.
Abarcan desde escáneres de vulnerabilidades hasta analizadores de tráfico de red, pasando por herramientas de monitoreo y diagnóstico.

Algunas de las herramientas más comunes utilizadas en auditorías informáticas son: Nessus, Wireshark, Metasploit, Burp Suite, Sqlmap, Maltego y OSSEC, entre otras.
Permiten identificar puntos débiles, detectar intrusiones, analizar el flujo de información y evaluar el cumplimiento normativo.



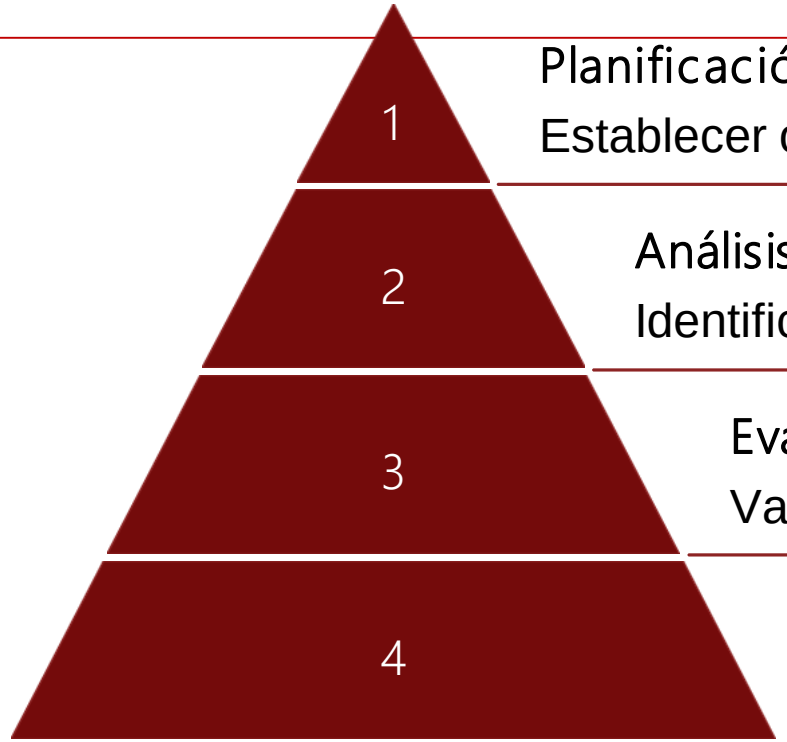
Metodología Octave para auditoría informática



La metodología Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation) es un enfoque integral para la evaluación de riesgos de seguridad de la información. Consiste en una serie de pasos estructurados que ayudan a identificar los activos críticos, analizar las amenazas y evaluar las vulnerabilidades de una organización.

Para ampliar ver: https://www.pmg-ssi.com/2021/09/metodologia-octave-para-el-

Metodología Margerit para auditoría informática



Planificación
Establecer objetivos y alcance de la auditoría

Análisis
Identificar riesgos y controles existentes

Evaluación
Valorar la efectividad de los controles

Recomendaciones
Proponer mejoras y un plan de acción

La metodología Margerit es un marco completo para realizar auditorías informáticas de manera sistemática y exhaustiva. Comienza con una etapa de planificación donde se definen los objetivos y el alcance del proyecto. Luego sigue un análisis detallado de los riesgos y los controles existentes en la organización. La evaluación permite valorar la eficacia de estos controles y finalmente se generan recomendaciones específicas para mejorar la seguridad informática.

Para ampliar ir a : https://www.ccn-cert.cni.es/es/documentos-publicos/1789-magerit-libro metodo/file?format=html

Evaluación de controles en auditoría informática

Revisión de controles técnicos

Durante la auditoría, el equipo evaluará los controles técnicos implementados, como firewalls, sistemas de detección de intrusos y configuración de servidores, para asegurar su eficacia y cumplimiento con las políticas de seguridad.

Inspección de controles físicos

Se realizarán inspecciones in situ para verificar la efectividad de los controles físicos, como sistemas de acceso, monitoreo por cámaras y resguardo de áreas críticas, que protejan la infraestructura tecnológica.

Evaluación de controles administrativos

Además, se revisarán los controles administrativos, como políticas de seguridad de la información, procedimientos de gestión de incidentes y concienciación de los usuarios, para evaluar su implementación y eficacia.

Reporte de hallazgos en auditoría informática
Un ejemplo

El reporte de hallazgos es un componente clave de la auditoría informática. En esta etapa, se documentan de manera clara y concisa los problemas, debilidades o riesgos identificados durante el proceso de evaluación. El informe debe proporcionar una visión general de los hallazgos más importantes, clasificados por nivel de criticidad y acompañados de recomendaciones específicas.

Hallazgo	Descripción	Nivel de Riesgo
Falta de controles de acceso adecuados	Se identificó que no hay controles suficientes para restringir el acceso a sistemas críticos. Varios usuarios tienen privilegios excesivos.	Alto
Vulnerabilidades en el sistema de backups	El proceso de respaldo de información presenta fallas y no se realiza de manera sistemática. Existe riesgo de pérdida de datos críticos.	Medio
Falta de monitoreo de actividad en la red	No se implementan herramientas ni procesos para el monitoreo y análisis del tráfico de red. Esto dificulta la detección temprana de incidentes de seguridad.	Alto

Recomendaciones y plan de acción en auditoría informática

Recomendaciones

Basado en los hallazgos de la auditoría, se brindan recomendaciones específicas y detalladas para mejorar la seguridad, eficiencia y cumplimiento de los sistemas y procesos informáticos.

Plan de Acción

Se establece un plan de acción claro y estructurado, con plazos, responsables y recursos definidos, para implementar las recomendaciones de manera efectiva y oportuna.

Seguimiento

Se diseña un sistema de seguimiento y monitoreo para evaluar el progreso y el impacto de las acciones implementadas, con el fin de asegurar el cumplimiento de los objetivos de la auditoría.

Beneficios de la Auditoría Informática

La auditoría informática ofrece múltiples beneficios a las organizaciones, como la identificación de riesgos, la mejora de controles internos y la optimización de recursos tecnológicos. Además, ayuda a garantizar el cumplimiento normativo y la seguridad de la información.

Al implementar recomendaciones de auditoría, las empresas pueden fortalecer su posición competitiva, aumentar la confianza de clientes y partes interesadas, y prepararse mejor para enfrentar amenazas cibernéticas.

Diferencias entre Consultor, Auditor y Perito Informático

CONSULTOR INFORMÁTICO

Función: El consultor informático asesora a las organizaciones en cuestiones relacionadas con la tecnología y los sistemas de información.

Enfoque: Su enfoque es más amplio y estratégico. Busca optimizar los procesos, mejorar la eficiencia y alinear la tecnología con los objetivos empresariales.

Actividades: Realiza análisis de necesidades, propone soluciones tecnológicas, diseña estrategias de implementación y brinda recomendaciones.

Fuente: Piattini, M., & del Peso CAP 26

Diferencias entre Consultor, Auditor y Perito Informático

AUDITOR INFORMATICO

Función: El auditor informático evalúa y verifica los sistemas de información y los controles internos de una organización.

Enfoque: Su enfoque es más específico y técnico. Busca identificar riesgos, vulnerabilidades y deficiencias en los sistemas.

Actividades: Realiza revisiones, pruebas y análisis exhaustivos de los procesos, la seguridad, la integridad de los datos y el cumplimiento normativo.

Fuente: Piattini, M., & del Peso CAP 26

Diferencias entre Consultor, Auditor y Perito Informático

PERITO INFORMATICO

Función: El perito informático actúa como experto en casos legales o judiciales relacionados con la informática.

Enfoque: Su enfoque es legal y forense. Ayuda a recopilar pruebas digitales, analiza incidentes de seguridad y presenta informes periciales.

Actividades: Participa en investigaciones, realiza análisis forenses de dispositivos y colabora con abogados y tribunales.

Fuente: Piattini, M., & del Peso CAP 26

Bibliografía de consulta

Echenique García, J. A. (2001). Auditoría en informática. Compañía Editorial Continental. 2da Edición

Piattini, M., & del Peso, E. (2008). Auditoria informática: Un enfoque práctico. 2ª Edición ampliada y revisada.

También pueden acceder a 2 informes de auditoría que se subieron en el aula virtual