

## Tema 01: Auditoría de sistemas operativos.

### INTRODUCCIÓN




Los sistemas operativos son parte fundamental de toda empresa, ya que poseen los equipos informáticos para su funcionamiento, incluso los equipos de comunicación, router, dispositivos móviles, etc., poseen un sistema operativo que necesita estar actualizado y bien configurado, por tanto, la importancia de auditar los sistemas operativos.

Auditoría de sistemas operativos



Para lo cual el auditor revisa lo siguiente:

1. Los procedimientos relacionados con la identificación y la selección del software del sistema.  
Mediante entrevistas a la gerencia, busca identificar:
  - Los requerimientos de software.
  - Las fuentes potenciales de software.
2. Análisis de costo/beneficio del software del sistema.  
Consiste en revisar la documentación del análisis costo/beneficio y las alternativas que proponen y determinan si cada alternativa potencial fue evaluada adecuadamente.
3. Instalación del software del sistema.  
Consiste en revisar el plan o procedimiento para la prueba del sistema, determinar si las pruebas se realizaron de acuerdo a ese plan y en forma exitosa, de no ser así investigar si todos los problemas se evaluaron y resolvieron antes de la instalación del software.
  - Tunning  
Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los subsistemas y del sistema en su conjunto.
  - Evaluación del sistema operativo.  
Es el aprovechamiento y explotación de los sistemas operativos, lenguajes, programas de aplicación, paquetes y los demás aspectos que integran el software institucional. La identificación de ello busca dictaminar si se satisfacen las necesidades de procesamiento de información de la empresa.
  - Optimización de los sistemas y subsistemas.  
Las técnicas de sistemas deben realizar acciones permanentes de optimización como consecuencia de la realización de tuning's preprogramados o específicos. El auditor verificará que las acciones de optimización fueron efectivas y no comprometieron la operatividad de los sistemas ni el plan crítico de producción diaria de explotación.



Existen en el mercado diferentes sistemas operativos, algunos deben ser comprados a una empresa en particular y otros son de software libre, pero no importando cual sea su arquitectura o el tipo de sistema operativo que posea una empresa, siempre es importante auditar el funcionamiento de los mismos y el procedimiento de mantenimiento que se

Texto del Audio

Existen en el mercado diferentes sistemas operativos, algunos deben ser comprados a una empresa en particular y otros son de software libre, pero no importando cual sea su arquitectura o el tipo de sistema operativo que posea una empresa, siempre es importante auditar el funcionamiento de los mismos y el procedimiento de mantenimiento que se les brinda para garantizar su correcto funcionamiento, además de evaluar otros sistemas alternativos que protegen los sistemas operativos, tal como los antivirus.

#### **Principales etapas que se deben seguir al momento de auditar un sistema operativo**



##### **A. Investigación Preliminar**

- Se determinan los recursos de cómputo de la empresa y la estructura organizacional de esta.
- Evalúa la importancia del sistema de información para los procesos de negocio objeto de la auditoría y el soporte que los recursos de cómputo dan a estos.
- Se conoce de manera global el sistema operativo sobre el cual se llevará a cabo la auditoría, identificando los elementos que apoyan la seguridad y administración.

Consideraciones

- Conocimiento global de la empresa.
- Conocimiento global del sistema operativo, evaluando las herramientas que proporciona como apoyo a la seguridad y a la administración.
  
- Herramientas o mecanismos para la realización de la Investigación Preliminar.
  - Entrevistas previas con el cliente.
  - Inspección de las instalaciones.
  - Investigación e indagación con el personal.
  - Revisión de documentación proporcionada por la empresa.
  - Revisión de informes de auditorías anteriores, si se han realizado.
  - Estudio y evaluación del sistema de control interno.
  
- Documentos a solicitar para la Investigación Preliminar.
  - Listado de aplicaciones en producción y directorio de datos.
  - Listado de empleados activos y despedidos en el último trimestre.
  - Documento de autorización a cada usuario del sistema y aprobación de derechos y privilegios.
  - Listados de monitoreo del sistema.
  - Listado de utilidades importantes, con los usuarios y grupos que las acceden.
  - Políticas de seguridad corporativa.
  - Documento de configuración inicial del sistema operativo y las autorizaciones para su actualización o cambio.
  - Documento de definición de las funciones en la administración del sistema y la seguridad.
  - Planes de capacitación y entrenamiento.
  - Contratos con entes externos relacionados con Tecnologías de la Información.
  - Informes de auditoría previos.

#### B. Identificación y Agrupación de Riesgos

Se identifica y clasifica los riesgos a los que está expuesto el sistema operativo objeto de la auditoría, ya sean propios o generados por entidades externas (personas, procedimientos, bases de datos, redes, etc.) que interactúan con el sistema.

Para identificar y clasificar los riesgos a los que está expuesto el sistema operativo objeto de la auditoría, existen varios métodos:

- Escenarios de Riesgos.

- Grupos de Riesgos.

Para su estudio se pueden dividir los diferentes tópicos a abordar en la investigación de auditoría:

- Instalación y Configuración Inicial.
- Seguridad Física.
- Seguridad Lógica.
- Documentación del Sistema.
- Mantenimiento y Soporte.
- Aspectos administrativos.
- Monitoreo y Auditoría.
- Planes de contingencia (planes de respaldo y recuperación).
- Administración e implementación de la seguridad.
- Servicios que soporta el sistema operativo (aplicaciones, web, correo, proxy, DNS y base de datos).

#### C. Evaluación de la seguridad en la empresa objeto de la auditoría

- Se determina si los controles existentes protegen apropiadamente la empresa contra los riesgos identificados.
- Existen cuatro métodos que pueden combinarse para realizar dicho control:
  - Análisis de riesgos.
  - Flujogramas de control.
  - Cuestionarios de control.
  - Matrices de control.

#### D. Diseño de Pruebas de Auditoría

Se definen los procedimientos de auditoría que permitan recolectar la evidencia que apoye los hallazgos y recomendaciones.

- Consideraciones  
Una vez realizados los pasos anteriores en este punto se tienen las bases para diseñar las pruebas de auditoría que se han de efectuar. Este es un trabajo de escritorio donde se determina en términos generales: el objetivo de la prueba, se describe brevemente (procedimientos a emplear), tipo de la prueba, técnicas a utilizar, recursos requeridos en cuanto a información, hardware, software y personal.
- Tipos de pruebas

- Pruebas de cumplimiento: busca determinar si existe el control para el riesgo identificado.
- Pruebas sustantivas: busca conocer la forma en que está implementado el control, en caso de que este exista.

Técnicas comúnmente usadas para el Diseño y Ejecución de Pruebas de Auditoría:

- Observación.
- Indagación.
- Conciliación (cruce de información con persona o documentos).
- Inspección.
- Investigación analítica: evaluar tendencias.
- Confirmación.
- TAAC'S: Técnicas de Auditorías Asistidas por Computadora.

#### E. Ejecutar Pruebas de Auditoría

Se obtiene evidencia sobre los controles establecidos, su utilización, y el entendimiento y ejecución de los mismos por parte de las personas.

- Consideraciones  
Se ejecutan las pruebas de auditoría diseñadas en el anterior paso, adjuntándose para cada prueba ejecutada en los soportes correspondientes.

#### F. Análisis del efecto de las debilidades de seguridad

Consiste en dos pasos:

- Identificar las debilidades.
- Determinar el impacto más probable que tendrá cada debilidad.

#### G. Elaboración de informe de auditoría

- Se comunica a las personas o entes involucrados en la organización con los sistemas los resultados de la auditoría, para que ellos hagan la gestión necesaria para implementar los controles que cubran aquellas situaciones de riesgo de mayor relevancia, y mantengan y optimicen los que funcionan eficientemente.

- Servir de apoyo en la toma de decisiones, gracias a la información que proveen.
- Hacer parte de la documentación para futuras auditorías.
- Consideraciones
  - Por ser información que de cierta manera puede afectar la imagen de la empresa si sale a la luz pública, debe ser de carácter confidencial.
  - La elaboración del informe debe ser cuidadosa en cuanto a la información que contiene, no debe dar lugar a ambigüedades, y los hallazgos y recomendaciones deben ser claramente descritos.
  - El informe debe estar documentado: información provista por la empresa y principalmente las pruebas de auditoría; pues esto es el sustento de los hallazgos, conclusiones y recomendaciones.

#### H. Seguimiento

La empresa debe tomar las recomendaciones consignadas en los informes de auditoría y dar inicio a un proceso de implementación de mejoras basado en dichas recomendaciones.

- Consideraciones
  - Implementar nuevos controles y tener en cuenta las recomendaciones generadas por la auditoría es responsabilidad de la empresa que contrató la auditoría.
  -

El seguimiento consiste en:

- Esta es la etapa final del proceso de auditoría, pero también es la etapa inicial de un proceso de retroalimentación que lleva a la mejora de los sistemas, el trabajo del auditor llega hasta la entrega de los respectivos informes, de aquí en adelante es decisión de la empresa implementar las recomendaciones e involucrar al antes auditor en el nuevo proceso. Este es el punto neurálgico de la auditoría, ya que de nada vale hacer un estudio minucioso si una empresa no está dispuesta a implementar las medidas o controles recomendados, por esta razón debe medirse el impacto costo - beneficio de las recomendaciones, ya que ninguna organización está dispuesta a pagar por la seguridad de algo más de lo que este vale.

#### Ejemplo de cuestionario para evaluar sistemas operativos

**-Ver aquí-**

[https://uvirtual.ufg.edu.sv/vmateriales/images/stories/pdf/recursos\\_ing/computacion/ASC0/un02tm01/un02tm01.pdf](https://uvirtual.ufg.edu.sv/vmateriales/images/stories/pdf/recursos_ing/computacion/ASC0/un02tm01/un02tm01.pdf)

## Actualización de sistemas operativos

Uno de los procesos necesarios para mantener los sistemas operativos con un comportamiento adecuado es mantenerlo actualizado.

Las actualizaciones son aplicaciones que los proveedores o fabricantes de un sistema operativo en específico pone a disposición de los usuarios una aplicación que debe ser instalada en el equipo en cuestión como parte de una mejora de funcionalidades o proteger de alguna vulnerabilidad.

Las actualizaciones pueden ser ejecutadas de forma automática o manualmente, lo importante es no olvidarse de realizarlas periódicamente.



Cabe mencionar que así como se actualizan los sistemas operativos de las computadoras, también deben actualizarse los equipos de comunicación, dispositivos móviles, router, etc., por tanto, se debe estar atento de actualizar cualquier hardware que contenga instalado un sistema operativo.

## Conclusiones



El éxito de una empresa depende de la eficiencia de sus sistemas de información. Una empresa puede tener un staff de gente de primera, pero tiene un sistema informático propenso a errores, lento, vulnerable e inestable; si no hay un balance entre estas dos cosas, la empresa nunca saldrá a adelante.

En cuanto al trabajo de la auditoría en sí, podemos remarcar que se precisa de gran conocimiento de informática, seriedad, capacidad, minuciosidad y responsabilidad; la auditoría de sistemas operativos debe hacerse por gente altamente capacitada, una auditoría mal hecha puede acarrear consecuencias drásticas para la empresa auditada, principalmente económicas.



## CONTROL DE LECTURA

### Parte I. Lea, analice y responda las siguientes preguntas

1. Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los subsistemas y del sistema en su conjunto:

- ☐ Investigación Preliminar.
- ☒ Tunning.
- ☐ Optimización de los sistemas y subsistemas.
- ☐ Ninguna de las anteriores.

2. Busca determinar si existe el control para el riesgo identificado:

- ☐ Pruebas sustantivas.
- ☒ Pruebas de cumplimiento.

3. La auditoría de sistemas operativos debe hacerse por gente altamente capacitada, una auditoría mal hecha puede acarrear consecuencias drásticas para la empresa auditada.

- ☒ Verdadero.
- ☐ Falso.

4. Implementar nuevos controles y tener en cuenta las recomendaciones generadas por la auditoría es responsabilidad de la empresa que efectuó la auditoría.

- ☐ Verdadero.
- ☐ Falso.

## CONTROL DE LECTURA

### Parte I. Lea, analice y responda las siguientes preguntas

1. Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los subsistemas y del sistema en su conjunto:

- ☐ Investigación Preliminar.
- ☒ Tunning.
- ☐ Optimización de los sistemas y subsistemas.
- ☐ Ninguna de las anteriores.



2. Busca determinar si existe el control para el riesgo identificado:

- ☐ Pruebas sustantivas.
- ☒ Pruebas de cumplimiento.



3. La auditoría de sistemas operativos debe hacerse por gente altamente capacitada, una auditoría mal hecha puede acarrear consecuencias drásticas para la empresa auditada.

- ☒ Verdadero.
- ☐ Falso.



4. Implementar nuevos controles y tener en cuenta las recomendaciones generadas por la auditoría es responsabilidad de la empresa que efectuó la auditoría.

- ☐ Verdadero.
- ☒ Falso.



## Tema 02: Auditoría de sistemas de bases de datos.

## INTRODUCCIÓN



Las bases de datos de las organizaciones forman parte del activo más importante que poseen, debido a que se almacena la información de un gran número de usuarios e información de otro tipo.

Si la base de datos cae en personas indebidas podrían desprestigiar a la organización publicando la información confidencial de sus clientes o utilizar los datos contenidos en las bases de datos para efectuar fraudes informáticos, es por ello la importancia de la auditoría de bases de datos.

Generalidades



La gran difusión de los Sistemas de Gestión de Bases de Datos (SGBD), junto con la consagración de los datos como uno de los recursos fundamentales de las empresas, ha hecho que los temas relativos a su control interno y auditoría cobren, cada día, mayor interés.

Normalmente la auditoría informática se aplica de dos formas distintas; por un lado, se auditan las principales áreas del departamento de informática: explotación, dirección, metodología de desarrollo, sistema operativo, telecomunicaciones, bases de datos, etc.; y, por otro, se auditan las aplicaciones (desarrolladas internamente, subcontratadas o adquiridas) que funcionan en la empresa. La importancia de la auditoría del entorno de bases de datos radica en que es el punto de partida para poder realizar la auditoría de las aplicaciones que utiliza esta tecnología.

**El valor de la información en las empresas**



La gran difusión de los Sistemas de Gestión de Bases de Datos (SGBD), junto con la consagración de los datos como uno de los recursos fundamentales de las empresas, ha hecho que los temas relativos a su control interno y auditoría cobren, cada día, mayor interés.

Las organizaciones son exitosas por el valor que le dan a su información, y es en este punto donde reside su mayor riesgo, en el acceso no controlado a la misma.

### **Seguridad de la información**

Las empresas están en un mayor riesgo de fraude, robo de datos, el incumplimiento de normativas, la pérdida de clientes y la pérdida de la marca o la reputación cuando los datos corporativos están sin vigilancia. Registrar todos los datos de acceso es un proceso que las empresas pueden tomar como parte de un programa integral para asegurar que sus datos estén seguros.

### **La auditoría de los datos**

La auditoría de los datos es una preocupación primordial para cualquier persona responsable de garantizar que las bases de datos corporativas estén protegidas y que dicha protección cumple las regulaciones gubernamentales. Las fases de la auditoría de datos son:

*Las fases de la auditoría de datos son:*

1. Identificación de las partes y del alcance de la auditoría

En esta fase se trata de identificar tanto a la entidad auditora como a la entidad auditada, siendo recomendable que el auditor y el responsable o el encargado del tratamiento creen una comisión o equipo de trabajo que tendrá por objeto:/p>

- Mantener una comunicación permanente y fluida con el auditor para el desarrollo de los trabajos que se realicen.
- Asumir y responsabilizarse internamente de que el trabajo de auditoría será realizado por el auditor con la colaboración de todo el personal que vaya a estar involucrado.

Asimismo, en esta fase se procede a examinar entre otros aspectos los siguientes:

- Obtención de los datos de carácter personal.
- Finalidad de los datos de carácter personal.
- Ficheros de datos de carácter personal.
- Consentimiento del afectado en la recogida de los datos.
- Responsable del fichero.
- Derechos de los afectados.
- Encargado del tratamiento.
- Acceso a los datos de carácter personal.
- Cesiones de datos.

## 2. Recogida de información

El auditor deberá recopilar información sobre:

- El grado de mantenimiento y cumplimiento del documento de seguridad, en especial de los apartados “Funciones” y “Obligaciones del personal”.
- Almacenamiento de información.
- Los registros de incidencias.
- Los accesos, copias de seguridad y salida de soportes.
- La relación de los usuarios autorizados.
- El inventario de soportes.

Entre los casos de recogida de información que suelen darse dentro del proceso de auditoría, cabe señalar los siguientes:

- Obtención por parte del auditor de información relativa al responsable y encargado del tratamiento de registros públicos.
- Petición por parte del auditor de información previa al inicio de las entrevistas con los distintos interlocutores de la empresa a través del comité creado al efecto.
- Petición por parte del auditor de información durante las entrevistas realizadas a los distintos interlocutores.
- Solicitud de información por parte del auditor, tras conocer determinados datos sobre la empresa auditada, a fin de comprobar la veracidad de los mismos.
- Entrega voluntaria de información al auditor por parte de los interlocutores.

- Apreciación directa del auditor en el examen de las medidas técnicas, lógicas y organizativas existentes en la empresa, así como de los hechos que acontezcan durante sus visitas a la entidad auditada.

### 3. Entrevistas. Check list o listado de comprobación

Para la recogida de esta información el auditor lleva a cabo una serie de entrevistas a las personas que van a estar involucradas en la auditoría. Estas personas son las siguientes:

- El responsable de seguridad nombrado por el responsable del fichero y por el encargado del tratamiento para velar y coordinar las medidas de seguridad establecidas en el RLOPD.
- El administrador o administradores de sistemas de la organización, que se encargan de la gestión y administración de los sistemas de información así como de la seguridad del mismo.
- Los usuarios, que son las personas que, dentro de la empresa, acceden a los datos de carácter personal procesados en los sistemas de información.

Lo más oportuno es que el auditor, de forma previa a la realización de las entrevistas, prepare un listado de aquellas personas con las que se entrevistará y a las que se les preguntará una serie de cuestiones mediante un check list o formulario elaborado al efecto.

### 4. Análisis de la información

Las peculiaridades que caracterizan este análisis son las siguientes:

- Debe cotejarse toda la información obtenida por el auditor de los distintos canales de la empresa auditada y, sobre todo, la obtenida a través de los cuestionarios realizados tanto al responsable de seguridad y administrador de sistemas, como a los distintos usuarios.
- Debe tratarse de un análisis por niveles de seguridad, es decir, deben analizarse, en primer lugar, las medidas de carácter general contempladas en el RLOPD y con posterioridad, por orden, las contempladas para el nivel básico, medio y alto.

### 5. Informe de auditoría

El informe de auditoría es el producto final del trabajo desempeñado por el auditor. Deberá ser analizado por el responsable de seguridad competente, que elevará las



conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la AEPD o, en su caso, de las autoridades de control de las comunidades autónomas.

El informe de auditoría deberá:

- Dictaminar sobre la adecuación de las medidas y controles establecidos a lo dispuesto en el RLOPD.
- Identificar las deficiencias y proponer las medidas correctoras o complementarias.
- Incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.
- Ser analizado por el responsable de seguridad, y elevar sus conclusiones al responsable del fichero para que adopte las medidas adecuadas.

#### **Auditoría de sistema de base de datos**



¿Qué es la auditoría de BD?

Es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en las bases de datos incluyendo la capacidad de determinar:

- Quién accede a los datos.
- Cuándo se accedió a los datos.
- Desde qué tipo de dispositivo/aplicación.
- Desde qué ubicación en la red.
- Cuál fue la sentencia SQL ejecutada.
- Cuál fue el efecto del acceso a la base de datos.
- Es uno de los procesos fundamentales para apoyar la responsabilidad delegada a IT por la organización frente a las regulaciones y su entorno de negocios o actividad.
- Quiénes participan en la auditoría de Base de Datos
- Auditores de Sistemas.
- Tecnología de Información.
- Cumplimiento Corporativo.
- Riesgo Corporativo.
- Seguridad Corporativa.
- Términos similares a auditoría de Base de Datos.
- Auditoría de Datos.
- Monitoreo de Datos.

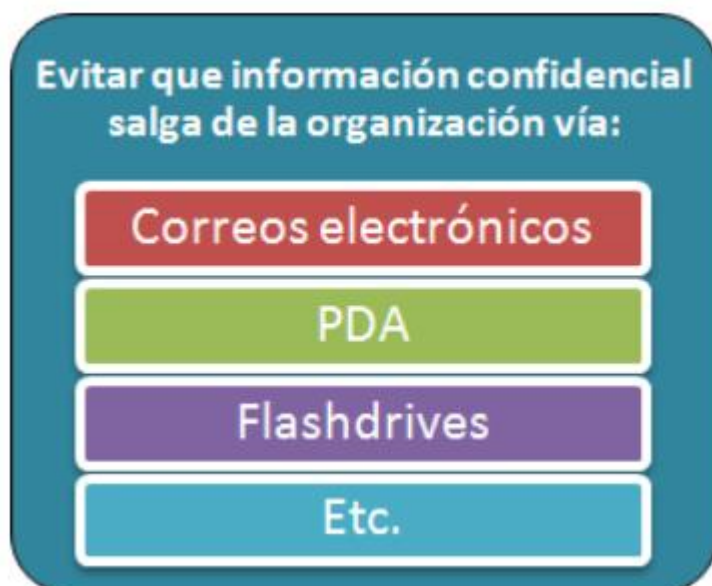
Seguridad de BD vs Auditoría de BD



<b>Los esfuerzos en seguridad de base de datos normalmente están orientados a:</b>
<ul style="list-style-type: none"> <li>■ Impedir el acceso externo.</li> <li>■ Impedir el acceso interno a usuarios no autorizados.</li> <li>■ Autorizar el acceso solo a los usuarios autorizados.</li> </ul>
<b>Con la auditoría de BD se busca:</b>
<ul style="list-style-type: none"> <li>■ Monitorear y registrar el uso de los datos por los usuarios autorizados o no.</li> <li>■ Mantener trazas de uso y del acceso a bases de datos.</li> <li>■ Permitir investigaciones forenses.</li> <li>■ Generar alertas en tiempo real.</li> </ul>

#### Prevención de Fuga de Información vs Auditoría de Base de Datos

Las herramientas de prevención de fuga de información (Data Leak Prevention) se encargan de:



La auditoría de BD es importante porque:

- Toda la información financiera de la organización reside en bases de datos y deben existir controles relacionados con el acceso a las mismas.
- Se debe poder demostrar la integridad de la información almacenada en las bases de datos.
- Establece estrictas normas para la protección y divulgación de información privada de los clientes de las instituciones financieras.
- La información de los clientes es almacenada en bases de datos.
- Implementar esquemas automáticos de auditoría para capturar la información de todas las personas que tienen acceso a la información.
- Mantener los logs de auditoría por un tiempo mínimo de 3 meses.
- Verificar diariamente los logs de todos los sistemas.

- Objetivos generales de la auditoría de BD
  - Mitigar los riesgos asociados con el manejo inadecuado de los datos.
  - Disponer de mecanismos que permitan tener trazas de auditoría completas y automáticas relacionadas con el acceso a las bases de datos incluyendo la capacidad de generar alertas con el objetivo de:
    - Apoyar el cumplimiento regulatorio.
    - Satisfacer los requerimientos de los auditores.
    - Evitar acciones criminales.
    - Evitar multas por incumplimiento.
- Aspectos clave de auditoría de BD
  - No se debe comprometer el desempeño de las bases de datos.
  - Soportar diferentes esquemas de auditoría.
  - Se debe tomar en cuenta el tamaño de las bases de datos a auditar y los posibles SLA establecidos.
  - Segregación de funciones.
  - El sistema de auditoría de base de datos no puede ser administrado por los DBA del área de IT.
  - Proveer valor a la operación del negocio.
  - Información para auditoría y seguridad.
  - Información para apoyar la toma de decisiones de la organización.
  - Información para mejorar el desempeño de la organización.
  - Auditoría completa y extensiva.
  - Cubrir gran cantidad de manejadores de bases de datos.

- Estandarizar los reportes y reglas de auditoría.

### *Características principales de un sistema de auditoría de BD*

Algunas de las características principales de un sistema de auditoría de bases de datos son:

- Sistema confiable e integral.
- Capaz de consolidar las trazas de auditoría.
- Reglas de auditoría basadas en necesidades específicas.
- No se debe afectar el desempeño de las bases de datos.
- Capaz de generar notificaciones en tiempo real.
- Capacidad para retener trazas por largos periodos de tiempo.
- Flexibilidad para crear reportes.
- Administrable y escalable en el tiempo.

### *Planificación de la auditoría de BD*

Al momento de realizar la auditoría de bases de datos se deben tomar en cuenta las siguientes actividades:

- Identificar todas las bases de datos de la organización.
- Clasificar los niveles de riesgo de los datos en las bases de datos.
- Analizar los permisos de acceso.
- Analizar los controles existentes de acceso a las bases de datos.
- Establecer los modelos de auditoría de BD a utilizar.
- Establecer las pruebas a realizar para cada BD, aplicación y/o usuario.

### *Consideraciones Generales*

- Se deben tomar en cuenta todas las capas de acceso a la información.
- Se debe tener importante atención en los accesos de los usuarios con privilegios de acceso.
- Se debe tratar de tener información contextual para determinar cómo se creó la violación al control.
- Se deben tener reglas de auditoría uniformes a través de todas las bases de datos y sistema.
- Se deben segregar las funciones entre los auditores y los usuarios con privilegios de acceso.
- Algunas aplicaciones enmascaran la identidad de los usuarios.
- Aplicaciones que utilizan un login común para el acceso a las bases de datos. Se deben evitar este tipo de configuraciones.
- Se debe solicitar la incorporación de los datos del usuario en la información de acceso a la base de datos.
- Se deben utilizar indicadores relacionados como el IP del usuario.

Establecer el proceso de auditoría de base de datos es un factor crítico de éxito para:

- Lograr el control de los datos y la información.
- Lograr el cumplimiento de regulaciones.
- Apoyar en la protección de los activos digitales.
- Apoyar las estrategias de control y prevención de fraude.

### **Tipos de auditores de los DBMS (Database Management System)**

Existen dos tipos de auditores:



Una práctica común para la mayoría de las empresas es utilizar cada una para diferentes propósitos, una para consultar sobre cómo llevar a cabo la auditoría; otra para realizar la auditoría. Esta separación de funciones entre las entidades de auditoría es necesaria para mantener la independencia en todo el proceso de auditoría y garantizar resultados objetivos.

### **La auditoría interna y la auditoría externa**

### **Auditoría Interna**

- Los auditores internos deben auditar todos los accesos a bases de datos, incluido el acceso por los usuarios autorizados o de confianza.
- Si no pueden producir un registro de quién ha accedido a los datos, cuándo se produjo este acceso, los datos que se alteraron y qué cambios se hicieron (en su caso), entonces el auditor debe revelar que la empresa tiene un registro de auditoría incompleto.

### **Auditoría Externa**

- Su función principal es examinar el negocio y advertir a la empresa sobre los riesgos potenciales y las debilidades en proceso de auditoría.
- Son plenamente responsables de la realización de una profunda y completa auditoría, que produce toda la documentación y la información necesaria para satisfacer los requisitos corporativos y de gobierno.

## **Técnicas de auditoría de acceso de base de datos**

Existen varias técnicas populares que pueden ser implementadas para auditar la estructura de la base de datos, tres de ellas son:

### *Técnicas de Auditoria*

#### **1. Trazas de auditoría en la BD**

Esta técnica es construida directamente usando las capacidades nativas de cada DBMS (Database Management System).

Algunos ítems comunes que pueden ser auditados por la mayoría de los DBMS son:

- Inicio de sesión y los intentos de sesión (ambos con éxito y los fracasos de los intentos).
- Reinicios del servidor de base de datos.
- Comandos emitidos por los usuarios con privilegios de administrador del sistema.
- Operaciones, seleccionar, insertar, actualizar y eliminar.
- Ejecución de procedimientos almacenados.
- Etc.

#### **2. Revisar y analizar el log de transacciones de la BD**

Cada DBMS utiliza logs de transacciones para capturar cada modificación a la base con fines de recuperación.

Existe software que interpreta estos registros e identifica qué datos fueron cambiados y por cuáles usuarios.

### 3. Monitoreo preventivo de las operaciones de DB en el servidor

Esta técnica captura todas las peticiones que se hacen a la base de datos.

Es importante que todas las sentencias de acceso sean auditadas, no solo las llamadas de red, porque no todas las sentencias van a través de la red. Esto es especialmente importante para las plataformas de mainframe, donde gran parte de la actividad está centralizada.

Las preguntas que se deberán responder son:

- ¿Quiénes accedieron a los datos?
- ¿En qué fecha y hora fue el acceso?
- ¿Qué programa o software de cliente se utiliza para acceder a los datos?
- ¿De qué lugar se emitió la solicitud?
- ¿Qué publicó la base de datos para tener acceso a los datos?
- ¿La petición fue exitosa?, en caso afirmativo, ¿cuántas filas de datos se recuperaron?
- Si la solicitud fue una modificación, ¿qué datos se han cambiado?

### Conclusiones

- La auditoría de los DBMS puede ser un componente fundamental para la seguridad de las bases de datos y el cumplimiento con las regulaciones gubernamentales porque advierten de posibles vulnerabilidades que deben atenderse para minimizar los riesgos en la seguridad de la información de las compañías.
- Existen, hoy en día, herramientas integradas en los DBMS o de terceros que pueden aumentar las capacidades de auditoría.

### CONTROL DE LECTURA

#### Parte I. Lea, analice y responda las siguientes preguntas

1. Normalmente la auditoría informática se aplica de dos formas distintas; por un lado, se auditan las principales áreas del departamento de informática y, por otro, se auditan las aplicaciones que funcionan en la empresa.



Falso.



Verdadero.

2. Registrar todos los datos de acceso es un proceso que las empresas pueden tomar como parte de un programa integral para asegurar que sus datos estén seguros.

☐

Falso.

☐

Verdadero.

3. Lo más oportuno es que el auditor, de forma previa a la realización de las entrevistas, prepare un listado de aquellas personas con las que se entrevistará y a las que se les preguntará una serie de cuestiones mediante un check list o formulario elaborado al efecto.

☐

Falso.

☐

Verdadero.

4. No es importante que todas las sentencias de acceso sean auditadas, solo las llamadas de red, porque todas las sentencias van a través de la red.

☐

Falso.

☐

Verdadero.



## CONTROL DE LECTURA

### Parte I. Lea, analice y responda las siguientes preguntas

1. Normalmente la auditoría informática se aplica de dos formas distintas; por un lado, se auditan las principales áreas del departamento de informática y, por otro, se auditan las aplicaciones que funcionan en la empresa.



- ☐ Falso.
- ☒ Verdadero.

2. Registrar todos los datos de acceso es un proceso que las empresas pueden tomar como parte de un programa integral para asegurar que sus datos estén seguros.



- ☐ Falso.
- ☒ Verdadero.

3. Lo más oportuno es que el auditor, de forma previa a la realización de las entrevistas, prepare un listado de aquellas personas con las que se entrevistará y a las que se les preguntará una serie de cuestiones mediante un check list o formulario elaborado al efecto.



- ☐ Falso.
- ☒ Verdadero.

4. No es importante que todas las sentencias de acceso sean auditadas, solo las llamadas de red, porque todas las sentencias van a través de la red.



- ☒ Falso.
- ☐ Verdadero.

## Tema 03: Auditoría de seguridad de los sistemas computacionales.



## INTRODUCCIÓN



La auditoría de seguridad de los sistemas computacionales es la revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado con la seguridad de un sistema computacional, sus áreas, personal, así como a las actividades, funciones y acciones preventivas y correctivas que contribuyan a salvaguardar la seguridad de los equipos computacionales, de las bases de datos, redes, sistemas, instalaciones y usuarios del mismo.

Importancia de la auditoría de seguridad informática.

Permite conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.



### Objetivos de la auditoría de seguridad informática

- Medir la confidencialidad, integridad y disponibilidad de los datos.
- Verificar que la política de seguridad se aplique correctamente y que todas las medidas tomadas conformen un todo coherente.
- Mejorar de forma continua la seguridad de sistemas computacionales mediante la adopción de medidas preventivas y correctivas.

### Tipos de seguridad

### Seguridad física

Se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. Por lo tanto, el auditor informático debe contemplar situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc.

### Seguridad lógica

Se refiere a la seguridad en el uso de software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. Implica también que se debe tener cuidado que no existan copias piratas, o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión de virus.



Los 4 pilares fundamentales para la seguridad de los sistemas computacionales

### PILARES FUNDAMENTALES



Iniciar



### **1) Disponibilidad de la información:**

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

### **2) Integridad de la información:**

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.

Grosso modo, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

### **3) Confidencialidad de la información:**

Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Grosso modo, la confidencialidad es el acceso a la información únicamente por personas que cuenten con la debida autorización.



#### 4) Autenticidad:

Es un modo de asegurar que los usuarios son quienes ellos dicen que son, que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacerlo.

#### Riesgos

Dentro de la seguridad de los sistemas computacionales se lleva a cabo la clasificación de las alternativas para manejar los posibles riesgos que un activo o bien puede tener dentro de los procesos en una empresa. Esta clasificación lleva el nombre de manejo de riesgos. El manejo de riesgos conlleva una estructura bien definida, con un control adecuado y su manejo, habiéndolos identificado, priorizados y analizados, a través de acciones factibles y efectivas. Para ello se cuenta con las siguientes técnicas de manejo del riesgo:

#### TÉCNICAS DE MANEJO DEL RIESGO



Iniciar



### • Evitar

El riesgo es evitado cuando la organización rechaza aceptarlo, es decir, no se permite ningún tipo de exposición. Esto se logra simplemente con no comprometerse a realizar la acción que origine el riesgo. Esta técnica tiene más desventajas que ventajas, ya que la empresa podría abstenerse de aprovechar muchas oportunidades.

#### **Ejemplo:**

*No instalar empresas en zonas sísmicas.*

### • Reducir

Cuando el riesgo no puede evitarse por tener varias dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible. Esta opción es la más económica y sencilla. Se consigue optimizando los procedimientos, la implementación de controles y su monitoreo constante.

#### **Ejemplo:**

*No fumar en ciertas áreas, instalaciones eléctricas anti flama y planes de contingencia.*

### • Retener, asumir o aceptar el riesgo

Es uno de los métodos más comunes del manejo de riesgos, es la decisión de aceptar las consecuencias de la ocurrencia del evento. Puede ser voluntaria o involuntaria, la voluntaria se caracteriza por el reconocimiento de la existencia del riesgo y el acuerdo de asumir las pérdidas involucradas. Esta decisión se da por falta de alternativas. La retención involuntaria se da cuando el riesgo es retenido inconscientemente.

#### **Ejemplo de asumir el riesgo:**

*Con recursos propios se financian las pérdidas.*

## • Transferir

Es buscar un respaldo y compartir el riesgo con otros controles o entidades. Esta técnica se usa ya sea para eliminar un riesgo de un lugar y transferirlo a otro, o para minimizar el mismo, compartiéndolo con otras entidades.

### **Ejemplo:**

*Transferir los costos a la compañía aseguradora.*

### **Fases de una auditoría**

- Enumeración de redes, topologías y protocolos.
- Identificación de sistemas y dispositivos.
- Identificación de los sistemas operativos instalados.
- Análisis de servicios y aplicaciones.
- Detección, comprobación y evaluación de vulnerabilidades.
- Medidas específicas de corrección.
- Recomendaciones sobre implantación de medidas preventivas.

### **Tipos de auditoría de seguridad de los sistemas computacionales**



### **Auditoría de seguridad interna**

- En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.

### **Auditoría de seguridad perimetral**

- En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores.

### **Test de intrusión**

- Es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.

### **Análisis forense**

- Es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperatividad del sistema, el análisis se denomina análisis postmortem.

### **Auditoría de páginas web**

- Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código sql, verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS), etc.

### **Auditoría de código de aplicaciones**

- Análisis del código tanto de aplicaciones de páginas Web como de cualquier tipo de aplicación, independientemente del lenguaje empleado.

Las amenazas en la seguridad de los sistemas computacionales



La auditoría de seguridad evalúa la eficacia de la seguridad instalada y en funcionamiento. Además debe determinarse si el sistema de seguridad contempla todas las amenazas.

Tiende a definir si la seguridad satisface las condiciones necesarias, detectar fallas o problemas y sugerir correcciones o

---

#### Texto del Audio

La auditoría de seguridad evalúa la eficacia de la seguridad instalada y en funcionamiento. Además debe determinarse si el sistema de seguridad contempla todas las amenazas. Tiende a definir si la seguridad satisface las condiciones necesarias, detectar fallas o problemas y sugerir correcciones o cambios en la búsqueda del mejor nivel de protección.

Lista de verificación para auditoría de seguridad de un sistema.

- Seguridad en la protección y conservación de locales, instalaciones, mobiliario y equipos.
- Seguridad para el personal informático y los usuarios del sistema.
- Seguridad en los accesos a las áreas de sistemas, así como a sus sistemas computacionales, información y software.
- Seguridad en los sistemas computacionales y dispositivos periféricos.
- Seguridad en la información institucional y bases de datos.
- Seguridad en los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional.
- Seguridad en los activos informáticos del área de sistemas.
- Seguridad en la arquitectura de las telecomunicaciones.
- Seguridad en los sistemas de redes, sistemas mayores y computadoras.
- Seguridad contra la piratería informática.
- Seguridad contra los virus informáticos.

**Seguridad en los accesos a las áreas de sistemas, así como a sus sistemas computacionales, información y software**





Es necesaria la protección y seguridad de los espacios físicos de las instalaciones donde se albergan los servidores, información institucional, bases de datos, etc. También se deben analizar los planes de contingencias informáticos.

### **Seguridad en la información institucional y bases de datos**

Se recomienda evaluar los siguientes elementos:

#### *Elementos a Evaluar*

- Auditoría de la seguridad en los sistemas computacionales.  
  
Evaluar la seguridad en el procesamiento de información.
- Auditoría de la seguridad del hardware.  
  
Realizar inventarios de hardware, equipos y periféricos asociados.
- Auditoría de la seguridad del software.
  - Realizar inventarios de software, paqueterías y desarrollos empresariales.
  - Evaluar las licencias, contratos, permisos y usos de los sistemas computacionales.
- Auditoría para verificar la captura, procesamiento de datos y emisión de resultados.
  - Evaluar la totalidad, veracidad y confiabilidad de la captura de información.
  - Evaluar la existencia, difusión, aplicación y uso del plan contra contingencias en los sistemas.
- Seguridad contra la piratería informática.
  - Auditoría de la prevención de actos premeditados que afecten el funcionamiento de los sistemas computacionales.
  - Protección contra los actos ilegales en contra de los sistemas, activos informáticos e información.
  - Protección contra mal uso de la información.
  - Protección contra la piratería y robo de información.

- Protección para el almacenamiento de la información.
  - Protección contra actos no intencionales.
  - Protección y seguridad para el desarrollo de programas y proyectos de sistemas.
- Seguridad contra los virus informáticos.
  - Protección y seguridad para los accesos al sistema computacional y a la información.
  - En el uso de contraseñas.
- Protección contra virus informáticos.
  - Uso de vacunas y buscadores de virus.
- Seguridad en los sistemas de redes, sistemas mayores y computadoras.
  - Protección y seguridad del hardware, componentes del sistema, periféricos y equipos asociados.
  - Mantenimiento preventivo y correctivo a la CPU.
  - Mantenimiento preventivo y correctivo al sistema de cómputo.
  - Mantenimiento preventivo y correctivo a los periféricos.
  - Mantenimiento preventivo y correctivo al equipo adicional.
  - Seguridad ante fenómenos sociales.
- Prevención ante cambios tecnológicos.
  - Inventario de las instalaciones físicas, a fin de evaluar la vigilancia y los accesos establecidos para la protección y seguridad de los bienes informáticos del área de sistemas.
  - Inventario del personal informático y usuarios del sistema, a fin de evaluar la protección de este importante recurso.
  - Inventario de las medidas de seguridad y protección para los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, incluyendo sus licencias, resguardos y copias de seguridad.

## **Recopilación de la información organizacional**

Se efectúa una revisión sistematizada del área, a través de los siguientes elementos:

### *Elementos a Evaluar*

1. Revisión de la estructura orgánica
  - Jerarquías (Definición de la autoridad lineal, funcional y de asesoría).
  - Estructura orgánica.
  - Funciones
2. Objetivos
  - Se deberá revisar la situación del recurso humano.

- Entrevistas con el personal de Informática.
    - a. Jefatura.
    - b. Análisis.
    - c. Programadores.
    - d. Operadores.
    - e. Personal de bases de datos.
    - f. Personal de comunicaciones y redes.
- 3. Conocer la situación en cuanto a:
  - Presupuesto.
    - Recursos financieros.
    - Recursos materiales.
    - Mobiliario y equipo.
    - Costos.
- 4. Elaborar un censo de recursos humanos y análisis de situación en cuanto a:
  - Número de personas y distribución por área.
    - Denominación de puestos.
    - Salario y conformación del mismo (prestaciones y adiciones).
    - Capacitación (actual y programa de capacitación).
    - Escolaridad.
    - Experiencia profesional.
    - Antigüedad (en la organización, en el puesto y en puestos similares fuera de la organización).
    - Historial de trabajo.
    - Índice de rotación.
- 5. Revisar el grado de cumplimiento de los documentos administrativos
  - Organización.
    - Normas y políticas.
    - Planes de trabajo.
    - Controles.
    - Estándares.
    - Procedimientos.

**Esta información nos servirá para determinar:**

- ❖ Si las responsabilidades en la organización están definidas adecuadamente.
- ❖ Si la estructura organizacional es adecuada a las necesidades.
- ❖ Si el control organizacional es el adecuado.
- ❖ Si se tienen los objetivos y políticas adecuadas, si están vigentes y si están bien definidas.
- ❖ Si existe la documentación de las actividades, funciones y responsabilidades.
- ❖ Si los puestos se encuentran definidos y señaladas sus responsabilidades.
- ❖ Si el análisis y descripción de puestos está acorde con el personal que los ocupa.
- ❖ Si se cumplen los lineamientos organizacionales.
- ❖ Si el nivel de salarios está de acuerdo con el mercado de trabajo.
- ❖ Si se tienen programas de capacitación adecuados y si se cumple con ellos.
- ❖ Si los planes de trabajo concuerdan con los objetivos de la empresa.
- ❖ Si se cuenta con el recurso humano necesario para garantizar la continuidad de la operación o si se cuenta con los "indispensables".
- ❖ Si se evalúan los planes y se determinan las desviaciones.
- ❖ Si se cumple con los procedimientos y controles administrativos.

Una forma de evaluar la forma en que se está desempeñando la gerencia de informática es mediante la evaluación de las funciones a realizar:

<b>Planeación:</b>	Determinar los objetivos del área y la forma en que se van a lograr estos objetivos.
<b>Organización:</b>	Proveer de las facilidades, estructura, división del trabajo, responsabilidades, actividades de grupo personal necesario para realizar las metas.
<b>Recursos Humanos:</b>	Seleccionando, capacitando, y entrenando al personal requerido para realizar las metas.
<b>Dirección:</b>	Coordinando las actividades, proveyendo liderazgo y guía, y motivando al personal.
<b>Control:</b>	Comparando lo real contra lo planeado, como base para realizar los ajustes necesarios.

### *Aspectos técnicos puntuales en la auditoría de seguridad de los sistemas computacionales*

- Política de seguridad informática:  
Se realiza una revisión de la política de seguridad actual, alcance de la política, objetivos, responsabilidades de los intervinientes, riesgos informáticos, etc.
- Análisis de riesgos:  
Qué se necesita proteger, de quién protegerlo y cómo protegerlo.  
Se establecerá según el perfil de la empresa, la estimación del riesgo de pérdida del recurso y la importancia del mismo para desempeñar su principal función.
- Análisis de red:  
Revisión de los elementos que conforman su red, junto con la disposición lógica de los mismos, tráfico de red y sistemas expuestos.
- Análisis de control y accesos:  
Se analizarán los distintos registros sobre conexiones e intentos de conexión sobre los elementos que participan en las funciones de la empresa, intentos de ataques, tráfico de red, etc.
- Análisis de integridad:  
Chequeo de los archivos más importantes de sus sistemas, análisis de modificaciones no deseadas y prevención.

### *Aspectos técnicos puntuales en la auditoría de seguridad de los sistemas computacionales*

- Revisión de sistemas críticos:  
Se analizarán los distintos servidores o sistemas críticos que posee su empresa con base al perfil y a la actividad principal de la misma.
- Revisión de estaciones de trabajo:  
Se analizarán terminales de trabajo de usuarios simples, para establecer una calificación de seguridad de usuarios.
- Calificación de la empresa:  
Se establecerá una calificación de cómo se encuentra la seguridad informática dentro de su empresa, esta será una suma de los distintos análisis efectuados y según la actividad principal de la misma.
- Propuestas e impactos de una PSI:  
Se establecerán propuestas para mejorar la seguridad de su empresa mediante la actualización de su política de seguridad informática, de poseerla, o se establecerá la adecuada para su organización. Se presentarán soluciones para afianzarla.
- Implementación de la PSI (Políticas de Seguridad Informáticas):  
Cómo se implementan las medidas y soluciones para maximizar el nivel de seguridad.

### **Disposiciones que acompañan la seguridad**

- Obtener una especificación de las aplicaciones, los programas y archivos de datos.
- Medidas en caso de desastre como pérdida total de datos, abuso y los planes necesarios para cada caso.
- Prioridades en cuanto a acciones de seguridad de corto y largo plazo.

- Verificar el tipo de acceso que tienen las diferentes personas de la organización, cuidar que los programadores no cuenten con acceso a la sección de operación y viceversa.

Adquirir tecnologías repelentes o protectoras:



Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

#### **Recomendaciones generales**



- ❖ Elija un asesor técnico capacitado.
- ❖ Educar a los empleados sobre el correcto uso de los equipos y del software.
- ❖ Mantener respaldos de todo el software relacionado con el sistema operativo.
- ❖ Mantener respaldos de toda su información crítica.
- ❖ Mantener y reforzar sus políticas corporativas de seguridad informática.
- ❖ Instalar software adecuado para prevenir eventuales ataques.
- ❖ Definir y controlar permanentemente los mecanismos de defensa.
- ❖ Asegurarse que los sistemas de auditoría estén funcionando.
- ❖ Mantener un aviso o banner en su sistema para notificar a usuarios no autorizados que podrían ser objeto de monitoreo.
- ❖ Pruebe periódicamente su red en busca de vulnerabilidades.
- ❖ Obligue a sus usuarios al cambio periódico de claves de acceso.
- ❖ Cancelar todas las claves de acceso de empleados que dejen la empresa por cualquier motivo.
- ❖ Mantener permanentemente actualizado su software antivirus.
- ❖ Restringir y monitorear el acceso de las computadoras a sus servidores internos.
- ❖ Utilice herramientas que controlen el acceso remoto a su red. En lo posible no use dicho tipo de acceso.
- ❖ Considere establecer un equipo que responda ante emergencias o mantenga contacto con organismos o empresas que presten dicho tipo de servicio.
- ❖ Desarrolle un plan corporativo de respuesta ante incidentes de seguridad.

## CONTROL DE LECTURA

### Parte I. Lea, analice y responda las siguientes preguntas

1. En la auditoría de seguridad interna, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores.



Falso.



Verdadero.

2. Es necesaria la protección y seguridad de los espacios físicos de las instalaciones donde se albergan los servidores, información institucional, bases de datos, etc.



Falso.



Verdadero.

3. Inyección de SQL es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados.



Falso.



Verdadero.

4. Dentro de la seguridad física se lleva a cabo la clasificación de las alternativas para manejar los posibles riesgos que un activo o bien puede tener dentro de los procesos en una empresa.



Falso.



Verdadero.



## CONTROL DE LECTURA

### Parte I. Lea, analice y responda las siguientes preguntas

1. En la auditoría de seguridad interna, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores.

- ☒ Falso.
- ☐ Verdadero.



2. Es necesaria la protección y seguridad de los espacios físicos de las instalaciones donde se albergan los servidores, información institucional, bases de datos, etc.

- ☐ Falso.
- ☒ Verdadero.



3. Inyección de SQL es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados.

- ☒ Falso.
- ☐ Verdadero.



4. Dentro de la seguridad física se lleva a cabo la clasificación de las alternativas para manejar los posibles riesgos que un activo o bien puede tener dentro de los procesos en una empresa.

- ☒ Falso.
- ☐ Verdadero.



## Tema 04: Auditoría de los sistemas de red.

## INTRODUCCIÓN



Las redes de computadoras son un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que transportan datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Como en todo proceso de comunicación se requiere de un emisor, un mensaje, un medio y un receptor.

La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información, asegurar la

### Generalidades

El acelerado crecimiento de la tecnología conlleva también el crecimiento de nuevos peligros.

Ahora también las infracciones desde dentro de una empresa en algunos casos son incluso, producidas por los propios empleados, y contra las cuales las organizaciones son más vulnerables.

Para el informático y para el auditor informático, el concepto que constituyen las redes no son sino el soporte físico-lógico donde viaja la información.

El auditor informático tendrá la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, por tanto, requiere un equipo de especialistas.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del hardware y de los soportes de datos, redes, así como a la de los edificios e instalaciones que los albergan. La seguridad lógica se refiere a la

seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

## **Auditoría de sistemas de red**

La auditoría de los sistemas de red es una serie de mecanismos mediante los cuales se pone a prueba una red informática, evaluando su desempeño y seguridad, a fin de lograr una utilización más eficiente y segura de la información.

El primer paso para iniciar una gestión responsable de la seguridad es identificar la estructura física (hardware, topología) y lógica (software, aplicaciones) del sistema (sea un equipo, red e intranet), y hacerle un análisis de vulnerabilidad para saber en qué grado de exposición nos encontramos; así, hecha esta "radiografía" de la red, se procede a localizar sus fallas más críticas, para proponer una estrategia de solución de los mismos; un plan de contención o blindaje ante posibles incidentes y un seguimiento continuo del desempeño del sistema.



**La auditoría de los sistemas de red ofrece una auditoría rigurosa y un análisis de sus redes actuales, con el fin de crear una base sólida para el posterior diseño de red y para proyectos de despliegue.**

**La auditoría presenta con toda precisión, asuntos clave relacionados con la red, cómo el lugar en el que las nuevas**

### **Texto del Audio**

La auditoría de los sistemas de red ofrece una auditoría rigurosa y un análisis de sus redes actuales, con el fin de crear una base sólida para el posterior diseño de red y para proyectos de despliegue.

La auditoría presenta con toda precisión, asuntos clave relacionados con la red, cómo el lugar en el que las nuevas aplicaciones empresariales generarán nuevas demandas de red. Ofrecen una imagen precisa de la capacidad de la red para hacer frente a las necesidades empresariales actuales, y de su grado de preparación para los crecientes requisitos del futuro.

La auditoría de sistemas de red ofrecen una clara imagen de tres áreas cruciales:

- Puntos de acción derivados de nuevas aplicaciones empresariales.
- Valoración del riesgo y comparación del coste con respecto a las ventajas.
- Revisión de las inversiones en red en la organización desde el punto de vista empresarial.

Una auditoría de sistemas de red no se limita a un análisis de la infraestructura física de red y sistemas operativos, su diseño es específico para cada empresa y tiene en cuenta aspectos que incluyen técnicas de control de funcionamiento, suministro de información, medidas de seguridad y análisis de coste y riesgo.

### Objetivos de la auditoría de los sistemas de red



### Ventajas

La auditoría de los sistemas de red ayuda a identificar gastos encubiertos mediante un inventario rápido y preciso. Un sólido servicio de gestión de activos con el fin de optimizar los niveles de servicio y de dotación de personal, y de reducir costes.

La auditoría de los sistemas de red le ofrece las herramientas necesarias para

### Texto del Audio

La auditoría de los sistemas de red ayuda a identificar gastos encubiertos mediante un inventario rápido y preciso. Un sólido servicio de gestión de activos con el fin de optimizar los niveles de servicio y de dotación de personal, y de reducir costes.

La auditoría de los sistemas de red le ofrece las herramientas necesarias para determinar la eficacia con que su red respalda sus operaciones empresariales y el grado de satisfacción del cliente sin que influyan cuestiones políticas internas.

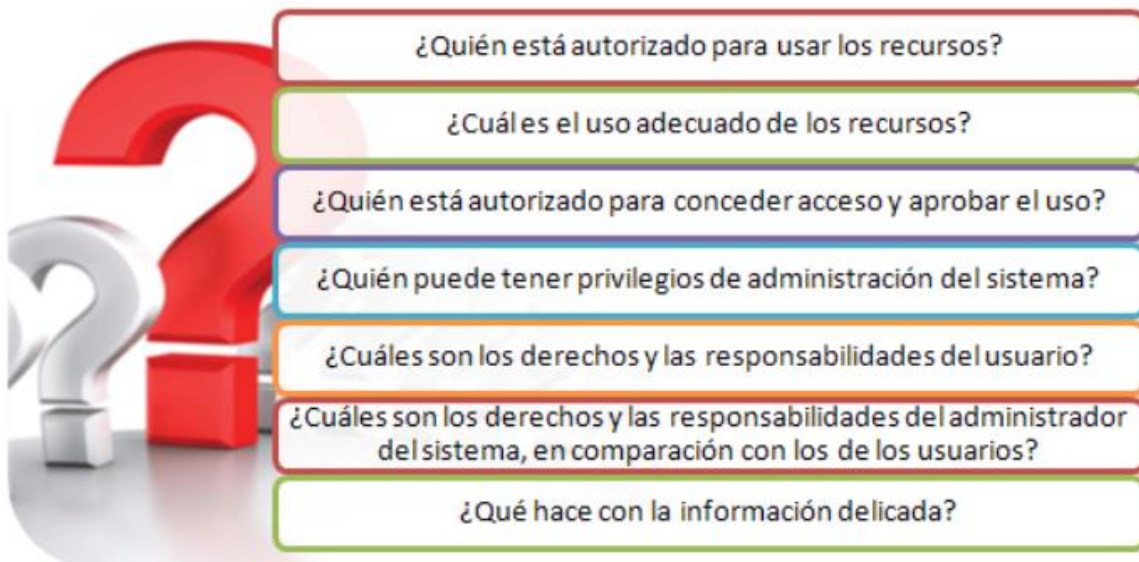
Si hay mayor productividad, hay que mejorar el funcionamiento de la red, identificando los problemas, aislando los errores para proceder a su eliminación.

La auditoría de sistemas de red permite la planificación anticipada de los sistemas TI realizando un seguimiento permanente de las tendencias de red e identificando las oportunidades.

La auditoría de sistemas de red permite realizar una evaluación del perímetro de seguridad de red y de la seguridad central interna con el objetivo de conocer si la red está preparada para las nuevas comunicaciones y aplicaciones.

### **Elaboración de políticas de red**

El primer paso es investigar el uso y responsabilidades de la red, lo cual permitirá que pueda abordarse la elaboración de una política de seguridad. Algunas de las preguntas pueden ser las siguientes:





## POLÍTICAS DE RED



## POLÍTICAS DE RED

Debe hacerse una lista de los usuarios que necesitan acceso a los recursos de la red. No es necesario enlistar a cada usuario. La mayoría de estos pueden dividirse en grupos como usuarios de contabilidad, docentes, estudiantes y personal administrativo.

También debe tomarse en cuenta una clase llamada usuarios externos, esta se compone de los usuarios que tengan acceso a la red desde otras ubicaciones los cuales pueden no ser empleados, o bien, pueden ser empleados que tengan acceso a la red desde sus hogares o durante un viaje.

## POLÍTICAS DE RED

Una vez determinados los usuarios autorizados a tener acceso a los recursos de la red, se deben establecer los lineamientos del uso aceptable de dichos recursos. Los lineamientos dependen de la clase de usuarios, como desarrolladores de software, estudiantes, profesores y usuarios externos.

La política debe establecer cuál tipo de uso es aceptable y cuál es inaceptable, así como cuál tipo de uso está restringido.

La política que la auditoría de sistemas de red permitirá elaborar es la "Política de uso aceptable de la red".

Si el acceso a un recurso de la red está restringido, debe considerar el nivel de acceso que tendrá cada tipo de usuario.

## POLÍTICAS DE RED

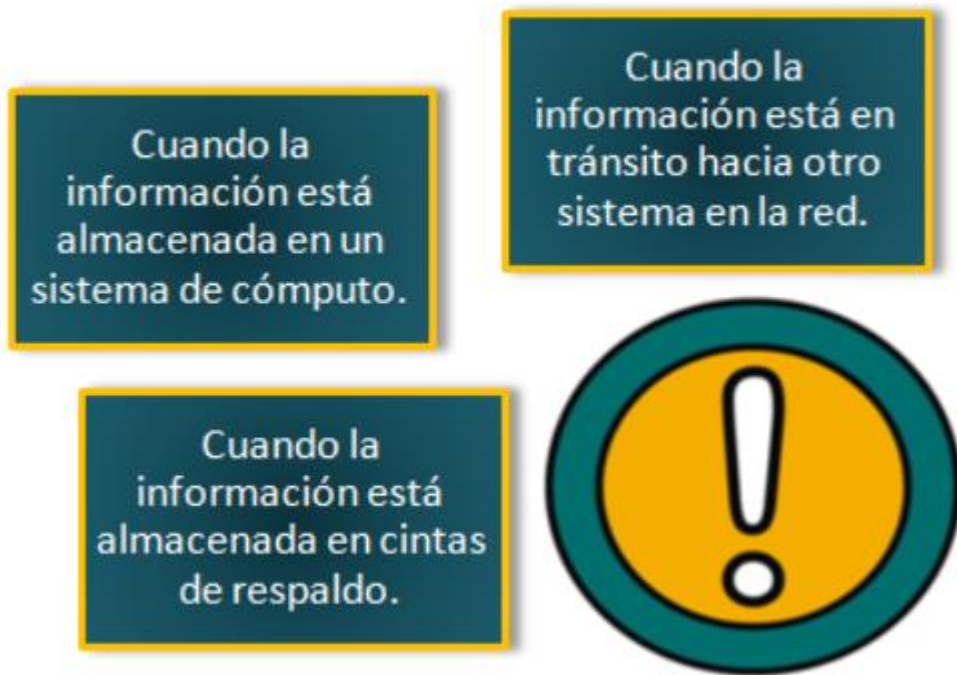
Es necesario crear procedimientos que permitan capacitar fácilmente a futuros administradores de sistemas acerca de las peculiaridades de un sistema determinado.

Por ejemplo, la creación de un procedimiento de creación de cuentas de usuario que debe ser sencillo y fácil de entender.

Esto asegura que se cometen menos errores y que sea más probable que lo sigan los administradores del sistema.

Un concepto importante en la auditoría de sistemas de red es la confidencialidad, la cual se define como mantener las cosas ocultas o secretas. Esta es una consideración muy importante para varios tipos de datos delicados.

La información es vulnerable de ser divulgada:



La información en tránsito puede protegerse mediante la encriptación o los Gateway de las firewalls. La encriptación puede usarse para proteger la información en las tres situaciones. El acceso a la información almacenada en cintas puede controlarse mediante la seguridad física, como puede ser guardar las cintas en una caja de seguridad o en un área inaccesible.

El acceso a la información que está almacenada en una computadora deberá de estar controlada mediante los permisos de archivo, las listas de control de acceso y otros mecanismos similares.

La auditoría de sistemas de red permite ofrecer un mecanismo de resistencia a la entrada de intrusos en la red. Además de recomendar sistemas como firewall puede usarse hardware como routers.

Una organización podría necesitar conexiones con sus demás sitios a través de redes grandes como Internet, por lo que es necesario implementar mecanismos de seguridad y políticas.

La auditoría debe documentar cómo restringir el acceso a una red externa a través de un solo sistema.

Texto del Audio

Una organización podría necesitar conexiones con sus demás sitios a través de redes grandes como Internet, por lo que es necesario implementar mecanismos de seguridad y políticas.

La auditoría debe documentar cómo restringir el acceso a una red externa a través de un solo



sistema.

Toda la protección de las conexiones de los sistemas de redes, no solamente puede ser protegida con sistemas en restricciones, la auditoría de sistemas de red debe garantizar en sus documentos que la empresa tenga que concientizar a los usuarios de proteger los sistemas de la red corporativa.

### Capas del modelo de red más utilizado

Las capas con las cuales se puede explicar cómo funcionan las redes, están dentro del modelo OSI, modelo de interconexión de sistemas abiertos, las cuales se explican brevemente a continuación:

**Nivel Aplicación:** proporciona servicios al usuario del Modelo OSI.

**Nivel Presentación:** traduce el formato y asignan una sintaxis a los datos para su transmisión en la red.

**Nivel Sesión:** proveer los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos.

**Nivel de Transporte:** este nivel actúa como un puente entre los tres niveles inferiores totalmente orientados a las comunicaciones y los tres niveles superiores totalmente orientados al procesamiento. Además, garantiza una entrega confiable de la información.

**Nivel de Red:** este nivel define el enrutamiento y el envío de paquetes entre redes.

**Nivel Enlace de Datos:** este nivel proporciona facilidades para la transmisión de bloques de datos entre dos estaciones de red. Esto es, organiza los 1's y los 0's del Nivel Físico en formatos o grupos lógicos de información.

**Nivel Físico:** define el medio de comunicación utilizado para la transferencia de información, dispone del control de este medio y especifica bits de control.

### Test de Penetración

Esta línea de negocio es un método de evaluación del estado de la seguridad de una red o un servidor, y consiste en realizar pruebas de intrusión, donde el analista busca ganar acceso al sistema, escalar privilegios, probar el ingreso real al sistema y, posteriormente, borrar los rastros de la intrusión.

Las pruebas se realizan de forma interna y externa, teniendo como criterio primordial la ética profesional del analista, y brindando garantías a nuestros clientes, de absoluta reserva y confidencialidad en el tratamiento de la información que contiene las vulnerabilidades de

seguridad identificadas. Dentro de esta línea de negocio, se pueden encontrar los siguientes productos:



La ética hacker es una nueva ética surgida de y aplicada a las comunidades virtuales o cibercomunidades, aunque no exclusivamente. La expresión se suele atribuir al periodista Steven Levy en su ensayo seminal *Hackers: Heroes of the Computer Revolution*, publicado en 1984, donde describe y enuncia con detalle los principios morales que surgieron a finales de los años 50 en el Laboratorio de Inteligencia Artificial del MIT y, en general, en la cultura de los aficionados a la informática de los años 60 y 70. Aquellos principios que se resumen en el acceso libre a la información y en que la informática puede mejorar la calidad de vida de las personas han constituido la base de la mayor parte de definiciones que se han elaborado posteriormente. Uno de sus mentores actuales ha sido el finlandés Pekka Himanen.

### Top 10 de las vulnerabilidades internas de las redes

#### 1. Los lectores USB

La ubiquidad de estos lectores ha llevado a los hackers a desarrollar malware específico como el conocido gusano Conficker, que se ejecuta de forma automática al conectar la llave al USB. Este problema se intensifica con las configuraciones por defecto de muchos sistemas operativos que ejecutan automáticamente la mayoría de los programas (incluyendo los maliciosos). Aconsejamos cambiar las políticas de autorun que vengan por defecto en la computadora. He aquí los pasos a seguir para un entorno Windows: <http://support.microsoft.com/kb/967715>

#### 2. Portátiles y Netbooks

Todas las compañías tienen información sensible que no debe salir de sus oficinas.

Esto se convierte en un peligro cuando la información está almacenada en un portátil no seguro. A menos que el portátil utilice un algoritmo de encriptación, los datos pueden ser recuperados por cualquiera. La solución: Implemente un sistema de archivado encriptado para los datos sensibles. Hay una amplia oferta de este tipo de soluciones, como la open source TrueCrypt. El control de end points que entran y salen del sistema interno es también importante.

3. Puntos de Acceso inalámbrico (APs)

Los ataques a redes inalámbricas realizados por Wardrivers son comunes y han causado graves daños. Por ejemplo, TJ Stores, propietario de Marshalls y TJMaxx, sufrió un ataque a través de este método; los intrusos penetraron en las computadoras de su oficina en los que se guardaba datos de transacciones de sus clientes como la tarjeta de crédito, de débito y cheques. Este ataque supuso para la compañía un coste de más de 500 millones de dólares. El protocolo de encriptación inalámbrica (WEP) contiene conocidas vulnerabilidades que se ven afectadas por ataques como Aircrack. Otros protocolos más robustos como el acceso inalámbrico protegido (WPA) y WPA2 son todavía propensos a sufrir ataques si no se utilizan unas claves seguras. Se recomienda usar el WPA2 Enterprise con RADIUS junto con un AP capaz de ofrecer autenticación y reforzar las medidas de seguridad.

4. Variedad de dispositivos USB

Si un end point puede leer y ejecutar datos desde un dispositivo, puede presentar tanto peligro como un pendrive. Tal es el caso de cámaras digitales, reproductores de MP3 e incluso, marcos digitales. En 2008, Best Buy declaró que habían encontrado un virus en los marcos de fotos Insignia que procedían directamente del fabricante. La solución es reforzar el control y las políticas de activos sobre qué y cuándo pueden estos dispositivos acceder al sistema.

5. Conexiones internas

Los empleados de una compañía pueden acceder, accidental o premeditadamente, a áreas de la red corporativa a las que no deberían tener acceso. Se deben cambiar las claves regularmente y cumplir con las políticas de autenticación y acceso.

6. El troyano humano

El troyano humano se adentra en la empresa camuflado, de hombre de negocios, con un modo de operario y en menos de un minuto puede infectar la red corporativa desde la sala de servidores. Hay que recordar a los empleados que deben pedir las autorizaciones a personas ajenas a la organización identificándoles.

7. Medios ópticos

Al igual que con los dispositivos USB que mencionábamos antes, es importante implementar y reforzar el control y las políticas de acceso respecto a los dispositivos que pueden acceder a la red como los CDs.

8. La mente prodigiosa

Además de estas medidas para mitigar las posibles amenazas que supone la tecnología digital, no debemos olvidar que la mente humana es una gran base de datos, ¿quién te observa mientras tecleas tus claves en la computadora? La mejor

salvaguardia es ser consciente y estar alerta de cualquier amenaza siempre que estemos manejando información sensible.

9. Smartphones y otros dispositivos digitales

Estos nuevos dispositivos presentan las mismas amenazas que los portátiles y las llaves USB. La importancia de estos dispositivos radica en su potencialidad para eludir las soluciones DLP tradicionales. Aplique las mismas reglas que a los dispositivos USB y medios ópticos.

10. Email  
Los emails pueden ser en sí mismos un foco de infección. Un correo electrónico es capaz de sustraer las credenciales de acceso de un empleado. Este robo puede ser utilizado para futuros ataques. En el caso de la seguridad del correo electrónico, identificar la fuente es clave. Podemos conocer quién es el emisor utilizando tecnología PGP o con unas cuantas preguntas antes de enviarle información sensible. Se debe reforzar el control de los accesos a las direcciones de alias así como recordar a los empleados las políticas de seguridad de la compañía.

## Conclusión

Toda empresa, que posea sistemas de red e información sin importar la complejidad de los mismos, deben de someterse a un control estricto de evaluación de eficacia y eficiencia. Hoy en día, un alto porcentaje de las empresas tienen toda su información estructurada en sistemas de redes informáticos, por tal razón la importancia que los sistemas de

### Texto del Audio

Toda empresa, que posea sistemas de red e información sin importar la complejidad de los mismos, deben de someterse a un control estricto de evaluación de eficacia y eficiencia. Hoy en día, un alto porcentaje de las empresas tienen toda su información estructurada en sistemas de redes informáticos, por tal razón la importancia que los sistemas de información funcionen correctamente.

En cuanto al trabajo de la auditoría, se puede remarcar que se precisa de gran conocimiento de informática, seriedad, capacidad, minuciosidad y responsabilidad; la auditoría de sistemas de redes debe hacerse por gente altamente capacitada, una auditoría mal realizada puede tener consecuencias para la empresa auditada, principalmente económicas.

## CONTROL DE LECTURA

### Parte I. Lea, analice y responda las siguientes preguntas

1. No es importante implementar y reforzar el control y las políticas de acceso respecto a los dispositivos que pueden acceder a la red como los CDs.



Falso.



Verdadero.

2. La auditoría de sistemas de red debe garantizar en sus documentos que la empresa tenga que concientizar a los usuarios de proteger los sistemas de la red corporativa.



Falso.



Verdadero.

3. El primer paso para iniciar una gestión responsable de la seguridad es identificar la estructura física y lógica del sistema.



Falso.



Verdadero.

4. La auditoría de sistemas de red permite la planificación anticipada de los sistemas TI realizando un seguimiento permanente de las tendencias de red e identificando las oportunidades.



Falso.



Verdadero.

## CONTROL DE LECTURA

### Parte I. Lea, analice y responda las siguientes preguntas

1. No es importante implementar y reforzar el control y las políticas de acceso respecto a los dispositivos que pueden acceder a la red como los CDs.

- ☒ Falso.  
☐ Verdadero.



2. La auditoría de sistemas de red debe garantizar en sus documentos que la empresa tenga que concientizar a los usuarios de proteger los sistemas de la red corporativa.

- ☐ Falso.  
☒ Verdadero.



3. El primer paso para iniciar una gestión responsable de la seguridad es identificar la estructura física y lógica del sistema.

- ☐ Falso.  
☒ Verdadero.



4. La auditoría de sistemas de red permite la planificación anticipada de los sistemas TI realizando un seguimiento permanente de las tendencias de red e identificando las oportunidades.

- ☐ Falso.  
☒ Verdadero.

