FORMULACIÓN DE CRITERIOS DE EVALUACIÓN PARA REALIZAR AUDITORÍAS A SISTEMAS DE INFORMACIÓN WEB.

JOHANNA KARINA GARCIA RESTREPO

ERICK JOSE RODRIGUEZ SARMIENTO

CORPORACION UNIVERSITARIA DE LA COSTA

POSTGRADOS

AUDITORIA DE SISTEMAS DE INFORMACION

BARRANQUILLA

2010

FORMULACIÓN DE CRITERIOS DE EVALUACIÓN PARA REALIZAR AUDITORÍAS A SISTEMAS DE INFORMACIÓN WEB.

Monografía para optar al título de
Especialista en Auditoria de Sistemas de Información

JOHANNA KARINA GARCIA RESTREPO
ERICK JOSE RODRIGUEZ SARMIENTO

CORPORACION UNIVERSITARIA DE LA COSTA
POSTGRADOS
AUDITORIA DE SISTEMAS DE INFORMACION
BARRANQUILLA
2010

Aprobada por el profesorado de la división de postgrados en cumplimiento de los requisitos exigidos para otorgar El título de Especialista en Auditoría de Sistemas de Información.

_____

Ing. Víctor Montaño
Director Postgrado

_____

Jesid Pacheco
Evaluador

_____

Osvaldo Puello
Asesor Técnico

_____

Manuel Sarmiento
Asesor Metodológico

AGRADECIMIENTOS

Johanna García Restrepo expresa su agradecimiento a:

Dios por siempre llevarme por el camino correcto, a mis padres por apoyarme, a los docentes por su valiosa orientación, dedicación, sugerencias y apoyo en cada uno de los pasos dados a lo largo del desarrollo de este proyecto.

DEDICATORIA

Johanna García Restrepo dedica este proyecto a:

Dios por guiarme,
A mis padres,
A mis compañeros,
Al cuerpo docente por su orientación,
A todas las personas involucradas
en el logro de este objetivo.

AGRADECIMIENTOS

Erik Rodríguez Sarmiento expresa su agradecimiento a:

Dios, porque es él quien guía mi camino.
A mis padres por su confianza y apoyo incondicional.
A mi novia por su colaboración y apoyo.
A mi familia, que siempre a creído en mi.
A mis profesores, que compartieron su conocimiento e hicieron de este proyecto una realidad.

DEDICATORIA

Erik Rodríguez Sarmiento dedica este proyecto a:

Todas esas personas que siempre creyeron en mí y me han brindado todo su apoyo.

CONTENIDO

INTRODUCCION

El interés actual de las empresas está impulsado por la búsqueda de la eficiencia y eficacia para lograr un incremento en la efectividad de los grupos de trabajo que la conforman. Las empresas actualmente se benefician de la flexibilidad y rapidez de la Intranet, como un sistema de información que interactúa en tiempo real y optimiza la toma de decisiones, esto debido al uso creciente del Internet; actualmente las compañías permiten a sus clientes, empleados, socios y proveedores acceder a sus sistemas de información. Por lo tanto, es fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios con el fin de proteger la información.

El interés de este grupo se centra en desarrollar un proyecto de investigación encaminado a establecer y diseñar criterios de evaluación para la auditoría a sistemas de información web, aplicado a la realización de auditorías de sistemas a empresas que tengan implementado algún sistema de información.

1. TEMA

Auditoría de Sistemas, aplicada a sistemas de información web.

2. TITULO

Formulación de criterios de evaluación para realizar auditorías a sistemas de información web.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 Identificación y descripción del problema

En las empresas de hoy en día, el intercambio de información es parte fundamental en la consecución de los objetivos del negocio, por tal motivo el manejo de la información se hace indispensable a la hora de mantener la continuidad.

Por tal motivo surge la necesidad de realizar un proyecto que incluya las pautas realmente importantes al momento de auditar un sistema de información, con el fin que cumplan con todas las normas y requerimientos necesarios para el manejo de la información de la forma más segura posible. Esto se realizara implementando una serie de guías que permitan agilizar y puntualizar el proceso de auditoría y no divagar en procesos innecesarios.

Además de la falta de conocimiento por parte de los profesionales que laboran en TI con respecto a la implementación y manejo de la seguridad de los sistemas de información y la falta de interés de la alta gerencia con todo lo referente a la seguridad de los sistemas de información, es necesario establecer criterios de evaluación apropiados para realizar una auditoría a sistemas de información web e implementarlo de una manera rápida y eficiente que cumpla con las expectativas de un sistema de información seguro.

3.2 Formulación del problema

¿Qué criterios de evaluación mínimos hay que tener en cuenta para realizar una auditoría de un sistema de información web de una empresa?

4. JUSTIFICACION

El interés actual de las compañías está impulsado por la búsqueda de la eficiencia y eficacia para lograr un incremento en la efectividad de los grupos de trabajo e investigación que los conforman. Estas empresas actualmente se benefician de la flexibilidad y rapidez de los Sistemas de información, como un conjunto que interactúa en tiempo real y optimiza la toma de decisiones.

El aspecto fundamental de este trabajo está relacionado con el interés por el manejo de los sistemas de información web, su confiabilidad, integridad y concientización en la transferencia de los datos sensibles de la compañía. Además desarrollará una efectiva metodología encaminada en suministrar guías de apoyo de acuerdo a un modelo implementado con Cobit y Owasp, con estas soluciones un auditor de sistema podrá ejecutar una auditoria a cualquier sistema de información y emitir las recomendaciones adecuadas para el mejoramiento del mismo, este proyecto servirá de apoyo a los directivos en la racionalización, administración, normalización y control de la información en sus cuatro fases: generación, tramitación, almacenamiento y conservación.

5. OBJETIVOS

5.1 Objetivo general

Formular criterios de evaluación para realizar auditorías a sistemas de información web.

5.2 Objetivos específicos

- ✓ Identificar las políticas básicas de seguridad y mantenimiento de los sistemas de información web y su plataforma.

- ✓ Definir los criterios de evaluación básicos realizar la auditoria a sistemas de información web.

- ✓ Especificar las normas básicas para la aplicación de auditorías a sistemas de información web y su plataforma.

- ✓ Especificar los controles básicos para la elaboración de guías de auditorías sistemas de información web.

6. MARCO DE REFERENCIAL

6.1 MARCO TEÓRICO

Para el desarrollo y soporte de este proyecto se investigó en fuentes tanto escritas como digitales, a continuación se detallan algunos conceptos básicos y se fundamenta este proyecto.

6.1.1 Sistema de información[1].

El término sistemas de información hace referencia a un concepto genérico que tiene diferentes significados según el campo del conocimiento al que se aplique dicho concepto, a continuación se enumeran algunos de dichos campos y el sentido concreto que un Sistema de Información tiene en ese campo:

- En informática, un sistema de información es cualquier sistema o subsistema de equipo de telecomunicaciones o computacional interconectados y que se utilicen para obtener, almacenar, manipular, administrar, mover, controlar, desplegar, intercambiar, transmitir o recibir voz y/o datos, e incluye tanto los programas de computación ("software" y "firmware") como el equipo de cómputo.
- En teoría de sistemas, un sistema de información es un sistema, automatizado o manual, que abarca personas, máquinas, y/o métodos organizados de recolección de datos, procesamiento, transmisión y diseminación de datos que representa información para el usuario.

[1]Análisis y diseño estructurado y orientado a objetos de sistemas informáticos, Autor Antonio Amescua, Editorial Mcgraw Hill

- En seguridad computacional, un sistema de información está descrito por tres componentes:

  - Estructura:

✓ Repositorios, que almacenan los datos permanente o temporalmente, tales como "buffers", RAM (memoria de acceso aleatorio), discos duros, caché, etc.

✓ Interfaces, que permiten el intercambio de información con el mundo no digital, tales como teclados, altavoces, monitores, escáneres, impresoras, etc.

✓ Canales, que conectan los repositorios entre sí, tales como "buses", cables, enlaces inalámbricos, etc. Una red de trabajo es un conjunto de canales físicos y lógicos.

  - Comportamiento:

✓ Servicios, los cuales proveen algún valor a los usuarios o a otros servicios mediante el intercambio de mensajes.

✓ Mensajes, que acarrean un contenido o significado hacia los usuarios o servicios.

  - En sociología los sistemas de información son sistemas sociales cuyo comportamiento está fuertemente influenciado por los objetivos, valores y creencias de los individuos y grupos, así como por el desempeño de la tecnología.

6.1.2 Sistema de información web[2].

Los Servicios Web proveen un marco para la aplicación basada en estándares del paradigma SOC, definiendo mecanismos estandarizados para describir, publicar/localizar e interactuar con aplicaciones en línea. Pero más allá de la idea básica de “describir, publicar, interactuar”, es necesario contar con mecanismos para la composición de servicios que permitan definir aplicaciones más complejas a partir de servicios básicos. Sin embargo, aunque el diseño e implementación de un servicio web resulta una tarea bastante simple, no se puede decir lo mismo del diseño y la implementación de los procesos de negocio. El modelado de negocio es una parte esencial del procesos de desarrollo de software que permite entender y describir los procesos de negocio implicados en el domino de aplicación. Sin embargo, pasar del modelado de procesos de negocio de alto nivel, realizado generalmente por los analistas o administradores del negocio y a menudo desde un punto de vista económico, a un lenguaje de composición que implemente dichos procesos a través de servicios web, no es una tarea sencilla.

6.1.3 Bases de datos[3]

El término de bases de datos fue escuchado por primera vez en 1963, en un simposio celebrado en California, USA. Una base de datos se puede definir como un conjunto de información relacionada que se encuentra agrupada ó estructurada.

---

[2] "http://www.kybeleconsulting.com/downloads/VDECASTRO_DesarrolloWebOrientadoServicios.pdf

[3]http://www.maestrosdelweb.com/
Introducción a los sistemas de bases de datos.
Fundamentos de Sistemas de Bases de Datos.

Desde el punto de vista informático, la base de datos es un sistema formado por un conjunto de datos almacenados en discos que permiten el acceso directo a ellos y un conjunto de programas que manipulen ese conjunto de datos.

Cada base de datos se compone de una o más tablas que guarda un conjunto de datos. Cada tabla tiene una o más columnas y filas. Las columnas guardan una parte de la información sobre cada elemento que queramos guardar en la tabla, cada fila de la tabla conforma un registro.

Se define una base de datos como una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.

6.1.3.1 Características

Entre las principales características de los sistemas de base de datos podemos mencionar:

- Independencia lógica y física de los datos.
- Redundancia mínima.
- Acceso concurrente por parte de múltiples usuarios.
- Integridad de los datos.
- Consultas complejas optimizadas.
- Seguridad de acceso y auditoría.
- Respaldo y recuperación.
- Acceso a través de lenguajes de programación estándar.

- Sistema de Gestión de Base de Datos (SGBD)

Los Sistemas de Gestión de Base de Datos (en inglés DataBase Management System) son un tipo de software muy específico, dedicado a servir de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan. Se compone de un lenguaje de definición de datos, de un lenguaje de manipulación de datos y de un lenguaje de consulta.

6.1.3.2 Ventajas de las bases de datos

- Control sobre la redundancia de datos: Los sistemas de ficheros almacenan varias copias de los mismos datos en ficheros distintos. Esto hace que se desperdicie espacio de almacenamiento, además de provocar la falta de consistencia de datos.

En los sistemas de bases de datos todos estos ficheros están integrados, por lo que no se almacenan varias copias de los mismos datos. Sin embargo, en una base de datos no se puede eliminar la redundancia completamente, ya que en ocasiones es necesaria para modelar las relaciones entre los datos.

- Consistencia de datos: Eliminando o controlando las redundancias de datos se reduce en gran medida el riesgo de que haya inconsistencias. Si un dato está almacenado una sola vez, cualquier actualización se debe realizar sólo una vez, y está disponible para todos los usuarios inmediatamente. Si un dato está duplicado y el sistema conoce esta redundancia, el propio sistema puede encargarse de garantizar que todas las copias se mantienen consistentes.

- Compartición de datos: En los sistemas de ficheros, los ficheros pertenecen a las personas o a los departamentos que los utilizan. Pero en los sistemas de bases de datos, la base de datos pertenece a la empresa y puede ser compartida por todos los usuarios que estén autorizados.

- Mantenimiento de estándares: Gracias a la integración es más fácil respetar los estándares necesarios, tanto los establecidos a nivel de la empresa como los nacionales e internacionales. Estos estándares pueden establecerse sobre el formato de los datos para facilitar su intercambio, pueden ser estándares de documentación, procedimientos de actualización y también reglas de acceso.

- Mejora en la integridad de datos: La integridad de la base de datos se refiere a la validez y la consistencia de los datos almacenados. Normalmente, la integridad se expresa mediante restricciones o reglas que no se pueden violar. Estas restricciones se pueden aplicar tanto a los datos, como a sus relaciones, y es el SGBD quien se debe encargar de mantenerlas.

- Mejora en la seguridad: La seguridad de la base de datos es la protección de la base de datos frente a usuarios no autorizados. Sin unas buenas medidas de seguridad, la integración de datos en los sistemas de bases de datos hace que éstos sean más vulnerables que en los sistemas de ficheros.

- Aumento de la concurrencia: En algunos sistemas de ficheros, si hay varios usuarios que pueden acceder simultáneamente a un mismo fichero, es posible que el acceso interfiera entre ellos de modo que se pierda información o se pierda la integridad. La mayoría de los SGBD gestionan el acceso

concurrente a la base de datos y garantizan que no ocurran problemas de este tipo.

- Mejora en los servicios de copias de seguridad: Muchos sistemas de ficheros dejan que sea el usuario quien proporcione las medidas necesarias para proteger los datos ante fallos en el sistema o en las aplicaciones. Los usuarios tienen que hacer copias de seguridad cada día, y si se produce algún fallo, utilizar estas copias para restaurarlos.

En este caso, todo el trabajo realizado sobre los datos desde que se hizo la última copia de seguridad se pierde y se tiene que volver a realizar. Sin embargo, los SGBD actuales funcionan de modo que se minimiza la cantidad de trabajo perdido cuando se produce un fallo.

6.1.3.3 Desventajas de las bases de datos

- Complejidad: Los SGBD son conjuntos de programas que pueden llegar a ser complejos con una gran funcionalidad. Es preciso comprender muy bien esta funcionalidad para poder realizar un buen uso de ellos.

- Costo del equipamiento adicional: Tanto el SGBD, como la propia base de datos, pueden hacer que sea necesario adquirir más espacio de almacenamiento. Además, para alcanzar las prestaciones deseadas, es posible que sea necesario adquirir una máquina más grande o una máquina que se dedique solamente al SGBD. Todo esto hará que la implantación de un sistema de bases de datos sea más cara.

- Vulnerable a los fallos: El hecho de que todo esté centralizado en el SGBD hace que el sistema sea más vulnerable ante los fallos que puedan producirse. Es por ello que deben tenerse copias de seguridad (Backup).

6.1.4 Conexiones seguras y seguridad en el www[4]

En un sistema conectado a Internet u otra red sin prestar la debida atención a los temas de seguridad, la información que se recibe pudo haber sido modificada en su tránsito, o puede no provenir del sitio del cual se cree que proviene. De igual manera, la información enviada puede ser interceptada en el camino, puede ser desviada o puede ser leída por personas no autorizadas.

En una red insegura, se pueden incrementar los controles en la seguridad para suplir las deficiencias. La realidad muestra que resulta más beneficioso considerar la mejora en la seguridad de la red, ya que de esta forma se evitarán sistemas y aplicaciones robustas, redundando en una sustancial mejora en la performance y los costos.

También debe considerarse la seguridad en el sistema utilizado. La seguridad en el sistema concierne a la protección del sistema y su entorno local, que funciona como extremo de una comunicación y donde corre la aplicación (pero sin incluir a estos últimos).

A la seguridad en el sistema corresponden medidas tales como:

---

[4]Internet. Traducción por David Egea, Editorial Marcombo, Año 2001 de obra original, Easy Internet, 4. Auflaje (Lackerbauer), Editorial Pearson, Año 2000

- ✓ Verificar que los proveedores de software sean confiables.
- ✓ Asegurar que el software instalado se encuentre libre de debilidades de seguridad.
- ✓ Actualizar periódicamente el software instalado con las últimas versiones o actualizaciones para minimizar los puntos débiles que todo software posee.
- ✓ Asegurar un sistema libre de virus y de Caballos de Troya.
- ✓ Minimizar los riesgos de penetración (restringiendo, por ejemplo, los puertos a Internet que no son utilizados).
- ✓ Prohibir la utilización de módems dentro de nuestra red.
- ✓ Asegurar una eficiente administración de los accesos al sistema, en elementos tales como: passwords que expiren en periodos cortos, no admitir passwords triviales, eliminación de cuentas obsoletas, etc.

6.1.5 Seguridad en la www

La seguridad en la www (World Wide Web), puede dividirse en dos categorías: La primera, se refiere a los riesgos a los que se ve expuesto un servidor Web, tal como la exposición de documentos a personas no autorizadas, o la posibilidad de que un cracker de ejecute código malicioso en dicho servidor.

La segunda, se refiere a comprometer las comunicaciones de los usuarios, tal como la captura de números de tarjeta de crédito, o cualquier otra información sensible que tenga algún valor en manos de personas inescrupulosas.

Para solucionar estos problemas, es necesario aplicar protocolos de seguridad para Web en servidores y navegadores (browsers). Los más utilizados son: SSL (Secure Socket Layer) y TLS (TransportLayer Security).

6.1.6 ¿Cuál es el problema de la seguridad en los servidores?

Como ya dijimos, el problema se presenta cuando usted completa, por ejemplo, un formulario colocando su información personal (e inclusive el número de alguna de sus tarjetas de crédito) y lo envía a un servidor Web, usted está enviando los datos contenidos en dicho formulario al Internet. Estos datos son transmitidos por el Internet pasando de máquina en máquina hasta llegar al destinatario.

El peligro es que sus datos puedan ser recogidos (robados) en cualquiera de las máquinas por las cuales pasan en el proceso de transmisión y caer en manos de cualquiera.

6.1.7 ¿Qué es un servidor seguro?

Un servidor seguro le garantiza la privacidad de los datos que usted transmite por la red. Dicha privacidad se consigue mediante un protocolo que brinde seguridad en la transmisión de información. La seguridad es el resultado de la comunicación entre un navegador que soporte el protocolo y un servidor que también soporte el mismo protocolo. Las últimas versiones de los navegadores Netscape Communicator, Mozilla Firefox, Google Chrome, Microsoft Internet Explorer, entre otros soportan protocolos que brindan seguridad en la transmisión de información como, por ejemplo, SSL y TLS.

6.1.8 ¿Cómo se puede saber que un servidor es seguro?

Lo sabe por la llave llena que aparece en la parte inferior izquierda de su navegador Netscape, o por el candado que aparece en la parte inferior derecha de su navegador Internet Explorer. También se puede apreciar que la dirección con la que va a conectarse varía ligeramente: ya que no empieza con "http://" sino con "https://". En Netscape Communicator abriendo la ventana Ver (View) y posteriormente haciendo clic en Información del Documento (DocumentInfo) encontrará todo lo relativo al nivel de seguridad de la comunicación con dicho servidor, su certificación, y la Autoridad de Certificante (CA). Lo mismo sucede con Internet Explorer, haciendo clic con el botón derecho del mouse directamente sobre el documento que está visualizando, seleccionando el ítem Propiedades y haciendo clic en el botón Certificados, obtendrá la información relativa al nivel de seguridad de dicho servidor.

6.1.9 ¿Cómo funciona el protocolo SSL?

Explicándolo en forma sencilla, tanto el navegador como el servidor Web acuerdan una clave de encriptado para esa comunicación, a partir de allí, encriptan los datos que usted envía hacia el servidor tanto como los que el servidor le envía a usted. De esta forma si algún individuo, durante el proceso de transmisión, consigue apropiarse de la información, no podrá leerlos ya que no dispone de las claves necesarias.

6.1.10 ¿Qué es el certificado de seguridad?

Un certificado de seguridad lo concede una entidad certificadora: la Autoridad Certificante. Esta entidad concede dicho certificado después de haber

comprobado los datos de la entidad solicitante. El certificado de servidor seguro se concede a una entidad cuyas referencias han sido comprobadas, para asegurar que efectivamente quien realizará las comunicaciones seguras es quien realmente dice que es y no alguien que pretende hacerse pasar por otro.

Ahora bien, teniendo ya un conocimiento amplio de sistemas de información web y su seguridad tanto física como lógica llevaremos a cabo el desarrollo de este proyecto en base a marcos de referencia que nos son de mucha ayuda a la hora de implementar una nueva tecnología en nuestra compañía, además, es indispensable también conocer cuáles son las mejores prácticas del mercado al ejecutar estos sistemas de información web, para el caso puntual de nuestro proyecto haremos un modelo a seguir con algunos marcos de referencia para esto Cobit nos brinda buenas prácticas a través de un marco de trabajo integrado por dominios y procesos que están fuertemente enfocadas en el control y un poco menos en la ejecución, estás prácticas nos ayudan a optimizar las inversiones facilitadas por TI, aseguran la entrega de servicio y además brindan una medida contra la cual juzgar cuando las cosas no vallan bien. Para que TI tenga éxito en satisfacer los requerimientos de la compañía es necesario implementar un sistema de control interno o un marco de trabajo estableciendo un vinculo con los requerimientos de la compañía, organizando las actividades de TI en un modelo de procesos, identificando los principales recursos de TI a ser utilizados y definiendo los objetivos de control gerenciales a ser estimados.

Otro factos importante para nuestro modelo es Owasp[5] (acrónimo de Open Web Application Security Project, en inglés 'Proyecto de seguridad de aplicaciones web abiertas') es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro, esta compañía gestiona los proyectos y su infraestructura. El proyecto Owasp, técnicamente, es una API para asegurarse que las entradas HTML/CSS del usuario estén en cumplimiento con las reglas de la aplicación. Otra forma de decirlo podría ser: Es una API que le ayuda a asegurarse que los clientes no provean código malicioso en el HTML para su perfil, comentarios, etc. que se quedan almacenados en el servidor. El termino código malicioso en términos de aplicaciones Web es generalmente relacionado solo con JavaScript. Hojas de estilo en cascada (CSS) son solo consideradas maliciosas cuando invocan a JavaScript. Sin embargo, hay muchas situaciones donde HTML y CSS "normales" pueden ser usados de una forma maliciosa.

Generalmente, los mecanismos de seguridad y los usuarios tienen una comunicación que es virtualmente de una vía, por una buena razón. Dejar al atacante potencial saber detalles acerca de la validación no se considera prudente, ya que permite que al atacante "aprenda" y "reconstruya" el mecanismo para debilidad. Estos tipos de fuga de información pueden también dañar en formas que usted no espera. Un mecanismo de ingreso que le dice al usuario, "Usuario invalido" revela el hecho de que un usuario con ese nombre no existe. Un usuario podría usar un diccionario o directorio telefónico o ambos para obtener remotamente una lista de usuarios validos. Usando esta

[5]http://www.owasp.org/index.php/Category:OWASP_AntiSamy_Project/es

información, un atacante podría lanzar un ataque de fuerza bruta o negación de servicio masivo de bloqueo de cuentas.

Desafortunadamente, eso no es muy usable en esta situación. Los usuarios típicos de Internet son poco efectivos cuando se trata de escribir HTML/CSS, entonces ¿Dónde obtienen su forma HTML? Usualmente la copian de alguna parte en la Web. Simplemente rechazando su entrada sin ninguna pista porque es frenante y molesto. Los usuarios molestos se van a alguna otra parte a hacer sus redes sociales.

Socioeconómicamente, AntiSamy es un facilitador para los que no tienen. Las compañías privadas como Google, MySpace, eBay, etc. han llegado soluciones propietarias para este problema. Esto presenta dos problemas. Uno es que las soluciones propietarias no son usualmente tan buenas, e incluso si lo fueran, pues naturalmente se niegan a compartirlas gratis. Afortunadamente, no nos importa. No vemos ninguna razón por la que solo estas compañías privadas deban tener esta funcionalidad, así que estoy liberando esto gratis bajo la licencia BSD.

Estos modelos pueden ser enfocados de la siguiente forma: COBIT enfocado a los procesos y a los riesgos, OWASP se utiliza para determinar y combatir las causas que hacen que el sistema de información pueda ser inseguro.

	COBIT	**OWASP**
Funciones	Procesos de TI	Configuración, revisión y pruebas de la seguridad
Áreas	4 dominios y 34 procesos	---
¿Para qué se usa?	Auditoria de sistemas de información	Determinar y combatir las causas que hacen que el software sea inseguro.
¿Propiedad de?	ISACA	Comunidad
Tipo	Framework	Proyecto de código abierto.

6.1.11 Alcance de la Auditoría Informática:

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoría informática, se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas. Ejemplo: ¿Se comprobará que los controles de validación de errores son adecuados y suficientes? La indefinición de los alcances de la auditoría compromete el éxito de la misma.

6.1.12 Control de integridad de registros:

Hay aplicaciones que comparten registros, son registros comunes. Si una aplicación no tiene integrado un registro común, cuando lo necesite utilizar no lo va encontrar y, por lo tanto, la aplicación no funcionaría como debería.

6.1.13 Control de validación de errores:

Se corrobora que el sistema que se aplica para detectar y corregir errores sea eficiente.

6.1.14 Características de la Auditoría Informática:

La información de la empresa y para la empresa, siempre importante, se ha convertido en un activo real de la misma, como sus stocks o materias primas si las hay. Por ende, han de realizarse inversiones informáticas, materia de la que se ocupa la Auditoría de Inversión Informática.

Del mismo modo, los sistemas informáticos han de protegerse de modo global y particular: a ello se debe la existencia de la auditoría de seguridad informática en general, o a la auditoría de seguridad de alguna de sus áreas, como pudieran ser desarrollo o técnica de sistemas.

Cuando se producen cambios estructurales en la informática, se reorganiza de alguna forma su función: se está en el campo de la auditoría de organización informática.

Estos tres tipos de auditorías engloban a las actividades auditoras que se realizan en una auditoría parcial. De otra manera: cuando se realiza una auditoria del área de desarrollo de proyectos de la informática de una empresa, es porque en ese desarrollo existen, además de ineficiencias, debilidades de organización, de inversiones, de seguridad o alguna mezcla de ellas.

Las empresas acuden a las auditorías externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse en clases:

6.1.15 Síntomas de descoordinación y desorganización:

- No coinciden los objetivos de tecnología de la información con los de la propia compañía.
- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.
- No se atienden las peticiones de cambios de los usuarios
- No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables.

- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de aplicaciones críticas y sensibles.
- Incremento desmesurado de costos.
- Necesidad de justificación de inversiones informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
- Desviaciones presupuestarias significativas.
- Costos y plazos de nuevos proyectos (deben auditarse simultáneamente a Desarrollo de Proyectos y al órgano que realizó la petición).
- Continuidad del servicio. Es un concepto aún más importante que la seguridad. Establece las estrategias de continuidad entre fallos mediante planes de contingencia totales y locales.
- Centro de proceso de datos fuera de control. Si tal situación llegara a percibirse, sería prácticamente inútil la auditoría. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio.

La operatividad de los sistemas ha de constituir entonces la principal preocupación del auditor informático. Para conseguirla hay que acudir a la realización de controles técnicos generales de operatividad y controles técnicos específicos de operatividad, previos a cualquier actividad de aquel.

Los controles técnicos generales son los que se realizan para verificar la compatibilidad de funcionamiento simultáneo del sistema operativo y el software de base con todos los subsistemas existentes, así como la compatibilidad del hardware y del software instalado. Estos controles son

importantes en las instalaciones que cuentan con varios competidores, debido a que la profusión de entornos de trabajo muy diferenciados obliga a la contratación de diversos productos de software básico, con el consiguiente riesgo de abonar más de una vez el mismo producto o desaprovechar parte del software abonado. Puede ocurrir también con los productos de software básico desarrollados por el personal de sistemas interno, sobre todo cuando los diversos equipos están ubicados en centros de proceso de datos geográficamente alejados. lo negativo de esta situación es que puede producir la inoperatividad del conjunto. Cada centro de proceso de datos tal vez sea operativo trabajando independientemente, pero no será posible la interconexión e intercomunicación de todos los centros de proceso de datos si no existen productos comunes y compatibles.

Los controles técnicos específicos, de modo menos acusado, son igualmente necesarios para lograr la operatividad de los sistemas. un ejemplo de lo que se puede encontrar mal son parámetros de asignación automática de espacio en disco que dificulten o impidan su utilización posterior por una sección distinta de la que lo generó. También, los periodos de retención de ficheros comunes a varias aplicaciones pueden estar definidos con distintos plazos en cada una de ellas, de modo que la pérdida de información es un hecho que podrá producirse con facilidad, quedando inoperativa la prueba de alguna de las aplicaciones mencionadas.

Todas las aplicaciones que se desarrollan son super parametrizadas, es decir, que tienen un montón de parámetros que permiten configurar cual va a ser el comportamiento del sistema. Una aplicación va a usar cierta cantidad de

espacio en disco. si no se analiza cual es la operación y el tiempo que le va a llevar ocupar el espacio asignado, y se pone un valor muy pequeño, puede ocurrir que un día la aplicación colapse. Si esto sucede en medio de la operación y la aplicación se cae, el volver a levantarla, con la nueva asignación de espacio, si hay que hacer reconversiones, etc., puede llegar a demandar muchísimo tiempo, lo que significa un riesgo enorme.

Una vez conseguida la operatividad de los sistemas, el segundo objetivo de la auditoría es la verificación de las normas teóricamente existentes en el departamento de informática y su coherencia con las del resto de la empresa. Para ello, habrán de revisarse sucesivamente y en este orden:

1. **Las Normas Generales de la Instalación Informática.** Se realizará una revisión inicial sin estudiar a fondo las contradicciones que pudieran existir, pero registrando las áreas que carezcan de normativa, y sobre todo verificando que esta normativa general informática no está en contradicción con alguna norma general no informática de la empresa.

2. Los Procedimientos Generales Informáticos. Se verificará su existencia, al menos en los sectores más importantes. Tampoco la detención de una nueva aplicación podría producirse si no existieran los procedimientos de backup y recuperación correspondientes.

3. Los Procedimientos Específicos Informáticos. Igualmente, se revisara su existencia en las áreas fundamentales. Así, Producción no debería utilizar una aplicación sin haber exigido a desarrollo la pertinente documentación. Del

mismo modo, deberá comprobarse que los procedimientos específicos no se opongan a los procedimientos generales. En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la normativa y los procedimientos generales de la propia empresa, a los que la informática debe estar sometida.

La explotación informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc. La explotación informática se puede considerar como una fabrica con ciertas peculiaridades que la distinguen de las reales. Para realizar la explotación informática se dispone de una materia prima, los datos, que son necesarios transformar, y que se someten previamente a controles de integridad y calidad. La transformación se realiza por medio del proceso informático, el cual está gobernado por programas. Obtenido el producto final, los resultados son sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente, al usuario.

Auditar Explotación consiste en auditar las secciones que la componen y sus interrelaciones. La explotación informática se divide en tres grandes áreas: planificación, producción y soporte técnico, en la que cada cual tiene varios grupos.

Control de Entrada de Datos:

Se analizará la captura de la información en soporte compatible con los sistemas, el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes. Se verificará que los controles de integridad y calidad de datos se realizan de acuerdo a norma.

Planificación y Recepción de Aplicaciones:

Se auditarán las normas de entrega de aplicaciones por parte de desarrollo, verificando su cumplimiento y su calidad de interlocutor único. Deberán realizarse muestreos selectivos de la documentación de las aplicaciones que se disponen para producción. Se evaluará la anticipación de contactos con desarrollo para la planificación a medio y largo plazo.

Centro de Control y Seguimiento de Trabajos:

Se analizará cómo se prepara, se lanza y se sigue la producción diaria. Básicamente, la explotación informática ejecuta procesos por cadenas o lotes sucesivos (Batch), o en tiempo real (Tiempo Real). Mientras que las Aplicaciones de Teleproceso están permanentemente activas y la función de explotación se limita a vigilar y recuperar incidencias, el trabajo batch absorbe una buena parte de los efectivos de explotación. En muchos centros de proceso de datos, éste órgano recibe el nombre de centro de control de batch. Este grupo determina el éxito de la explotación, en cuanto que es uno de los factores más importantes en el mantenimiento de la producción.

Batch y Tiempo Real:

Las Aplicaciones que son batch son aplicaciones que cargan mucha información durante el día y durante la noche se corre un proceso enorme que

lo que hace es relacionar toda la información, calcular cosas y obtener como salida, por ejemplo, reportes. O sea, recolecta información durante el día, pero todavía no procesa nada. Es solamente un tema de "Data Entry" que recolecta información, corre el proceso Batch (por lotes), y calcula todo lo necesario para arrancar al día siguiente.

Las aplicaciones que son tiempo real u online, son las que, luego de haber ingresado la información correspondiente, inmediatamente procesan y devuelven un resultado. Son sistemas que tienen que responder en tiempo real.

Centro de Control de Red y Centro de Diagnosis:

El centro de control de red suele ubicarse en el área de producción. Sus funciones se refieren exclusivamente al ámbito de las Comunicaciones, estando muy relacionado con la organización de software de comunicaciones de técnicas de sistemas. Debe analizarse la fluidez de esa relación y el grado de coordinación entre ambos. Se verificará la existencia de un punto focal único, desde el cual sean perceptibles todas las líneas asociadas al sistema. El centro de diagnosis es el ente en donde se atienden las llamadas de los usuarios-clientes que han sufrido averías o incidencias, tanto de software como de hardware. El centro de diagnosis está especialmente indicado para informáticos grandes y con usuarios dispersos en un amplio territorio. Es uno de los elementos que más contribuyen a configurar la imagen de la informática de la empresa. Debe ser auditada desde esta perspectiva, desde la sensibilidad del usuario sobre el servicio que se le dispone. No basta con

comprobar la eficiencia técnica del centro, es necesario analizarlo simultáneamente en el ámbito de usuario.

6.1.16 Auditoría Informática de Desarrollo de Proyectos o Aplicaciones:

La función de desarrollo es una evolución del llamado análisis y programación de sistemas y aplicaciones. A su vez, engloba muchas áreas, tantas como sectores informatizables tiene la empresa. Muy escuetamente, una Aplicación recorre las siguientes fases:

- Prerrequisitos del Usuario (único o plural) y del entorno
- Análisis funcional
- Diseño
- Análisis orgánico (Pre programación y Programación)
- Pruebas
- Entrega a Explotación y alta para el Proceso.

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costos, podrá producirse la insatisfacción del usuario. Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.

Una auditoría de aplicaciones pasa indefectiblemente por la observación y el análisis de cuatro consideraciones:

1. Revisión de las metodologías utilizadas: Se analizaran éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la aplicación y el fácil mantenimiento de las mismas.

2. Control Interno de las Aplicaciones: se deberán revisar las mismas fases que presuntamente han debido seguir el área correspondiente de desarrollo:

- Estudio de viabilidad de la aplicación.
- Definición lógica de la aplicación.
- Desarrollo técnico de la aplicación.
- Diseño de programas.
- métodos de pruebas.
- Documentación.
- Equipo de programación.

3. Control de Procesos y Ejecuciones de Programas Críticos: El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no se corresponde con el programa fuente que desarrolló, codificó y probó el área de desarrollo de aplicaciones. Se ha de comprobar la correspondencia exclusiva entre el programa codificado y su compilación. Si los programas fuente y los programa módulo no coincidieran podría provocar, desde errores de bulto que producirían graves y altos costos de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial-informativo, etc. Por ende, hay normas muy rígidas en cuanto a las librerías de programas; aquellos programas fuente que hayan sido dados por bueno por desarrollo, son entregados a prueba con el fin de que éste:

- Copie el programa fuente en la librería de fuentes de prueba, a la que nadie más tiene acceso
- Compile y monte ese programa, depositándolo en la librería de módulos de prueba, a la que nadie más tiene acceso.
- Copie los programas fuente que les sean solicitados para modificarlos, arreglarlos, etc. en el lugar que se le indique. Cualquier cambio exigirá pasar nuevamente al primer punto.

Como este sistema para auditar y dar el alta a una nueva aplicación es bastante ardua y compleja, hoy (algunas empresas lo usarán, otras no) se utiliza un sistema llamado U.A.T (UserAcceptance Test). Este consiste en que el futuro usuario de esta aplicación use la aplicación como si la estuviera usando en producción para que detecte o se denoten por sí solos los errores de la misma. Estos defectos que se encuentran se van corrigiendo a medida que se va haciendo el U.A.T. Una vez que se consigue el U.A.T., el usuario tiene que dar el Sign Off ("Esto está bien"). Todo este testeo, auditoría lo tiene que controlar, tiene que evaluar que el testeo sea correcto, que exista un plan de testeo, que esté involucrado tanto el cliente como el desarrollador y que estos defectos se corrijan. Auditoría tiene que corroborar que el U.A.T. prueba todo y que el Sign Off del usuario sea un Sign Off por todo.

6.1.17 Herramientas y Técnicas para la Auditoría Informática:

Cuestionarios:

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los

diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando la cumplimentación de cuestionarios pre impresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos pre impresos hubieran proporcionado.

Entrevistas:

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.

2. Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
3. Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

Checklist:

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada.

Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la cumplimentación sistemática de sus Cuestionarios, de sus Checklists.

Hay opiniones que descalifican el uso de las Checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar Checklist, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de Checklist. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el

modo y el orden de su formulación. Las empresas externas de auditoría informática guardan sus Checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar la Checklist de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las Checklists utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios o Checklists responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

a. Checklist de rango

Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo). Ejemplo de Checklist de rango:

Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al Centro de Cálculo. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tienen los siguientes significados:

1: Muy deficiente.
2: Deficiente.
3: Mejorable.
4: Aceptable.
5: Correcto.

Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan encorsetadas ni clasificadas previamente. Basta con que el auditor lleve un pequeño guión. La cumplimentación de la Checklist no debe realizarse en presencia del auditado.

- ¿Existe personal específico de vigilancia externa al edificio?

- No, solamente un guarda por la noche que atiende además otra instalación adyacente.

<Puntuación: 1>

- El personal de Comunicaciones, ¿Puede entrar directamente en la Sala de Computadoras?

- No, solo tiene tarjeta el Jefe de Comunicaciones. No se la da a su gente más que por causa muy justificada, y avisando casi siempre al Jefe de Explotación.

<Puntuación: 4>

El resultado sería el promedio de las puntuaciones: (1 + 4) /2 = 2,5 Deficiente.

b. Checklist Binaria

Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente.

Ejemplo de Checklist Binaria:

Se supone que se está realizando una Revisión de los métodos de pruebas de programas en el ámbito de Desarrollo de Proyectos.

- ¿Existe Normativa de que el usuario final compruebe los resultados finales de los programas?

<Puntuación: 1>

- ¿Existe una norma por la cual las pruebas han de realizarse con juegos de ensayo o copia de Bases de Datos reales?

<Puntuación: 0>

Las Checklists de rango son adecuadas si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación de la Checklist binaria. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.

Las Checklists Binarias siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión

de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del <si o no> frente a la mayor riqueza del intervalo.

No existen Checklists estándar para todas y cada una de las instalaciones informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

Trazas y/o Huellas:

Con frecuencia, el auditor informático debe verificar que los programas, tanto de los sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa.

Muy especialmente, estas "Trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo.

Por lo que se refiere al análisis del sistema, los auditores informáticos emplean productos que comprueban los valores asignados por técnica de sistemas a cada uno de los parámetros variables de las Librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado

por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio para según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

No obstante la utilidad de las Trazas, ha de repetirse lo expuesto en la descripción de la auditoría informática: el auditor informático emplea preferentemente la amplia información que proporciona el propio sistema: Así, los ficheros de <Accounting> o de <contabilidad>, en donde se encuentra la producción completa de aquél, y los <Log> de dicho sistema, en donde se recogen las modificaciones de datos y se pormenoriza la actividad general.
Del mismo modo, el Sistema genera automáticamente exacta información sobre el tratamiento de errores de maquina central, periféricos, etc.

Log:

El log vendría a ser un historial que informa que fue cambiando y cómo fue cambiando (información). Las bases de datos, por ejemplo, utilizan el log para asegurar lo que se llaman las transacciones. Las transacciones son unidades atómicas de cambios dentro de una base de datos; toda esa serie de cambios se encuadra dentro de una transacción, y todo lo que va haciendo la Aplicación (grabar, modificar, borrar) dentro de esa transacción, queda grabado en el log. La transacción tiene un principio y un fin, cuando la transacción llega a su fin, se vuelca todo a la base de datos. Si en el medio de la transacción se cortó por x razón, lo que se hace es volver para atrás. El log te permite analizar

cronológicamente que es lo que sucedió con la información que está en el sistema o que existe dentro de la base de datos.

6.1.18 Software de interrogación:

Hasta hace ya algunos años se han utilizado productos software llamados genéricamente <paquetes de auditoría>, capaces de generar programas para auditores escasamente calificados desde el punto de vista informático.

Más tarde, dichos productos evolucionaron hacia la obtención de muestreos estadísticos que permitieran la obtención de consecuencias e hipótesis de la situación real de una instalación.

En la actualidad, los productos Software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada. Estos productos son utilizados solamente por los auditores externos, por cuanto los internos disponen del software nativo propio de la instalación.

Del mismo modo, la proliferación de las redes locales y de la filosofía "Cliente-Servidor", han llevado a las firmas de software a desarrollar interfaces de transporte de datos entre computadoras personales y mainframe, de modo que el auditor informático copia en su propia PC la información más relevante para su trabajo.

Cabe recordar, que en la actualidad casi todos los usuarios finales poseen datos e información parcial generada por la organización informática de la

Compañía. Efectivamente, conectados como terminales al "Host", almacenan los datos proporcionados por este, que son tratados posteriormente en modo PC. El auditor se ve obligado (naturalmente, dependiendo del alcance de la auditoría) a recabar información de los mencionados usuarios finales, lo cual puede realizar con suma facilidad con los polivalentes productos descritos. Con todo, las opiniones más autorizadas indican que el trabajo de campo del auditor informático debe realizarse principalmente con los productos del cliente.

Finalmente, ha de indicarse la conveniencia de que el auditor confeccione personalmente determinadas partes del Informe. Para ello, resulta casi imprescindible una cierta soltura en el manejo de procesadores de Texto, paquetes de gráficos, hojas de cálculo, etc.

6.1.19 Metodología de Trabajo de Auditoría Informática

El método de trabajo del auditor pasa por las siguientes etapas:

- Alcance y Objetivos de la Auditoría Informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoría.
- Confección y redacción del Informe Final.
- Redacción de la Carta de Introducción o Carta de Presentación del Informe final.

Definición de Alcance y Objetivos

El alcance de la auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar.

A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoría, es decir cuales materias, funciones u organizaciones no van a ser auditadas.

Tanto los alcances como las excepciones deben figurar al comienzo del informe final.

Las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar. Deben comprender los deseos y pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas.

Una vez definidos los objetivos (objetivos específicos), éstos se añadirán a los objetivos generales y comunes de a toda auditoría Informática: La operatividad de los Sistemas y los Controles Generales de Gestión Informática.

Estudio Inicial

Para realizar dicho estudio ha de examinarse las funciones y actividades generales de la informática.

Para su realización el auditor debe conocer lo siguiente:

Organización:

Para el equipo auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. Para realizar esto en auditor deberá fijarse en:

1) **Organigrama:**

El organigrama expresa la estructura oficial de la organización a auditar. Si se descubriera que existe un organigrama fáctico diferente al oficial, se pondrá de manifiesto tal circunstancia.

2) **Departamentos:**

Se entiende como departamento a los órganos que siguen inmediatamente a la Dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.

3) **Relaciones Jerárquicas y funcionales entre órganos de la Organización:**

El equipo auditor verificará si se cumplen las relaciones funcionales y jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes.

Las de jerarquía implican la correspondiente subordinación. Las funcionales por el contrario, indican relaciones no estrictamente subordinables.

4) **Flujos de Información:**

Además de las corrientes verticales intradepartamentales, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extradepartamentales.

Los flujos de información entre los grupos de una organización son necesarios para su eficiente gestión, siempre y cuando tales corrientes no distorsionen el propio organigrama. En ocasiones, las organizaciones crean espontáneamente

canales alternativos de información, sin los cuales las funciones no podrían ejercerse con eficacia; estos canales alternativos se producen porque hay pequeños o grandes fallos en la estructura y en el organigrama que los representa.

Otras veces, la aparición de flujos de información no previstos obedece a afinidades personales o simple comodidad. Estos flujos de información son indeseables y producen graves perturbaciones en la organización.

5) **Número de Puestos de trabajo**

El equipo auditor comprobará que los nombres de los puestos de trabajo de la organización corresponden a las funciones reales distintas. Es frecuente que bajo nombres diferentes se realicen funciones idénticas, lo cual indica la existencia de funciones operativas redundantes, esta situación pone de manifiesto deficiencias estructurales; los auditores darán a conocer tal circunstancia y expresarán el número de puestos de trabajo verdaderamente diferentes.

6) **Número de personas por Puesto de Trabajo**

Es un parámetro que los auditores informáticos deben considerar. La inadecuación del personal, determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

7) **Entorno Operacional**

El equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse.

Este conocimiento previo se logra determinando, fundamentalmente, los siguientes extremos:

a. Situación geográfica de los Sistemas:

Se determinará la ubicación geográfica de los distintos Centros de Proceso de Datos en la empresa. A continuación, se verificará la existencia de responsables en cada unos de ellos, así como el uso de los mismos estándares de trabajo.

b. Arquitectura y configuración de Hardware y Software:

Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica de las compañías, los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

c. Inventario de Hardware y Software:

El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware figurarán las CPUs, unidades de control local y remoto, periféricos de todo tipo, etc. El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.

d. Comunicación y Redes de Comunicación:

En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones. Igualmente, poseerán información de las Redes Locales de la Empresa.

8) Aplicaciones bases de datos y ficheros

El estudio inicial que han de realizar los auditores se cierra y culmina con una idea general de los procesos informáticos realizados en la empresa auditada. Para ello deberán conocer lo siguiente:

a. Volumen, antigüedad y complejidad de las Aplicaciones

b. Metodología del Diseño

Se clasificará globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones. Si se han utilizados varias a lo largo del tiempo se pondrá de manifiesto.

c. Documentación

La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes. La documentación de programas disminuye gravemente el mantenimiento de los mismos.

d. Cantidad y complejidad de Bases de Datos y Ficheros.

El auditor recabará información de tamaño y características de las Bases de Datos, clasificándolas en relación y jerarquías. Hallará un promedio de número de accesos a ellas por hora o días. Esta operación se repetirá con los ficheros, así como la frecuencia de actualizaciones de los mismos. Estos datos proporcionan una visión aceptable de las características de la carga informática.

9) Determinación de recursos de la auditoría Informática

Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

Recursos materiales

Es muy importante su determinación, por cuanto la mayoría de ellos son proporcionados por el cliente. Las herramientas software propias del equipo van a utilizarse igualmente en el sistema auditado, por lo que han de convenirse en lo posible las fechas y horas de uso entre el auditor y cliente. Los recursos materiales del auditor son de dos tipos:

a. Recursos materiales Software

Programas propios de la auditoria: Son muy potentes y flexibles. Habitualmente se añaden a las ejecuciones de los procesos del cliente para verificarlos.

Monitores: Se utilizan en función del grado de desarrollo observado en la actividad de técnica de sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

b. Recursos materiales Hardware

Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las computadoras del auditado. Para lo cual habrá de convenir, tiempo de máquina, espacio de disco, impresoras ocupadas, etc.

Recursos Humanos

La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado dependen de la materia auditable. Es igualmente reseñable que la auditoría en general suele ser ejercida por

profesionales universitarios y por otras personas de probada experiencia multidisciplinaria.

Perfiles Profesionales de los auditores informáticos

Profesión	**Actividades y conocimientos deseables**
Informático Generalista	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de Explotación.
Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costes	Economista con conocimiento de Informática.

	Gestión de costes.

10) Elaboración del Plan y de los programas de trabajo

Una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo. Decidido éste, se procede a la programación del mismo.

El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

a. Si la Revisión debe realizarse por áreas generales o áreas específicas. En el primer caso, la elaboración es más compleja y costosa.

b. Si la auditoría es global, de toda la Informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.

c. En el plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos.

d. En el Plan se establecen los recursos y esfuerzos globales que van a ser necesarios.

e. En el Plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.

f. El Plan establece disponibilidad futura de los recursos durante la revisión.

g. El Plan estructura las tareas a realizar por cada integrante del grupo.

h. En el Plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Una vez elaborado el Plan, se procede a la Programación de actividades. Esta ha de ser lo suficientemente como para permitir modificaciones a lo largo del proyecto.

11) Actividades de la Auditoría Informática

Auditoría por temas generales o por áreas específicas:

La auditoría Informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.

Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad.

6.1.20 Técnicas de Trabajo:

- Análisis de la información recabada del auditado.
- Análisis de la información propia.
- Cruzamiento de las informaciones anteriores.
- Entrevistas.
- Simulación.
- Muestreos.

Herramientas:

- Cuestionario general inicial.
- Cuestionario Checklist.
- Estándares.
- Monitores.
- Simuladores (Generadores de datos).

- Paquetes de auditoría (Generadores de Programas).
- Matrices de riesgo.

12)Informe Final

La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad.

Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

6.1.21 Estructura del informe final:

El informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente.

- Definición de objetivos y alcance de la auditoría.
- Enumeración de temas considerados: Antes de tratarlos con profundidad, se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría.
- Cuerpo expositivo: Para cada tema, se seguirá el siguiente orden a saber:

a. Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real

b. Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.

c. Puntos débiles y amenazas.

d. Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.

e. Redacción posterior de la Carta de Introducción o Presentación.

Modelo conceptual de la exposición del informe final:

- El informe debe incluir solamente hechos importantes.
- La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.
- El Informe debe consolidar los hechos que se describen en el mismo.

El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:

a. El hecho debe poder ser sometido a cambios.

b. Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.

3. No deben existir alternativas viables que superen al cambio propuesto.

4. La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.

La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.

Flujo del hecho o debilidad:

1 – Hecho encontrado.

- Ha de ser relevante para el auditor y pera el cliente.
- Ha de ser exacto, y además convincente.
- No deben existir hechos repetidos.

2 – Consecuencias del hecho

- Las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

3 – Repercusión del hecho

- Se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.

4 – Conclusión del hecho

- No deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.

5 – Recomendación del auditor informático

- Deberá entenderse por sí sola, por simple lectura.
- Deberá estar suficientemente soportada en el propio texto.
- Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.
- La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

Carta de introducción o presentación del informe final:

La carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargo o contrato la auditoría. Así como pueden existir tantas copias del informe final como solicite el cliente, la auditoría no hará copias de la citada carta de introducción.

La carta de introducción poseerá los siguientes atributos:

- Tendrá como máximo 4 folios.
- Incluirá fecha, naturaleza, objetivos y alcance.
- Cuantificará la importancia de las áreas analizadas.
- Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- Presentará las debilidades en orden de importancia y gravedad.
- En la carta de Introducción no se escribirán nunca recomendaciones.

Las Recomendaciones del Informe son de tres tipos:

1. Recomendaciones correspondientes a la zona roja. Serán muy detalladas e irán en primer lugar, con la máxima prioridad. La redacción de las recomendaciones se hará de modo que sea simple verificar el cumplimiento de la misma por parte del cliente.

2. Recomendaciones correspondientes a la zona amarilla. Son las que deben observarse a medio plazo, e igualmente irán priorizadas.

3. Recomendaciones correspondientes a la zona verde. Suelen referirse a medidas de mantenimiento. Pueden ser omitidas. Puede detallarse alguna de este tipo cuando una acción sencilla y económica pueda originar beneficios importantes.

7 METODOLOGIA

7.1 TIPO DE ESTUDIO

INVESTIGATIIVO – EXPLORATORIO, se hicieron investigaciones y se exploró acerca de las diferentes metodologías existentes para la realización de auditoría a sistemas de información web.

7.2 METODO

Empírico - investigativo

7.3 TECNICAS E INSTRUMENTOS PARA LA RECOLECCION DE INFORMACIÓN

7.3.1 Fuentes primarias

El presente estudio se realizó a través de una investigación exploratoria - investigativa, que se centró básicamente en adquisición de documentación por medio de tesis y monografías anteriormente realizadas en cuando a la seguridad e infraestructura de los sistemas de información web, que dio las primeras luces cuando establecimos la necesidad de implementar criterios de evaluación a auditorias de sistemas de información web.

El método usado para la recolección de los datos fue estructurado directo, por medio de monografías, tesis, libros, sitios web especializados, ya que estos son de fácil acceso para el estudio requerido.

7.3.2 Fuentes secundarias

Como medio de sustentación secundario para este proyecto utilizamos sitios web especializados en auditoria de sistemas de información web, tesis y libros digitales.

8 DELIMITACION

8.1 Delimitación espacial

El desarrollo de este proyecto se llevó a cabo en la ciudad de Barranquilla en las instalaciones de la Corporación Universitaria de la Costa, en el segundo semestre del año 2010.

8.2 Delimitación temporal

El desarrollo de esta investigación se hizo a corto plazo, llevándose a cabo en un lapso de seis meses a partir del mes de marzo del año 2009 y culminando entonces en el mes de septiembre del año 2010.

8.3 Delimitación financiera

Los recursos para la realización del presente proyecto, fueron aportados por los integrantes del grupo (Computadores personales con acceso a Internet, servicio de impresión, etc.) además de los recursos logísticos.

8.4 Limitaciones

No se tuvo ninguna limitación, se pudo acceder a toda la información de libros, revistas, tesis e investigaciones hechas anteriormente.

9 RESULTADO

Tomando en cuenta los procesos de Cobit y las actividades que propone Owasp, al momento de realizar una auditoría a un sistema de información se debe tener en cuenta los siguientes criterios:

1. Realizar un reconocimiento de las políticas y procedimientos que giran en torno al sistema de información web.

a) Solicitar los manuales y políticas de gestión del sistema de información web.

b) Solicitar bitácora de procedimientos y actualizaciones realizadas al sistema de información web.

c) Solicitar políticas de clasificación de la información, usando esquemas apropiados que garanticen la integridad de los datos.

d) Solicitar planos de las instalaciones físicas donde se encuentran ubicados los equipos del sistema de información.

2. Evaluación de los procedimientos de operación, revisión de la seguridad y parametrización de la plataforma incluyendo sistema operativo, servidor de aplicación y base de datos que soportan el sistema de información web.

a) Evaluación de las políticas y procedimientos definidos para la administración de la plataforma tecnológica considerando las normas asociadas al centro de cómputo y medidas de seguridad lógicas adoptadas.

b) Medidas de control para el monitoreo del procesamiento en línea y por lote (batch) así como para el aseguramiento de la disponibilidad del sistema.

c) Esquemas de generación, administración, retención y custodia de copias de respaldo de la información.

d) Seguridad física y ambiental de la locación donde reside la plataforma (servidor) que soporta estas aplicaciones

e) Evaluación de los parámetros de seguridad lógica establecidos a nivel de sistema operativo.

f) Evaluación de la configuración de la seguridad y los procedimientos de administración de las bases de datos.

g) Análisis de segregación funcional en las responsabilidades de administración de la seguridad física y lógica, así como de la segregación de acceso al ambiente de producción, pruebas y desarrollo.

h) Evaluación de la validación en requerimientos de seguridad tales como transferencia y almacenamiento seguro de información.

i) Evaluación del monitoreo periódico del sistema de información y de su infraestructura.

j) Evaluación del monitoreo y cambios realizados al sistema de información web, plataforma e infraestructura.

3. Evaluación de los procedimientos y controles para implementar cambios

a) Evaluación de los procedimientos y controles para la implementación de cambios a nivel aplicativo, sistema operativo y red, desde que nace el requerimiento hasta su implementación:

i. Aprobaciones sobre los requerimientos y análisis efectuado.

ii. Asegurar que las políticas y estándares sean los adecuados y que brinde la documentación necesaria a implementar.

iii. Comprobación del nivel de seguridad sea acorde con el nuevo procedimiento a implementar.

iv. Revisión de requisitos de seguridad.

v. Revisión y diseño de la arquitectura tecnológica.

vi. Pruebas realizadas.

vii. Medidas preventivas antes del paso a producción.

viii. Aprobaciones para el paso a producción.

ix. Plan de regreso a la versión anterior

b) Revisión de los controles para el mantenimiento de programas fuentes.

c) Revisión de políticas para efectuar cambios de emergencia.

4. Evaluación de la seguridad y control del sistema de información y análisis de seguridad en la definición y administración de usuarios y perfiles.

a) Funciones que se debe desempeñar de acuerdo a su cargo según RRHH.

b) Evaluación de los privilegios, roles y funciones de los usuarios sobre el sistema de información.

c) Frecuencia de las actividades realizadas por los funcionarios y validación de los datos.

d) Identificación y documentación de los eventos más críticos.

e) Realización de pruebas de vigilancia y monitoreo de la seguridad del sistema de información.

f) Evaluación de manejo de llaves criptográficas.

g) Evaluación de medidas de detección, prevención y corrección de software malicioso.

h) Monitorear incidentes de seguridad reales y potenciales.

5. Evaluación de la funcionalidad del sistema para establecer si los controles de validez e integridad están acordes con las necesidades de la empresa:

a) Evaluación de la configuración de las redes de comunicación.

b) Evaluación de las vulnerabilidades del sistema de información de acuerdo a la forma en que este envía los datos por la red.

c) Evaluación de configuración adecuada de firewall y otras barreras para proteger la transferencia y almacenamiento de la información.

d) Evaluación del desempeño del sistema de información y de su infraestructura.

e) Identificar medidas para la mejora del desempeño del sistema de información.

Consecución de los objetivos

Para la consecución de los objetivos y para lograr un adecuado funcionamiento del sistema de información se debe realizar una serie de pruebas que se describen a continuación:

- Requerimiento del negocio.
- Verificar cumplimiento de requerimientos técnicos y legales de acuerdo a la actividad económica de la empresa.
- Verificación de autenticación y número de intentos fallidos no superen a lo establecido.

- Garantizar la confidencialidad, integridad y disponibilidad de la información.
- Revisión de la transferencia y almacenamiento de información esté cifrada.
- Realización de pruebas de intrusión orientadas a identificar vulnerabilidades del sistema de información web.
- Restricciones de los operadores del sistema de información al código fuente.
- Verificar estándar en la creación y utilización de perfiles y contraseñas.
- Cifrar información usando cifrado no reversible, para evitar ataques de diccionario.

10 CONCLUSIONES Y RECOMENDACIONES

El auditor debe realizar listas de chequeo que le indique si se están llevando a cabo los procesos fundamentales para el negocio, además, debe realizar entrevistas con las personas involucradas teniendo en cuenta la organización jerárquica del negocio y su plan estratégico, este último debe estar alineado con los objetivos del negocio. También es necesario para este tipo de auditoría que se cuente con software de apoyo que garantice de una manera mucho más confiable un resultado que satisfaga las necesidades tanto de la compañía como de la gerencia.

Se recomienda utilizar herramientas que permitan ejercer en mayor o menor medida, tener control sobre los procesos, donde COBIT se caracteriza por decirnos que debemos buscar, esto a nivel administrativo y OWASP que es un proyecto GNU, que nos presenta una metodología para configura y verificar la seguridad de sistemas de información Web.

Para garantizar la seguridad de un sistemas de información web es necesario establecer: capacitaciones al personal, planes de continuidad y contingencia, políticas, procedimientos, manuales, minutogramas, bitácoras, etc. Que garanticen que los múltiples elementos que interactúan realicen las funciones para los cuales están destinados, así como que la infraestructura que lo soporta cumpla con los controles necesarios como: firewall, anti-malware, actualizaciones, parches, sistemas de respaldo, equipos con la suficiente capacidad, UPS, plantas eléctricas, entre muchos otros.

De igual manera se debe concientizar a la alta gerencia y a los funcionarios de que no importa cuántos y que tan buenos sean los controles que tengamos, sino que estos se cumplan y estén bien configurados.

BIBLIOGRAFIA

- www.books.google.com.co
- www.desarrolloweb.com
- www.maestrosdelweb.com
- www.owasp.org/index.php/Category:OWASP_AntiSamy_Project/es
- www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
- www.it-institute.org
- www.itil-officialsite.com/home/home.asp
- www.kybeleconsulting.com
- Análisis y diseño estructurado y orientado a objetos de sistemas informáticos, Autor Antonio Amescua, Editorial Mcgraw Hill, 2009
- Internet sin fronteras, Autor Angus J. Kenedy, Editorial Ediciones B, Año 2005.
- Internet. Traducción por David Egea, Editorial Marcombo, Año 2001 de obra original, Easy Internet, 4. Auflaje (Lackerbauer), Editorial Pearson, Año 2000
- Introducción a los sistemas de bases de datos C.J. Date: Pearson Educación, 2001. ISBN 968-444-419-2.
- Fundamentos de Sistemas de Bases de Datos Ramez A. Elmasri&Shamkant B. Navathe: Addison-Wesley, 2002 [3ª edición]. ISBN 84-782-9051-6.

ANEXOS

- Formatos para realización de la auditoria.

  Fuente: Modulo de auditoría a base de datos

  Ubicación: Medio magnético.

- Lista de chequeo básica para la auditoria.

  Fuente: Recopilación de información de la especialización.

  Ubicación: Medio magnético.

- Guías de pruebas de la OWASP.

  Fuente: www.dragonjar.org/owasp-testing-guide-3-0-en-espanol.xhtml

  Ubicación: Medio magnético.

- Herramientas para realizar pruebas.

  Fuente:

  www.net.taringa.net/posts/downloads/4709189/Wireshark-1_2_2.html

  www.taringa.net/posts/downloads/1065403/Port-Scanners-Nmap-_-Superscan-_edit_.html

www.taringa.net/posts/downloads/2716599/Retina-Network-Security-Scanner-v5_15_7-PRO-_Full_.html

http://saquenariquelme.taringa.net/posts/downloads/785792/Soft-para-redes---Freeware.html

http://software.ruletero.net/2010/09/03/nsauditor-network-security-auditor-2-0-6-0-portable-taringa/.

http://buscar.tipete.com/content/espia-pcs-y-redes-con-gfi-languard-security-scanner-taringa

http://new.taringa.net/posts/downloads/4476641/Sniffer-Colasoft-Capsa-6_9-Enterprise.html

Ubicación: Medio magnético