COMPENDIO DEL AUTOR

AUDITORIA TI

UNIDAD 1

CONCEPTOS GENERALES DE LA AUDITORÍA INFORMÁTICA

Autor: Norma Valencia C.

FR0018/ v3.01

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

ÍNDICE

1. Unidad 1: Conceptos Generales de Auditoría Informática

Tema 1: Introducción a la Auditoría TI

Objetivo

Entender conceptos relacionados a la auditoría informática, control interno y al análisis de riesgo para reconocer las funciones y usos.

Introducción

La auditoría existe desde la época media, nace como un órgano de control por la necesidad de revisar actividades o funciones específicas y de esa manera comprobar de manera independiente el buen uso, proceso y resultado de algo en particular.

Con esto se pretende establecer que la auditoría es una disciplina uniforme, que tiene antecedentes, conceptos y aplicaciones, y que su única diferencia es el objetivo que se busca alcanzar con su realización.

Vamos a entender el concepto general de auditoria para adentrarnos en la auditoria de TI que es el tema focal de esta materia.

2. Información de los subtemas

2.1 Subtema 1: Antecedentes, Definición, Objetivos y Clases de Auditoría Informática

La palabra auditoría es tan antigua como la humanidad, proviene del latín audire que significa oír, inicialmente el auditor juzgaba la verdad o falsedad de los ingresos y egresos de un negocio, principalmente oyendo. Podemos resumir entonces que la auditoria nació en el momento que fue necesario evaluar que los valores reportados en un negocio sean los correctos y directamente relacionada con la contabilidad, sin embargo, al pasar los años se fue incorporando en otros temas como la parte administrativa, medicina, educación, sistemas, etc.

American Accounting Association (AAA, 1972) definió a autoría como: Un proceso sistemático que permite la revisión objetiva de una o varias actividades, funciones específicas, operaciones o resultados de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización.

William Thomas Porter y John C. Burton definen la Auditoría como “el examen de la información por una tercera persona distinta de quien la preparó y del usuario, con la intención de establecer su veracidad; y el dar a conocer los resultados de este examen, con la finalidad de aumentar la utilidad de tal información para el usuario...” (Porter, 1983)

Una vez que tenemos claro el concepto de auditoría, vamos a revisar su clasificación:

Fuente propia

POR SU LUGAR DE ORIGEN

Identifica la forma en que se hace la auditoría y la relación laboral con el auditor.

Interno. – Es realizado por un auditor que se encuentra en relación laboral con la empresa a la que audita, conoce del negocio por lo que puede hacer una evaluación más detallada, pero debe evitar la injerencia de altos mandos en sus conclusiones.

Externo. - Normalmente realizada por empresas auditoras donde el auditor tiene total libertad de realizar un análisis objetivo con resultados totalmente independientes, sin

embargo, conoce poco de la empresa por lo que requiere de una participación del personal de la empresa.

POR SU AREA DE APLICACIÓN

Clasifica a la auditoria de acuerdo con la rama donde es utilizada:

Auditoria Financiera. – La primera auditoria en existir y consiste en la revisión de los libros contables y estados financieros para dictaminar su veracidad.

Auditoria Administrativa. – Esta auditoria consiste en evaluar funciones, actividades y operaciones desde el punto de vista administrativo, con el fin de ver que se cumplan normas, políticas y reglamentos, así como el buen uso de los recursos de la empresa.

Auditoria Operacional. – Esta auditoría se realiza a las actividades de una empresa, con el fin de evaluar su existencia, suficiencia, eficacia, eficiencia y el correcto desarrollo de sus operaciones.

Auditoria Integral. – Esta auditoría se realiza con equipo multidisciplinario que evalúa de manera integral todas las áreas que participan en la parte operativa de la empresa, así como la comunicación, procedimientos interrelacionados entre ellas.

Auditoria Gubernamental. – Esta auditoría se realiza a entidades gubernamentales con el fin de evaluar el buen uso y cumplimiento del presupuesto, así como el cumplimiento de lineamientos y regulaciones emitidas por el estado.

Auditoria informática. – Esta auditoria se encarga de llevar a cabo la evaluación de sistemas computacionales, software, información usada por los empleados de una empresa, instalaciones, redes, telecomunicaciones, equipos, centro de cómputo y demás.

AUDITORIAS ESPECIALIZADAS EN ÁREAS ESPECIFÍCAS

Son auditorias más especializadas que requieren métodos y análisis que las tradicionales.

Auditoría al área médica (evaluación médico-sanitaria). – Es una auditoría realizada por especialista de la salud para determinar el buen uso de recursos, procedimientos y atención.

Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería). Es una auditoria que se realiza a la edificación de construcciones, cimientos, obra negra, acabados de casas, edificios, puentes o cualquier otro tipo de construcción civil para evaluar la correcta aplicación de cálculos y procedimientos.

Auditoría fiscal. – Es un auditoria que se centra en comprobar los estados financieros para determinar el valor de impuestos tributarios.

Auditoría laboral. – Es una auditoría que analiza las funciones, operaciones, contratos, beneficios, seguridad de las personas.

Auditoría de proyectos de inversión. – Auditoría encargada de evaluar el buen uso de recursos y consecución de objetivo de un plan o programa de inversión.

Auditoría a la caja chica o caja mayor (arqueos). – Auditoría periódica sobre el flujo de efectivo otorgado a caja chica para su buen manejo.

Auditoría al manejo de mercancías (inventarios). – Auditoria que se encarga de verificar que las existencias físicas concuerden con los registros contables, con los justificantes de las salidas y entradas y con las incidencias de éstas.

Auditoría ambiental. – Auditoria que se encarga de analizar el medio ambiente para determinar las medidas preventivas y, en su caso, correctivas que disminuyan y eviten la contaminación.

OBJETIVOS DE LA AUDITORIA DE SISTEMAS

Ahora que tenemos claro el concepto de auditoria y en especial el de auditoría de sistemas con toda su clasificación, vamos a entender los 6 objetivos que busca la auditoria de sistemas.

1. Realizar una evaluación con personal capacitado y especializado en el área de sistemas, de esa forma emitir una conclusión independiente sobre las operaciones del sistema y la gestión administrativa del área de informática.
2. Evaluar el uso de los recursos financieros en las áreas del centro de información, así como del aprovechamiento de los recursos computacionales.
3. Evaluar el uso y aprovechamiento de los equipos de cómputo, equipos, instalaciones del centro de cómputo, así como el uso de sus recursos involucrados para el procesamiento de información.
4. Evaluar el aprovechamiento de los sistemas de procesamiento, sistemas operativos, lenguajes, programas y el desarrollo de nuevos sistemas.

5. Evaluar el cumplimiento de los lineamientos que regulan las funciones y actividades del área, los procesos de sistemas de información, así como el cumplimiento de políticas y normas.
6. Realizar la evaluación de las áreas, actividades y funciones de una empresa, con sistemas computacionales con el fin de que sean soporte para el desarrollo de auditorías por medio de la computadora.

2.2 Subtema 2: Principales Áreas de la Auditoría Informática

Enfocándonos específicamente a la auditoria informática podemos resumir las áreas en:

AUDITORÍA DE SISTEMAS COMPUTACIONALES

Veremos un concepto general para amplificarlo en las siguientes unidades de la presente materia.

Auditoría informática. - Esta auditoria se encarga de llevar a cabo la evaluación de sistemas computacionales, software, información usada por los empleados de una empresa, instalaciones, redes, telecomunicaciones, equipos, centro de cómputo y demás.

Auditoría con la computadora. – Es la auditoria donde se utiliza equipos de cómputo y programas para evaluar actividades y operaciones que pueden ser o no computarizadas, pero si son aptas para ser automatizadas.

Auditoría sin la computadora. – Es una auditoria que se enfoca a evaluar funciones, operaciones del personal de sistemas, pero desde un punto de vista operativo, financiero y administrativo sin el uso de sistemas computacionales.

Auditoría a la gestión informática. – Es una auditoria que evalúa la gestión administrativa y operacional del centro de cómputo y todo lo que esto conlleva.

Auditoría al sistema de cómputo. – Es una auditoría mas especializada que la anterior que evalúa el funcionamiento del software, hardware, comunicaciones. Adicionalmente también se evalúa el diseño, uso, aplicación y operación de los programas de la empresa.

Auditoría en el entorno de la computadora. – Esta auditoria evalúa todos los aspectos que permiten el buen funcionamiento del sistema como métodos de acceso, almacenamiento, etc.

Auditoría sobre la seguridad de sistemas computacionales. – Esta auditoría evalúa todo lo que implica seguridad en un sistema tanto como accesos y uso para mantener a salvo los equipos informáticos y sistemas.

Auditoría a los sistemas de redes. – Es una auditoría especifica de las redes considerando la tipología, protocolos, accesos, conexiones, etc.

Auditoría integral a los centros de cómputo. - Es una auditoria que revisa de manera exhaustiva, sistemática y global todas las actividades y operaciones de un centro de cómputo.

Auditoría ISO-9000 a los sistemas computacionales. – Es una auditoria que revisa los sistemas computacionales enmarcado en las normas y procedimientos dictados en el ISO-9000.

Auditoría outsorcing. – Es una auditoria que busca evaluar la calidad en el servicio de asesoría o procesamiento externo de información que proporciona una empresa a otra.

Auditoría ergonómica de sistemas computacionales. – Es una auditoria que evalúa la calidad, eficiencia y utilidad del entorno hombre-máquina-medio ambiente que rodea el uso de sistemas computacionales en una empresa.

2.3 Subtema 3: Tipos de Delitos Informáticos Comunes

Empecemos por definir que es un delito informático o ciberdelitos.

El incremento del uso de la tecnología ha permitido que exista más posibilidad a que personas hagan mal uso de ella.

Según la organización de las Naciones Unidas (UNODC) dice que un delito informático es un número ilimitado de actos contra la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos. En Ecuador se definió como toda actividad ilegal o ilícita que se haya realizado mediante el uso de la tecnología como computadora, internet, etc. Ya existe una ley que sanciona estos delitos informáticos desde el 10 de agosto del 2014 en el código orgánico integral penal.

Enfocándonos en Ecuador podemos resumir los tipos de delitos mas comunes son:

- Suplantación de identidad
- Falsificación y uso de documentos falsos
- Apropiación fraudulenta por medios electrónicos
- Acceso no consentido a un sistema informático, telemático de comunicaciones
- Contacto con finalidad sexual con menores de 18 años por medios electrónicos
- Ataque a la integridad de sistemas informáticos
- Interceptación ilegal de datos
- Entre otros

Podemos ver como estos casos van aumentando año tras año en el siguiente cuadro elaborado por la fiscalía general del estado y publicado en el diario El Universo en el año 2020.

NÚMERO DE DENUNCIAS SOBRE DELITOS INFORMÁTICOS EN ECUADOR

Tipos de delitos	2014*	2015	2016	2017	2018	2019	2020**	
Suplantación de identidad	1355	3920	4152	3676	4180	4607	2162	24 052
Falsificación y uso de documento falso	1048	2594	3117	3183	3292	3231	1448	17 913
Apropiación fraudulenta por medios electrónicos	507	1280	1045	960	1451	1746	1033	8022
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	54	141	145	218	236	246	175	1215
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	21	80	108	159	202	166	85	821
Ataque a la integridad de sistemas informáticos	49	77	76	86	87	113	51	539
Interceptación ilegal de datos	38	55	82	63	41	87	45	411
Transferencia electrónica de activo patrimonial	17	59	47	54	38	49	31	295
Revelación ilegal de base de datos	29	24	24	22	44	34	18	195
Total	**3118**	**8230**	**8796**	**8421**	**9571**	**10 279**	**5048**	**53 463**

*Desde agosto - **Hasta agosto

Fuente Fiscalía general del Estado y publicada por diario El Universo

2.4 Subtema 4: Tipos de Vulnerabilidades, Tipos de Amenazas, Tipos de Ataque

Si enfocamos las vulnerabilidades y amenazas a nivel empresarial podemos observar el siguiente cuadro que muestra los ataques a empresas latinoamericanas en el año 2016 luego de realizar una encuesta a profesionales de TI de Argentina, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela.

En primer lugar, tenemos a **Malware** que es cualquier tipo de software malicioso diseñado para dañar o deshabilitar cualquier dispositivo, servicio o red. Su objetivo principal es robar, cifrar o hasta borrar información para obtener dinero. Existen varios tipos:

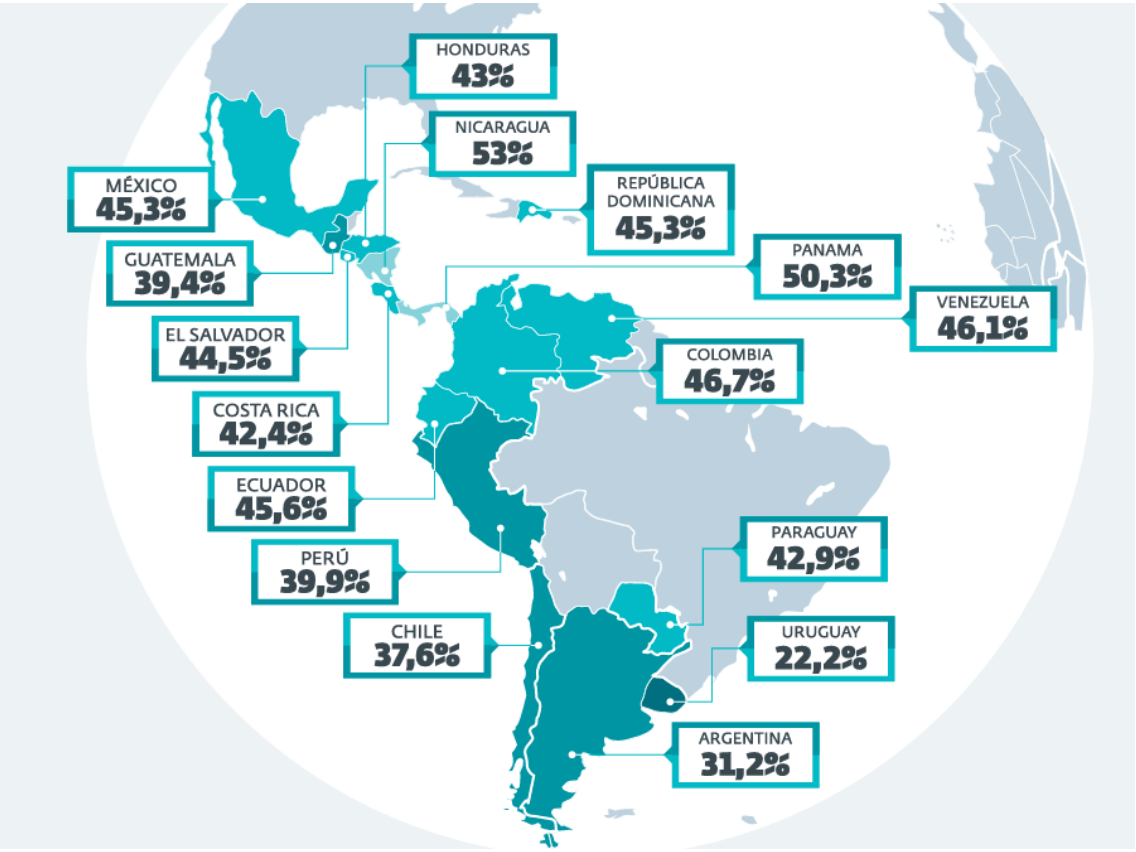
El adware es un software no deseado diseñado para mostrar anuncios en su pantalla.
El spyware observa las actividades del usuario en el dispositivo y se las comunica al autor del software.

Un virus que se adjunta a otro programa y, cuando se ejecuta se replica modificando otros programas del ordenador e infectándolos.
Los gusanos son un tipo de malware similar a los virus, que se replica por sí solo con el fin de diseminarse por otros ordenadores en una red, normalmente provocando daños y destruyendo datos y archivos.

Un troyano, o caballo de Troya, es uno de los más peligrosos. Normalmente se presenta como algo útil para engañar al usuario, obtienen acceso no autorizado al ordenador y roban información financiera.

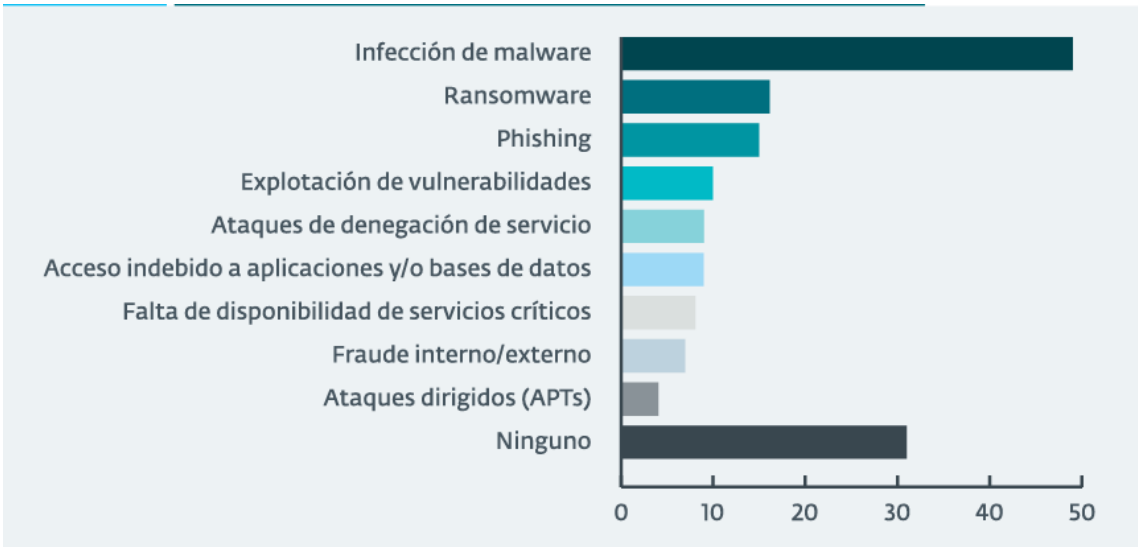
El rootkit es un tipo de malware que proporciona al atacante privilegios de administrador en el sistema infectado.
Un registrador de pulsaciones de teclas es malware que graba todas las pulsaciones de teclas del usuario, almacena la información recopilada y se la envía al atacante, que

busca información confidencial, como nombres de usuario, contraseñas o detalles de la tarjeta de crédito.



Infecciones de malware a empresas por país 2016

El **ransomware** es un tipo de malware que bloquea el acceso del usuario al dispositivo o cifra sus archivos y después lo fuerza a pagar un rescate para devolvérselos. El ransomware se ha reconocido como el arma preferida de los delincuentes informáticos porque exige un pago rápido y provechoso en criptomoneda de difícil seguimiento. El código que subyace en el ransomware es fácil de obtener a través de mercados ilegales en línea y defenderse contra él es muy difícil.



Incidentes de seguridad de empresas latinoamericanas 2016

Fuente: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

El **Phishing** es la suplantación de identidad (phishing) El phishing es un método para engañarle y hacer que comparta contraseñas, números de tarjeta de crédito, y otra información confidencial haciéndose pasar por una institución de confianza en un mensaje de correo electrónico o llamada telefónica como por ejemplo campañas falsas de bancos e incluso en la actualidad han obtenido información con campañas falsas en empresas como Apple, mercado libre, Facebook e Instagram.

Por todo lo antes mencionado se vuelve clave tener una auditoria de TI completa que permita a las empresas salvaguardar su información critica de ella y de sus clientes.

3. Preguntas de Comprensión de la Unidad 1

1. Pregunta de comprensión Nro. 1
¿Qué es auditoria?

American Accounting Association (AAA, 1972) definió a autoría como: Un proceso sistemático que permite la revisión objetiva de una o varias actividades, funciones específicas, operaciones o resultados de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización.

William Thomas Porter y John C. Burton definen la Auditoría como "el examen de la información por una tercera persona distinta de quien la preparó y del usuario, con la intención de establecer su veracidad; y el dar a conocer los resultados de este examen, con la finalidad de aumentar la utilidad de tal información para el usuario..." (Porter, 1983)

2. Pregunta de comprensión Nro. 2
¿Qué es auditoría interna y externa?

Identifica la forma en que se hace la auditoría y la relación laboral con el auditor.
Interno. – Es realizado por un auditor que se encuentra en relación laboral con la empresa a la que audita, conoce del negocio por lo que puede hacer una evaluación más detallada, pero debe evitar la injerencia de altos mandos en sus conclusiones.
Externo. - Normalmente realizada por empresas auditoras donde el auditor tiene total libertad de realizar un análisis objetivo con resultados totalmente independientes, sin embargo, conoce poco de la empresa por lo que requiere de una participación del personal de la empresa.

3. Pregunta de comprensión Nro. 3
¿Nombre algunos ejemplos de delitos informáticos en Ecuador?

Suplantación de identidad
Falsificación y uso de documentos falsos
Apropiación fraudulenta por medios electrónicos
Acceso no consentido a un sistema informático, telemático de comunicaciones
Contacto con finalidad sexual con menores de 18 años por medios electrónicos
Ataque a la integridad de sistemas informáticos

4. Pregunta de comprensión Nro. 4

¿Cuáles son los objetivos de la auditoría informática?

1. Realizar una evaluación con personal capacitado y especializado en el área de sistemas, de esa forma emitir una conclusión independiente sobre las operaciones del sistema y la gestión administrativa del área de informática.
2. Evaluar el uso de los recursos financieros en las áreas del centro de información, así como del aprovechamiento de los recursos computacionales.
3. Evaluar el uso y aprovechamiento de los equipos de cómputo, equipos, instalaciones del centro de cómputo, así como el uso de sus recursos involucrados para el procesamiento de información.
4. Evaluar el aprovechamiento de los sistemas de procesamiento, sistemas operativos, lenguajes, programas y el desarrollo de nuevos sistemas.
5. Evaluar el cumplimiento de los lineamientos que regulan las funciones y actividades del área, los procesos de sistemas de información, así como el cumplimiento de políticas y normas.
6. Realizar la evaluación de las áreas, actividades y funciones de una empresa, con sistemas computacionales con el fin de que sean soporte para el desarrollo de auditorías por medio de la computadora.

5. Pregunta de comprensión Nro. 5

¿Qué es phishing?

Es la suplantación de identidad (phishing) El phishing es un método para engañarle y hacer que comparta contraseñas, números de tarjeta de crédito, y otra información confidencial haciéndose pasar por una institución de confianza en un mensaje de correo electrónico o llamada telefónica Beneficiosa.

4. Material Complementario

Los siguientes recursos complementarios son sugerencias para que se pueda ampliar la información sobre el tema trabajado, como parte de su proceso de aprendizaje autónomo:

Bibliografía de apoyo:

- Auditoría en sistemas computacionales, Carlos Muñoz Razo, 2002

Links de apoyo:

- https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf
- https://es.malwarebytes.com/malware/

5. Bibliografía

» CEVALLOS MORENO MARCO ANTONIO. (2011). AUDITORÍA INFORMÁTICA (1 Ejemplar disponible en Biblioteca)