AUDITORÍA INFORMÁTICA: CONCEPTUALIZACIÓN

MATERIAL DE FORMACIÓN

MATERIAL DE FORMACIÓN 3

1

Contenido

1. CUALIDADES DEL AUDITOR

1.1 CONOCIMIENTOS PREVIOS: FORMACIÓN PROFESIONAL Y NORMATIVA

El auditor debe ser una persona:

- **Analítica.** La cualidad analítica le ayuda al auditor evaluar y recomendar de una manera óptima el resultado de la actividad.
- **Observadora.** Esto ayudará, en gran parte, a conocer lo que realmente pasa en los procesos y métodos analizados, además de tomar mejores evidencias.
- **Imparcial.** No debe dejarse llevar por algún tipo de prejuicio o relación con el auditado y realizar la auditoría con total profesionalismo. El auditor no participará, en evaluar operaciones, en las cuales anteriormente tuvo alguna responsabilidad.
- **Discreta.** El auditor debe mantener la discreción necesaria para mantener la información suministrada por la empresa en completa reserva y confidencialidad, sabiendo que puede poseer información sensible sobre los procesos y métodos de la organización auditada.
- **Independiente.** El auditor debe adoptar una actitud de independencia de criterio, respecto a la entidad examinada y mantener libre de cualquier situación que terceras personas pudiesen señalarle como incompatibles con su integridad y objetividad.

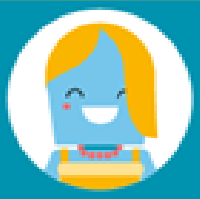
Imagen 1. **Cualidades del auditor.**

Fuente: (SENA – Equipo de Adecuación Didáctica y Gráfica de Recursos Educativos Risaralda, 2014).

1.2 Formación profesional y normativa

La auditoría debe desarrollarse, por personas con la formación profesional y técnica requerida por el campo que está auditando, además de poseer las certificaciones que requiera la ley.

El auditor debe tener experiencia en el campo, de hecho es recomendable que ya haya participado en otras auditorías. Esta experiencia profesional práctica necesaria se obtiene participando, en la ejecución de trabajos de auditoría, bajo la supervisión y revisión de un auditor en ejercicio.

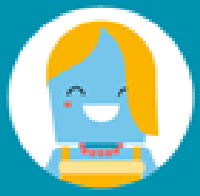


De igual manera debe destacarse como experto en la materia auditada. Su conocimiento técnico y estudios profesionales deben de ser superiores a los auditados, o por lo menos ser par de ellos; de no ser así, se podrá apoyar en expertos de diferentes áreas en la medida que lo requiera para formar un equipo multidisciplinario, con el fin de realizar la auditoría. Además, el auditor debe estar en una continua actualización de sus conocimientos técnicos y en las normas actualizadas.

También debe conocer muy bien los procesos del departamento a auditar y las normas o resoluciones que afectan directamente dichos procesos.

En lo que respecta a la auditoría informática, también conocida como tecnología de la información, el auditor debe poseer bases en las siguientes áreas:

- Rediseño de sistemas de información.
- Desarrollo organizacional.
- Análisis y diseño.
- Comunicaciones.
- Planeación.
- Administración de proyectos.



De igual manera, se espera que todo auditor en sistemas de información tenga conocimientos básicos en:

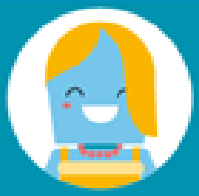
- Finanzas y contabilidad.
- Sistemas de información.
- Auditoría.
- Procesamiento electrónico de datos.
- Telecomunicaciones.
- Teoría general de sistemas.
- Métodos numéricos.
- Administración de empresas.

2. ENTRENAMIENTO

El entrenamiento que reciba el auditor se debe estimar cada año. De hecho se han hecho propuestas para que se realice un plan de entrenamiento al auditor, por lo menos durante tres semanas, pero esta recomendación se debe estudiar, pues al tener una empresa con tecnología nueva en lo referente a hardware y software, se estimará un tiempo más largo, comparándolo por ejemplo, con una empresa que lleve varios años trabajando ajustado a la misma tecnología.

Otro tema que se debe de tomar en cuenta es la cantidad de veces que se cambian los procesos, las regulaciones de la empresa, las normalizaciones y certificaciones, y las regulaciones legales.

Además, el factor de la experiencia del auditor incide en el tiempo de entrenamiento a recibir, entre más años experiencia tenga el auditor, menor debe



ser el tiempo que requiere su entrenamiento, por el contrario, si es un auditor que recién empieza, se requerirá un mayor tiempo en su preparación y entrenamiento.

2.1 Técnicas en el entrenamiento

El auditor informático debe poseer las capacidades para desarrollar las siguientes técnicas:

- **Comparación de programas**

Técnica empleada para realizar una comparación de código entre la versión de un programa en ejecución y la versión de un programa piloto, la cual ha sido alterada en forma indebida para encontrar diferencias.

- **Mapeo y rastreo de programas**

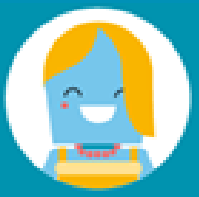
Esta técnica utiliza un software especializado, el cual permite analizar los programas en ejecución, indicando el número de veces que cada línea de código es procesada y las de las variables de memoria que estuvieron presentes.

- **Análisis de código de programas**

Técnica usada para analizar los programas de una aplicación. El análisis puede efectuarse en forma manual.

- **Datos de prueba**

Se utiliza para verificar que los procedimientos de control, incluidos los programas de una aplicación, funcionen correctamente. Los datos de prueba consisten en la preparación de una serie de transacciones, las cuales contienen tanto datos correctos como datos erróneos predeterminados.



- **Datos de prueba integrados**

Técnica muy similar a la anterior, con la diferencia que en esta se debe crear una entidad falsa dentro de los sistemas de información.

- **Análisis de bitácoras**

Técnica para evaluar los tipos de bitácoras, sea en forma manual o por medio de programas especializados, tales como bitácoras de fallas del equipo, bitácoras de accesos no autorizados, bitácoras de uso de recursos, bitácoras de procesos ejecutados.

- **Simulación paralela**

Técnica muy utilizada que consiste en desarrollar programas o módulos que simulen a los programas de un sistema en producción. El objetivo es procesar los dos programas o módulos de forma paralela e identificar diferencias entre los resultados de ambos.

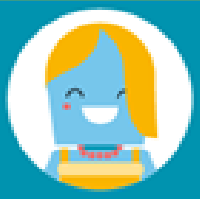
Imagen 2. **Técnicas en el entrenamiento.**

Fuente: (SENA – Equipo de Adecuación Didáctica y Gráfica de Recursos Educativos Risaralda, 2014).

3. ALGUNAS CERTIFICACIONES DE AUDITORÍA

En Colombia existen varias certificaciones referentes a la informática y a los sistemas de información, algunas de estas normas son:

- **La ISO 9001**: establece la estructura de un Sistema de Gestión de la Calidad en red de procesos.



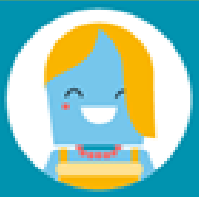
- **La ISO/IEC 27001**: enfocada en seguridad de la información, especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).
- **Certificación auditor CISA** (*Certified Information Systems Auditor*): es el nombre de la certificación de referencia en el mundo de la auditoría tecnológica

Estas certificaciones implican un tiempo de entrenamiento dependiendo de certificaciones anteriores, pues el auditor la primera vez que se certifique en alguna de esas normas necesitará un mayor tiempo que el auditor que ya esté certificado y solo requiera una actualización de la norma.

4. DELITOS INFORMÁTICOS

Los delitos informáticos, por su mundo intangible, son difíciles de explicar y de comprender o conceptualizar plenamente. Incluso varios autores y organismos lo han intentado definir el delito informático como:

- Los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos (Convenio de Ciberdelincuencia Europeo, 2001).
- La especificidad del delito informático, le viene dada por dos factores fundamentales: las acciones se vinculan al funcionamiento de una máquina



y, en buena parte de los supuestos, recae sobre un objeto intangible o inmaterial (Choclán-Montalvo, 1997).

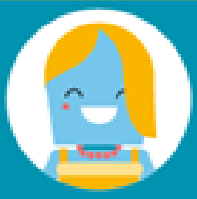
- La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnere los derechos del titular de un elemento informático, ya sea hardware o software (Davara-Rodríguez, 2007).
- Podría ser delito informático, todo comportamiento criminal en el que aparezca involucrado un ordenador; de este modo, casi cualquier delito con esta peculiaridad podría ser, eventualmente delito informático (Aldama-Baquedano, 1993).

Existen multitud de opiniones o formas para definirlo, llegando incluso algunos expertos a concluir que no constituyen una nueva categoría delictiva y que no se han de diferenciar los delitos informáticos, de los delitos comunes que ya se vienen castigando: delitos contra las personas, el honor, la libertad, la seguridad pública o de la Nación. La única diferencia entre ellos es el medio por el cual se llevan a cabo, pero como el resultado final es el mismo, no cabe diferencia alguna.

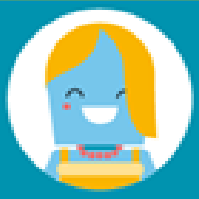
En Colombia existe la Ley 1273 de 2009 denominada *De la protección de la información y de los datos*, en la cual se ha tratado de encuadrar los delitos informáticos, algunos de ellos son: robo, hurto, fraudes, falsificaciones, estafa, sabotaje, etc.

Las categorías propuestas por la ley son las siguientes:

-



- De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos:
- Acceso abusivo a un sistema informático.
- Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Interceptación de datos informáticos.
- Daño informático.
- Uso de software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales.
- Circunstancias de agravación punitiva: se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

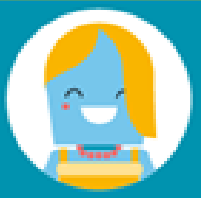


- **Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales del sector financiero, nacionales o extranjeros.**
- **Por servidor público en ejercicio de sus funciones.**
- **Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.**
- **Revelando o dando a conocer el contenido de la información en perjuicio de otro.**
- **Obteniendo provecho para sí o un tercero.**
- **Con fines terroristas o generando un riesgo para la seguridad o defensa nacional.**
- **Utilizando como instrumento un tercero de buen fe.**
- **Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada, con equipos computacionales.**

En su mayoría, un acusado enfrentaría una pena de prisión de cuarenta y ocho a noventa y seis meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, y solo en el caso de interceptación de datos informáticos, sería una pena de prisión, de treinta y seis a setenta y dos meses.

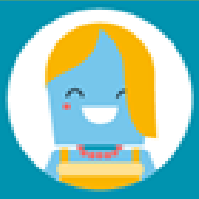
Por otro lado, los dos siguientes son más penalizados:

- **De los atentados informáticos y otras infracciones.**
- Hurto por medios informáticos y semejantes, pena de prisión de 3 a 8 años.
- Transferencia no consentida de activos, pena de prisión de 48 a 120 meses y multa de 200 a 1.500 salarios mínimos vigentes.



En este tipo de delitos existen dos tipos de sujetos:

Activos.	Pasivos.
Son aquellos que comenten el acto delictivo y que poseen conocimientos de informática necesarios para ello.	Son las víctimas sobre quienes recae la conducta de acción u omisión que realiza el sujeto activo.



CONCLUSIONES

Quien quiera perfilarse como auditor en informática no solo debe poseer ciertas cualidades, sino que constantemente requiere un entrenamiento y estar actualizado sobre las diversas certificaciones requeridas en el ámbito de las auditorías. De igual manera, reconocer qué es un delito informático.

Por ello, es relevante que quien esté interesado en ser auditor informático tenga en cuenta la importancia de seguir preparándose para ofrecer alternativas de mejora a las empresas que son auditadas.

BIBLIOGRAFÍA

Aguirre Sánchez, Y. (Sin fecha). *Propuesta de implantación del área de auditoría en informática en un órgano legislativo*. Consultado el 10 de abril de 2016, en http://olea.org/~yuri/propuesta-implantacion-auditoria-informatica-organo-legislativo/

Aldama-Baquedano, C. (1993). *Los medios informáticos*. Poder Judicial (30), 9-26.

Choclán-Montalvo, J. A. (1997). *Estafa por computación y criminalidad económica vinculada a la informática*. Actualidad Penal (47), 22-28.

Davara, M. Á. (2002). *Fact Book del comercio electrónico*. Ediciones Arazandi, Segunda Edición.

Echenique García, J. A. (2001). *Auditoría en informática*. Segunda edición. McGraw Hill: México.

Consejo de Europa. Ministerio de Asuntos Exteriores. Oficina de Interpretación de Lenguas. *Convenio sobre la ciberdelincuencia.* Consultado el 9 de abril de 2016, en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf

Normas y procedimientos de auditoría. (Sin fecha). Instituto Mexicano de Contadores Públicos (IMCP). Consultado el 10 de abril de 2016, en http://www.oas.org/juridico/spanish/mesicic3_mex_anexo11.pdf

BIBLIOGRAFÍA

Ministerio de Tecnologías de la Información y las Comunicaciones. (2009). *Ley nro. 1273 de 2009.* Consultado el 9 de abril de 2016, en http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Imágenes

CONTROL DE DOCUMENTO

Autores	Nombre	Cargo	Dependencia	Fecha
Expertos temáticos	Julián Andrés Sierra Dixon Fernando Cano	Expertos temáticos.	Equipo de Adecuación Didáctica y Gráfica de Recursos Educativos Risaralda	6 de abril de 2016
Revisión	Sandra Milena Henao Melchor. Víctor Hugo Suárez	Guionistas.	Equipo de Adecuación Didáctica y Gráfica de Recursos Educativos Risaralda	13 de abril de 2016
	Andrés Felipe Valencia Pimienta	Líder	Equipo de Adecuación Didáctica y Gráfica de Recursos Educativos Risaralda	15 de abril de 2016

Créditos

Equipo
Centro de Diseño e Innovación Tecnológica Industrial
Servicio Nacional de Aprendizaje – SENA –
Dosquebradas, Risaralda

Subdirector de Centro: Jhon Freddy Amaya Taborda

Líder: Andrés Felipe Valencia Pimienta

Expertos temáticos:
Julián Andrés Sierra
Dixon Fernando Cano

Asesores pedagógicos:
Andrés Felipe Valencia Pimienta
Sandra Milena Henao Melchor

Guionistas:
Víctor Hugo Suárez
Sandra Milena Henao Melchor

Diseñadores:
Lina Marcela Cardona Osorio
Mario Fernando López Cardona

Desarrolladores *Front End*:
Cristian Fernando Dávila López

Pasantes
Carlos Arturo Valencia
Jorge Andrés González H.