AUDITORÍA INFORMÁTICA

AUTOR: ORLANDO ESPINOZA B.

MARZO: 2021

San Marcos

MIEMBRO DE LA RED ILUMNO

San Marcos

Universidad San Marcos

Bachillerato en Ingeniería en Sistemas

Auditoria informática

San José, Marzo / 2021.

Primer Edición.

Recopilador: Orlando Espinoza B.

Tabla de Contenido

Auditoría informática

En la página web referenciada como #1, se indica lo siguiente: “La Auditoría Informática es un proceso que consiste en recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos ya que esta lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, cumple con las leyes y regulaciones establecidas”. Este es el este concepto que abarca muchos ámbitos, en adelante se detallará algunos tipos.

Conceptos de auditoría de sistemas

En la página WEB, Wikipedia lo define como: “Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo y/o corrección siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

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

Contiene las siguientes fases:

- Enumeración de redes, topologías y protocolos
- Verificación del Cumplimiento de los estándares internacionales. ISO, COBIT, etc.
- Identificación de los sistemas operativos instalados
- Análisis de servicios y aplicaciones
- Detección, comprobación y evaluación de vulnerabilidades
- Medidas específicas de corrección
- Recomendaciones sobre implantación de medidas preventivas”.

Tipos de auditoría informática

En la página web referenciada como #1, se definen los siguientes tipos:

- **Auditoría de la gestión**: la contratación de bienes y servicios, documentación de los programas, etc.
- **Auditoría legal del Reglamento de Protección de Datos**: Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.
- **Auditoría de los datos**: Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.
- **Auditoría de las bases de datos**: Controles de acceso, de actualización, de integridad y calidad de los datos.
- **Auditoría de la seguridad**: Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
- **Auditoría de la seguridad física**: Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.
- **Auditoría de la seguridad lógica**: Comprende los métodos de autenticación de los sistemas de información.
- **Auditoría de las comunicaciones**. Se refiere a la auditoría de los procesos de autenticación en los sistemas de comunicación.
- **Auditoría de la seguridad en producción**: Frente a errores, accidentes y fraudes.
- **Auditoría a empleados**: Frente a errores, accidentes y fraudes, accesos no autorizados y vulnerabilidad de claves.

Normativas

Las normas sirven para implementar los procesos que son utilizadas para proteger el almacenamiento, procesamiento y transmisión de la información digital de forma segura, disponible y confiable.

A nivel mundial se tienen algunas normas de seguridad informática que se detallan a continuación

Normas ISO 27000

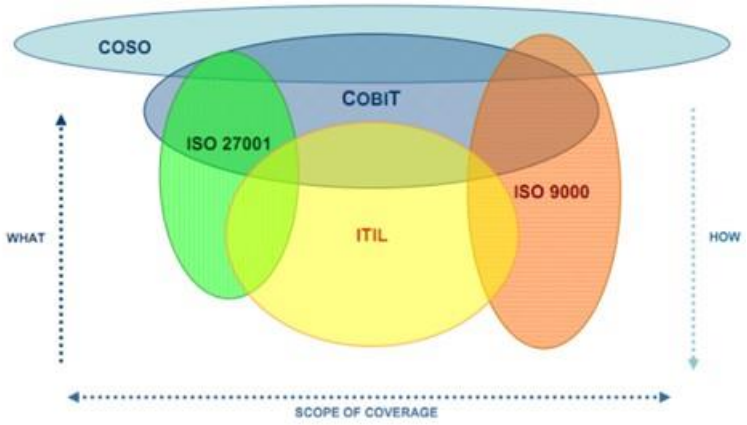
La principal norma que se aplica a nivel internacional es la familia de las normas ISO 27000 establecida por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que son los organismos encargados de establecer estándares

y guías relacionadas con sistemas de gestión y que se puedan aplicar en cualquier tipo de organización. Esta norma es un conjunto de estándares de seguridad que proporciona un marco para la gestión de la seguridad. Su base es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos o procesos autorizados cuando lo requiera.



Relación con otras normas

Ley Sarbanes-Oxley o Ley SOX

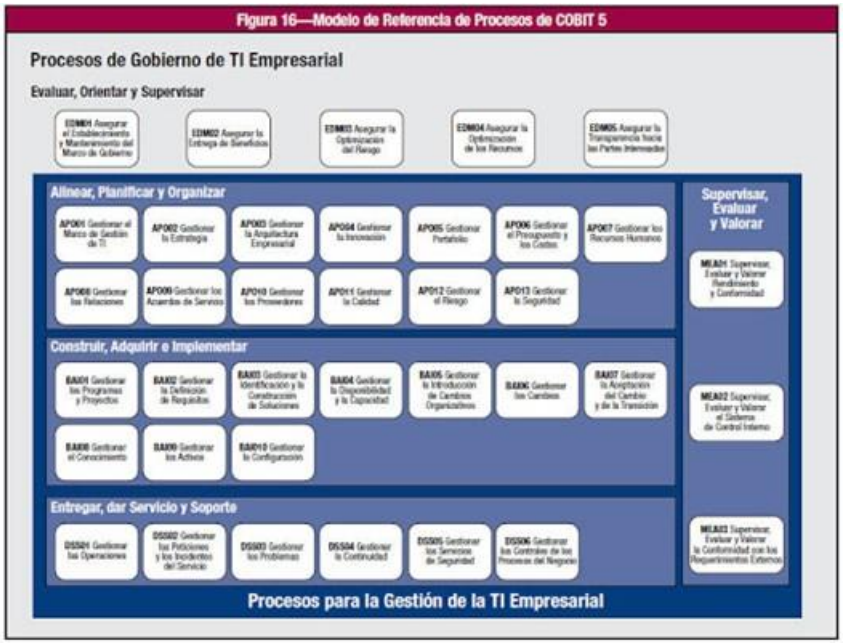
Se implementó en los EEUU a raíz de los escándalos financieros de corrupción realizados por grandes corporativas pues hicieron perder la confianza a la población tanto para las auditorias como los sistemas financieros. El propósito principal es monitorear las empresas cotizantes en la bolsa de valores para evitar que las acciones sean alteradas de forma dudosa. Su finalidad es evitar fraudes y riesgos de bancarrota y proteger a los inversionistas dueños de las acciones.

Esta ley mejora la calidad de la información financiera basándose en normas contables internacionales, control interno y gobierno corporativo. También implementa el control del almacenamiento de la información, también obliga a los departamentos de tecnología de información establecer protocolos de autenticación para el almacenamiento y recuperación de la información.

COBIT

Los Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT por sus siglas en inglés) es un framework o marco de trabajo con guías de mejores prácticas dirigido al gobierno, gestión, control y supervisión de la tecnología de la información.

Hay varias versiones, pero la que está en vigencia e implementación es la denominada COBIT 5 que consisten en 37 procesos: 5 procesos de gobierno, 3 procesos de supervisión y 29 procesos de gestión:



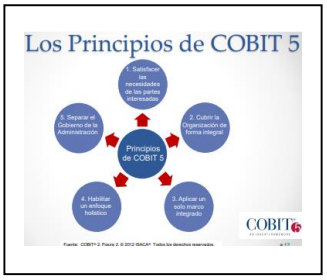
Procesos Catalizadores

Para la implementación de cada proceso, se definen una serie de practicas con entradas, salidas, indicadores de medición y una matriz RACI que define los dueños del proceso, responsables de la gestión, los consultados y los informados.

Este marco de trabajo es definido por la Asociación de Auditoría y Control de Sistemas de Informacion (ISACA por sus siglas en inglés).

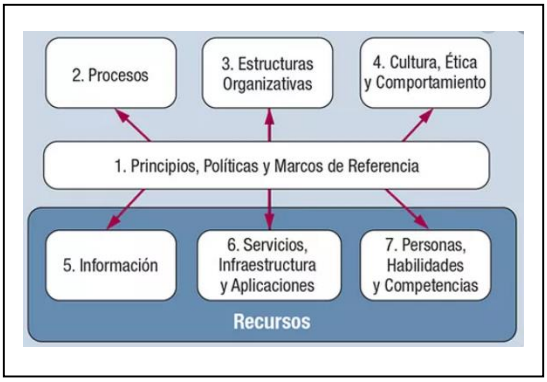
Se basa en 5 principios

1. Satisfacer las necesidades de las partes interesadas
2. Cubrir la organización de forma integral
3. Aplicar un solo marco integrado
4. Habilitar un enfoque holístico
5. Separar el Gobierno de la Gestión



Cuenta con 7 habilitadores en la empresa:

1. Principios, Políticas y Marcos de Referencia
2. Procesos
3. Estructura Organizacional
4. Cultura, Ética y Comportamiento
5. Información
6. Servicios, Infraestructura y Aplicaciones
7. Personas, Habilidades y Competencias



El informe de auditoría informática

El informe es el documento donde se identifican los resultados obtenidos durante la evaluación o la auditoria informática. Debe reflejar los objetivos, alcances, observaciones, recomendaciones y conclusiones del proceso de evaluación relacionados con el área de informática.

Se exponen observaciones, debilidades, áreas de oportunidades y acciones de mejora, plazos sugeridos para su atención, involucrados y responsables.

Entre los requisitos del informe se tienen:

- Ser veraz: La información debe reflejar la verdadera situación de la empresa
- Estar documentada formalmente: Planes, matriz de riesgos, entrevistas aplicadas, cuestionarios, observaciones, FODA, recomendaciones, revisiones formales.
- Contar con recomendaciones y soluciones para cada observación.
- Reflejar áreas de oportunidades como: capacitación, actualización, formalización de procesos de administración y desarrollo de sistemas.

Para elaborarlo se debe:

1. Aplicar herramientas de recopilación

2. Registrar las situaciones encontradas de las desviaciones halladas durante la revisión
3. Comentar las situaciones encontradas con los auditados
4. Encontrar en conjunto con los auditados, las causas de las desviaciones y sus posibles soluciones
5. Analizar, depurar y corregir las desviaciones encontradas
6. Jerarquizar las desviaciones encontradas y concentrar las mas importantes en el formado de situaciones relevantes
7. Comentar las situaciones relevantes con los directivos del área de sistemas y confirmar las causas y soluciones
8. Concentrar, depurar y elaborar el informe final de auditoria, así como el dictamen del auditor
9. Presentar el informe y dictamen final al cuerpo directivo de la empresa.

Bibliografía

1. Chicano, E. (2019). Auditoría de seguridad informática. IC Editorial.
2. Cañon, L. (2015). Ataques Informáticos Ethical Hacking y conciencia de seguridad informática en niños. (Trabajo de Fin de Grado). Universidad Piloto, Colombia

Páginas WEB revisadas.

1. Wikipedia), (15/02/2021), Auditoría Informática, Recuperado de la página: https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica
2. Wikipedia), (15/02/2021), Auditoría de seguridad de sistemas de información, Recuperado de la página: https://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3n
3. Nueva ISO 9001:2015, (15/02/2021),¿Quiere saber lo que significa la gestión de calidad?, https://www.nueva-iso-9001-2015.com/2018/10/quiere-saber-lo-que-significa-la-gestion-de-calidad/

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica