



GOBIERNO DEL
ESTADO DE MÉXICO



TECNOLOGICO DE ESTUDIOS SUPERIORES DE IXTAPALUCA

MATERIA:

AUDITORÍA DE LA SEGURIDAD INFORMÁTICA

PROFESOR:

KEVIN RAMIREZ VITE

ESTUDIANTE:

LAURA RAMOS GONZÁLEZ

GRUPO:

1951

TRABAJO:

GLOSARIO

FECHA DE ENTREGA:

10 DE SEPTIEMBRE DEL 2020

1. La auditoría informática: es el proceso de recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.
2. Auditar: consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización.
3. Fiabilidad: se define como la probabilidad de que un sistema se comporte tal y como se espera de él. En general, un sistema será seguro por la que se mide el tiempo de funcionamiento sin fallos.
4. Una auditoría de seguridad informática: 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.
5. Confidencialidad: es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
6. Certificaciones: es un procedimiento destinado a que un organismo independiente y autorizado valide o dictamine la calidad del sistema aplicado por una organización partiendo y verificando si la misma cumple o no lo dispuesto por un determinado referencial o modelo de calidad, reconocido y oficial.
7. Teleproceso: se refiere al procesamiento de datos provenientes de terminales en una unidad central
8. Sistema operativo: es un conjunto de programas o software, destinado a permitir la comunicación entre el usuario y la máquina de forma cómoda y eficiente.
9. Administración de riesgos: es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza a través de una secuencia de actividades humanas que incluyen la identificación, el análisis y la evaluación de riesgo, para luego establecer las estrategias de su tratamiento utilizando recursos gerenciales
10. Control interno: es el sistema integrado por un conjunto de acciones, actividades, planes, normas, registros, procedimientos y métodos, acordados dentro de una empresa para promover la eficiencia operacional y el cumplimiento de las políticas gerenciales
11. La auditoría interna: es la realizada con recursos materiales y personas que pertenecen a la empresa auditada.

12. La auditoría externa, conocida también como auditoría independiente: la efectúan profesionistas que no dependen de la empresa, ni económicamente ni bajo cualquier otro concepto, y a los que se conoce un juicio imparcial merecedor de la confianza de terceros.
13. Sistema de Seguridad Informática: es un conjunto de medios administrativos, medios técnicos y personal que de manera interrelacionada garantizan niveles de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados
14. Programa de seguridad: es el resultado de una estrategia trazada para proteger a la organización y sus activos; por lo tanto, debe perseguir objetivos específicos que se desean alcanzar
15. Vulnerabilidad (en términos de informática): es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma
16. La tecnología informática (hardware, software, redes, bases de datos, etc.): es una herramienta estratégica que brinda rentabilidad y ventajas competitivas a los negocios
17. Análisis de sistemas: es la ciencia encargada del análisis de sistemas grandes y complejos, y la interacción entre los mismos.
18. Rentabilidad: Relación existente entre los beneficios que proporciona una determinada operación o cosa y la inversión o el esfuerzo que se ha hecho; cuando se trata del rendimiento financiero; se suele expresar en porcentajes.
19. Auditoría financiera: es un procedimiento mediante el cual las empresas someten al examen de un experto (sea éste de la organización o independiente de ella) su informado económico- financiera. contenida ésta en los estados financieros, en el estado de origen y aplicación de fondos y justificantes de los mismos, al objeto de asegurar su integridad y razonabilidad, en concordancia con los principios de contabilidad generalmente aceptados.
20. Auditoría organizativa: en el campo de aplicación de la auditoría organizativa entraría el análisis de la adecuación de los procedimientos establecidos y de las funciones distribuidas físicamente, según las necesidades y problemas de la empresa.
21. Auditoría de gestión: tiene por misión conocer si las principales decisiones de gestión en la empresa han sido tomadas de una forma consistente. Entre otros aspectos estudia si las informaciones existentes son suficientes y óptimas para apoyar la decisión y si los procesos de estudio son razonables.

22. Auditoría integral: es la revisión exhaustiva, sistemática y global que realiza un equipo multidisciplinario de profesionales a todas las actividades y operaciones de una empresa, con el propósito de evaluarla de manera integral, todas sus áreas administrativas.
23. Auditoría gubernamental: Es la revisión exhaustiva, sistemática y concreta que se realiza a todas las actividades y operaciones de una entidad gubernamental.
24. El examen que comporta una auditoria informática abarca una serie de controles, verificaciones, juicios, etc., para concluir en un conjunto de recomendaciones y un plan de acción. Es la elaboración de este plan de acción lo que diferencia la auditoria informática de lo que, por lo visto hasta ahora, podría ser una auditoría de gestión.
25. La auditoría tradicional concluye emitiendo un juicio del estado de todo aquello que se ha verificado, la auditoría informática avanza un paso más y se atreve a elaborar un plan de actuación.
26. Auditoría fiscal: Consiste en verificar el correcto y oportuno pago de los diferentes impuestos y obligaciones fiscales de los contribuyentes desde el punto de vista físico (SHCP), direcciones o tesorerías de hacienda estatales o tesorerías municipales.
27. Auditoria de legalidad: este tipo de auditoria tiene como finalidad revisar si la dependencia o entidad, en el desarrollo de sus actividades, ha observado el cumplimiento de disposiciones legales que sean aplicables (leyes, reglamentos, decretos, circulares, etc)
28. Auditoría permanente: se realiza periódicamente a lo largo del ejercicio económico.
29. Auditoría total: afecta a todos los elementos de la empresa.
30. los auditores exponen en su informe aquellos puntos débiles que hayan podido detectar, así como las recomendaciones sobre los cambios convenientes a introducir, en su opinión, en la organización de la compañía