INSTITUTO POLITÉCNICO NACIONAL
SECRETARIA ACADÉMICA
DIRECCIÓN DE EDUCACION MEDIA SUPERIOR
CENTRO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS No. 13
“RICARDO FLORES MAGÓN”

GUÍA

de estudiopara presentar ETS de la UNIDAD DE APRENDIZAJE

AUDITORIA INFORMÁTICA

Semestre 2026-2

TURNO VESPERTINO

Integrantes de la academia: José Arturo González Zárate.

Fecha de Elaboración: 27/04/2026

FORMATO DE LA GUÍA DE ESTUDIO

Área:	Nombre de la Unidad de Aprendizaje:	Nivel/semestre:
Tecnológica	**Auditoria Informática.**	**Sexto**

Instrucciones generales de la guía:

La guía tiene no tiene valor.

Para revisión del examen:

- El alumno deberá solicitar el formato de revisión de examen en el área Tecnológica.
- Lo anterior deberá realizarse en plazo no mayor a 48 horas a partir de que se le notifico la calificación correspondiente.

Presentación:

Esta guía de estudio tiene como propósito fundamental facilitar al estudiante la comprensión y el dominio de los principios, metodologías y estándares requeridos para realizar una Auditoría Informática efectiva.

Al utilizar esta guía, el alumno será capaz de:

- Aplicar las técnicas y herramientas necesarias para evaluar la eficiencia, seguridad y cumplimiento normativo de los sistemas de información y la infraestructura tecnológica de una organización.

- Identificar riesgos, proponer controles y elaborar informes de auditoría que brinden valor a la toma de decisiones gerenciales.

Objetivos

- Dominio Normativo y Metodológico: Comprender y aplicar las normativas, estándares (como COBIT, ISO 27001) y metodologías formales para planificar y ejecutar auditorías de sistemas de información.
- Evaluación de Riesgos y Controles: Adquirir la habilidad de identificar, evaluar y mitigar los riesgos asociados a los activos de información, así como de verificar la efectividad de los controles internos implementados.
- Elaboración de Informes Profesionales: Desarrollar la capacidad de documentar los hallazgos de la auditoría y elaborar informes ejecutivos claros y objetivos, con recomendaciones accionables para la dirección y gerencia.

Justificación

Esta guía de estudio es una herramienta esencial para que el estudiante adquiera el conocimiento necesario para focalizar el estudio en los conceptos y casos prácticos de mayor relevancia evaluativa (riesgos, controles, *compliance*), asegurando que el estudiante adquiera la confianza y el dominio necesarios para responder con precisión a los reactivos del examen y obtener la calificación aprobatoria. Ofrece una síntesis estructurada y rigurosa de los marcos de referencia (COBIT, MAGERIT, ISO 27001) y las fases metodológicas de la auditoría.

Estructura y contenidos

1. **UNIDAD I:**
   FUNDAMENTOS DE LA AUDITORIA INFORMATICA

   1.1. Distingue los tipos de auditoría informática en las organizaciones de acuerdo a la normatividad vigente.

   1.2. Identifica la importancia de la auditoría informática en las organizaciones de acuerdo con la normatividad vigente.

   1.3. Distingue los tipos de auditoría informática que se llevan a cabo dentro de una organización para mantener su operatividad de acuerdo con la normatividad vigente.

2. **UNIDAD II:**
   METODOLOGIAS Y ESTANDARES EN AUDITORIAS INFORMATICAS

   2.1. Analiza las metodologías y estándares en auditorias informáticas para la eficaz administración de los recursos tecnológicos en una organización de acuerdo a la normatividad.

   2.2. Interpreta las metodologías y estándares de los recursos informáticos en las organizaciones como herramientas de evaluación.

   2.3. Analiza las etapas administrativas para llevar a cabo una auditoría informática interna en una organización de acuerdo con la metodología o estándar vigente.

3. **UNIDAD III:**
   IMPLEMENTACION DE UNA AUDITORIA INFORMATICA

   3.1. Implementa una auditoría informática en una organización respecto a su infraestructura tecnológica de acuerdo con la normatividad vigente.

   3.2. Desarrolla los procedimientos tanto organizativos como operativos en una organización para llevar a cabo una auditoría informática de acuerdo con la normatividad vigente.

   3.3. Implementa un plan para llevar a cabo una auditoría informática en una organización bajo la normatividad vigente.

Evaluación

Esta guía es solo de preparación para el examen a título de suficiencia por lo cual no tiene valor alguno.

Materiales para la elaboración de la guía

Para llevar a cabo la realización de los ejercicios de esta guía es necesario contar con los siguientes elementos:

- Computadora con Sistema Operativo Windows 10 o superior.
- Software de Maquina Virtual.
- Acceso a Internet.

1. ELEMENTOS TEORICOS

1.1. INTRODUCCION

Para cualquier organización, desde un pequeño negocio hasta una gran administración pública, sus sistemas de información son vitales. Estos sistemas almacenan datos, procesan transacciones y entregan servicios. Pero, ¿qué pasaría si fallaran? La gestión de riesgos es el proceso sistemático para responder a esa pregunta.

La metodología MAGERIT se basa en una idea central: "conocer para confiar". No se trata de eliminar todos los peligros (lo cual es imposible), sino de entenderlos para poder controlarlos. El objetivo es conocer qué podría suceder con nuestros sistemas para poder operar con un nivel de confianza aceptable, sabiendo que los incidentes están bajo control.

Esta guía ofrece un resumen de los principios, metodologías y marcos de referencia para la auditoría y la gestión de riesgos en sistemas de información. La auditoría informática se define como un proceso de evaluación sistemático y objetivo de los recursos informáticos ***(hardware, software, datos e instalaciones)*** con el fin de medir su eficiencia, eficacia y alineación con los objetivos organizacionales. Su propósito es garantizar la adecuada utilización de los recursos, controlar el cumplimiento de metas y proporcionar una base para la toma de medidas correctivas.

El pilar fundamental de la seguridad y la gobernanza de TI es la gestión de riesgos, un proceso continuo que busca mantener un entorno controlado minimizando las amenazas a un nivel aceptable. Metodologías como MAGERIT, promovida por la Administración Pública española, ofrecen un enfoque estructurado para este fin. Dicho método se centra en el análisis de los componentes clave del riesgo: los activos (recursos con valor para la organización), las amenazas (eventos que pueden causar daño) y las salvaguardas (mecanismos de protección). A través de la evaluación del impacto potencial y la probabilidad de ocurrencia, se determina el riesgo residual, que es el nivel de riesgo que persiste tras la implementación de controles.

1.2. FUNDAMENTOS DE LA AUDITORIA INFORMATICA

La auditoría es una evaluación aplicable no solo al ámbito financiero o administrativo, sino a cualquier área de una organización. Su finalidad es clarificar la situación de la institución, controlar el cumplimiento de objetivos, garantizar el uso adecuado de los recursos y permitir la implementación de medidas correctivas para optimizar la eficiencia y eficacia.

- **AUDITORÍA DE SISTEMAS:** Se encarga de la revisión, evaluación y examen de los métodos y procedimientos de uso en una institución para determinar el diseño, aplicación y buen uso de los sistemas informáticos.

- **AUDITORÍA INFORMÁTICA:** Es un examen y evaluación del software, hardware, sistemas e información utilizados por una organización. Su objetivo es mejorar procesos, medir la eficiencia y eficacia en el uso de los recursos informáticos, evaluar su uso adecuado y los resultados que aportan a la organización.

1.2.1. TIPOS DE AUDITORIA INFORMATICA

La auditoría de la información se desglosa en varias especialidades, cada una con un enfoque específico para cubrir las diversas facetas de los sistemas tecnológicos de una organización.

TIPO DE AUDITORÍA	DESCRIPCIÓN Y ENFOQUE
A la Gestión Informática	Se enfoca en la revisión y control de las funciones y actividades del personal del área informática, así como las actividades administrativas, instalaciones y mantenimiento.
De la Seguridad de Sistemas	Se aplica a todo lo relacionado con la seguridad de un sistema de cómputo: personal, actividades, funciones y acciones preventivas, correctivas y detectivas.
A los Sistemas de Redes	Enfocada en los sistemas de comunicación y redes, incluyendo el software institucional y el acceso a bases de datos.
Integral a Centros de Cómputo	Es una revisión exhaustiva, sistemática y global de todas las actividades de un centro de sistematización, evaluando el uso de equipos, redes y funciones del personal.
Ergonómica de Sistemas	Evalúa la interacción hombre-máquina-medio ambiente para garantizar calidad, eficiencia y un entorno de trabajo adecuado que no exponga al personal a daños en su salud.
Preventiva	Busca prevenir eventos de alto riesgo (como ataques DoS o inyección SQL) y proponer correcciones antes de que ocurran incidentes, ayudando a prevenir fraudes y pérdidas.

1.3. OBJETIVOS DE UNA AUDITORIA INFORMATICA

Los objetivos de una auditoría informática son multifacéticos y cruciales para la gobernanza de TI. Los fines principales incluyen:

- Realizar una evaluación profesional e independiente de las operaciones del sistema y la gestión del área de informática.
- Evaluar el uso y aprovechamiento de los recursos financieros, técnicos y materiales del centro de cómputo, incluyendo equipos, periféricos e instalaciones.
- Evaluar la eficiencia de los sistemas de procesamiento, sistemas operativos, lenguajes y aplicaciones.
- Verificar el cumplimiento de planes, programas, estándares, políticas y normativas que regulan las funciones y actividades del área de TI.
- Apoyarse en sistemas computacionales y programas especiales para auditar otras áreas y funciones de la institución.

1.4. SISTEMA DE INFORMACION Y SUS VULNERABILIDADES

Un sistema informático es un conjunto de componentes físicos (hardware) e intangibles (software) que interactúan para almacenar, procesar y recolectar datos, con el propósito de generar nueva información. Su funcionamiento adecuado depende del equilibrio y la seguridad de sus tres aspectos fundamentales.

1.4.1. COMPONENTES Y FUNCIONAMIENTO

El funcionamiento de un sistema informático se basa en un ciclo de tres actividades principales:

- **ENTRADA:** Recepción de datos a través de periféricos.
- **PROCESAMIENTO:** La unidad central de proceso (CPU) y la memoria interna manipulan los datos.
- **SALIDA:** Presentación de la nueva información resultante a los usuarios. Este ciclo se complementa con la retroalimentación, que permite a los usuarios evaluar la salida para corregir o mejorar las entradas futuras.

ASPECTO	DESCRIPCIÓN
Físico (Hardware)	Conformado por todos los componentes tangibles y periféricos que integran un computador, como superordenadores, computadoras de escritorio y PDAs.
Lógico (Software)	Componente intangible que incluye programas, aplicaciones y sistemas operativos que permiten al computador realizar diversas funciones.
Humano	Personas que operan el equipo informático y son responsables de crear nuevas aplicaciones y mejorar el procesamiento de datos.

1.4.2. SEGURIDAD FIDICA Y LOGICA

La protección de los sistemas informáticos se divide en dos grandes áreas: la seguridad física y la seguridad lógica.

- **SEGURIDAD FÍSICA:** Consiste en establecer barreras y procedimientos de control para proteger el hardware y las instalaciones contra amenazas físicas. Estas amenazas pueden ser producto de desastres naturales (inundaciones, terremotos, temperaturas extremas) o de la acción humana (sabotajes, disturbios, falsificaciones). Las recomendaciones incluyen mantener los equipos actualizados, contar con personal técnico capacitado, controlar el acceso físico y gestionar los riesgos de vulnerabilidad de los equipos.
- **SEGURIDAD LÓGICA:** Se orienta a proteger el software (programas, aplicaciones, datos) contra amenazas como virus, ataques informáticos o fallos en los procesos. Busca asegurar que solo el personal autorizado pueda acceder y modificar la información, mediante mecanismos como la delimitación de acceso a programas, el cumplimiento de reglamentos de uso y la verificación de que la información se envía y recibe por los destinatarios correctos.

1.4.3. NIVELES DE SEGURIDAD INFORMATICA

Para determinar el grado de confianza de un software y proteger la infraestructura de cómputo, se establecen varios niveles de seguridad.

NIVEL	DESCRIPCIÓN	SUBNIVELES
Nivel D	Protección mínima. Diseñado para sistemas poco confiables que no cumplen con normas de seguridad específicas y son inestables.	N/A
Nivel C	Protección discrecional y controlada. Cada usuario tiene acceso únicamente a la información que le corresponde.	• **C1:** Protección de seguridad discrecional. • **C2:** Protección de acceso controlado, monitoreada por un administrador.
Nivel B	Acceso obligatorio y controlado. Utiliza normas y reglas para controlar el acceso a información de carácter secreto y privado.	• **B1:** Seguridad etiquetada (clasificación jerárquica). • **B2:** Seguridad estructurada (permisos para todos los datos). • **B3:** Dominios de seguridad (protección de dominios con hardware).
Nivel A	Protección verificada. Considerado el nivel de seguridad más elevado y formalmente verificado.	N/A

1.4.4. VULNERABILIDADES COMUNES

Una vulnerabilidad es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de los datos. A continuación, se presentan algunas de las más relevantes.

VULNERABILIDAD	DESCRIPCIÓN	SOLUCIÓN SUGERIDA
Privilegios Excesivos	Se conceden privilegios de base de datos a usuarios o aplicaciones que exceden los requerimientos de su función.	Implementar control de acceso a nivel de consulta para restringir las operaciones a los datos mínimos requeridos.
Abuso de Privilegios	Usuarios con acceso legítimo abusan de sus privilegios para fines no autorizados o malintencionados.	Generar políticas de control de acceso que no solo definan a qué datos se accede, sino también cómo se accede (ubicación, tiempo, volumen).
Inyección de SQL	Un atacante aprovecha vulnerabilidades en aplicaciones web para enviar consultas de base de datos no autorizadas, a menudo con privilegios elevados.	Implementar seguridad y auditoría de bases de datos, y control de acceso a nivel de consulta para detectar consultas no autorizadas.
Denegación de Servicio (DoS)	Un ataque que busca agotar los recursos de un sistema (red, CPU, memoria) para que no pueda atender a usuarios legítimos.	Prevenir en múltiples capas (red, aplicaciones, bases de datos), incluyendo IPS (Sistema de Prevención de Intrusiones) y controles de velocidad de conexión.

1.5. METODOLOGIA SISTEMATICA DE GESTION DE RIESGOS: "MAGERIT"

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es un método sistemático promovido por la Administración Pública española para identificar, analizar y tratar los riesgos que afectan a los sistemas de información. La gestión de riesgos es un pilar del buen gobierno y un requisito legal en normativas como el Esquema Nacional de Seguridad (ENS) de España.

El proceso de gestión de riesgos, alineado con la norma ISO 31000, es un ciclo continuo que abarca las siguientes fases:

- **ESTABLECIMIENTO DEL CONTEXTO:** Definir los parámetros externos e internos que enmarcan la gestión de riesgos.
- **APRECIACIÓN DEL RIESGO:** Incluye la identificación, análisis y evaluación de los riesgos.
- **TRATAMIENTO DEL RIESGO:** Selección e implementación de medidas para modificar el riesgo.
- **COMUNICACIÓN Y CONSULTA:** Intercambio continuo de información con las partes interesadas.
- **SEGUIMIENTO Y REVISIÓN:** Supervisión constante de los riesgos y la eficacia de los controles.

1.5.1. ACTIVOS

Un activo es cualquier componente de un sistema de información susceptible de ser atacado, con consecuencias para la organización. Los activos clave son la información y los servicios, pero estos dependen de otros como:

- Software (aplicaciones)
- Hardware (equipos informáticos)
- Comunicaciones (redes)
- Personal (usuarios, operadores)
- Instalaciones y equipamiento auxiliar
- Valoración y Dimensiones

Los activos se valoran no por su costo, sino por el perjuicio que causaría su degradación. Esta valoración puede ser cuantitativa (monetaria) o cualitativa (escalas de niveles) y se mide a través de varias dimensiones de seguridad:

DIMENSIÓN	DESCRIPCIÓN
Confidencialidad	Garantiza que la información solo sea accesible por personal autorizado.
Integridad	Asegura que la información no ha sido alterada de manera no autorizada.
Disponibilidad	Garantiza que los usuarios autorizados tengan acceso a la información y servicios cuando lo requieran.
Autenticidad	Asegura que una entidad (usuario, sistema) es quien dice ser.
Trazabilidad	Permite determinar quién hizo qué y en qué momento (accountability).

1.5.2. AMENAZAS

Una amenaza es cualquier evento que puede materializarse sobre un activo causando un daño. Se clasifican según su origen:

- **NATURALES:** Terremotos, inundaciones.
- **INDUSTRIALES:** Fallos eléctricos, contaminación.
- **ERRORES O ACCIDENTES:** Causados por personas de forma no intencionada.
- **ATAQUES DELIBERADOS:** Acciones intencionadas para causar daño.

Las amenazas se valoran en función de su probabilidad (o frecuencia de ocurrencia) y la degradación (el daño que causarían al activo).

1.5.3. SALVAGUARDAS

Son los procedimientos o mecanismos tecnológicos implementados para reducir el riesgo. Pueden ser preventivas (reducen la probabilidad de que ocurra un incidente) o de otros tipos, como las que limitan el daño o permiten la recuperación. Su eficacia se mide en una escala de 0% a 100%, dependiendo de su idoneidad, implementación y uso.

TIPO DE SALVAGUARDA	OBJETIVO PRINCIPAL
Preventiva	Reduce la probabilidad de que una amenaza ocurra.
Limitante	Reduce el daño (impacto) si la amenaza se materializa.

1.5.4. IMPACTO Y RIESGO (POTENCIAL Y RESIDUAL)

El análisis culmina con la estimación de dos métricas clave, antes y después de considerar las salvaguardas:

- **IMPACTO:** Es la medida del daño sobre el activo si una amenaza se materializa.
  - **IMPACTO POTENCIAL:** Daño calculado sin considerar las salvaguardas existentes.
  - **IMPACTO RESIDUAL:** Daño remanente después de aplicar las salvaguardas.
- **RIESGO:** Es la estimación del daño probable, combinando el impacto con la probabilidad de ocurrencia de la amenaza.
  - **RIESGO POTENCIAL:** Riesgo sin considerar las salvaguardas.
  - **RIESGO RESIDUAL:** El riesgo que permanece después de que las salvaguardas han sido implementadas. Este es el riesgo que la dirección debe decidir si acepta.

1.5.5. TRATAMIENTO DEL RIESGO

Una vez evaluado el riesgo residual, la dirección debe decidir cómo tratarlo. Las opciones incluyen:

- **ELIMINAR:** Suprimir la fuente del riesgo (ej. descontinuar un servicio).
- **MITIGAR:** Reducir la probabilidad o el impacto del riesgo mediante la implementación de nuevas salvaguardas.
- **COMPARTIR:** Transferir el riesgo a un tercero (ej. contratar un seguro).
- **FINANCIAR (ACEPTAR):** Asumir formalmente el riesgo residual, considerándolo aceptable para la organización.

1.6. MARCO DE REFRENCIA PARA EL CONTROL Y LA GOBERNANZA DE "TI"

Para implementar una gestión de riesgos y un control interno efectivos, las organizaciones se apoyan en marcos de referencia estandarizados que proporcionan principios, prácticas y herramientas.

1.6.1. COBIT (Control Objectives for Information and Related Technologies)

COBIT es un marco creado para auditar la gestión y el control de los sistemas de información y tecnología (TI). Su objetivo es ayudar a las organizaciones a alinear sus estrategias de TI con sus objetivos de negocio. Se estructura en cuatro dominios principales que agrupan los procesos de TI.

DOMINIO	CÓDIGO	DESCRIPCIÓN	PROCESOS DE EJEMPLO
Planificación y Organización	PO	Cubre las estrategias y tácticas para identificar cómo la TI puede contribuir a los objetivos de la organización.	• **PO1 :** Definir un Plan Estratégico de TI. • **PO9 :** Evaluar Riesgos.
Adquisición e Implementación	AI	Se enfoca en la identificación, desarrollo o adquisición de soluciones de TI y su implementación y mantenimiento.	• **AI2 :** Adquirir y Mantener Software. • **AI6 :** Administrar Cambios.
Servicio y Soporte	DS	Se refiere a la entrega de los servicios de TI, incluyendo operaciones, seguridad y soporte a usuarios.	• **DS4 :** Asegurar Servicio Continuo. • **DS5 :** Garantizar la Seguridad.
Monitoreo y Evaluación	M	Consiste en supervisar todos los procesos de TI para garantizar su calidad, eficacia y cumplimiento.	• **M1 :** Monitorear los procesos. • **M2 :** Evaluar el control interno.

1.6.2. ITIL (Information Technology Infrastructure Library)

ITIL se originó en la década de 1980 por iniciativa del gobierno británico con el objetivo de organizar y controlar el área informática de manera más eficiente. Hoy en día, es un conjunto de mejores prácticas para la gestión de servicios de TI (ITSM). Su propósito es transformar los departamentos de TI de un modelo tecnológico tradicional a un modelo de gestión enfocado en la entrega de servicios de calidad, alineados con las estrategias, metas y objetivos de la organización. ITIL sigue un ciclo de calidad similar a PDCA: Planificación, Realización, Verificación y Validación.

1.7. APLICACIÓN PRACTICA Y CICLO DE VIDA

La gestión de riesgos y la auditoría no son ejercicios teóricos, sino procesos prácticos que se integran en el ciclo de vida de los sistemas de información y culminan en acciones concretas.

1.7.1. SEGURIDAD EN EL CICLO DE VIDA DEL SOFTWARE

Es un hecho reconocido que considerar la seguridad desde el inicio del desarrollo de un sistema es más efectivo y económico que hacerlo a posteriori. La seguridad debe estar "embebida en el sistema desde su primera concepción". Metodologías de desarrollo como MÉTRICA v3 integran la seguridad en cada fase del ciclo de vida del software:

FASE DEL CICLO DE VIDA	ACTIVIDADES DE SEGURIDAD RELEVANTES
Especificación	Definir requisitos de seguridad, perfiles de usuario, y requisitos de monitorización y registro (logs).
Adquisición / Desarrollo	Asegurar que los contratos incluyan cláusulas de seguridad. Aplicar técnicas de programación segura y gestionar el control de versiones y acceso al código fuente.
Aceptación	Realizar pruebas funcionales de los servicios de seguridad, incluyendo simulación de ataques y pruebas de intrusión controlada (hacking ético).
Despliegue y Operación	Establecer normativas y procedimientos para la gestión de usuarios, claves, incidentes y análisis de registros (logs).
Mantenimiento	Analizar el impacto en el riesgo de cualquier cambio o nueva funcionalidad antes de su aprobación e implementación.

1.7.2. PROTECCION ACTIVA Y MANTENIMIENTO DEL SISTEMA

Estos procesos formalizan la evaluación de la seguridad de un sistema:

- **AUDITORÍA:** Es un examen independiente para comprobar la idoneidad de los controles y su conformidad con las políticas. Un análisis de riesgos suele ser el primer paso de una auditoría.

- **CERTIFICACIÓN:** Es la confirmación por parte de un tercero acreditado de que un producto, proceso o sistema de gestión (ej. un SGSI bajo ISO 27001) es conforme con los requisitos establecidos.

- **ACREDITACIÓN:** Es un proceso formal que legitima a un sistema para un propósito específico, como el manejo de información clasificada.

2. CUESTIONARIO DE REPASO

2.1. ¿Cuál es el propósito principal de una auditoría informática según el texto "Auditoría Informática"?
El propósito principal de una auditoría informática es realizar un examen y evaluación del software, hardware, sistemas e información de una organización. Su finalidad es medir la eficiencia y eficacia en el uso de los recursos informáticos, evaluar su adecuada utilización y mejorar los procesos organizacionales basándose en los resultados obtenidos.

2.2. Explique la diferencia fundamental entre seguridad física y seguridad lógica.
La seguridad física se enfoca en proteger los sistemas contra amenazas tangibles y físicas, creando barreras y controles para prevenir daños por desastres naturales o acciones humanas como sabotajes. Por otro lado, la seguridad lógica se ocupa de combatir amenazas relacionadas con el software y la parte intangible del sistema, como programas y aplicaciones, protegiendo contra accesos no autorizados o fallos en los procesos lógicos.

2.3. ¿Qué es la metodología MAGERIT y cuál es su objetivo principal?
MAGERIT es una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información promovida por la Administración Pública española. Su objetivo principal es ofrecer un método sistemático para analizar los riesgos a los que están expuestos los sistemas de información, permitiendo a las organizaciones conocerlos, gestionarlos y mantenerlos bajo control para asegurar el cumplimiento de sus objetivos.

2.4. ¿Cuáles son los tres elementos fundamentales que se analizan en el método de análisis de riesgos de MAGERIT?
Los tres elementos fundamentales en el análisis de riesgos de MAGERIT son los activos, las amenazas y las salvaguardas. Los activos son los recursos del sistema de información que tienen valor para la organización. Las amenazas son los eventos que pueden dañar esos activos, y las salvaguardas son las medidas de defensa implementadas para proteger los activos contra las amenazas.

2.5. Defina los conceptos de riesgo potencial y riesgo residual según la metodología MAGERIT.
El riesgo potencial es el riesgo teórico al que está expuesto un sistema si no se considera ninguna salvaguarda o medida de protección; es una estimación del daño probable en un escenario sin defensas. Por el contrario, el riesgo residual es el riesgo que permanece en el sistema una vez que se han implementado y considerado las salvaguardas, representando el nivel de riesgo que la dirección de la organización decide aceptar.

2.6. ¿Cuál es la finalidad del marco de control interno COSO?

El marco COSO proporciona directrices para la implementación, gestión y control de un sistema de control interno en cualquier organización. Su finalidad es ofrecer un grado de seguridad razonable en la consecución de los objetivos institucionales en tres categorías: eficacia y eficiencia de las operaciones, confiabilidad de la información financiera, y cumplimiento de las leyes y normativas aplicables.

2.7. Describa brevemente los cuatro dominios del modelo COBIT.

El modelo COBIT se estructura en cuatro dominios principales. "Planeación y Organización" cubre las estrategias y la forma en que la TI puede contribuir a los objetivos de negocio. "Adquisición e Implementación" se enfoca en identificar, desarrollar o adquirir e implementar soluciones de TI. "Servicio y Soporte" se refiere a la entrega de los servicios requeridos, incluyendo operaciones, seguridad y continuidad. Finalmente, "Monitoreo" evalúa de forma periódica todos los procesos de TI para garantizar su calidad y cumplimiento.

2.8. ¿Qué es una vulnerabilidad en un sistema de información y qué riesgo implica?

Una vulnerabilidad es una debilidad o un fallo en un sistema de información que pone en peligro la seguridad de los datos. El riesgo que implica es que un atacante puede explotar esta debilidad para comprometer la integridad (modificar datos), la disponibilidad (impedir el acceso) o la confidencialidad (robar información) del sistema.

2.9. ¿Cuáles son los tres aspectos necesarios para el funcionamiento adecuado de un Sistema Informático?

Para el funcionamiento adecuado de un sistema informático se requieren tres aspectos clave. El aspecto físico corresponde al hardware y todos los periféricos que componen el computador. El aspecto lógico se refiere al software, es decir, los programas y aplicaciones que permiten la funcionalidad del equipo. Finalmente, el aspecto humano está conformado por las personas que operan el sistema y crean nuevas aplicaciones.

2.10. ¿Cuál es el propósito de un Plan de Seguridad según la metodología MAGERIT?

El propósito de un Plan de Seguridad, también llamado plan de mejora o plan director, es materializar las decisiones tomadas para el tratamiento de los riesgos identificados en un análisis. Este plan traduce dichas decisiones en acciones y proyectos concretos, como la implementación o mejora de salvaguardas, para llevar el riesgo residual a los niveles aceptados por la dirección de la organización.

Información Adicional

- Ninguna

Bibliografía Básica

- Arens, A. A., Elder, R. J., & Beasley, M. S. (2019). *Auditoría: Un enfoque integral* (17.a ed.). Pearson Education.
- ISACA. (2019). *COBIT 2019 Framework: Introduction and Methodology*. ISACA.
- Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing* (5.a ed.). Pearson Education.