Comenzado el	Monday, 7 de October de 2024, 19:23
Estado	Finalizado
Finalizado en	Monday, 7 de October de 2024, 20:16
Tiempo empleado	53 minutos 6 segundos
Calificación	Sin calificar aún

Pregunta **1**

Finalizado

Puntúa como 2,00

Mencione los pasos de la Metodología que permite realizar Auditorias Informáticas.

La Metodología para realizar Auditorías Informáticas consiste en:

1. **Estudio preliminar**: se definen el grupo de trabajo y qué actividades se va a realizar. También se solicita documentación de la organización y se realizan entrevistas, buscando conocer qué controles realiza, qué planes sigue la organización (si existen), qué normativas, procedimientos y reglamentaciones se siguen.

2. **Revisión y evaluación de los controles y seguridades**: se analizan diagramas de procesos y otros tipos de documentación que se haya podido conseguir y se revisan los procedimientos crítcos relacionados con la seguridad como los backups.

3. **Exámen detallado de las áreas críticas**: se planifica y divide el trabajo, se analizan en profundidad cada defecto detectado en etapas anteriores (durante este paso no deben modificarse los objetos analizados).

4. **Comunicación de los resultados**: se realizan informes preliminares (en caso de haberlos) y un informe final que contiene todos los detalles de la auditoría, comenzando con el motivo y los objetivos de la auditoría y terminando con los resultados y conclusiones.

Pregunta 2

Finalizado

Puntúa como 1,50

Defina objetivos y funciones de un Comité de Informática.

El Comité de Informática tiene como objetivo ser un espacio en el cual puedan interactuar los usuarios de los sistemas informáticos y los encargados de gestionar estos sistemas, dando lugar a la discusión para buscar un mejor uso de los recursos informáticos en la organización.

Tiene como función aprobar el Plan Estatégico de Sistemas de Información propuesto por el Departamento de Informática, así como también aprobar las inversiones en tecnología que se consideren necesarias. Otra de sus funciones es la de fijar prioridades en los proyectos informáticos y también realizar un seguimiento de las actividades que el Departamento de informática llava a cabo.

Pregunta 3

Finalizado

Puntúa como 1,50

Describa los denominados Datos Personales Sensibles y especifique que dice la ley con respecto a la forma en que deben tratarse y que medidas de seguridad recomienda implementar para garantizar su confidencialidad.

Se denomina Datos Personales Sensibles a todos aquellos datos de una persona relacionados a su afiliación política, convicciones religiosas, detalles de su vida sexual, afiliaciones sindicales, detalles sobre la salud personal y conviciones filosóficas o morales.

La ley especifica que no se pueden crearse registros con este tipo de información, excepto para utilizarlos con fines estadísticos, pero en este caso no se debe poder identificar a las personas a quienes refiere la información. Otro caso en que puede recolectarse esta información es cuando asociaciones religiosas, sindicales o políticas desean llevar un registro de sus miembros; cuando se deben utilizar ciertos datos como antecendentes penales, que pueden ser solicitados por autoridades específicas bajo algunas reglamentaciones; también pueden ser registrados por organismos de salud, y es información que debe ser guardada bajo secreto profesional. La ley también especifica que nadie puede ser obligado a brindar datos sensibles si no se encuentra en un contexto autorizado por la ley.

Pregunta **4**

Finalizado

Puntúa como 1,50

Describa las cuatro propiedades de la firma digital.

Las cuatro propiedades de la firma digital son:

- No repudio: el emisor no puede negar haber firmado el documento, por lo que el receptor está protegido frente a esa afirmación.

- Integridad de la información: da validez de forma comprobable a poder decir que la información del documento no fue modificada luego de ser firmado.

- Autenticidad del origen del mensaje: permite atribuir el origen inequívocamente al autor de la firma.

- Exclusividad: permite asegurar que la firma verdaderamente está bajo control del firmante.

Pregunta **5**

Correcta

Se puntúa 1,50 sobre 1,50

Asocie las respuestas con la clasificación que corresponda:

Controles Detectivos ✔	Identifican el error en el momento en que se presentan, pero no lo evitan, actuando como alarmas que permiten registrar el problem
Controles Correctivos ✔	Permiten investigar y rectificar los errores y sus causas.
Controles Preventivos ✔	Establecen las condiciones necesarias para que el error no se produzca.

Respuesta correcta

La respuesta correcta es: Controles Detectivos → Identifican el error en el momento en que se presentan, pero no lo evitan, actuando como alarmas que permiten registrar el problema y sus causas., Controles Correctivos → Permiten investigar y rectificar los errores y sus causas., Controles Preventivos → Establecen las condiciones necesarias para que el error no se produzca.

Pregunta 6

Finalizado

Puntúa como 2,00

Describa como intervienen el cifrado y huella digital (o hash) en el proceso de firma y validación

Para llevar a cabo el proceso de firma, se parte del documento que se desea firmar calculando un digesto usando una funcion hash previamente definida. Este digesto es luego cifrado utilizando una clave privada del firmante. Luego, el documento, el digesto cifrado y la clave pública del firmante son enviados a quien corresponda.

Quien desee validar la firma del documento utilizará la clave pública del firmante (que es la única que puede descifrar lo cifrado por la clave privada del firmante) para obtener un digesto descifrado. A su vez, también se utiliza la misma función hash para calcular un nuevo digesto a partir del documento recibido. Si ambos digestos coinciden entonces significa que la firma es válida, el documento no fue modificado. También significa que el firmante no puede repudiar la firma del documento, ya que el digesto fue descifrado exitosamente con su clave pública.