PREGUNTAS DE PARCIAL

Mencione los pasos de la metodología que permite realizar Auditorías Informáticas

1. **Estudio Preliminar:** Se define el grupo de trabajo y que 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), que normativas, procedimientos, y reglamentaciones se siguen
2. **Revision y evaluacion 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 críticos relacionados con la seguridad como los backups
3. **Examen detallado de las áreas críticas:** Se planifica y divide el trabajo, se analizan en profundidad cada defecto 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

Defina objetivos y funciones de un Comité de Seguridad de la Información.

El objetivo del Comité de Seguridad de la información es tener un lugar de encuentro en donde gente de la empresa y usuarios puedan debatir asuntos de tratamiento de información que afecten a la empresa. Permite a los usuarios conocer las necesidades de la organización y ayudarlos a fijar prioridades, como a su vez fomentar la utilización de los recursos informáticos. Las funciones que debe cumplir son: Aprobar planes estratégicos de sistemas de información, fijar propiedades en grandes proyectos, vigilar las actividades del manejo de la información, aprobar inversiones en tecnología de la información

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

Los Datos Personales Sensibles son aquellos que revelan información de la persona, en relación a cuestiones como su vida sexual, raza, religión, política, salud, y de otra índole, los cuales la persona no se encuentra obligada a informar, y solamente podrán ser utilizados en distintos contextos determinados

La ley de protección de datos personales establece que: no se pueden crear bases de datos que contengan datos personales sensibles, o que los infieran, sino que solo pueden ser tratados o utilizados con fines estadísticos, científicos o de interés general de la sociedad. Sí se permite crear bases de datos que contengan datos personales sensibles cuando se trate de organizaciones que deseen registrar sus miembros como por ejemplo la Iglesia o entes políticos. Del mismo modo pueden recolectar y tratarse este tipo de datos ante situaciones de índole judicial, o ante profesionales de la salud (manteniendo el secreto profesional). En cuanto a las medidas de seguridad para garantizar la confidencialidad de los datos personales sensibles se indica en primer lugar que el responsable del tratamiento de los datos deberá

mantenerlos en secreto y solamente cederlos en casos que lo requiera, ya sea por cuestiones de seguridad o judiciales. Además, se recomiendan distintos aspectos como por ejemplo garantizar canales de comunicación cifrados al momento de establecer contacto entre la persona que dará la información y quien la recaude, y también garantizar los correspondientes certificados de seguridad que permitan que otros agentes externos puedan acceder a los formularios en el momento en que la información sensible está siendo proporcionada. Lo mismo también debe tenerse en cuenta si es necesario el traslado de los datos a los fines mencionados anteriormente, en el sentido de prever que los datos no puedan ser tomados por personas ajenas a las que recolectaron los mismos

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 austro de la firma
Exclusividad: Permite asegurar que la firma verdaderamente está bajo control del firmante

Describa cómo intervienen el cifrado y huella digital (o hash) en el proceso de firma y validación
En el proceso de firma y validación, se intenta proteger un documento de manera digital mediante un proceso matemático de encriptación en el cual al realizar la firma digital del mismo se generan 2 claves, una pública la cual será proporcionada por el creador a cualquier persona que quiera tener acceso a ese documento, y una privada la cual solo poseerá el creador. La clave privada no debe ser difundida ya que con esta se tendrá acceso de edición al documento, esto asegura que el único editor que tendrá este documento será el propietario del mismo. En caso de que el propietario no ponga el documento en solo lectura, el archivo podrá editarse por terceros, pero quedará registrado y todos podrían darse cuenta que el documento fue alterado.

Describa los objetivos del control Obligación de Respaldo y Recuperación de la ley 25326

La obligación de respaldo y recuperación de la Ley 25.326 tiene como objetivo garantizar que los datos personales estén siempre disponibles y puedan recuperarse en caso de pérdida o incidente, preservando su integridad y confidencialidad mediante procedimientos formales, medidas de seguridad y pruebas periódicas que aseguren la continuidad y protección de la información.

Describa los objetivos del Control Entorno de Desarrollo de la Ley 25326

El control de Entorno de Desarrollo en la Ley 25.326 tiene como objetivo asegurar que, durante las etapas de desarrollo, prueba o mantenimiento de sistemas, los datos personales no se vean expuestos a riesgos innecesarios. Para ello, se busca implementar políticas de desarrollo seguro, utilizando técnicas de enmascaramiento o disociación de la información, de modo que no se empleen datos reales de los titulares. En caso de ser necesario usarlos, deben aplicarse las mismas medidas de seguridad que en los entornos productivos, garantizando siempre la confidencialidad, integridad y disponibilidad de la información.

Describa los objetivos del Control Notificación ante incidentes de seguridad de la Ley 25326

El control de **Notificación ante incidentes de seguridad** busca que, si ocurre un problema con los datos personales (por ejemplo, filtración, pérdida o acceso no autorizado), la organización tenga un responsable designado, registre lo sucedido y avise a la autoridad de control. El objetivo es reaccionar rápido, minimizar daños y evitar que vuelva a pasar, protegiendo siempre a los dueños de los datos.

Defina y mencione los tres pilares en los que se basa la Seguridad de la Información.

Los tres pilares en los que se basa la Seguridad de la Información son la integridad, la confidencialidad, y la accesibilidad.

Confidencialidad: los datos que se tengan recabados solamente sean utilizados por quienes corresponda, para actividades lícitas del tratamiento de los mismos, y no sean cedidos a terceros ni publicados sin consentimiento.

Integridad de la información: refiere a que se procure la veracidad de los datos que se tengan, y que los mismos sean confiables.

Datos sean accesibles: es decir que puedan ser consultados en el momento que se necesite.

Describa los Objetivos del control Interno Informático

El control interno informático tiene como objetivo principal proteger la información y los recursos tecnológicos, garantizando su seguridad. Busca asegurar que los datos sean confiables, oportunos y veraces en todo el proceso, desde su captura hasta la generación de informes. Además, promueve el uso de métodos y procedimientos que permitan un funcionamiento eficiente de los servicios informáticos, estableciendo normas y políticas que regulen su uso dentro de la empresa. Finalmente, procura que el diseño e implementación de los sistemas computarizados se realicen de manera adecuada, para brindar un procesamiento de la información eficaz y útil para la organización.

- Establecer como prioridad la SEGURIDAD y Protección de la información y de todos los recursos tecnológicos
- Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa
- Implementar los métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa.
- Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.
- Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa

AUTOEVALUACIONES:

Describa características del Control Interno Informático

- Controlar que todas las actividades se realicen cumpliendo los procedimientos y normas fijados por la Dirección.
- Definir, implantar y ejecutar mecanismos y controles.
- Evaluar su bondad y asegurar el cumplimiento de normas legales.
- Colaborar y apoyar el trabajo de Auditoría Informática

Explique las etapas de un proceso de Análisis de Riesgos.

El proceso de análisis de riesgos se puede tratar de 3 formas distintas:

Prevenir el riesgo: Para ello se debe obtener y mantener un determinado nivel de seguridad. Son acciones que permiten evitar el fallo y disminuir las consecuencias. Las personas deben realizar un uso profesional de los entornos físicos. Ejemplos: Selección del personal. Medidas de protección generales. Potencia eléctrica. Sistema contra incendios. Control de acceso. Ubicación del centro de cómputos. Ubicación del edificio. Elementos de construcción.

Actuar mediante un riesgo: Ante un desastre existe un Plan de Contingencia que permita afrontarlo. El Plan de Contingencia se compone de un Plan de Recuperación Ante Desastres más un Centro Alternativo de Procesamiento de Datos. El Plan de Recuperación debe: Realizar un análisis de riesgos de los sistemas críticos. Establecer un período crítico de recuperación. Realizar un análisis de aplicaciones críticas, priorizando procesos. Determinar las prioridades de procesos por día y por su orden. Establecer objetivos de recuperación. Asegurar capacidad de comunicaciones y servicios de copias de seguridad.

Actuar después de un riesgo: Esto se realiza mediante planes de seguros, que compensan las pérdidas, gastos y/o responsabilidades que puedan surgir una vez detectado y corregido el fallo. Tipos de seguros: Del centro de procesamiento. De los medios de Software. Gastos del plan de contingencias. Gastos por la pérdida del negocio

La Ley de Protección de Datos personales se refiere a Base de Datos en cualquier tipo de soporte que administre una organización VERDADERO

Defina y mencione las diferencias entre Seguridad Informática y Seguridad de la Información
Seguridad Informática: se enfoca en **proteger sistemas, redes y computadoras** frente a ataques, fallas o accesos no autorizados. Su ámbito es principalmente **tecnológico**.
Seguridad de la Información: es más amplia, busca proteger la **información en cualquier forma** (digital, papel, verbal) garantizando su **confidencialidad, integridad y disponibilidad**, incluso más allá de la tecnología

Mencione las diferencias entre firma digital y firma electrónica
Firma digital: utiliza un procedimiento de cifrado que vincula de forma única al firmante con el documento. Tiene validez jurídica plena, garantiza autenticidad, integridad y no repudio, y debe ser verificada por terceros autorizados.
Firma electrónica: es cualquier conjunto de datos asociados a un documento electrónico (como una imagen escaneada de la firma). No utiliza cifrado, no tiene la misma presunción legal de validez y ofrece menor nivel de seguridad.

Cómo se gestionan los riesgos en un Plan de Seguridad Informática según la norma 27001
Para gestionar los riesgos en el plan de seguridad informática según la norma 27001, se deben identificar los mismos y tratarlos. En primer término se deben identificar los riesgos vinculados a la pérdida de confidencialidad, integridad y disponibilidad; identificar los dueños que tienen asignados los riesgos, valorar las consecuencias y el impacto de los mismos, como así también valorar la probabilidad de su repercusión. Por ejemplo, suelen basarse en estadísticas de hechos que han ocurrido en el pasado. Para el tratamiento de dichos riesgos se deben seleccionar las opciones adecuadas de tratamiento de riesgos teniendo en cuenta la apreciación de los riesgos para así decidir qué hacer con ellos, se puede tratar los riesgos de distintas maneras: transfiriéndolos, reduciéndolos, evitándolos o asumirlos. En caso de que el riesgo sea de alta probabilidad o de alto impacto se puede controlar el mismo mediante los controles que obran en el anexo A de la ley 27001.

Controles detectivos: Identifican el error en el momento que se presentan, pero no lo evitan, actuando como alarmas que permiten registrar el problema

Controles Correctivos: Permiten investigar y rectificar los errores y sus causas

Controles preventivos: Establecen las condiciones necesarias para que el error no se reproduzca

Controles Detectivos: Registrar y revisar todas las operaciones del usuario
Controles Detectivos: Registrar y revisar los intentos de acceso no autorizado

Controles Preventivos: Contratar seguro
Controles Preventivos: Realizar copias de seguridad
Controles Preventivos: Realizar análisis de vulnerabilidades del software
Controles Correctivos: Restaurar una copia de seguridad
Controles Correctivos: Revisión de las cámaras de seguridad