Preguntas de examen

1. ***Explique en qué consiste la actividad de controlar llevada a cabo por la dirección informática.***

   La actividad de controlar, desarrollada por la dirección informática, consiste en realizar un *seguimiento permanente* de las *distintas actividades del departamento de tecnología*. Estos controles se realizan en diversas áreas como seguridad e higiene laboral, contratos, seguros, entre otras y en todo momento se está asegurando el cumplimiento de la normativa legal.

   Respuesta:

   La actividad de controlar llevada a cabo por la dirección informática se refiere a la implementación de procesos y procedimientos que aseguran que las actividades informáticas se realicen de acuerdo con las políticas, normativas y estándares establecidos por la organización. Este control es fundamental para garantizar la eficiencia, la seguridad y la integridad de los recursos informáticos.

   ### Elementos del Control

   1. **Verificación de Procedimientos**: Asegurar que todas las actividades informáticas cumplen con los procedimientos establecidos.
   2. **Cumplimiento Normativo**: Garantizar que se respetan las leyes y regulaciones aplicables.
   3. **Evaluación de Riesgos**: Identificar y gestionar los riesgos asociados con el uso de recursos informáticos.
   4. **Control Interno Informático (CII)**: Implementar un control diario de las actividades para verificar su conformidad con los estándares.
   5. **Auditoría Informática (AI)**: Recoger y evaluar evidencias para determinar si los sistemas informáticos protegen los activos y mantienen la integridad de los datos.
   6. **Monitoreo Continuo**: Realizar un seguimiento continuo de las operaciones para detectar desviaciones o problemas.
   7. **Control de Acceso**: Establecer protocolos para identificar y autenticar a los usuarios autorizados.
   8. **Gestión de Cambios**: Controlar todos los cambios en el sistema para prevenir vulnerabilidades.
   9. **Mantenimiento de Registros**: Llevar un registro de todas las actividades y accesos al sistema.
   10. **Evaluación de Eficiencia**: Medir la eficacia del uso de los recursos informáticos para optimizar su rendimiento.

   Importancia del Control

   El control realizado por la dirección informática es vital para:

   11. **Proteger Activos**: Salvaguardar la información y los recursos de la organización.
   12. **Integridad de los Datos**: Asegurar que los datos sean precisos y estén protegidos contra manipulaciones.

13. **Eficiencia Organizacional**: Mejorar los procesos y el uso de recursos, minimizando costos y maximizando el rendimiento.
14. **Cumplimiento Legal**: Evitar sanciones y multas por incumplimiento de normativas.

La dirección informática debe abordar el control como una actividad continua que no solo busca cumplir con normas, sino también mejorar la operatividad y la seguridad de la infraestructura tecnológica de la organización.

---

2. ***Dé ocho ejemplos de Control Interno Informático que considere vitales de implementar. Ordenarlos según su orden de prioridad.***

    1. Backups regulares de los datos, a fin de resguardar la información
    2. Actualizaciones del software
    3. ***QSY una paja***

---

3. ***¿Cuál es el objeto de la Ley 25326 de Protección de Datos Personales?***

    La ley 25326 nace en Argentina en el año 2000 y se reglamenta, posteriormente, en el año 2002. Esta ley tiene el objetivo de proteger los datos personales (DP). Esto es, como su nombre lo indica, proteger los datos personales de personas físicas como empresas. Los datos personales representan a todo tipo de información concreta determinada o determinable tanto de personas físicas como ideales (la empresa). La ley excluye a los datos en archivos de uso doméstico, de informaciones periodísticas o los recopilados con fines estadísticos.

    Otra:

    La Ley 25.326 de Protección de Datos Personales tiene como principal objetivo la **protección integral de los datos personales** que se encuentran en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos. Esta ley busca garantizar:

    1. **Derecho al honor y a la intimidad**: Protege la dignidad y la privacidad de las personas.
    2. **Acceso a la información**: Permite que los individuos tengan acceso a la información que se registra sobre ellos.
    3. **Aplicabilidad**: Se aplica tanto a datos de personas físicas como a aquellos relativos a personas jurídicas (entidades).
    4. **Condiciones de tratamiento**: Establece que el tratamiento de datos debe ser realizado respetando los principios de legalidad, finalidad, veracidad, y confidencialidad.
    5. **Limitaciones**: No puede afectar las bases de datos ni las fuentes de información periodísticas.
    6. **Regulación de archivos**: Los archivos, registros o bancos de datos deben estar debidamente registrados y cumplir con requisitos técnicos de seguridad.

    La ley fue sancionada y promulgada parcialmente el 4 de octubre del 2000

Principios Generales

Los principios generales que rigen la protección de datos personales bajo esta ley incluyen:

7. **Licitud**: El tratamiento de datos debe ser legal y justo.
8. **Finalidad**: Los datos deben ser recolectados para fines específicos y legítimos.
9. **Proporcionalidad**: Los datos recogidos deben ser adecuados, relevantes y no excesivos en relación con la finalidad para la cual se procesan.
10. **Seguridad**: Se deben implementar medidas técnicas y organizativas para garantizar la seguridad y confidencialidad de los datos personales.

Derechos de los Titulares

Los titulares de los datos tienen derechos fundamentales, tales como:

11. **Acceso**: Conocer qué datos se tienen sobre ellos.
12. **Rectificación**: Solicitar la corrección de datos incorrectos o desactualizados.
13. **Cancelación**: Pedir la eliminación de sus datos cuando ya no sean necesarios.
14. **Oposición**: Oponerse al tratamiento de sus datos en ciertas circunstancias.

La ley establece un marco claro para la protección de datos personales en Argentina, promoviendo la transparencia y el respeto por la privacidad de los individuos

---

4. ***¿Cuáles son las normas aplicables en nuestro país para la protección de Datos Personales?***

   En Argentina, la protección de datos personales está regulada principalmente por la **Ley 25.326**, que establece un marco normativo para garantizar el derecho a la intimidad y el honor de las personas en relación con sus datos personales. A continuación se detallan los aspectos más relevantes de esta ley.

   1. Objetivo de la Ley

   La Ley.326 tiene como objetivo la protección integral de los datos personales almacenados en archivos, registros o bancos de datos, asegurando el derecho al honor y a la intimidad de las personas, así como el acceso a la información que sobre ellas se registre.

   2. Principios Generales

   Los principios generales de la ley abarcan:

   1. **Calidad de los Datos**: Los datos deben ser ciertos, adecuados y pertinentes para la finalidad para la cual fueron recolectados.
   2. **Consentimiento**: El tratamiento de datos personales requiere el consentimiento del titular, salvo en excepciones específicas.
   3. **Confidencialidad**: Los responsables del tratamiento deben mantener el secreto profesional respecto a los datos.

   3. Derechos de los Titulares de Datos

   Los titulares de datos tienen varios derechos, entre los cuales se incluyen:

4. **Derecho de Información**: Solicitar información sobre la existencia de archivos que contengan sus datos personales **5**.
5. **Derecho de Acceso**: Obtener información sobre sus datos personales dentro de un plazo específico **5**.
6. **Derecho de Rectificación**: Exigir la corrección de datos inexactos o incompletos **12**.

4. Responsabilidades de los Responsables de Datos

Los responsables de datos deben:

7. Implementar medidas de seguridad para proteger la confidencialidad y la integridad de los datos.
8. Notificar a los titulares sobre el uso de sus datos y obtener su consentimiento previo.
9. Cancelar los datos cuando ya no sean necesarios para la finalidad para la cual fueron recolectados [9].

5. Sanciones y Control

La ley establece sanciones para aquellos que incumplan sus disposiciones, que pueden incluir multas y la obligación de reparar daños. Además, se contempla la posibilidad de acción de protección de datos personales que puede ser ejercida por los afectados **7**.

6. Excepciones a la Ley

Se permiten ciertas excepciones donde no es necesario el consentimiento del titular, como en el ámbito de la defensa nacional o seguridad pública, siempre y cuando se cumplan criterios específicos **9**.

Conclusión

La Ley.326 establece un marco robusto para la protección de datos personales en Argentina, garantizando derechos a los ciudadanos y responsabilidades a los responsables del tratamiento de datos. La legislación busca equilibrar el uso de datos personales con el respeto a la privacidad y la intimidad de las personas.

---

5. ***¿En qué consisten los Datos Personales y cómo deben ser los mismos?***

¿Qué son los Datos Personales?

Los datos personales son definidos como "información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables". Esto incluye una amplia gama de datos que pueden identificar a una persona, como su nombre, dirección, número de identificación, entre otros.

Cómo deben ser los Datos Personales

La regulación de los datos personales se basa en varios principios clave que aseguran su tratamiento legal y ético:

1. **Consentimiento**: El tratamiento de datos personales es ilícito si el titular no ha prestado un consentimiento libre, expreso e informado, el cual debe constar por escrito o en un medio equiparable.

2. **Calidad de los Datos**: Los datos personales deben ser ciertos, adecuados, pertinentes y no excesivos en relación con los fines para los cuales fueron obtenidos. Deben ser exactos y actualizados cuando sea necesario.
3. **Finalidad**: Al recolectar datos, se debe informar claramente sobre la finalidad del tratamiento y quiénes serán los destinatarios de estos datos.
4. **Limitaciones en la Recolección**: No se puede obtener datos sensibles sin una autorización legal y solo en casos de interés general.
5. **Seguridad de los Datos**: Se deben adoptar medidas técnicas y organizativas para garantizar la seguridad y confidencialidad de los datos personales, evitando su adulteración, pérdida o acceso no autorizado.
6. **Deber de Confidencialidad**: Tanto el responsable como las personas que intervengan en el tratamiento de datos están obligadas a mantener el secreto profesional respecto a estos datos, incluso después de finalizar su relación con el titular.
7. **Derechos del Titular**: Los titulares de datos tienen derechos de acceso, rectificación y supresión de sus datos.
8. **Destrucción de Datos**: Los datos personales deben ser destruidos cuando ya no sean necesarios para los fines para los cuales fueron recolectados.

Conclusiones: La protección de datos personales implica un marco legal que establece derechos y obligaciones tanto para los titulares de los datos como para aquellos que los manejan. Se busca garantizar la privacidad y la seguridad de la información personal, promoviendo un tratamiento responsable y ético de los datos.

---

6. ***¿Qué derechos tengo como titular de los Datos Personales?***

Como titular de datos personales, tienes varios derechos establecidos en la legislación vigente. A continuación se detallan estos derechos:

1. **Derecho de Acceso**: Tienes el derecho a solicitar y obtener información sobre tus datos personales incluidos en bancos de datos, tanto públicos como privados. Este derecho incluye conocer la finalidad del tratamiento de tus datos y la identidad de los responsables.
2. **Derecho de información**: Puedes solicitar información al organismo de control sobre la existencia de archivos o bases de datos personales, así como sus finalidades y responsables. Esta información debe estar disponible de manera pública y gratuita.
3. **Derecho de Rectificación**: Si tus datos personales son inexactos o incompletos, tienes el derecho a que sean rectificados o actualizados. El responsable de los datos debe realizar estas modificaciones dentro de un plazo máximo de cinco días hábiles después de recibir tu solicitud.
4. **Derecho de Supresión**: Tienes derecho a solicitar la supresión de tus datos personales cuando estos ya no sean necesarios para los fines para los cuales fueron recolectados, o si has retirado tu consentimiento, entre otras razones.
5. **Derecho a la Confidencialidad**: Los responsables de tratar tus datos están obligados a mantener la confidencialidad de los mismos y a adoptar las medidas necesarias para garantizar su seguridad y evitar tratamientos no autorizados.

6. **Derecho a la Limitación del Tratamiento**: Puedes solicitar que el tratamiento de tus datos se limite en ciertas situaciones, como cuando impugnas la exactitud de los datos.
7. **Derecho a la Portabilidad de los Datos**: Tienes derecho a recibir tus datos personales en un formato estructurado, de uso común y legible, y a transmitírselo a otro responsable si así lo deseas.
8. **Derecho de Oposición**: Puedes oponerte al tratamiento de tus datos en situaciones específicas, como cuando se utilicen para fines de mercadotecnia directa.
9. **Derecho a No Ser Sometido a Decisiones Individuales Automatizadas**: Tienes derecho a no ser objeto de decisiones basadas únicamente en tratamientos automatizados que afecten significativamente tus derechos y libertades.
10. **Derecho a Promover Acciones Judiciales**: Si consideras que se han vulnerado tus derechos, puedes promover acciones de protección de datos o hábeas data ante las autoridades competentes.

Estos derechos están diseñados para proteger tu información personal y garantizar que tengas control sobre cómo se utilizan tus datos.

---

7. ***¿Cómo debe ser el consentimiento al dar Datos Personales? ¿En qué casos no es necesario?***

   El consentimiento para el tratamiento de datos personales debe ser:

   1. **Libre**: El titular de los datos debe tener la capacidad de decidir sin presiones.
   2. **Expreso**: Debe ser claro y explícito, no implícito.
   3. **Informado**: El titular debe recibir información previa sobre:
      - La finalidad para la que se tratarán los datos.
      - Quiénes serán los destinatarios de los datos.
      - La existencia del archivo o banco de datos.
      - El carácter obligatorio o facultativo de las respuestas.
      - Las consecuencias de proporcionar o no los datos.
      - La posibilidad de ejercer derechos de acceso, rectificación y supresión de los datos.

   El consentimiento debe constar por escrito o en un medio que permita equipararlo, asegurando que se notifique al requerido sobre la información relevante.

   Casos en los que no es necesario el consentimiento

   4. **Fuentes de acceso público**: Cuando los datos se obtienen de fuentes de acceso público irrestricto.
   5. **Funciones estatales**: Si los datos se recaban para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.
   6. **Listados específicos**: Cuando los datos se limitan a nombre, documento nacional de identidad, ocupación, fecha de nacimiento y domicilio.
   7. **Relaciones contractuales**: Si los datos derivan de una relación contractual, científica o profesional del titular, y son necesarios para su desarrollo.

8. **Entidades financieras**: En operaciones realizadas por entidades financieras y en la información que reciben de sus clientes, conforme a lo dispuesto en la ley [8].

Estas excepciones están diseñadas para equilibrar el derecho a la privacidad con la necesidad de facilitar ciertos procesos administrativos y operativos.

---

8. ***¿Cuál es la autoridad de aplicación de la Ley y cuáles son sus funciones?***

La autoridad de aplicación de la Ley de Protección de Datos Personales en Argentina es el órgano de control designado para supervisar y garantizar el cumplimiento de esta ley.

El **órgano de control** tiene varias funciones y atribuciones esenciales, entre las cuales se incluyen:

1. **Asesoramiento**: Asistir y asesorar a las personas sobre los derechos garantizados por la ley y los medios legales disponibles para su defensa.
2. **Normativa**: Dictar normas y reglamentaciones necesarias para el desarrollo de actividades relacionadas con la protección de datos.
3. **Censo de Archivos**: Realizar un censo de archivos, registros o bancos de datos que estén bajo la ley y mantener un registro permanente de los mismos.
4. **Control de Normativas**: Controlar la observancia de las normas de integridad y seguridad de datos impuestas por la ley.
5. **Acceso Judicial**: Solicitar autorización judicial para acceder a locales, equipos o programas de tratamiento de datos para verificar infracciones.
6. **Solicitud de Información**: Pedir información a entidades públicas y privadas, que deben proporcionar los documentos y elementos solicitados.
7. **Sanciones Administrativas**: Imponer sanciones administrativas por violaciones a las normas de protección de datos.
8. **Garantía de Confidencialidad**: Asegurar la confidencialidad y seguridad de la información y los elementos proporcionados durante el proceso de supervisión.

Estas funciones son cruciales para proteger los derechos de los titulares de datos personales y asegurar el cumplimiento de la ley.

---

9. ***¿Se pueden ceder los Datos Personales?***

La cesión de datos personales está regulada y **se permite bajo ciertas condiciones específicas**. A continuación, se detallan las disposiciones relevantes sobre la cesión de datos personales.

Condiciones para la Cesión

1. **Consentimiento del Titular**: La cesión de datos personales solo puede realizarse con el consentimiento previo, libre, expreso e informado del titular de los datos. Este consentimiento debe ser notificado claramente, informando sobre la finalidad de la cesión y la identidad del cesionario.
2. **Excepciones al Consentimiento**: No es necesario obtener el consentimiento en ciertos casos, como:

    - Cuando la cesión está dispuesta por ley.
    - Si los datos se obtienen de fuentes de acceso público.
    - Para funciones del Estado o cumplimiento de obligaciones legales.
3. **Obligaciones del Cesionario**: El cesionario de los datos queda sujeto a las mismas obligaciones legales que el cedente, y ambos serán responsables ante el organismo de control y el titular de los datos por el cumplimiento de estas obligaciones.
4. **Cesión de Datos Sensibles**: En situaciones relacionadas con salud pública, emergencia o estudios epidemiológicos, se pueden ceder datos personales relativos a la salud, siempre que se preserve la identidad de los titulares mediante mecanismos de disociación adecuados.

Prohibiciones y Restricciones

5. **Transferencias Internacionales**: Está prohibida la transferencia de datos personales a países que no ofrezcan un nivel de protección adecuado, salvo en supuestos específicos como colaboración judicial o intercambio de datos médicos, siempre que se respeten las regulaciones establecidas.
6. **Plazo de Conservación**: Los datos personales deben ser destruidos una vez que se cumpla la finalidad para la cual fueron tratados, salvo que exista autorización expresa para su conservación.
7. **Derecho de Supresión**: Los titulares de los datos tienen derecho a solicitar la supresión de sus datos, que no procederá si esto causa perjuicios a derechos o intereses legítimos de terceros o si existe una obligación legal de conservarlos [3].

Resumen

La cesión de datos personales es posible bajo condiciones específicas que garantizan la protección de los derechos del titular. Es esencial contar con el consentimiento del titular, a menos que exista una disposición legal que lo exima. Los cesionarios deben cumplir con las mismas obligaciones que los cedentes y se deben seguir protocolos estrictos para la protección de datos sensibles.

---

10. ***¿Qué es la ofimática? ¿Qué características poseen los entornos ofimáticos y cuáles las consecuencias que posibilitan la Auditoría sobre los mismos? (ESTO ME PARECE QUE NO VA)***

    La ofimática se define como todo sistema informatizado que genera, procesa, almacena, recupera, comunica y presenta datos relacionados con el funcionamiento de las oficinas. Incluye diversas aplicaciones y herramientas, tales como:

    1. **Procesadores de texto**: Software para crear y editar documentos de texto.
    2. **Hojas de cálculo**: Aplicaciones para realizar cálculos y analizar datos mediante tablas.
    3. **Bases de datos personales**: Sistemas para almacenar y gestionar información.
    4. **Control de expedientes**: Herramientas para gestionar documentos y archivos.
    5. **Sistemas de almacenamiento óptico**: Métodos para guardar información de forma digital.
    6. **Agendas de contactos**: Aplicaciones para organizar información de contactos.

7. **Correo electrónico**: Herramienta de comunicación para el intercambio de mensajes.
8. **Control de flujo de trabajo**: Sistemas que automatizan procesos laborales.

Características de los entornos ofimáticos

9. **Distribución de aplicaciones**: Las aplicaciones están distribuidas por diferentes departamentos en lugar de estar centralizadas.
10. **Responsabilidad delegada**: La responsabilidad sobre ciertos controles se transfiere a usuarios finales que no son profesionales de la informática.
11. **Interfaz amigable**: Interfaces gráficas que facilitan el acceso a los datos sin necesidad de conocimientos técnicos avanzados.
12. **Acceso compartido**: Permiten la colaboración entre diferentes usuarios a través de herramientas de trabajo en grupo.
13. **Almacenamiento de datos**: Integración de sistemas para el almacenamiento y recuperación de información.
14. **Facilidad de uso**: Herramientas diseñadas para ser intuitivas y fáciles de utilizar por cualquier empleado.
15. **Integración de sistemas**: Posibilidad de interconectar diferentes aplicaciones para optimizar la gestión de datos.
16. **Flexibilidad**: Adaptabilidad a las necesidades cambiantes de las oficinas y los equipos de trabajo.

Consecuencias para la Auditoría en entornos ofimáticos

17. **Adquisiciones poco planificadas**: Falta de organización en la compra de equipos y software.
18. **Desarrollos ineficaces**: Proyectos que no cumplen con los estándares de calidad debido a una gestión deficiente.
19. **Conciencia de seguridad**: Los usuarios pueden no estar al tanto de la importancia de la seguridad de la información.
20. **Deficiencias en copias de seguridad**: Inadecuada protección de datos que aumenta el riesgo de pérdida de información.
21. **Escasa formación del personal**: Falta de capacitación en el uso de tecnologías ofimáticas y en prácticas de seguridad.
22. **Documentación insuficiente**: Ausencia de registros adecuados que respalden las operaciones realizadas.
23. **Control de inventario**: Problemas en la verificación y mantenimiento del inventario de equipos y aplicaciones.
24. **Evaluación de políticas**: Necesidad de revisar y actualizar las políticas de mantenimiento y adquisición en la organización.

Estas consecuencias destacan la importancia de implementar auditorías efectivas para garantizar el buen funcionamiento y la seguridad de los entornos ofimáticos.

---

11. ***Enunciar controles recomendables en entornos ofimáticos y fundamentar su aplicación. (ESTO ME PARECE QUE NO VA)***

12. ***¿Cuál es el objetivo de una Auditoría de la Seguridad Física? Identificar Áreas de Seguridad Física y Fuentes de su Auditoría.***

La seguridad física busca proteger **físicamente** cualquier recursos del sistema. Para ello, aplica barreras físicas y procedimientos de control, a fin de prevenir y detectar amenazas a los recursos e información confidencial.

Áreas de seguridad física:

1. Habitaciones con servidores de datos
2. Habitaciones de telecomunicaciones
3. Habitaciones con equipos informáticos

Fuentes de su auditoría

4. Auditorías anteriores
5. Políticas, normas y planes de seguridad

Otra respuesta

Objetivo

El objetivo principal de una Auditoría de la Seguridad Física es garantizar la integridad y continuidad de los activos humanos, lógicos y materiales en un Centro de Procesamiento de Datos. Esto se logra mediante el análisis de riesgos y la identificación de áreas que requieren atención en términos de seguridad física. Los auditores evalúan varios aspectos para asegurar que los servicios se proporcionen de manera segura y eficiente.

Áreas de Seguridad Física

Las áreas que deben reforzar la seguridad física incluyen:

6. **Centro de procesamiento de datos e instalaciones**: Se deben revisar las cámaras acorazadas, oficinas, almacenes, servidores, y la ubicación del CPD.
7. **Equipos y comunicaciones**: Inspeccionar la ubicación y acceso a computadoras, impresoras y medios de telecomunicaciones.
8. **Seguridad física del personal**: Evaluar accesos y egresos, rutas de evacuación y normas de uso de instalaciones.
9. **Sistema de control de acceso**: Asegurar que solo personal autorizado tenga acceso a áreas sensibles.
10. **Medidas de protección contra incendios**: Verificar la efectividad de los sistemas contra incendios instalados.
11. **Condiciones del entorno físico**: Evaluar el clima, la iluminación y otros factores que puedan afectar la seguridad.
12. **Mantenimiento de equipos**: Asegurar que todo el equipo esté bien mantenido y en condiciones óptimas.
13. **Políticas de seguridad**: Revisar las políticas y procedimientos de seguridad establecidos por la organización.

Fuentes de la Auditoría Física

Para llevar a cabo una Auditoría de Seguridad Física, se deben considerar diversas fuentes de información, tales como:

14. **Políticas, normas y planes de seguridad**: Documentos oficiales que guían las prácticas de seguridad.
15. **Auditorías anteriores**: Resultados de auditorías previas que puedan ofrecer contexto y antecedentes.
16. **Contratos de seguros**: Revisar las coberturas y condiciones de los seguros existentes.
17. **Informes de técnicos y consultores**: Evaluaciones técnicas sobre las instalaciones, electricidad y otros aspectos.
18. **Informes de accesos y visitas**: Registros que detallan quién accede a las instalaciones y cuándo.
19. **Pruebas de evacuación**: Resultados de simulacros de evacuación realizados.
20. **Políticas del personal**: Reglas que rigen el comportamiento y acceso del personal a las instalaciones.
21. **Documentación sobre rotación laboral**: Información sobre cambios en el personal que puedan afectar la seguridad.

Estos elementos son cruciales para realizar una auditoría efectiva y establecer un entorno seguro dentro de la organización.

---

13. ***Describa qué es y cuál es el contenido de un Informe de Auditoría.***

El informe de la auditoría es el documento más importante de la auditoría. En este se presentan resultados obtenidos durante la evaluación. Debe estar completo.

Sarasa: El informe de auditoría debe contener un esbozo, análisis y resultados de las diversas problemáticas a estudiar durante la auditoría.

Otra:

El informe de auditoría es la comunicación formal al cliente de alcances, resultados y conclusiones de la auditoría llevada a cabo. Contiene además de las falencias encontradas, un plan de acciones que permite revertir la situación teniendo en cuenta aspectos económicos de los RH, cumplimiento de normas y una evaluación global de toda la auditoría. Se compone de:

1. Identificación del informe/cliente/empresa a auditar
2. Objetivos de la auditoría
3. Normativas aplicadas y excepciones
4. Alcance de la auditoría
5. Conclusiones/Resultados
6. Informes previos/Fecha del informe
7. Identificación y firma del auditor

---

14. ***¿Con qué elementos hay que trabajar para realizar el Informe de Auditoría? (NI IDEA?)***

Tal vez habla de los activos que son considerados, onda, los recursos humanos, el inventario, las redes de comunicación, etc.

15. ***¿Qué es el Plan de Contingencia y qué aspectos se deben tener en cuenta para su preparación?***

    El plan de contingencia o recuperación es un documento orientado a definir políticas o estrategias de respuesta ante desastres o situaciones conflictivas que puedan interrumpir el normal funcionamiento de la organización. Incluye en él, medidas para recuperación ante desastres y para mantener la continuidad operativa.

    Ejemplo: El sistema puede tener un componente crítico de Hardware, si se te rompe y no podes importarlo cagaste.

    Se consideran los siguientes aspectos:

    1. **Análisis de Riesgos**: Identificar los sistemas críticos y realizar un análisis de riesgos para evaluar las vulnerabilidades.
    2. **Prioridad de Procesos**: Establecer la prioridad de los procesos críticos por día y su orden de recuperación.
    3. **Objetivos de Recuperación**: Definir objetivos claros para la recuperación de sistemas y datos.
    4. **Capacidades de Comunicación**: Asegurar que existan capacidades de comunicación efectivas, así como servicios de copias de seguridad.
    5. **Evaluación de Equipos**: Verificar que el equipamiento existente se ajuste a las necesidades de la organización, evitando obsolescencia y subutilización.
    6. **Seguridad de la Información**: Implementar medidas para proteger la información confidencial y garantizar la integridad de los datos.
    7. **Procedimientos de Respaldo**: Asegurarse de que los procedimientos de generación de copias de respaldo sean fiables y efectivos.
    8. **Manejo de Emergencias**: Preparar planes de acción ante cortes de energía y otras emergencias que puedan afectar la operación.
    9. **Monitoreo de Seguridad**: Establecer sistemas para detectar accesos no autorizados y registrar eventos de seguridad.
    10. **Seguros**: Considerar la necesidad de seguros que cubran pérdidas y daños que puedan surgir tras un desastre.

---

16. ***¿Qué aspectos debe considerar el auditor al evaluar como la dirección o gerencia de informática organiza y coordina las actividades de sus sectores o áreas?***

    La coordinación y organización entre el sector IT y las demás áreas de una organización es un punto de conflicto. Por lo tanto, el auditor debe analizar múltiples características dentro de esta comunicación. En primer lugar, se debe analizar la ubicación del departamento dentro de la organización, es decir, que jerarquía o que peso tiene el director del área dentro de la organización. Además, dentro de la comunicación, el auditor debe analizar los documentos correspondientes a como debe llevarse a cabo la comunicación y verificar si esto se cumple. etc.

---

17. ***De su opinión sobre quién o quienes deben realizar cada una de las actividades (organizar y coordinar).***

- Dirección de la organización: Lidera la organización y coordina actividades, asegurando que se cumplan objetivos del plan estratégico.
- Comité de informática:
    - Aprueba el plan estratégico y las inversiones asociadas
    - Fija prioridades de los proyectos
    - Facilita comunicación entre departamento de informática y áreas usuarias
    - Vigila la actividad del departamento de informática
- Auditor: evalúa la organización y coordinación dentro del departamento, asegurando que se sigan las normas, procedimientos y estándares, así como se cumplan los objetivos establecidos.

---

1. ***Diferencias y similitudes entre Control Interno Informático (CII) y Auditoría Informática (AI).***

   Similitudes:

   - Ambos se realizan por expertos
   - Verifican el cumplimiento de controles internos, normas impuestas y procedimientos

   Diferencias:

   - El CII funciona diariamente, mientras que una AI se realiza de manera eventual
   - El CII responde al gerente de área de informática, mientras que la AI al general
   - El CII se realiza por gente dentro de la organización, mientras que la AI por alguien externo
   - El CII no sale del área de informática, mientras que la AI trabaja además con áreas externas que hacen uso de esta.
   - El CII busca controlar y hacer más eficiente y eficaz la actividad tecnológica dentro de la organización, mientras que la AI tiene como objeto detectar errores y/o fraudes.

---

2. ***Emita una opinión sobre como justifica la inversión necesaria en CII y AI.***

   En la actualidad, mantener una organización en correcto funcionamiento requiere explícitamente de una buena gestión de la tecnología utilizada dentro de la misma. Esto se debe a que todas las áreas dentro de la organización son usuarias de esta tecnología. Ya sea desde utilizar internet hasta gestionar las finanzas de la organización por un sistema de gestión integral (SIG). Por lo tanto, garantizar el funcionamiento eficiente y eficaz de un área tan transversal para la empresa es fundamental. Entonces, realizar controles internos informáticos permite garantizar que este sector “se mantenga en línea” a fin de cumplir los objetivos de la empresa de manera eficiente y eficaz, cumpliendo normativas, procedimientos y estándares definidos de forma previa. Por otro lado, la auditoría informática es de gran utilidad para detectar posibles errores o fraudes que, de otra manera, pasarían desapercibidos. A fin de visualizar aún más la importancia de la inversión en estas dos actividades, se pueden presentar ejemplos de utilidad de ambas. En primer lugar, la auditoría informática puede detectar posibles fraudes por parte de los recursos humanos, permitiendo de esta manera ahorrar vastas sumas de dinero. En cuanto al CII, puede suceder

que el procedimiento para la carga de inventario a través del sistema no se esté realizando de forma adecuada y, en consecuencia, se esté malgastando tiempo, en este caso el CII podría detectar esta mala práctica y, de esta manera, ahorrar mucho tiempo.

---

3. ***¿Qué aspectos se deben tener en cuenta al auditar un desarrollo de software (esto me parece que no llegamos a ver → voy a versear)?***
    - Verificar el cumplimiento de normas y estándares para el desarrollo de software
    - Analizar riesgos asociados al software, tanto operativos como de seguridad
    - Verificar controles de seguridad desarrollados
    - Comprobar que la política de backups de la información sea correcta
    - Revisar la documentación existente
    - Comunicarse con los usuarios

---

4. ***¿Cómo motivaría al personal del área de desarrollo (tampoco va creo)?***
5. ***Detalle la metodología de la Auditoría Informática.***
6. ***¿Qué son los delitos informáticos (esto no llegamos a ver)?***
7. ***¿En qué consiste una Auditoría de las Bases de Datos?***
8. ***¿Quiénes son los titulares del derecho de propiedad intelectual?***
9. ***¿Qué son las obras de software y base de datos?***

Preguntas autoevaluación 2021

Pregunta 1: Explique las etapas de un proceso de Análisis de Riesgos.

El proceso de análisis de riesgos se compone de varias etapas esenciales que permiten identificar, evaluar y mitigar los riesgos en una organización:

1. **Antes del Riesgo**

    Esta fase implica la implementación de medidas preventivas para mantener un nivel adecuado de seguridad y evitar fallos. Las acciones incluyen:

    - **Selección del personal**: Asegurar que el personal esté capacitado y sea competente.
    - **Medidas de protección generales**: Establecer protocolos de seguridad física.
    - **Potencia eléctrica**: Garantizar un suministro eléctrico estable.
    - **Sistema contra incendios**: Implementar sistemas de detección y extinción de incendios.
    - **Control de acceso**: Restringir el acceso a áreas críticas.
    - **Ubicación del centro de cómputos**: Elegir ubicaciones seguras y accesibles.
    - **Ubicación del edificio**: Considerar la seguridad del entorno del edificio.
    - **Elementos de construcción**: Utilizar materiales que fortalezcan la seguridad física **7**.
2. **Durante el Riesgo**

En esta etapa, se deben implementar medidas de contingencia para responder a desastres. Las acciones incluyen:

- **Plan de Contingencia**: Desarrollar un plan que contemple la respuesta a incidentes.
- **Análisis de riesgos de sistemas críticos**: Identificar y priorizar los sistemas más vulnerables.
- **Período crítico de recuperación**: Establecer plazos para la recuperación de operaciones.
- **Análisis de aplicaciones críticas**: Evaluar y priorizar las aplicaciones que son esenciales para la operación.
- **Objetivos de recuperación**: Definir metas específicas para la restauración de servicios.
- **Capacidad de comunicaciones**: Asegurar que las comunicaciones se mantengan durante la crisis.
- **Servicios de copias de seguridad**: Implementar y verificar los procedimientos de respaldo **7**.

3. **Después del Riesgo**

   Una vez que se ha gestionado el incidente, es fundamental evaluar los daños y tomar medidas para la recuperación y la mitigación de futuros riesgos. Esto incluye:

   - **Planes de seguros**: Asegurar que existan pólizas que cubran las pérdidas.
   - **Compensación de pérdidas**: Evaluar los gastos y responsabilidades que puedan surgir.
   - **Análisis de lecciones aprendidas**: Revisar el evento para identificar mejoras en los planes de contingencia.
   - **Actualización de protocolos**: Modificar los procedimientos de seguridad según lo aprendido.
   - **Entrenamiento del personal**: Capacitar nuevamente al personal en base a la experiencia adquirida **78**.

El análisis de riesgos es un proceso continuo que requiere atención constante. Las etapas descritas permiten a las organizaciones prepararse adecuadamente ante incidentes, minimizando así el impacto en sus operaciones.

Respuesta real?:

Para realizar un proceso de **Análisis de Riesgos**, en un primer lugar se deben **identificar** los mismos de acuerdo al **criterio de riesgos** que hayan sido establecidos por la organización, es decir, que estén dentro del alcance de riesgos que serán analizados. Posteriormente, se deberá **identificar** cuál es la **amenaza** de los riesgos, es decir, cuál será el impacto de que el riesgo se materialice y cuáles son las posibles consecuencias de ello. Adicionalmente, también debe analizarse la determinación de la probabilidad de ocurrencia de los riesgos que hayan sido identificados, lo cual permitirá definir una frecuencia de materialización de los mismos. Por último, se deberá realizar el **análisis del riesgo**, es decir definir distintos niveles de impacto de los riesgos, lo cual permitirá priorizar el tratamiento de los mismos dependiendo de la importancia que se le haya dado y el nivel de impacto que tenga. También se debe tener en cuenta para esto último, realizar un análisis del **costo de tratar los riesgos** (ya sea aceptando, mitigando, transfiriendo o evitando los mismos), en relación con el beneficio que pueda obtenerse.

Pregunta 2: Defina y mencione las diferencias entre Seguridad Informática y Seguridad de la Información.

Seguridad de la información refiere al resguardo y protección de la información independientemente de como se almacene, es decir, la información puede ser digital, física u otro tipo de almacenamiento, asegurando su confidencialidad, integridad y disponibilidad. Mientras que, por otro lado, seguridad informática refiere a la protección y resguardo de los sistemas informáticos.

Respuesta otro:

Cuando se habla de Seguridad Informática se está refiriendo exclusivamente a aspectos técnicos de la protección de los datos almacenados en los distintos medios digitales. En cambio, la Seguridad de la información, posee una definición más integral de Seguridad, en tanto tiene en cuenta la protección de toda la información de la cual se vale una Organización para cumplir con sus objetivos, independientemente del medio por el cual se almacene. De esta forma la Seguridad de la Información intenta cubrir todos los intercambios o flujos de información que se realizan entre los distintos componentes de una organización, dado que estos generan un riesgo de que ocurran incidentes de seguridad, como puede ser que un tercero acceda a información que no debería o que se haga un mal uso de la misma. Además la Seguridad de la Información tiene en cuenta los aspectos necesarios para que los datos sean accesibles en el momento que se necesite, y en cuidar también la integridad de los mismos.

Pregunta 3: Describa los objetivos del Control Interno Informático

El control interno informático (CII) es una actividad que se realiza en fin de garantizar ‘’tranquilidad’’. Se realizan con frecuencia diaria y tienen como objetivos principales la gestión eficiente y eficaz de la información y los recursos tecnológicos de la organización. Para ello, se busca por un lado proteger la información, resguardándola ante posibles accesos no garantizados a la misma, manteniéndola de esta manera íntegra, veraz y confiable. Por otro lado, busca mejorar los procesos tecnológicos de la organización, haciéndolos más eficientes y asegurando que se cumplan las normas, procedimientos y políticas que los regulan.

Respuesta IA

El Control Interno Informático (CII) tiene como objetivos principales garantizar la eficacia y eficiencia de los sistemas informáticos, así como la protección de los activos y la integridad de los datos. Entre sus propósitos se incluyen la prevención, detección y corrección de errores o irregularidades que puedan afectar el funcionamiento de los sistemas. Esto se logra mediante la verificación del cumplimiento de normas y estándares establecidos por la dirección de la organización, así como la implementación de controles que mitiguen riesgos operativos y de seguridad. Los auditores informáticos también analizan la fiabilidad de la información, evalúan la continuidad de las operaciones y diseñan pruebas anti-fraude basadas en análisis de riesgos, buscando así mejorar la efectividad, eficiencia y medición del riesgo empresarial

Respuesta otro

El Control Interno Informático es el sistema que se encarga de realizar una serie de tareas rutinarias dentro de una organización, con el objetivo de controlar que los procesos que se lleven adelante se realicen teniendo en cuenta los procedimientos, normas, o estándares que hayan sido definidos por la Dirección de la Organización. Además se verifica que cumpla con las restricciones legales de las actividades que se realicen. De ese modo uno de los objetivos es implementar técnicas, métodos y

procedimientos que ayuden al desarrollo de las funciones, procesos, tareas que deba realizar la Organización para cumplir con los objetivos organizacionales. Además, se tiene como objetivo implementar y hacer cumplir las normas, políticas o legislaciones que regulen las actividades de la empresa, como por ejemplo acerca de la protección de los datos personales. En relación con esto, otro de los objetivos es garantizar y controlar la Seguridad de la Información dentro de la organización, promoviendo entonces técnicas para garantizar la veracidad y confiabilidad en la captación y procesamiento de datos, y así también el diseño y la implementación de sistemas que realicen tratamiento de los datos de acuerdo a los criterios mencionados anteriormente.

Pregunta 4: Cómo se gestionan los riesgos en un Plan de Seguridad Informática según la norma ISO 27001

La norma ISO 27001 llamada “seguridad de la información, ciberseguridad y protección de la privacidad” presenta un marco robusto para proteger la información para los sistemas de gestión de la seguridad de la información (SGSI). …

Otro

De acuerdo a la norma 27001, la Gestión de Riesgos que se halla inmerso dentro de un **Plan de Seguridad Informática**, debe comenzar con la planificación de la gestión, etapa en la cual se deberán definir las políticas que llevará adelante la organización en cuanto a los riesgos. Esto comienza definiendo cuáles son los objetivos organizacionales relacionados con la Seguridad, para posteriormente poder determinar el **alcance** de la gestión de los riesgos, es decir, qué hechos serán considerados como tales, a qué integrantes de la organización les competerá, y quiénes serán los **responsables** del posterior análisis y tratamiento de los mismos. Así también se deberá definir cuál es la metodología a aplicar al momento de continuar con la gestión de los riesgos. Como una segunda etapa, se puede mencionar la **identificación** de las **amenazas** de los riesgos, lo cual se realiza definiendo cuáles son los criterios de aceptación de riesgos, y posteriormente el análisis de los mismos, teniendo en cuenta estos criterios. Para llevar adelante el análisis de los riesgos, se deberá tener en cuenta identificar cuál es la amenaza de los riesgos, es decir, cuál será el impacto de que el riesgo se materialice y cuáles son las posibles consecuencias de ello. Adicionalmente, también debe analizarse la determinación de la **probabilidad de ocurrencia** de los riesgos que hayan sido identificados, lo cual permitirá definir una frecuencia de materialización de los mismos. Por último, se deberá realizar el **análisis** del riesgo, es decir definir distintos niveles de **impacto** de los riesgos, lo cual permitirá priorizar el **tratamiento** de los mismos dependiendo de la importancia que se le haya dado y el nivel de impacto que tenga. También se debe tener en cuenta para esto último, realizar un análisis del costo de tratar los riesgos (ya sea aceptando, mitigando, transfiriendo o evitando los mismos), en relación con el beneficio que pueda obtenerse. Una vez realizadas todas las etapas anteriores, se deberá llevar adelante la decisión acerca del modo de tratar los riesgos, con su correspondiente control posterior, que permita verificar que se ha realizado de manera correcta la opción elegida. Los distintos modos de tratamiento de los riesgos pueden ser:

Evitar: consiste en realizar acciones para eliminar las situaciones que originan los riesgos. **Mitigar**: consiste en llevar adelante las actividades necesarias para disminuir el impacto que tengan los riesgos sobre la Organización. **Transferir**: se refiere a dejar en manos de terceros las consecuencias de que se materialicen los riesgos, como puede ser un seguro. **Aceptar**: refiere a dejar que el riesgo ocurra, documentando lo que ocurra al seleccionar esta opción

Pregunta 5: Mencione las diferencias entre firma digital y firma electrónica

En nuestro país, se considera a la **firma digital** a través de la ley N° 25 506 como el resultado de aplicarle a un documento determinado un procedimiento matemático con información de exclusivo conocimiento del informante. Esta firma, además, debe ser chequeable de forma tal que permita identificar al firmante y se pueda detectar posibles alteraciones en el documento posteriores a la firma. Mientras que, por otro lado, la **firma electrónica** refiere a un conjunto de datos que no cumplen con los requisitos necesarios para ser considerados para una firma digital. En pocas palabras, la firma digital es un método que permite al emisor de otorgarle autoridad propia a un documento, de una forma segura y verificable ante posibles modificaciones. Mientras que, en la firma electrónica el emisor puede imprimir su autoridad pero sin una forma veraz de verificarla, sino que si se quiere probar, es el mismo emisor el que debe probarla, ya que la firma en si no demuestra autoridad.

Otro (esta vez copió y pegó el sorete)

La firma digital es el resultado de aplicar cierto procedimiento de cifrado a un documento digital, de modo tal que requiere información de la persona que será firmante, y sobre la cual éste tiene control. Además, este tipo de firmas requiere ser verificadas por los terceros que necesiten acreditar la veracidad de esa firma. De este modo representa un medio para demostrar la autenticidad de los documentos, brindando seguridad tanto a quien es autor como a quien lo recibe para su posterior uso. Además este tipo de firmas tiene eficacia jurídica y se presume como válida. Por otro lado, la firma electrónica, carece de la presunción de validez que tiene la firma digital, ya que no cuenta con todos los requisitos legales para ello. La firma electrónica no posee un mecanismo de cifrado como el que posee la firma digital, dado que es simplemente un conjunto de datos electrónicos que están asociados a un determinado documento que también es electrónico.

Pregunta 6: Describa los objetivos del Control Notificación ante incidentes de seguridad de la Ley 25326 (NI IDEA)

Los objetivos del Control Notificación ante incidentes de seguridad de la Ley 25.326 se centran en garantizar la protección integral de los datos personales y la correcta gestión de incidentes que puedan comprometer la seguridad de dicha información. Esto incluye la obligación de los responsables de datos de notificar a las autoridades pertinentes y a los titulares afectados sobre incidentes de seguridad que puedan afectar sus datos, promoviendo así la transparencia y la confianza en el manejo de la información personal. Además, el órgano de control debe supervisar el cumplimiento de las normativas, brindar asistencia a los ciudadanos sobre sus derechos, y establecer sanciones por incumplimientos, asegurando así la integridad y la confidencialidad de los datos personales en archivos y registros

Respuesta otro

Ante incidentes de seguridad la Ley 25326 plantea una serie de acciones que deben llevarse adelante, de las cuales se pueden identificar los siguientes objetivos: Tratar los eventos y consecuentes incidentes de seguridad que puedan afectar los datos personales, su detección, evaluación, contención y respuesta. Realizar un control periódico para verificar que se estén cumpliendo los objetivos organizacionales referidos a la Seguridad de la Información, y realizar informes respecto a ello. Realizar actividades de corrección del entorno técnico y operativo, de modo posterior a la ocurrencia del incidente. Establecer procedimientos de gestión ante incidentes de seguridad, lo cual implica establecer una persona que sea responsable de la comunicación en estos casos. Además, al ocurrir un incidente se debe elaborar el correspondiente informe que tenga

de contenido mínimo la naturaleza de la violación, la categoría de datos personales que fueron afectados, quiénes fueron los usuarios afectados, la medidas que adoptará el responsable para mitigar el incidente, y cuáles son las medidas que se aplicarán para evitar ese tipo de incidentes. Generación de procedimientos o técnicas en la organización tendientes a evitar los incidentes de seguridad que puedan ocurrir. Dar aviso de los incidentes que ocurran a la AAIP (Agencia de Acceso a la Información Pública).

Pregunta 7: Describa características del Control Interno Informático

Respuesta otro (copió y pegó)

Las características que tiene el Control Interno Informático es que se encarga de definir, implantar y ejecutar mecanismos y controles. Además, evalúa la bondad y el cumplimiento de las normas legales en los procesos que define la organización. Por otro lado, apoya y colabora con el trabajo de la Auditoría Informática, como así también controla que todas las actividades se realicen conforme a los procedimientos y normas definidos por la Dirección de la Organización.

Pregunta 8: La Ley de Protección de Datos personales se refiere a Base de Datos en cualquier tipo de soporte que administre una organización

Verdadero, puede ser cualquier archivo, registro, banco o base de datos tanto físico como digital que almacene información.