Comenzado el	viernes, 15 de octubre de 2021, 18:58
Estado	Finalizado
Finalizado en	lunes, 18 de octubre de 2021, 15:52
Tiempo empleado	2 días 20 horas
Calificación	Sin calificar aún

Pregunta 1

Finalizado

Puntúa como 1,00

Describa características del Control Interno Informático

El Control Interno Informátco se caracteriza por definir, implantar y ejecutar mecanismos y controles; evaluar su bondad y asegurar el cumplimiento de normas legales; colaborar y apoyar el trabajo de la auditoria informática y controlar que todas las actividades se realicen cumpliendo los procedimientos y normas fijados por la dirección.

Pregunta 2

Finalizado

Puntúa como 1,00

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 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

d) analice los riesgos de seguridad de la información:

1) valorando las posibles consecuencias que resultarían si los riesgos identificados en el punto 6.1.2 c) 1) llegasen a materializarse,

2) valorando de forma realista la probabilidad de ocurrencia de los riesgos identificados en el punto 6.1.2 c) 1),

3) determinando los niveles de riesgo;

e) evalúe los riesgos de seguridad de la información:

1) comparando los resultados del análisis de riesgos con los criterios de riesgo establecidos en el punto 6.1.2 a),

2) priorizando el tratamiento de los riesgos analizados.

La organización debe conservar información documentada sobre el proceso de apreciación de riesgos de seguridad de la información.

Pregunta 3

Correcta

Puntúa 1,00 sobre 1,00

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

Seleccione una:

- (•) Verdadero ✓
- ( ) Falso

La respuesta correcta es 'Verdadero'

Pregunta 4

Finalizado

Puntúa como 1,00

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

La seguridad informática Solo hace alusión a los aspectos técnicos de la seguridad, es decir se refiere a la protección de los datos en formato digital almacenados o en transito. Por otra parte la seguridad de la información tiene un enfoque integral respecto a la protección e la información dentro de una organización, es decir independientemente al medio en el que se almacene o transmita, ya sea, digital, papel, cintas, conversaciones, personas, etc.

Pregunta 5

Finalizado

Puntúa como 1,00

Describa los objetivos del Control Interno Informático

Sus objetivos son:

Establecer como prioridad la seguridad y Protección de la información 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.

Pregunta 6

Finalizado

Puntúa como 1,00

Mencione las diferencias entre firma digital y firma electrónica

De acuerdo con la legislación argentina, firma electrónica y firma digital no son lo mismo. La Ley 25.506 (reglamentada por el Decreto 182/19) estableció las condiciones para el empleo de la firma digital y su eficacia jurídica. La firma digital es un mecanismo criptográfico asimétrico que permite identificar el autor fácilmente y garantizar la integridad de ese documento, evitando su alteración. Así, una persona contará con un certificado digital emitido por una entidad certificante autorizada, y con dos claves, una pública y una privada. La pública será a la que tendrán acceso los terceros y la privada solo bajo la órbita de conocimiento y control del titular. Cuando una persona desea enviar a otra un documento por medio de este sistema, una vez que lo prepara lo enviará agregándole la clave pública del receptor. De esta manera solo podrá ser abierto, leído y/o modificado por aquel que tenga la clave privada. La firma electrónica, por su parte, no cumple con tales requisitos, por lo cual tiene un grado de seguridad inferior.

Pregunta 7

Finalizado

Puntúa como 1,00

Como se gestionan los riesgos en un Plan de Seguridad Informática según la norma 27001

Para gestionar los riesgos en el plan de seguridad informatica segun la norma 27001, se deben identificar los mismos y tratarlos.

En primer termino se deben indentificar los riesgos vinculados a la perdida de confidencialidad, integridad y disponibilidad; identificar los dueños que tienen asignados los riesgos, valorar las consecuencias y el impacto de los mismos, como así tambien 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 seleccional las opciones adecuadas de tratamiento de riesgos teniendo en cuenta la apreciación de los riesgos para asi decidir que 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.

Pregunta 8

Finalizado

Puntúa como 1,00

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

Los objetivos son tratar los eventos y consecuentes incidentes de seguridad que puedan afectar los datos personales, etiquetar incidentes cuando sucedan dar una respuesta a incidentes de seguridad, evaluar probabilidad de ocurrencia, corrección de entornos técnicos y operativos para evitar futuros incidentes y notificar los incidentes a la Agencia de Acceso a la Informacion Publica.

◄ Avisos

Ir a...

Constitución de grupos y definición de la organización ►