Comenzado el	domingo, 17 de octubre de 2021, 20:16
Estado	Finalizado
Finalizado en	domingo, 17 de octubre de 2021, 21:36
Tiempo empleado	1 hora 19 minutos
Calificación	Sin calificar aún

Pregunta 1
Finalizado
Puntúa como 1,00

Explique las etapas de un proceso de Análisis de Riesgos.

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
Finalizado
Puntúa como 1,00

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

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
Finalizado
Puntúa como 1,00

Describa los objetivos del Control Interno Informático

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
Finalizado
Puntúa como 1,00

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

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
Finalizado
Puntúa como 1,00

Mencione las diferencias entre firma digital y firma electrónica

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
Finalizado
Puntúa como 1,00

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

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
Finalizado
Puntúa como 1,00

Describa características del Control Interno Informático

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 normales 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
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'