Investigación Gestión de riesgos # 2

TEMA 5. Evaluación de Riesgos

Desarrolle la investigación en grupos de trabajos.

Nombre y Apellido

Cédula

Introducción

El proceso de identificación y evaluación de riesgos de una organización es un esfuerzo continuo porque los tipos de amenazas cambian y nunca desaparecen por completo. El objetivo de la administración de riesgos es reducir estas amenazas a un nivel aceptable. Existen diferentes niveles de administración de riesgos. Las organizaciones deben administrar adecuadamente los riesgos para proteger la información y los sistemas de información. La gestión de riesgos también ayuda a evitar acciones legales, interrupciones en las operaciones y protege la reputación de las organizaciones.

Objetivos

Explore el proceso de gestión de riesgos

Parte 1: Explique los niveles de acción del riesgo

Parte 2: Explique los conceptos de Gestión de riesgos

Parte 3: Explique los procesos de Gestión de riesgos

Recursos necesarios

Computadora personal o dispositivo móvil con acceso a internet

Instrucciones

Parte 1: Niveles de acción del riesgo

La gestión de riesgos es la identificación, evaluación y priorización de riesgos. Las organizaciones administran el riesgo de una de cuatro maneras. Cada una puede ser una opción adecuada, según las circunstancias y el tipo de riesgo en cuestión:

· **Prevención (eliminación) -** La prevención de riesgos es la eliminación o eliminación completa del riesgo de una amenaza específica. Por ejemplo, evitar o eliminar la amenaza de que los usuarios compartan o usen mal las contraseñas podría implicar la implementación de un sistema de autenticación de huellas digitales en todas las estaciones de trabajo de los usuarios.

· **Mitigación (reducción) -** La mitigación de riesgos implica la implementación de controles que permiten a la organización continuar realizando una actividad mientras se utilizan mecanismos para reducir el riesgo de una amenaza particular. Una organización también podría aumentar sus controles técnicos y la supervisión de la red para reducir el riesgo de amenazas operativas.

· **Transferencia -** Las organizaciones pueden transferir el riesgo de amenazas específicas. El riesgo financiero de una amenaza puede administrarse mediante la compra de una póliza de seguro o la contratación de un contratista para hacer frente a amenazas específicas.

· **Aceptar -** Aceptar el riesgo implica identificar las amenazas, pero no implementar procesos de mitigación solo después de que se haya tomado una decisión consciente al respecto. La decisión consciente se informa mediante el análisis de los diversos componentes del riesgo antes de continuar.

Paso 1: Administrar el riesgo.

En este paso, describirá ejemplos de administración de riesgos asociados con amenazas específicas a la información o los sistemas de información de la organización.

a. Regularmente, se requiere que una organización maneje información confidencial de los clientes. La divulgación de esta información representa un riesgo grave para la organización.

Pregunta:

¿Qué pasos podría implementar la organización para eliminar el riesgo asociado con el envío o la transferencia accidental de esta información?

b. La organización ha tenido varios problemas de empleados que comparten contraseñas o usan contraseñas débiles.

Preguntas:

Nombre dos maneras de mitigar este riesgo.

R.

Dé dos ejemplos de riesgo de transferencia de una organización.

R.

Paso 2: Explore los niveles de riesgo.

El proceso de identificación y evaluación de riesgos de una organización es un esfuerzo continuo porque los tipos de amenazas cambian y nunca desaparecen por completo. El objetivo de la administración de riesgos es reducir estas amenazas a un nivel aceptable.

Preguntas:

Realice una búsqueda en Internet utilizando los siguientes términos: negligencia, debido cuidado y diligencia debida para responder las siguientes preguntas:

¿Qué es la negligencia? Dé un ejemplo de las consecuencias de la negligencia.

R.

Defina el debido cuidado y la debida diligencia y explique la diferencia entre estos dos términos:

R.

Parte 2: Conceptos de Gestión de Riesgos

La administración de riesgos es una técnica utilizada para identificar y evaluar los factores que pueden amenazar la información y los sistemas de información. El estudio del análisis de riesgos incluye varios términos y conceptos de uso común, incluidos los siguientes:

Activos - Los activos son cualquier cosa de valor que se utiliza y es necesaria para completar una tarea empresarial. Los activos incluyen elementos tangibles e intangibles, como equipos, código de software, datos, instalaciones, personal, valor de mercado y opinión pública. La gestión de riesgos se trata de proteger los activos valiosos de la organización.

Amenazas - Las amenazas son un acto malicioso o un evento inesperado que daña los sistemas de información u otros recursos de la organización relacionados. Pueden ser acciones intencionales que provocan la pérdida o el daño de un activo. Las amenazas también pueden ser involuntarias, como un accidente, un desastre natural o una falla del equipo.

Vulnerabilidad - Las vulnerabilidades son cualquier falla o debilidad que permita que una amenaza cause daño y dañe un activo. Algunos ejemplos pueden ser el código de falla, las configuraciones incorrectas y el incumplimiento de los procedimientos.

Impacto - El impacto del riesgo es el daño sufrido por un evento que causa la pérdida de un activo o la interrupción del servicio. Este daño puede medirse cuantitativa o cualitativamente en función del impacto en las operaciones de la organización.

Riesgo - El riesgo es la probabilidad de pérdida debido a una amenaza a los recursos de una organización.

Contramedidas - Las contramedidas son una acción, un dispositivo o una técnica que reducen una amenaza o una vulnerabilidad mediante su eliminación o prevención. Un ejemplo sería el software antivirus, los firewalls, las políticas y la capacitación.

Evaluación de riesgos - La evaluación de riesgos es el proceso de identificación de vulnerabilidades y amenazas y la evaluación de los posibles impactos para determinar dónde implementar controles de seguridad.

¿Qué es una evaluación de riesgos de seguridad? Una evaluación de riesgos identifica, cuantifica y prioriza los riesgos y las vulnerabilidades en un sistema. Una evaluación de riesgos identifica amenazas reconocidas y agentes de amenazas y la probabilidad de que estos factores den lugar a una exposición o pérdida.

Caso de Estudio:

Una empresa administra una base de datos de clientes que da seguimiento a las compras en línea de los productos. Estas compras se realizan con cuentas de PayPal o tarjetas de crédito. El servidor de bases de datos tiene varias vulnerabilidades. La base de datos está en un servidor en la sala de servidores en la sede central de la empresa. El servidor costó $25,000 USD. La base de datos consta de los 40,000 clientes y más de 1.5 millones de transacciones. El servidor registra más de 120 transacciones por día, lo que genera más de 25,000 por día en ventas. La base de datos se respalda a diario a las 2 A.M. Todos los pedidos también se rastrean y se registran en sistemas separados en caso de falla del servidor. Este proceso puede demorar hasta 50 horas-personas en ingresar manualmente todos los días.

Nombre al menos dos tipos de vulnerabilidades que el personal de ciberseguridad debe analizar:

R.

Describa las posibles amenazas al servidor en función de las vulnerabilidades que identificó:

R.

Describa el impacto en la organización debido a las siguientes amenazas:

● Vulneración de datos:

R.

● Ransomware

R.

● Fallo de hardware:

R.

Enumere una contramedida para las siguientes amenazas al servidor de base de datos de la organización:

● Vulneración de datos:

R.

● Ataque de ransomware:

R.

● Fallo de hardware:

R.

● Malware

R.

Parte 3: Procesos de Gestión de riesgos

La gestión de riesgos es un proceso formal que reduce el impacto de las amenazas y las vulnerabilidades. No puede eliminar el riesgo por completo, pero puede administrar el riesgo a un nivel aceptable. La administración de riesgos mide el impacto de una amenaza y el costo de implementar controles o contramedidas para mitigar la amenaza. Todas las organizaciones aceptan algún riesgo. El costo de un control nunca debe superar el valor del activo que está protegiendo.

Paso 1: Estructurar y evaluar el riesgo

Identifique las amenazas a través de la organización que aumentan el riesgo. Las amenazas identificadas incluyen procesos, productos, ataques, posibles fallos o interrupciones de los servicios, percepción negativa de la reputación de una organización, responsabilidad legal potencial o pérdida de propiedad intelectual.

Después de identificar un riesgo, se lo evalúa y analiza para determinar la gravedad de la amenaza. Algunas amenazas pueden paralizar a toda una organización, mientras que otras amenazas solo inconvenientes menores. El riesgo se puede priorizar por el impacto financiero (un análisis cuantitativo) o el impacto a escala en la operación de una organización (un análisis cualitativo).

En nuestro ejemplo, se han identificado las siguientes vulnerabilidades. Asigne un valor cuantitativo a cada riesgo según las respuestas de su comité. Proporcione justificación para el valor que determinó.

Pregunta:

Utilice el caso de estudio para formular sus respuestas.

● Violación de datos que afecta a todos los clientes:

R.

● Falla de hardware del servidor que requiere reemplazo de hardware:

R.

● Ransomware que afecta a toda la base de datos del servidor:

R.

● Inundación de la sala de servidores causada por la activación de los rociadores contra incendios:

R.

Paso 2: Responder al riesgo

Este paso implica desarrollar un plan de acción para reducir la exposición general al riesgo de la organización. La administración clasifica y prioriza las amenazas; un equipo determina cómo responder a cada amenaza. El riesgo se puede eliminar, mitigar, transferir o aceptar.

Pregunta:

Clasifique las vulnerabilidades y proponga posibles contramedidas para cada amenaza.

● Violación de datos que afecta a todos los clientes:

R.

● Falla de hardware del servidor que requiere reemplazo de hardware:

R.

● Ransomware que afecta a toda la base de datos del servidor:

R.

● Inundación de la sala de servidores causada por la activación de los rociadores contra incendios:

R.

Paso 3: Monitorear el riesgo

Revise continuamente las reducciones de riesgo debido a acciones de eliminación, mitigación o transferencia. No todos los riesgos se pueden eliminar, por lo que las amenazas que se aceptan deben ser monitoreadas de cerca. Es importante comprender que siempre hay algún riesgo presente y aceptable. A medida que se implementan las contramedidas, el impacto del riesgo debe disminuir. Se requiere un monitoreo constante y la revisión de nuevas contramedidas.

Pregunta:

¿Qué acciones podrían disminuir el impacto de una amenaza de ransomware?

R.