**UNIVERSIDAD TECNOLÓGICA DE PANAMÁ**

**CENTRO REGIONAL DE CHIRIQUÍ**

**FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES**

**LICENCIATURA EN INGENIERÍA DE SISTEMAS DE INFORMACIÓN**

MATERIA 6 CRÉDITOS:

SEGURIDAD INFORMÁTICA

**INVESTIGACIÓN:**

**GESTIÓN DE RIESGO**

**DOCENTE:**

MGTR. LEANDRO ESPINOZA MONTENEGRO

**ESTUDIANTE:**

|  |  |
| --- | --- |
| ABREGO, NEFTHALY | 4-806-103 |

DEYBI MOJICA 8-930-2000

2024

Contenido

[Introducción 3](#_Toc161558524)

[Objetivos 3](#_Toc161558525)

[Parte 1: Niveles de acción del riesgo 4](#_Toc161558526)

[Paso 1: Administrar el riesgo. 5](#_Toc161558527)

[Pregunta: 5](#_Toc161558528)

[Preguntas: 5](#_Toc161558529)

[Respuesta 6](#_Toc161558530)

[Dé dos ejemplos de riesgo de transferencia de una organización. 7](#_Toc161558531)

[Respuesta: 7](#_Toc161558532)

[Paso 2: Explore los niveles de riesgo. 8](#_Toc161558533)

[Preguntas: 8](#_Toc161558534)

[¿Qué es la negligencia? Dé un ejemplo de las consecuencias de la negligencia. 8](#_Toc161558535)

[Defina el debido cuidado y la debida diligencia y explique la diferencia entre estos dos términos: 9](#_Toc161558536)

[Parte 2: Conceptos de Gestión de Riesgos 10](#_Toc161558537)

[Caso de Estudio: 12](#_Toc161558538)

[R. 12](#_Toc161558539)

[R. 13](#_Toc161558540)

[R. 13](#_Toc161558541)

[R. 14](#_Toc161558542)

[R. 14](#_Toc161558543)

[R. 14](#_Toc161558544)

[R. 14](#_Toc161558545)

[R. 14](#_Toc161558546)

[Malware R. 14](#_Toc161558547)

[Parte 3: Procesos de Gestión de riesgos 14](#_Toc161558548)

[Paso 1: Estructurar y evaluar el riesgo 14](#_Toc161558549)

[Pregunta: 16](#_Toc161558550)

[R. 16](#_Toc161558551)

[R. 16](#_Toc161558552)

[Paso 2: Responder al riesgo 16](#_Toc161558553)

[Pregunta: 16](#_Toc161558554)

[R. 18](#_Toc161558555)

[Paso 3: Monitorear el riesgo 18](#_Toc161558556)

[Pregunta: 18](#_Toc161558557)

**Investigación Gestión de riesgos # 2 TEMA 5. Evaluación de Riesgos**

# 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

Computadora personal o dispositivo móvil con acceso a internet

# 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.

1. 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?

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

### Preguntas:

Nombre dos maneras de mitigar este riesgo.

### Respuesta

Para la mitigación de este riesgo se deben establecer políticas de contraseñas, esto permiten obligar a los usuarios a cumplir estándares de longitud, incluso pueden implementarse controles estrictos en donde solo un usuario es responsable de establecer las configuraciones de contraseñas en servicios, equipos personales y aplicaciones.[1] Esta política establecería controles para no utilizar contraseñas por defecto, implementación de técnicas de autenticación, doble autenticación, contraseñas robustas, contraseñas distintas para cada servicio.

Además, el uso de doble factor de autenticación permite que los usuarios que deseen acceder a sus servicios verifiquen con otro método como un código de correo, una aplicación de tokens, esto aumenta la dificultad para intentos que buscan introducirse en el sistema y permite alertar al usuario de un intento de acceso no autorizado.[2]

**Para evitar el riesgo de envió no autorizado de información:**

Implementar una política de seguridad de datos implica establecer directrices claras sobre qué datos se consideran confidenciales, cómo deben ser almacenados y transferidos, así como las consecuencias de su divulgación no autorizada, como se menciona en una cita de la norma ISO 27001.[3]

Para garantizar la seguridad de estos datos, es fundamental utilizar métodos de cifrado tanto en reposo como en tránsito de los datos con las mejores tecnologías. Esto implica codificar la información de manera que solo pueda ser descifrada por individuos autorizados que posean la clave correspondiente.[4]

Además, se debe implementar un sistema de controles de acceso que restrinja el acceso a la información confidencial únicamente a aquellos empleados que realmente lo necesiten, esto permite lograr mediante la asignación de permisos de usuario, roles y grupo.[5]

Otro aspecto crucial es la capacitación de los empleados en materia de seguridad de datos. Es esencial que estén conscientes de la importancia de proteger la información confidencial y de cómo hacerlo adecuadamente, como se recomienda en un recurso proporcionado por Stay Safe Online.

### Dé dos ejemplos de riesgo de transferencia de una organización.

### Respuesta:

Primer método puede ser la transferencia del riesgo con un partner o asesores idóneos especializado en la ciberseguridad para establecer mejores objetivos, acceder a talentos especializados como analistas de riesgo, auditores informáticos para mejorar los métodos de control interno y obtener recomendaciones de ciberseguridad.[6]

La segunda forma es contratar seguros que cubran la infraestructura informática una herramienta esencial para proteger sus activos frente a una amplia gama de amenazas, como filtraciones de seguridad, ataques cibernéticos, virus informáticos, conducta deshonesta de empleados o descuidos que puedan ocasionar la pérdida de datos o el robo de identidad, entre otros posibles incidentes. Estos seguros están diseñados específicamente para proporcionar cobertura contra virus y ataques de hackers, tanto en el entorno digital como en el físico.[7]

## 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.

#### Respuesta

La negligencia puede entenderse como la falta de atención o cuidado que una persona debería haber tenido en una situación determinada. Es como no actuar con precaución en una situación en la que se supone que debemos actuar responsablemente. Desde una perspectiva legal, negligencia significa no tomar medidas para proteger a otros de daños cuando estamos obligados a hacerlo. En otras palabras, esto no respeta el deber de diligencia que se espera de nosotros en una situación determinada.[8]

Ejemplo, en el área de administración de sistemas, la negligencia podría manifestarse como no actualizar el software y los parches de seguridad, lo que podría dejar los sistemas vulnerables a ciberataques como ransomware o intrusiones de piratas.

En el ámbito de las redes, la negligencia puede dar lugar a cortafuegos mal configurados o a la imposibilidad de implementar medidas de autenticación sólidas, lo que podría permitir a los atacantes obtener acceso a la red y comprometer la seguridad de los datos.

La negligencia en ciberseguridad podría resultar en una falta de capacitación adecuada del personal en prácticas de ciberseguridad, lo que podría llevar a errores humanos que faciliten ataques, como hacer clic en enlaces maliciosos o revelar información confidencial a personas no autorizadas.

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

#### Respuesta

Debido cuidado: El debido cuidado profesional se refiere a la responsabilidad y la atención meticulosa que un profesional debe aplicar en el ejercicio de su labor. Esto implica tomar todas las precauciones necesarias para garantizar que se cumplan los estándares éticos y técnicos requeridos en su campo de trabajo.[9] El debido cuidado profesional implica que los profesionales de TI, como administradores de sistemas, ingenieros de redes y expertos en ciberseguridad, lleven a cabo sus funciones con un alto nivel de competencia, integridad, atención a los detalles y responsabilidad. Esto significa que el trabajador tiene un grado de diligencia elevado durante las actividades que realiza profesionalmente como proteger los activos a su tutela, un cuidado indebido puede producir daños colaterales pudiéndose considerar delitos imprudentes.[10]

Debida diligencia: Como las empresas están siempre envueltas en incertidumbre, por ello el deber de ampliar siempre conocimientos para conocer el contexto en el que el profesional se desenvuelve permite mejorar la identificación de riesgos y rastrear oportunidades de mejora, esto permite identificar y posteriormente reaccionar a los eventos. La debida diligencia es el proceso de estudiar, auditar, investigar y evaluar los riesgos y oportunidades en las operaciones que ejecuta una empresa.[11] Según la universidad de Oxford en derecho, la debida diligencia son las medidas razonablemente tomadas por una persona para evitar cometer un acto ilícito o delito.

La debida diligencia en ciberseguridad es un proceso fundamental que se centra en realizar una investigación exhaustiva para identificar y evaluar todos los activos de información de una empresa, así como los sistemas de seguridad utilizados para proteger dichos activos. Este proceso puede incluir, además, la evaluación de la capacidad de la organización para enfrentar y recuperarse de posibles ciberataques.[12]

Entre los componentes clave de la debida diligencia en ciberseguridad se encuentran la adquisición de registros de incidentes de seguridad, la revisión de procedimientos para la gestión de incidentes, la auditoría del software utilizado y la revisión de auditorías de cumplimiento recientes.[12]

Algunas investigaciones de debida diligencia en ciberseguridad pueden ir más allá, incluyendo el análisis forense del tráfico de red de la empresa para detectar posibles fugas de datos en curso o pasadas.[12]

**Explicación de diferencias:**

Negligencia: Un administrador de sistemas no instala una actualización de seguridad crítica que corrige una vulnerabilidad conocida. Un atacante explota la vulnerabilidad para obtener acceso a los sistemas de la organización y robar datos confidenciales.

Debido cuidado: Un administrador de sistemas instala todas las actualizaciones de seguridad críticas y realiza copias de seguridad regulares de los datos. Un ataque de ransomware interrumpe los sistemas de la organización, pero los datos se pueden restaurar desde la copia de seguridad.

Debida diligencia: Un administrador de sistemas realiza una prueba de penetración para identificar vulnerabilidades en los sistemas de la organización. Se implementa una medida de seguridad avanzada para mitigar una vulnerabilidad crítica.

El debido cuidado se refiere a la responsabilidad de proteger los intereses y activos de una compañía. Esto implica tomar medidas precautorias y preventivas para evitar posibles riesgos o daños que puedan afectar a la organización. Por otro lado, la debida diligencia se trata de llevar a cabo de manera sistemática y cuidadosa todas las actividades necesarias para mantener el esfuerzo del debido cuidado. Esto significa que no basta con tener conciencia de la importancia de proteger los intereses de la empresa, sino que también se deben implementar acciones concretas de manera consistente y metódica para garantizar que esos intereses estén protegidos de manera efectiva y continua.

## 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.