NORMATIVAS DE CIBERSEGURIDAD

Unidad 2. Actividad 6

10 DE ENERO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.-

Metodología de Análisis y Gestión de Riesgos de los Sistemas Informáticos.

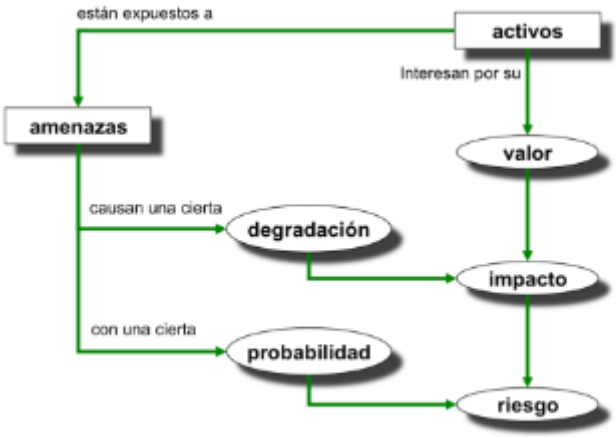

Ilustración 7. Elementos del análisis de riesgos potenciales

La metodología de análisis y gestión de riesgos de los sistemas de información es un proceso estructurado que permite identificar, evaluar y mitigar los riesgos relacionados con la seguridad de la información en una organización. Una metodología general que se puede adaptar según las necesidades y características específicas de un entorno:

Contextualización:

- Definición del alcance: Establece qué sistemas y activos estarán sujetos al análisis de riesgos. Define también los límites del entorno a estudiar.

- Objetivos y requisitos: Documenta los objetivos de negocio y los requisitos de seguridad asociados. Esto proporciona el marco para evaluar la importancia de los activos y los riesgos asociados.

Identificación de Activos:

- Listado de Activos: Enumera todos los activos de información relevantes, desde servidores y bases de datos hasta datos sensibles y personal clave.

- Clasificación: Categoriza los activos según su importancia para la continuidad del negocio y su impacto en caso de una amenaza.

Identificación de Amenazas y Vulnerabilidades:

- Amenazas potenciales: Enumera y describe las amenazas que podrían afectar a los activos. Pueden incluir amenazas físicas, cibernéticas, humanas, etc.

- Vulnerabilidades existentes: Identifica las debilidades y vulnerabilidades en los sistemas y procesos que podrían ser explotadas por las amenazas.

Análisis de Riesgos:

- Probabilidad e impacto: Evalúa la probabilidad de que ocurra cada amenaza y el impacto potencial en los activos afectados.

- Cálculo de riesgos: Calcula el riesgo multiplicando la probabilidad por el impacto. Esto proporciona una medida cuantitativa o cualitativa de la magnitud del riesgo.

Clasificación de Riesgos:

- Priorización: Clasifica los riesgos según su nivel de riesgo. Esto ayuda a concentrar los esfuerzos en los riesgos más críticos.

Evaluación de Riesgos:

- Aceptación y Mitigación: Decide qué riesgos son aceptables y cuáles requieren medidas de mitigación. Establece prioridades para abordar los riesgos más urgentes o críticos.

Mitigación de Riesgos:

- Desarrollo de Controles: Identifica y desarrolla estrategias y controles para reducir la probabilidad o el impacto de los riesgos identificados.

- Implementación: Asigna responsabilidades para implementar y mantener estos controles. Puede implicar actualizaciones de software, entrenamiento del personal, políticas de seguridad, entre otros.

Monitoreo Continuo:

- Revisión Regular: Establece un proceso para revisar y actualizar la evaluación de riesgos regularmente, especialmente en respuesta a cambios en el entorno de seguridad o en la organización.

- Ajuste de Estrategias: Ajusta las estrategias de mitigación según sea necesario para mantener la eficacia frente a las amenazas cambiantes.

Documentación y Comunicación:

- Documentación Detallada: Registra todo el proceso de análisis y gestión de riesgos en documentación detallada. Esto proporciona una referencia clara y un historial de las decisiones tomadas.

- Comunicación a Interesados: Comunica los resultados a todas las partes interesadas, desde el personal de TI hasta la alta dirección. Destaca los riesgos críticos y las medidas de mitigación.

Cultura de Seguridad:

- Concientización: Fomenta una cultura de seguridad, involucrando a todos los niveles de la organización. La concientización sobre la importancia de la gestión de riesgos y la seguridad de la información es clave para el éxito a largo plazo.