Plan de tratamiento de riesgos y vulnerabilidades

INSTITUTO DE FINANCIAMIENTO, PROMOCIÓN
Y DESARROLLO DE MANIZALES

2026

A continuación, se detalla el paso a paso desde el enfoque proactivo al reactivo del plan de tratamiento de vulnerabilidades

Del punto 1 al punto 3, se definirán actividades previas de vital importancia para que el tratamiento de vulnerabilidades sea posible:

1. **Identificación de Activos y Vulnerabilidades:**

Identificación de activos

a) **Inventario de Activos:** Consultar inventario completo de todos los activos de la organización. Esto incluye hardware (computadoras, servidores, dispositivos de red), software (aplicaciones, sistemas operativos), datos (información confidencial, bases de datos) y recursos humanos (personal con acceso a sistemas críticos).

b) **Clasificación de Activos:** Una vez identificado los activos, se clasifican en función de su importancia y valor para la organización.

c) **Etiquetado de Activos:** se asignan etiquetas o identificadores únicos a cada activo para facilitar su seguimiento y gestión.

d) **Mapeo de Datos:** se identifica dónde residen los datos críticos y cómo fluyen a través de la organización, con el fin de protegen la información confidencial.

Identificación de Vulnerabilidades:

a) **Análisis de Riesgos:** se realiza un análisis de riesgos para identificar las amenazas potenciales a los activos y evaluar su impacto y probabilidad.

b) **Escaneo de Vulnerabilidades:** se utilizan herramientas de escaneo de vulnerabilidades para buscar activamente vulnerabilidades conocidas en los sistemas y redes.

c) **Pruebas de Penetración:** se realizan pruebas de penetración o "pen tests" para simular ataques reales y descubrir posibles vulnerabilidades antes de que los ciberdelincuentes.

d) **Gestión de Parches:** se mantienen actualizados los sistemas y aplicaciones con los últimos parches de seguridad.

e) **Monitoreo Continuo:** se implementa un sistema de monitoreo de seguridad continuo para detectar y responder a nuevas vulnerabilidades a medida que surgen.

f) **Gestión de Incidentes:** se establece un proceso sólido de gestión de incidentes para responder rápidamente a cualquier explotación de vulnerabilidades que pueda ocurrir.

2. **Priorización de Vulnerabilidades:**

a) **Clasificación de Activos:** se identifican y clasifican los activos según su importancia para la organización.
b) **Evaluar el Impacto:** se determina el impacto potencial de una vulnerabilidad en los activos críticos.
c) **Evaluar la Probabilidad:** se evalúa la probabilidad de que una vulnerabilidad fuese explotada.
d) **Priorizar en Función del Índice de Riesgo:** Priorizar las vulnerabilidades según el índice de riesgo calculado. Las vulnerabilidades con un alto índice de riesgo se deben abordar primero, ya que representaban las mayores amenazas para los activos críticos.
e) **Considere el Contexto:** Además del índice de riesgo, se considera el contexto en el que se opera.
f) **Monitorización Continua:** Una vez priorizado y abordado las vulnerabilidades, se establece un proceso de monitorización continua para evaluar nuevos riesgos y vulnerabilidades a medida que surgen.
g) **Comunicación y Documentación:** se debe comunicar claramente las prioridades de las vulnerabilidades y las acciones a tomar a todas las partes interesadas y levantar el informe o acta de garantía del tratamiento dato al reporte de vulnerabilidades realizado.

3. **Evaluación de Riesgos:**

a) **Identificación de Activos:** se comienza por identificar y catalogar todos los activos críticos para la organización. Estos incluyen hardware, software, datos, personal, instalaciones físicas y más.
b) **Identificación de Amenazas:** se identifican las amenazas que podrían afectar a los activos.
c) **Evaluación de Impacto:** se evalúa el impacto potencial de cada amenaza en los activos. Esto implico considerar el impacto en la confidencialidad, integridad y disponibilidad de la información y los sistemas.
d) **Evaluación de Probabilidad:** se estima la probabilidad de que cada amenaza se materialice y cause un impacto en tus activos.
e) **Cálculo de Riesgo:** se combina la evaluación de impacto y probabilidad para calcular el nivel de riesgo para cada amenaza.
f) **Identificación de Controles Existentes:** se Identifican los controles de seguridad existentes con el fin de evaluar si pueden mitigar el riesgo.
g) **Priorización basada en Impacto y Probabilidad:** se evalúa el impacto y la probabilidad de explotación de cada vulnerabilidad y se prioriza en función de estos factores.
h) **Abordar las Vulnerabilidades Priorizadas:** se comienza por abordar las vulnerabilidades de mayor prioridad, implementando controles de seguridad adicionales, aplicando parches, actualizando configuraciones, etc.

Es desde este punto donde se definirá el flujo de tratamiento a las vulnerabilidades luego de exponer a alto nivel cada paso del desarrollo de dicho plan:

4. **Desarrollo de Planes de Mitigación:**

a) **Aplicación de Parches y Actualizaciones de Software:** se deben aplicar parches y actualizaciones de softwares para la mitigación y prevención de vulnerabilidades.
b) **Reconfiguración de Sistemas:** es necesario reconfiguraciones en los sistemas y ajustar las políticas de acceso, deshabilitar los servicios no utilizados para cerrar las brechas de seguridad.
c) **Control de Acceso y Autenticación:** Se refuerza de ser necesario el control de acceso y la autenticación involucrando la implementación de autenticación de dos factores (2FA), políticas de contraseñas más fuertes y una revisión de los permisos de usuario.
d) **Pruebas de Validación:** se realizan pruebas de validación para asegurarse de que las vulnerabilidades se hayan abordado correctamente.

5. **Asignación de Responsabilidades:** se definen los responsables de llevar a cabo cada tarea, se incluyen administradores de sistemas, equipos de seguridad, proveedores parte de la cadena de suministros, entre otros a los que haya lugar.

6. **Programación de Tareas:** se priorizan las vulnerabilidades, se establece una fecha límite para la mitigación. Para los proveedores, se solicita la creación de un cronograma para abordar las vulnerabilidades halladas en su infraestructura según su prioridad.

7. **Documentación y Registro:** se realiza un acta de finalización de las remediaciones de las vulnerabilidades, así como las fechas de implementaciones de controles claves que hayan sido necesarios. Se almacena información de la evidencia de cumplimiento con el Retest del antes y el después de las vulnerabilidades tratadas.

8. **Capacitación y Concienciación:** se realiza capacitación y concientización a empleados de la organización con el fin de fortalecer la seguridad cibernética y reducir riesgos de ataques

9. **Revisión Periódica:** se establece una programación anual para la revisión del plan de tratamiento de vulnerabilidades donde se identifican posibles cambios en la infraestructura y alguna adecuación en base a la forma de identificar o tratar las vulnerabilidades.

Desde este apartado, procedemos a presentar la forma en la que se les dará tratamiento a las vulnerabilidades halladas en los ejercicios de Ethical Hacking que son realizados periódicamente por la organización y los hallazgos realizados por las operaciones de monitoreo continuo de nuestro centro de operaciones de seguridad

10. Modelo Operativo de tratamiento:

El tratamiento dado a las distintas vulnerabilidades halladas en los reportes de ejercicios de Ethical Hacking y del monitoreo continuo, estará enfocado en la siguiente estructura y forma:

Categorización de Vulnerabilidades:

1. Vulnerabilidades Críticas:

Descripción: Estas vulnerabilidades representan una amenaza inmediata y significativa para la seguridad de nuestros sistemas. Pueden ser aprovechadas de manera rápida y tienen el potencial de causar daños graves.

Acción Inmediata Requerida: Se requiere una acción inmediata y prioritaria para mitigar estas vulnerabilidades y reducir el riesgo de explotación.

Plazo Objetivo: El tratamiento de vulnerabilidades críticas debe comenzar de inmediato y completarse en un plazo de [72 Horas], priorizando la protección de activos críticos.

Responsable: [Profesional Universitario TI] será el encargado de coordinar la respuesta inmediata a estas vulnerabilidades. Esto puede implicar la aplicación de parches, cambios de configuración o medidas de mitigación temporales.

2. Vulnerabilidades de Alta Gravedad:

Descripción: Estas vulnerabilidades presentan un riesgo significativo para la seguridad, aunque no requieren una respuesta inmediata. Pueden ser explotadas si no se abordan en un plazo razonable.

Acción Requerida: Programar la aplicación de parches o soluciones para abordar estas vulnerabilidades de manera efectiva y reducir el riesgo asociado.

Plazo Objetivo: El tratamiento de vulnerabilidades de alta gravedad debe comenzar en un plazo de [10 días] y completarse antes de que se conviertan en una amenaza significativa.

Responsable: [Profesional Universitario TI]] supervisará el proceso de tratamiento y garantizará que se cumplan los plazos establecidos.

3. Vulnerabilidades de Gravedad Media:

Descripción: Estas vulnerabilidades representan un riesgo moderado para la seguridad y pueden abordarse de manera más gradual.

Acción Requerida: Planificar y aplicar soluciones de manera oportuna para reducir el riesgo.

Plazo Objetivo: El tratamiento de vulnerabilidades de gravedad media debe comenzar en un plazo de [20 días] y completarse dentro de este período.

Responsable: [Profesional Universitario TI]] se encargará de coordinar la identificación y corrección de estas vulnerabilidades, asegurando que se cumplan los plazos establecidos.

4. Vulnerabilidades de Baja Gravedad:

Descripción: Estas vulnerabilidades presentan un riesgo bajo o son difíciles de explotar. Pueden tratarse de manera más flexible.

Acción Requerida: Programar correcciones en bloques de mantenimiento.

Plazo Objetivo: El tratamiento de vulnerabilidades de baja gravedad puede programarse en un ciclo de [1 Mes] y se incluirá en las actualizaciones programadas.

Responsable: [Profesional Universitario TI] será el encargado de garantizar que se aborden durante los bloques de mantenimiento.

Esta estructura proporciona una visión más detallada y contextualizada de cómo abordar cada categoría de vulnerabilidad, incluyendo descripciones, acciones requeridas, plazos objetivos y responsables. Adaptada a las necesidades específicas de nuestra organización.

Para concluir:

En este plan de tratamiento de vulnerabilidades, hemos establecido una estructura sólida y detallada para abordar de manera efectiva las vulnerabilidades que pueden afectar la seguridad de nuestros sistemas y datos. A través de la categorización adecuada de las vulnerabilidades en función de su gravedad y el establecimiento de plazos objetivos claros, hemos creado un marco que nos permite priorizar y gestionar eficazmente las amenazas.

Es fundamental destacar que la seguridad cibernética es un esfuerzo continuo que requiere la colaboración de todos los miembros de nuestra organización. La identificación temprana y la respuesta adecuada a las vulnerabilidades son esenciales para mantener la integridad y la confidencialidad de nuestros activos digitales.

Además, la documentación y la revisión regular de este plan son esenciales para asegurarnos de que nuestras prácticas de seguridad estén actualizadas y alineadas con las últimas amenazas y mejores prácticas. La evaluación constante de nuestros procesos de tratamiento de vulnerabilidades nos permitirá adaptarnos y mejorar continuamente nuestra postura de seguridad.

En resumen, este plan de tratamiento de vulnerabilidades proporciona una guía sólida para abordar las vulnerabilidades de manera eficiente y mitigar los riesgos de seguridad. La seguridad cibernética es una responsabilidad compartida y, al seguir este plan, estamos comprometidos en proteger nuestros sistemas y datos de manera proactiva y efectiva.