

**GASIC 6 – Seguridad en Redes**

**Preguntas de Auditoría**

**Pruebas de vulnerabilidad del Sistema**

**Competencias Básicas del Auditor**

1. **Conocimiento en seguridad de la información:** El auditor debe tener un profundo conocimiento de los principios y conceptos fundamentales de seguridad de la información, incluyendo la confidencialidad, integridad y disponibilidad de los datos.
2. **Conocimientos de redes:** Es esencial tener un conocimiento sólido de las redes de computadoras, incluyendo protocolos, topologías, componentes de red y arquitecturas.
3. **Comprensión de estándares y normativas:** Familiaridad con estándares de seguridad de la información como ISO 27001, NIST, CIS Controls y otras normativas aplicables. Debe comprender los requisitos de cumplimiento y saber cómo evaluar el cumplimiento de la organización.
4. **Herramientas de auditoría:** Ser capaz de utilizar herramientas de auditoría y análisis de seguridad, como escáneres de vulnerabilidades, herramientas de prueba de penetración, y sistemas de detección de intrusiones (IDS/IPS).
5. **Habilidades de análisis:** Ser capaz de analizar la configuración de dispositivos de red, registros de eventos y otros datos para identificar vulnerabilidades y problemas de seguridad.
6. **Gestión de riesgos:** Comprender cómo evaluar y gestionar los riesgos de seguridad en una infraestructura de red, incluyendo la identificación, análisis y mitigación de riesgos.

# Visión General

Las pruebas de vulnerabilidad en sistemas son un componente esencial para evaluar la efectividad de los controles de seguridad y detectar posibles puntos de fallo antes de que puedan ser explotados. Estas pruebas permiten no solo identificar debilidades técnicas, sino también evaluar la respuesta organizacional frente a amenazas potenciales. Implementar un enfoque estructurado, basado en controles y planes definidos, asegura que las vulnerabilidades se detecten y gestionen de manera proactiva, reduciendo riesgos y fortaleciendo la postura de seguridad en redes.

**1.1 Desarrollo de un Plan de Evaluación de Control**

El proceso comienza con la elaboración de un plan detallado que defina el alcance de la evaluación, los controles que serán verificados, y los procedimientos específicos a emplear, como pruebas de rendimiento, escaneo de vulnerabilidades y simulaciones de amenazas internas. Este plan debe asignar roles y responsabilidades claros al equipo de evaluación y detallar las herramientas y tecnologías necesarias. La implementación de casos de prueba automatizados y la instrumentación de seguridad permiten una validación exhaustiva y replicable, mientras que las pruebas de fuga de datos y amenazas internas garantizan una evaluación integral.

**1.2 Pruebas de Penetración y Evaluaciones Técnicas**

La ejecución de pruebas de penetración, tanto internas como externas, debe realizarse con frecuencia definida, asegurando que incluyan ejercicios avanzados, como simulaciones de "red team" y análisis de reconocimiento ambiental. Estas pruebas permiten simular los intentos de adversarios de comprometer sistemas, identificando vulnerabilidades explotables. Además, los informes resultantes deben analizarse minuciosamente para determinar las acciones correctivas necesarias, como actualizaciones de sistemas o la implementación de nuevos controles, priorizando siempre las áreas más críticas para la organización.

**1.3 Auditoría y Validación Posterior a las Pruebas**

Una vez completadas las pruebas, los hallazgos deben documentarse en informes detallados que permitan a la organización evaluar el cumplimiento de los objetivos establecidos. Los resultados deben ser validados mediante la modificación de reglas o capacidades de detección, en caso de ser necesario, asegurando que las técnicas utilizadas durante las pruebas sean incorporadas en las estrategias de defensa. Este enfoque no solo cierra brechas detectadas, sino que también fomenta una mejora continua en las capacidades de seguridad, proporcionando indicadores claros para medir el impacto y la efectividad de las pruebas realizadas.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Desarrollar un plan de evaluación de control que describa el alcance de la evaluación que incluya:      1.1 Controles y mejoras de control en evaluación      1.2 Procedimientos de evaluación que se utilizarán para determinar la eficacia del control      1.3 Entorno de evaluación, equipo de evaluación y roles y responsabilidades de evaluación      1.4 Incluir como parte de las evaluaciones de control:          1.4.1 seguimiento en profundidad          1.4.2 instrumentación de seguridad          1.4.3 casos de prueba de seguridad automatizados          1.4.4 escaneo de vulnerabilidades          1.4.5 pruebas de usuarios malintencionados          1.4.6 evaluación de amenazas internas          1.4.7 pruebas de rendimiento y carga          1.4.8 evaluación de fuga o pérdida de datos  2. Incorporar dentro de la evaluación de vulnerabilidades técnicas:      2.2 analizar y verificar los informes para determinar qué actividad de respuesta y reparación es necesaria.      2.3 identificar los riesgos asociados y las acciones a realizar, una vez identificada una posible vulnerabilidad técnica. Estas acciones pueden consistir en la actualización de los sistemas vulnerables o en la aplicación de otros controles.  3. Emplear un proceso de prueba de penetración con una frecuencia definida por la organización, que sea anunciada o no anunciado que intente eludir los controles asociados con los puntos de acceso físico a la instalación.      3.1 Emplear ejercicios de red team para simular los intentos de los adversarios de comprometer los sistemas organizacionales de acuerdo con las reglas de enfrentamiento aplicables. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Usar de forma continua un portafolio de tecnologías, servicios y activos soportados (p. ej., escáneres de vulnerabilidad, fuzzers y sniffers, analizadores de protocolos) para identificar vulnerabilidades de seguridad de la información.  2. Asegurar que el plan de evaluación de control sea revisado y aprobado por el funcionario autorizador o el representante designado antes de realizar la evaluación.     2.1 Evaluar los controles en el sistema y su entorno de operación para determinar hasta qué punto los controles se implementan correctamente, funcionan según lo previsto y producen el resultado deseado con respecto al cumplimiento de los requisitos de seguridad y privacidad establecidos.      2.2 Producir un informe de evaluación de control que documente los resultados de la evaluación.      2.3 Proporcionar los resultados de la evaluación de control a un responsable designado por la organización  3. Emplear un agente o equipo independiente de pruebas de penetración para realizar pruebas de penetración en el sistema o los componentes del sistema.       3.1 Seleccionar el evaluador o equipo de evaluación adecuado para el tipo de evaluación que se realizará. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Realizar pruebas de penetración externas periódicas basadas en los requisitos del programa, al menos una vez al año.      1.1 Las pruebas de penetración externas deben incluir reconocimiento empresarial y ambiental para detectar información explotable y para determinar la idoneidad de la protección de la red.      1.2 Las pruebas de penetración requieren habilidades y experiencia especializadas y deben realizarse a través de una persona calificada. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Establecer indicadores para la prueba de vulnerabilidad del sistema según metas y objetivos establecidos. |
| NIVEL 5 [Optimizado]: La organización se centra en la mejora continua y está diseñada para girar y responder a las oportunidades y los cambios. | 1. Corregir los resultados de las pruebas de penetración según la política de la empresa para el alcance y la priorización de la corrección.  2. Validar las medidas de seguridad después de cada prueba de penetración.      2.1 Si se considera necesario, se deben modificar los conjuntos de reglas y las capacidades para detectar las técnicas utilizadas durante las pruebas. |

1. **Preguntas de Auditoría para las Pruebas de Vulnerabilidad del Sistema**

|  |
| --- |
| Temática: Proceso de Prueba de Penetración |
| Los procesos de prueba de penetración es un componente esencial de la gestión de la seguridad cibernética y garantiza que estas pruebas se realicen de manera adecuada y ética, lo que a su vez contribuye a fortalecer la postura de seguridad de una organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se realizan pruebas de penetración internas y externas de forma periódica como se especifica en los requisitos del programa de seguridad?   + ¿Las pruebas de penetración externas incluyen el reconocimiento empresarial y ambiental para detectar información explotable y evaluar la idoneidad de la protección de la red?   + ¿Los resultados de las pruebas se corrigen de acuerdo con la política de la empresa para el alcance y la priorización de la corrección?     - ¿Se lleva a cabo una validación de las medidas de seguridad después de cada prueba de penetración?     - ¿Se modifican los conjuntos de reglas y capacidades de detección según sea necesario para detectar las técnicas utilizadas durante las pruebas?     - Evalúe si ha habido actualizaciones en las reglas de detección o en las capacidades de seguridad después de pruebas de penetración recientes y si estas actualizaciones están relacionadas con las técnicas detectadas.   + ¿Las pruebas se realizan por personal con habilidades y experiencia especializadas? ¿Se ha designado a una persona calificada para supervisar y dirigir las pruebas?   + ¿Se ha establecido un alcance claro para las pruebas de penetración, que incluya sistemas, aplicaciones o redes específicas que deben ser evaluadas?   + ¿Se mantienen registros adecuados de todas las pruebas de penetración, incluyendo detalles sobre los sistemas evaluados, las fechas de realización y los hallazgos? * ¿Se realiza la correcta documentación y resguardo de los registros de las pruebas de penetración en la organización?   + ¿Se documentan detalladamente todas las fases de las pruebas de manera completa y precisa los detalles de las pruebas de penetración realizadas, incluyendo el alcance, los métodos utilizados y los resultados obtenidos?   + ¿Los registros se almacenan en un lugar seguro y de acceso restringido, incluyendo pruebas, informes y resultados?   + ¿Se implementa un proceso de revisión y aprobación de los registros de pruebas de penetración antes de su almacenamiento final? * ¿La comunicación de los resultados de las pruebas de penetración logra ser efectiva? ¿Se logra obtener aprendizaje y una mejora continua en base a los resultados?   + ¿Cómo se comunican los resultados de las pruebas de penetración a los responsables y partes interesadas?   + ¿Los informes de resultados de las pruebas de penetración son comprensibles para el personal técnico y no técnico?¿Qué nivel de detalle se proporciona en los informes de vulnerabilidad?   + ¿Se lleva a cabo una revisión posterior a la prueba para aprender lecciones y mejorar los procesos?¿Se documentan las acciones correctivas y las recomendaciones derivadas de las pruebas de penetración? * ¿La organización utiliza de forma continua un portafolio de tecnologías y activos para identificar vulnerabilidades de seguridad en sus sistemas?   + ¿Se ha documentado un plan o programa que establezca la frecuencia y el alcance del uso de estas herramientas?   + ¿Se han definido procedimientos para el manejo de las vulnerabilidades detectadas?   + Evalúe los registros de incidentes pasados para verificar que se siguieron los procedimientos establecidos para el manejo de vulnerabilidades.   + ¿Se realiza seguimiento para verificar la efectividad de las correcciones de vulnerabilidades? |

|  |
| --- |
| Temática: Plan de Evaluación de Control |
| El plan de evaluación de control que se utiliza para evaluar la efectividad de los controles internos en una organización es importante ya que con este es donde se debe comprender cómo se ha diseñado y cómo se está implementando. Con esto se puede asegurar de que se sigan mejores prácticas en la evaluación de los controles internos de una organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿En la organización existen objetivos claros y bien definidos en el plan de evaluación de vulnerabilidades del sistema?   + ¿Existe un proceso de evaluación de riesgos dentro de la organización?     - ¿Se ha realizado una evaluación de riesgos para determinar qué controles deben evaluarse y con qué frecuencia? y ¿Bajo qué pauta se evalúan los riesgos de la organización?   + ¿Los objetivos del plan de evaluación son coherentes con los objetivos de seguridad de la organización?     - Revise el documento para identificar y verificar la existencia de objetivos claramente establecidos, como identificar y remediar vulnerabilidades críticas o mejorar la seguridad del sistema.   + ¿Se ha considerado la criticidad de los sistemas y datos al definir?     - ¿Se incluyen en las evaluaciones de control elementos como seguimiento en profundidad, instrumentación de seguridad, casos de prueba de seguridad automatizados, escaneo de vulnerabilidades, pruebas de usuarios malintencionados, evaluación de amenazas internas, pruebas de rendimiento y carga, y evaluación de fuga o pérdida de datos?     - ¿Los riesgos críticos han sido identificados y se les da prioridad?   + ¿El plan de evaluación de control aborda específicamente los controles y mejoras de control que se están evaluando?¿Incluye información sobre el entorno de evaluación, el equipo de evaluación y los roles y responsabilidades de evaluación?   + ¿Se ha definido el alcance del plan de evaluación de vulnerabilidades de manera adecuada y completa?     - ¿Se ha establecido un cronograma o plazo para la ejecución de las pruebas de vulnerabilidad y la presentación de resultados?     - ¿Se han identificado claramente los tipos de vulnerabilidades que se buscarán durante las pruebas? * ¿Se revisa y aprueba el plan de evaluación de control por parte del funcionario autorizador o el representante designado antes de realizar la evaluación?   + ¿Se evalúan los controles en el sistema y su entorno de operación para determinar si se implementan correctamente y cumplen con los requisitos de seguridad y privacidad?   + ¿Se produce un informe de evaluación de control que documenta los resultados de la evaluación?   + ¿Los resultados de la evaluación de control se proporcionan a un responsable designado por la organización? * ¿Se ha implementado un proceso de gestión de cambios en la organización?   + ¿Se tienen en cuenta los cambios en los procesos y sistemas de la organización al planificar y ejecutar evaluaciones de control?   + ¿Cómo se asegura que los controles se mantengan efectivos después de cambios significativos?   + ¿Se han documentado todos los procesos en la gestión de cambios en la organización?   + ¿Cuál es el alcance de los procesos de gestión de cambios en la organización? * ¿Se ha establecido un proceso para analizar y verificar los informes de vulnerabilidad técnica para determinar las acciones necesarias de respuesta y reparación?   + ¿Existe un registro o sistema de seguimiento que documente las actividades de respuesta y reparación necesarias para abordar las vulnerabilidades técnicas identificadas?   + ¿Se identifican los riesgos asociados con las vulnerabilidades técnicas y se definen acciones específicas para mitigar estos riesgos?   + ¿Las acciones de respuesta y reparación recomendadas se implementan de manera oportuna y eficaz una vez identificada una posible vulnerabilidad técnica? |