

**GASIC 8– Seguridad en el Desarrollo y Adquisición de Software**

**Preguntas de Auditoría**

**Revisión y Evaluación Continua de Vulnerabilidades**

**Competencias Básicas del Auditor**

1. **Conocimiento Profundo en Desarrollo de Software Seguro:** Entender los principios de seguridad en el desarrollo de software, incluyendo buenas prácticas de codificación, diseño seguro, y consideraciones de seguridad en el ciclo de vida del desarrollo.
2. **Experiencia en Identificación de Vulnerabilidades:** Tener habilidades para identificar y evaluar vulnerabilidades en el código y el diseño del software, incluyendo análisis estático y dinámico, pruebas de penetración y revisión de arquitecturas.
3. **Conocimiento en Criptografía y Protección de Datos:** Comprender los principios de la criptografía y cómo se aplica en la protección de datos sensibles dentro del software, incluyendo la gestión segura de claves y la integridad de los datos.
4. **Habilidades en Pruebas de Seguridad y Evaluación de Riesgos:** Ser capaz de realizar pruebas de seguridad exhaustivas para evaluar la resistencia del software frente a posibles ataques, así como evaluar los riesgos asociados con el software.
5. **Conocimientos en Cumplimiento y Normativas:** Estar familiarizado con los requisitos de cumplimiento y normativas relevantes en el ámbito de la seguridad del software, como GDPR, PCI DSS, y normas ISO/IEC.
6. **Capacidad Analítica:** Ser capaz de analizar datos de seguridad y tendencias para identificar posibles amenazas y vulnerabilidades emergentes en el software.
7. **Habilidades de Comunicación Técnica:** Ser capaz de comunicar de manera efectiva los hallazgos de seguridad a los desarrolladores, gerentes y otros interesados, y proponer recomendaciones claras y prácticas.
8. **Conocimientos en Gestión de Incidentes y Respuesta a Incidentes:** Entender los procedimientos y prácticas para la gestión de incidentes de seguridad en el software, incluyendo la capacidad de respuesta rápida y eficaz.

# Visión General

Implica un proceso dinámico y sistemático para identificar, analizar y mitigar posibles debilidades en las aplicaciones y sistemas. Este enfoque proactivo se integra a lo largo de todo el ciclo de vida del software, desde la fase inicial de diseño hasta la operación continua. Incluye actividades como pruebas de seguridad, análisis estático y dinámico del código, así como la utilización de herramientas especializadas para descubrir y evaluar posibles riesgos. La visión general de este proceso busca no solo detectar vulnerabilidades existentes, sino también prever y abordar nuevas amenazas emergentes, garantizando la robustez y seguridad sostenible de los sistemas desarrollados o adquiridos. Además, la revisión constante se alinea con las mejores prácticas de ciberseguridad, permitiendo respuestas rápidas y adaptativas frente a un panorama de amenazas en constante evolución.

A continuación, se presentarán puntos importantes a considerar, explicando un poco mejor a lo que la visión general de este documento se refiere:

**1.1** **Evaluación Continua de Vulnerabilidades:**

La evaluación continua de vulnerabilidades implica la implementación de un proceso dinámico que busca identificar de manera proactiva debilidades en el software a lo largo de su ciclo de vida. Esto incluye actividades como pruebas de seguridad, análisis de código y el uso de herramientas especializadas para detectar posibles riesgos y asegurar una respuesta oportuna a las amenazas existentes.

**1.2** **Integración en el Ciclo de Vida del Software:**

La integración de la evaluación de vulnerabilidades en todo el ciclo de vida del software es esencial. Desde las etapas iniciales de diseño hasta la implementación y operación continua, este enfoque garantiza una cobertura completa, permitiendo la identificación y mitigación temprana de riesgos potenciales.

**1.3** **Pruebas de Seguridad:**

Las pruebas de seguridad constituyen una parte integral de la evaluación continua de vulnerabilidades. Incluyen tanto pruebas estáticas, que examinan el código fuente en busca de posibles fallos, como pruebas dinámicas, que evalúan el comportamiento del software en tiempo de ejecución. Ambos enfoques son esenciales para una evaluación exhaustiva.

**1.4** **Adaptabilidad a Amenazas Emergentes:**

La evaluación continua de vulnerabilidades no solo se centra en amenazas actuales, sino que también se orienta a la anticipación de riesgos emergentes. La adaptabilidad a nuevas amenazas implica estar al tanto de las tendencias de ciberseguridad y ajustar las estrategias de evaluación para abordar proactivamente desafíos en constante evolución.

**1.5** **Respuesta Rápida y Sostenibilidad:**

La visión general de la evaluación continua de vulnerabilidades destaca la importancia de una respuesta rápida y sostenible. Esto implica la identificación ágil de riesgos, la implementación eficiente de medidas correctivas y la adopción de prácticas que aseguren la resistencia a largo plazo frente a amenazas persistentes.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Realizar pruebas para garantizar que la configuración, incluida la configuración predeterminada, funcione como se esperaba. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Verificar que la configuración aprobada esté implementada para el software. 2. Documentar el propósito, opciones, valor predeterminado y más de cada configuración. 3. Utilizar mecanismos técnicos para registrar cómo los administradores pueden implementar y evaluar cada configuración. 4. habilitar las funciones del compilador que generan advertencias sobre código mal protegido durante el proceso de compilación. 5. Implementar el concepto de ""compilación limpia"", donde todas las advertencias del compilador se tratan como errores y se eliminan, excepto aquellas que se consideran falsos positivos o irrelevantes. 6. hacer que las configuraciones de herramientas aprobadas estén disponibles como configuración como código para que los desarrolladores puedan usarlas fácilmente. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Monitorear bases de datos de vulnerabilidades y otras fuentes de informes de vulnerabilidades. 2. Utilizar fuentes de inteligencia sobre amenazas para comprender mejor cómo se explotan las vulnerabilidades. 3. Revisar automáticamente los datos de procedencia y composición del software para identificar nuevas vulnerabilidades. 4. realizar todas las compilaciones en un entorno de compilación dedicado y altamente controlado. 5. habilitar funciones del compilador que aleatorizan u ofuscan las características de ejecución, como el uso de la ubicación de la memoria, que de otro modo serían predecibles y, por lo tanto, potencialmente explotables. 6. Probar para asegurarse de que las funciones funcionen como se esperaba y no causen inadvertidamente problemas operativos u otros problemas. 7. Verificar continuamente que se estén utilizando las configuraciones aprobadas. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Configurar la cadena de herramientas para realizar pruebas y análisis de código automatizados regularmente. |
| 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. Establecer un programa de divulgación de vulnerabilidades y tener un Equipo de Respuesta a Incidentes de Seguridad de Productos (PSIRT). 2. Utilizar el software de seguimiento de problemas para registrar cada vulnerabilidad y realizar cálculos de riesgo para cada una. 3. Tomar decisiones basadas en riesgos sobre la mitigación de vulnerabilidades y publicar avisos de seguridad. 4. Registrar la causa raíz de los problemas descubiertos y las lecciones aprendidas. 5. Agregar mecanismos para detectar automáticamente instancias futuras de problemas identificados. 6. Planificar e implementar cambios en las prácticas apropiadas del SDLC. |

1. **Preguntas de Auditoría para Revisión y Evaluación Continua de Vulnerabilidades**

|  |
| --- |
| Temática: Monitoreo de bases de datos de vulnerabilidades |
| Implica realizar una evaluación exhaustiva de los procesos y sistemas destinados a la detección y gestión de posibles debilidades en las bases de datos. Este proceso abarca la revisión de las metodologías empleadas para la identificación proactiva de vulnerabilidades, la efectividad de las herramientas y técnicas utilizadas, así como la capacidad para gestionar y responder de manera adecuada a las amenazas identificadas. La auditoría se centra en confirmar que las bases de datos críticas para la aplicación estén debidamente protegidas, que se realicen análisis regulares de seguridad y que las actualizaciones de las bases de datos se gestionen de manera segura. Además, se evalúa la capacidad del sistema para mantenerse al día con las actualizaciones de vulnerabilidades y para integrar de manera eficiente estos datos en los procesos de desarrollo y adquisición, asegurando un entorno seguro y resiliente.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo se realiza la identificación proactiva de vulnerabilidades en las bases de datos?   + ¿Qué herramientas y procesos se utilizan para la detección proactiva de vulnerabilidades, incluyendo análisis de código y escaneo de seguridad?   + ¿Se implementa un monitoreo continuo para asegurar la detección temprana de vulnerabilidades?   + ¿Se revisan y actualizan regularmente las técnicas de identificación para mantenerse al día con las nuevas amenazas? * ¿Cuál es la efectividad de las herramientas y técnicas utilizadas en el monitoreo de vulnerabilidades?   + ¿Las herramientas de monitoreo son capaces de identificar con precisión las vulnerabilidades críticas sin generar un alto número de falsos positivos?   + ¿Se realizan pruebas de validación para asegurar que las herramientas utilizadas son efectivas en la identificación de amenazas?   + ¿Las herramientas y técnicas se evalúan y mejoran continuamente en función de los resultados de estas pruebas? * ¿Cómo se gestionan y responden a las amenazas identificadas en las bases de datos?   + ¿Existen protocolos claros para la priorización de vulnerabilidades y la implementación de parches o mitigaciones?   + ¿Se realiza un seguimiento efectivo para asegurar que las medidas de mitigación se implementen adecuadamente? * ¿Qué medidas de seguridad están implementadas para proteger la integridad y confidencialidad de las bases de datos críticas, como cifrado y control de acceso?   + ¿Se realizan auditorías regulares para verificar que las medidas de seguridad están siendo efectivas?   + ¿Las bases de datos críticas son monitoreadas continuamente para detectar intentos de acceso no autorizado o compromisos?   + ¿Los análisis de seguridad cubren todas las posibles vulnerabilidades y se revisan los resultados para identificar áreas de mejora? * ¿Con qué frecuencia se realizan los análisis de seguridad en las bases de datos, y esta frecuencia es adecuada para el entorno de amenazas actual? * ¿Se documentan los resultados de los análisis y se implementan acciones correctivas cuando se identifican debilidades? * ¿Cómo se gestionan las actualizaciones de vulnerabilidades en las bases de datos?   + ¿Existe un proceso documentado para la aplicación de parches y actualizaciones en las bases de datos?   + ¿Se asegura que las actualizaciones se realicen de manera oportuna y sin afectar la disponibilidad del sistema? * ¿Las actualizaciones son evaluadas previamente para evitar que introduzcan nuevas vulnerabilidades o problemas en el sistema? * ¿Cómo se integran los datos de vulnerabilidades en los procesos de desarrollo y adquisición de software?   + ¿Las bases de datos de vulnerabilidades se sincronizan con los procesos de desarrollo y adquisición para asegurar que se consideren en todas las etapas del ciclo de vida del software?   + ¿Los equipos de desarrollo tienen acceso a información actualizada sobre vulnerabilidades para implementar medidas de seguridad adecuadas?   + ¿Se evalúa regularmente la interoperabilidad entre las bases de datos de vulnerabilidades y los procesos de desarrollo para asegurar una integración efectiva? |

|  |
| --- |
| Temática: Utilización de fuentes de inteligencia sobre amenazas |
| Implica llevar a cabo un exhaustivo análisis de cómo la organización recopila, interpreta y aplica información proveniente de diversas fuentes de inteligencia de amenazas. Este proceso abarca la revisión de las fuentes seleccionadas, la calidad de la información recopilada, y la capacidad para traducir esos datos en medidas de seguridad efectivas. La auditoría se centra en evaluar la capacidad de la organización para identificar amenazas emergentes, comprender la relevancia de la inteligencia de amenazas para sus activos específicos y ajustar proactivamente las estrategias de seguridad en consecuencia. Además, se verifica la integración de la inteligencia de amenazas en los procesos de revisión continua, asegurando que la información se utilice de manera eficiente para fortalecer la postura de seguridad y mitigar riesgos potenciales en el desarrollo y adquisición de software.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Qué criterios se utilizan para seleccionar las fuentes de inteligencia sobre amenazas, y cómo se asegura que estas fuentes sean confiables y relevantes?   + ¿Las fuentes elegidas son revisadas y actualizadas regularmente para asegurar su pertinencia en el contexto de la organización?   + ¿Se documenta el proceso de selección y evaluación de las fuentes de inteligencia para garantizar su coherencia y efectividad? * ¿Qué procedimientos se siguen para filtrar y validar la autenticidad de la información proveniente de las fuentes de inteligencia?   + ¿Existen mecanismos para actualizar y corregir la inteligencia de amenazas en caso de que se identifiquen datos incorrectos o irrelevantes? * ¿Cómo se interpreta y traduce la inteligencia de amenazas en medidas de seguridad concretas?   + ¿Se dispone de un proceso estructurado para interpretar la inteligencia de amenazas y traducirla en medidas de seguridad específicas?   + ¿Se pueden proporcionar ejemplos de cómo la organización ha utilizado inteligencia de amenazas para implementar medidas de seguridad concretas?   + ¿Se evalúa regularmente la efectividad de las medidas de seguridad implementadas en respuesta a la inteligencia de amenazas? * ¿Cómo se asegura la relevancia de la inteligencia de amenazas para los activos específicos de la organización?   + ¿La inteligencia de amenazas se adapta y se ajusta al perfil de riesgo específico de la organización y a sus activos críticos?   + ¿Existen procedimientos para revisar y adaptar continuamente la inteligencia de amenazas en función de la naturaleza cambiante de las operaciones de la organización?   + ¿Se asegura que la inteligencia de amenazas se enfoque en los riesgos más relevantes para la organización? * ¿Cómo se ajustan las estrategias de seguridad en respuesta a la inteligencia de amenazas?   + ¿Existen ejemplos de ajustes específicos en las estrategias de seguridad basados en la inteligencia de amenazas reciente?   + ¿La organización demuestra agilidad y capacidad de adaptación en respuesta a cambios en el panorama de amenazas?   + ¿Se revisan y actualizan regularmente las estrategias de seguridad para asegurar que estén alineadas con la inteligencia de amenazas más reciente? * ¿Cómo se integra la inteligencia de amenazas en los procesos de revisión continua de vulnerabilidades?   + ¿La inteligencia de amenazas se incorpora de manera coherente en los procesos de revisión y evaluación continua de vulnerabilidades?   + ¿Se asegura que la información de inteligencia de amenazas informe las decisiones de seguridad y priorización de riesgos?   + ¿Se revisa la efectividad de la integración de la inteligencia de amenazas en los procesos de revisión y ajuste de vulnerabilidades? |