

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

**Preguntas de Auditoría**

**Seguridad del Software**

**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

La seguridad del software en el contexto del desarrollo y adquisición de aplicaciones implica la implementación de medidas y prácticas destinadas a proteger el software contra amenazas, vulnerabilidades y ataques maliciosos a lo largo de su ciclo de vida. Esto incluye el diseño seguro, la codificación resistente a ataques, la implementación de controles de seguridad, pruebas exhaustivas para identificar vulnerabilidades, la gestión adecuada de vulnerabilidades y parches, así como la adquisición de software de fuentes confiables y seguras. La seguridad del software busca garantizar la integridad, confidencialidad y disponibilidad de los sistemas y datos que dependen de él, contribuyendo a un entorno de TI más seguro y confiable.

**1.1 Protección de Datos y Privacidad:**

La protección de datos y la privacidad son fundamentales en la seguridad del software, asegurando que la información confidencial se maneje de manera segura y se cumplan las regulaciones de privacidad. Esto incluye la implementación de controles de acceso, cifrado de datos sensibles y el cumplimiento de normativas como el GDPR.

**1.2 Gestión de Vulnerabilidades y Parches:**

La gestión de vulnerabilidades y parches es esencial para mantener la seguridad del software a lo largo del tiempo. Esto implica la identificación proactiva de vulnerabilidades, la aplicación oportuna de parches de seguridad y la respuesta rápida a nuevas amenazas.

**1.3 Evaluación de Seguridad del Software:**

La evaluación de la seguridad del software es un proceso continuo que implica la realización de pruebas de seguridad, auditorías y revisiones periódicas para identificar posibles debilidades y asegurar que el software cumpla con los estándares de seguridad.

**1.4 Gestión de Incidentes y Respuesta:**

La gestión de incidentes y respuesta es crucial para mitigar y responder rápidamente a cualquier incidente de seguridad que pueda afectar al software. Esto implica la implementación de planes de respuesta a incidentes, la asignación de roles y responsabilidades, y la realización de simulacros de respuesta.

**1.5 Educación y Concienciación en Seguridad:**

La educación y concienciación en seguridad son importantes para involucrar a todos los usuarios y desarrolladores en la importancia de la seguridad del software. Esto incluye la capacitación en buenas prácticas de seguridad, la promoción de una cultura de seguridad y la sensibilización sobre las amenazas actuales.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. |  |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. La formación incluye todos los temas del nivel de madurez 1 y añade herramientas más específicas, técnicas y demostraciones  1.1 La formación es obligatoria para todos los empleados y contratistas.  1.2 La formación incluye aportaciones de las PYME internas y de los alumnos.  1.3 La formación incluye demostraciones de herramientas y técnicas desarrolladas internamente.  1.4 Utiliza los comentarios para mejorar y hacer más relevante la formación futura. 2. Capacitar al equipo de desarrollo (campeones de seguridad, en particular) o colabore con un experto en modelado de riesgos para crear modelos y analizar cómo utilizar un enfoque basado en riesgos para comunicar los riesgos y determinar cómo abordarlos, incluida la implementación de mitigaciones.  2.1 La formación es obligatoria para todos los empleados y contratistas.  2.2 La formación incluye aportaciones de las PYME internas y de los alumnos.  2.3 La formación incluye demostraciones de herramientas y técnicas desarrolladas internamente.  2.4 Utiliza los comentarios para mejorar y hacer más relevante la formación futura. 3. Los responsables de seguridad reciben la formación adecuada  3.1 Los responsables de seguridad informan periódicamente a los equipos de seguridad y desarrollo de aplicaciones sobre el estado general de las iniciativas y correcciones de seguridad.  3.2 El responsable de seguridad revisa los resultados de las pruebas externas antes de añadirlos al aplicaciones pendientes 4. La organización promueve el uso de un único portal entre los diferentes equipos y unidades de negocio  4.1 El portal se utiliza para obtener información puntual, como la notificación de incidentes de seguridad. El portal es ampliamente reconocido por desarrolladores y arquitectos como un repositorio centralizado de la información de seguridad de aplicaciones específica de la organización.  4.2 Todo el contenido se considera persistente y permite búsquedas  4.3 El portal proporciona acceso a métricas de seguridad específicas de la aplicación |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Se utiliza un sistema de gestión del aprendizaje (LMS) para realizar el seguimiento de la formación y las certificaciones.  1.1 La formación se basa en normas, políticas y procedimientos internos  1.2 Se utilizan programas de certificación o registros de asistencia para determinar el acceso a sistemas y recursos de desarrollo |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Mantener uno o más repositorios de software de módulos para admitir funciones y servicios de seguridad estandarizados. 2. Determinar configuraciones seguras para módulos que admitan características y servicios de seguridad estandarizados y hacer que estas configuraciones estén disponibles (por ejemplo, como configuración como código) para que los desarrolladores puedan usarlas fácilmente. 3. Definir criterios para los cuales las características y servicios de seguridad deben ser respaldados por el software que se desarrollará. 4. Mantener registros de todos los estudiantes que completen con éxito cada curso de formación u otras actividades de formación autorizadas, así como de aquellos que han fracasado. 5. Mantener registros de todo el personal que ha sido eximido de la formación. 6. Mantener los registros de todos los estudiantes que completen con éxito su formación requerida. 7. Poner los registros de formación a disposición del personal apropiado para su consideración en las asignaciones |
| 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. Evaluar los proyectos terminados o en curso para determinar si el conocimiento del personal es adecuado para realizar las tareas del proyecto. 2. Proporcionar un mecanismo para evaluar la eficacia de cada curso de formación, con respecto a los objetivos de aprendizaje establecidos (o rendimiento) individual, del proyecto o de la organización. 3. Obtener evaluaciones de los estudiantes sobre cómo las actividades de formación han satisfecho sus necesidades. |

1. **Preguntas de Auditoría para Protección del Código y Software**

|  |
| --- |
| Temática: Capacitación al equipo de desarrollo |
| Esto implica revisar y evaluar el programa de formación y sensibilización en seguridad que se proporciona a los desarrolladores. Esto incluye verificar la cobertura de temas relevantes, como las mejores prácticas de codificación segura, el manejo de datos sensibles, el uso seguro de herramientas y bibliotecas, y la comprensión de las amenazas y vulnerabilidades comunes en el desarrollo de software. La auditoría también evaluará la efectividad de la capacitación en la implementación práctica de medidas de seguridad en el código y en el cumplimiento de estándares de seguridad, así como la concienciación del equipo sobre la importancia de la seguridad en el ciclo  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cuáles son los temas cubiertos en el programa de capacitación en seguridad del software?   + ¿El contenido del programa de capacitación incluye aspectos clave de seguridad del software, como desarrollo seguro, manejo de vulnerabilidades y protección de datos?   + ¿Se comparan los temas del programa con las mejores prácticas y estándares de seguridad reconocidos, como OWASP y NIST?   + ¿Se revisa y actualiza periódicamente el contenido para incluir las amenazas y técnicas más recientes? * ¿Cómo se adapta la capacitación a las necesidades específicas del equipo y del proyecto?   + ¿Se realizan encuestas de habilidades o análisis de riesgos para identificar las necesidades específicas de capacitación del equipo?   + ¿El programa de capacitación se personaliza para abordar los desafíos particulares del proyecto en curso?   + ¿Se realizan ajustes en la capacitación basados en los resultados de las evaluaciones de desempeño del equipo? * ¿Cómo se imparte la capacitación? ¿Qué métodos y recursos se utilizan?   + ¿Se utilizan métodos de enseñanza variados, como talleres prácticos, módulos en línea y sesiones presenciales, para adaptarse a diferentes estilos de aprendizaje?   + ¿Los materiales didácticos son accesibles y efectivos, y fomentan la participación activa de los participantes?   + ¿La interacción entre los formadores y los participantes es dinámica y facilita la comprensión de los conceptos de seguridad? * ¿Cómo se evalúa la efectividad de la capacitación en seguridad del software?   + ¿Se aplican pruebas de conocimientos al finalizar la capacitación para medir la comprensión de los temas por parte de los participantes?   + ¿Existe un seguimiento para verificar cómo los conocimientos adquiridos se aplican en proyectos reales?   + ¿Se recogen y analizan feedbacks de los participantes para mejorar continuamente el programa de capacitación? * ¿Cómo se fomenta la participación y el compromiso del equipo con la capacitación en seguridad del software?   + ¿Se implementan iniciativas de motivación, como reconocimientos o incentivos, para fomentar la participación activa en la capacitación?   + ¿Los miembros del equipo perciben la capacitación como relevante y valiosa para su trabajo diario?   + ¿Se realizan entrevistas o encuestas para entender mejor las opiniones del equipo sobre la capacitación y ajustar el programa en consecuencia? * ¿Cómo se asegura la continuidad y actualización de la capacitación en seguridad del software?   + ¿Existen planes a largo plazo para ofrecer sesiones de capacitación recurrentes y mantener al equipo actualizado sobre las últimas tendencias en seguridad?   + ¿El programa de capacitación se revisa regularmente para incluir nuevos temas y amenazas emergentes en el ámbito de la seguridad del software?   + ¿Se integra un proceso de mejora continua en el programa para asegurar que la capacitación evolucione junto con los cambios en el entorno de desarrollo y seguridad? |

|  |
| --- |
| Temática: Uso de un único portal entre los diferentes equipos y unidades de negocio |
| Esto implica revisar cómo se implementa y utiliza esta plataforma compartida. Esto incluye evaluar la integración de herramientas y recursos de seguridad, como la gestión de vulnerabilidades, pruebas de seguridad, y la gestión de incidentes, en un único portal. La auditoría se enfoca en garantizar que el portal facilite la colaboración efectiva entre los equipos, promueva la transparencia en la gestión de la seguridad del software, y permita una visión global de la postura de seguridad en toda la organización. Además, se evalúa si el portal cumple con los requisitos de seguridad, como la protección de datos sensibles y el cumplimiento de normativas, y si se proporciona la capacitación adecuada para su uso eficiente por parte de los equipos y unidades de negocio.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Qué herramientas y recursos de seguridad se integran en el portal único?   + ¿La lista de herramientas y recursos disponibles en el portal cubre todas las funcionalidades necesarias para la seguridad del software?   + ¿Las herramientas integradas están bien conectadas con otros sistemas y procesos de la organización?   + ¿Se realizan evaluaciones regulares para asegurar que las herramientas siguen siendo adecuadas y actualizadas? * ¿Cómo se gestiona el acceso y los permisos dentro del portal único?   + ¿Existen controles de acceso robustos que aseguran que solo usuarios autorizados pueden acceder a información sensible?   + ¿Los roles y permisos asignados a los usuarios son revisados y actualizados regularmente para reflejar cambios en las responsabilidades?   + ¿Las políticas de seguridad relacionadas con la gestión de identidades son claras y seguidas estrictamente? * ¿Cómo se promueve la colaboración y la comunicación entre los equipos a través del portal único?   + ¿El portal incluye funciones de colaboración, como herramientas para compartir información y comunicación en tiempo real entre equipos?   + ¿Los usuarios encuentran que estas funciones facilitan la colaboración efectiva?   + ¿Se recogen y analizan las opiniones de los usuarios para mejorar la experiencia de colaboración a través del portal? * ¿Cómo se asegura la disponibilidad y el rendimiento del portal único?   + ¿Existen acuerdos de nivel de servicio (SLA) que definan claramente las expectativas de disponibilidad y rendimiento del portal?   + ¿Se implementan medidas de monitoreo continuo para asegurar que el portal funcione de manera óptima?   + ¿Se revisan y actualizan los SLA y las medidas de monitoreo según sea necesario para mejorar la confiabilidad del portal? * ¿Cómo se garantiza la seguridad de los datos almacenados y procesados en el portal único?   + ¿Se han implementado medidas de seguridad, como el cifrado de datos y la gestión de claves, para proteger la información almacenada en el portal?   + ¿Las políticas de retención de datos son claras y se cumplen estrictamente?   + ¿Se realizan pruebas de vulnerabilidad y auditorías regulares para identificar y corregir posibles fallos de seguridad? * ¿Cómo se mide la efectividad y el impacto del portal único en la seguridad del software?   + ¿Se utilizan métricas de rendimiento para evaluar la adopción del portal por parte de los usuarios y su impacto en la seguridad del software?   + ¿El portal ha contribuido a una mejor detección de amenazas y a la reducción de incidentes de seguridad?   + ¿Se identifican y aplican mejoras continuas en el portal basado en las métricas de rendimiento y retroalimentación de los usuarios? |

|  |
| --- |
| Temática: Utilización de un sistema de gestión del aprendizaje (LMS) |
| Esto implica revisar cómo se implementa y utiliza esta plataforma educativa en el contexto de la seguridad del software. Esto incluye evaluar la calidad y relevancia de los cursos y materiales de formación ofrecidos, así como la efectividad del LMS para impartir conocimientos sobre las mejores prácticas de seguridad, el cumplimiento de normativas y estándares, y la gestión de riesgos en el desarrollo de software. La auditoría también se enfoca en la participación y el compromiso de los usuarios con el LMS, la efectividad de las evaluaciones y seguimientos del progreso, y la alineación del contenido con las necesidades específicas de seguridad del software de la organización. Además, se verifica la seguridad del LMS en cuanto a la gestión de accesos, la protección de datos y la disponibilidad del sistema.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Qué cursos y materiales de formación relacionados con la seguridad del software están disponibles en el LMS?   + ¿El catálogo de cursos y materiales cubre todas las áreas clave de la seguridad del software necesarias para la organización?   + ¿Los cursos disponibles se alinean con las necesidades de formación identificadas por la organización?   + ¿Se revisa y actualiza regularmente el catálogo de cursos para mantener su relevancia? * ¿Cómo se adapta el contenido del LMS a las necesidades y roles específicos relacionados con la seguridad del software en la organización?   + ¿El contenido del LMS se personaliza para diferentes roles, como desarrolladores, analistas de seguridad y gerentes de proyecto?   + ¿Se han realizado entrevistas o encuestas para evaluar la relevancia y utilidad del contenido para las funciones específicas de los usuarios?   + ¿Se ajusta el contenido en función del feedback recibido para asegurar su pertinencia y efectividad? * ¿Cómo se mide la efectividad de la formación en seguridad del software a través del LMS?   + ¿Se utilizan métricas de rendimiento, como los resultados de exámenes y la finalización de cursos, para evaluar la efectividad de la formación?   + ¿Se recogen encuestas de satisfacción y retroalimentación de los usuarios sobre la utilidad de los cursos?   + ¿Se realizan análisis periódicos para identificar áreas de mejora en la formación? * ¿Cómo se promueve y fomenta la participación y el compromiso de los usuarios con la formación en seguridad del software a través del LMS?   + ¿Se implementan incentivos o reconocimientos para motivar a los usuarios a participar activamente en los cursos?   + ¿Se integran los cursos de seguridad del software en los objetivos de desarrollo personal de los empleados?   + ¿Se monitorea la participación y se ajustan las estrategias de motivación según sea necesario para mejorar el compromiso? * ¿Cómo se asegura la disponibilidad, confidencialidad e integridad de los datos de los usuarios en el LMS?   + ¿Se utilizan métodos de autenticación robustos para proteger el acceso a los datos del LMS?   + ¿Los datos de los usuarios están cifrados y protegidos por políticas de privacidad estrictas?   + ¿Se auditan regularmente las políticas y medidas de seguridad para asegurar que se mantienen efectivas? * ¿Cómo se garantiza la actualización y relevancia continua del contenido de seguridad del software en el LMS?   + ¿El contenido del LMS se revisa periódicamente por expertos en seguridad del software para asegurar su relevancia?   + ¿Se integran las últimas tendencias y mejores prácticas de seguridad en el contenido disponible?   + ¿Existen procesos claros para la actualización continua del contenido en respuesta a cambios en el entorno de seguridad? |