

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

**Preguntas de Auditoría**

**Definición del Proceso**

**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 definición de procesos en el desarrollo de software es una práctica que asegura la claridad y consistencia en las actividades que componen un proyecto, integrando objetivos de seguridad desde su inicio. Desde el punto de vista de un auditor, la documentación y el seguimiento detallado de estos procesos son esenciales para evaluar su efectividad, identificar riesgos y garantizar que las acciones ejecutadas cumplan con los estándares de seguridad establecidos por la organización.

**1.1 Planificación y Documentación del Proceso**

El proceso debe comenzar con un plan documentado que defina objetivos, actividades clave y recursos asignados. Este plan debe ser revisado por las partes interesadas relevantes, incorporando ajustes según sea necesario para reflejar las realidades operativas. Desde la perspectiva de un auditor, la revisión del plan permite verificar su alineación con los objetivos organizacionales y su capacidad para abordar riesgos potenciales. Además, la descripción formal del proceso debe ser evaluada para asegurar que incluya mecanismos de control y seguimiento que permitan una ejecución medible y auditable.

**1.2 Participación de las Partes Interesadas**

Un proceso efectivo requiere la identificación y participación activa de las partes interesadas, quienes deben ser informadas sobre sus roles y responsabilidades en el desarrollo del software. Desde el punto de vista de la auditoría, el registro de estas interacciones y la evidencia de su participación en momentos clave del proceso son elementos críticos para evaluar si la comunicación y el involucramiento han sido adecuados y efectivos en el cumplimiento de los objetivos de seguridad.

**1.3 Monitoreo y Evaluación de Resultados**

La evaluación del desempeño del proceso en relación con el plan es una actividad continua que permite identificar desviaciones significativas y problemas en su ejecución. Para el auditor, es esencial revisar los logros y los resultados frente a los objetivos documentados, así como analizar las acciones correctivas tomadas para resolver problemas detectados. Además, la evidencia de cierre adecuado de dichas acciones proporciona garantías sobre la capacidad de la organización para gestionar problemas de manera efectiva.

**1.4 Adaptación y Ajustes del Proceso**

El proceso definido debe adaptarse a las necesidades específicas del proyecto, partiendo de los estándares organizacionales. Para un auditor, es clave evaluar cómo estos ajustes se han documentado y si las modificaciones responden a las guías de adaptación establecidas. Asimismo, la revisión de los registros asegura que las lecciones aprendidas y las mejoras se integren en el proceso, fomentando su evolución para futuros proyectos.

**1.5 Gestión de Medidas y Activos del Proceso**

La recopilación y almacenamiento de métricas relacionadas con el proceso y los productos generados es un aspecto que un auditor revisa para evaluar la madurez y efectividad de la organización. El acceso centralizado a estas métricas, junto con la documentación de lecciones aprendidas, proporciona una base sólida para proponer mejoras en los activos del proceso y garantizar su alineación con los objetivos de seguridad. Estas prácticas aseguran que el desarrollo de software sea auditable, repetible y alineado con los estándares establecidos.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Definir y documentar el plan para realizar el proceso. 2. Definir y documentar la descripción del proceso. 3. Revisar el plan con las partes interesadas relevantes y obtener su acuerdo.  3.1 Modificar el plan según sea necesario. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Identificar a las partes interesadas relevantes a este proceso y la involucración apropiada. 2. Comunicar las partes interesadas relevantes identificadas a las personas que planifican el proyecto y otros planes, según proceda. 3. Involucrar a las partes interesadas relevantes según lo planificado. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Evaluar el progreso y el rendimiento reales frente al plan de realización del proceso. 2. Revisar los logros y los resultados del proceso frente al plan de realización del proceso. 3. Revisar las actividades, el estado y los resultados del proceso con el nivel de gerencia más cercano al responsable del proceso e identificar las cuestiones. 4. Identificar y evaluar los efectos de las desviaciones significativas del plan de realización del proceso. 5. Identificar los problemas en el plan de realización del proceso y en la ejecución del proceso. 6. Tomar acciones correctivas cuando no se satisfacen los requisitos y los objetivos, cuando se identifican las cuestiones o cuando el progreso difiere significativamente del plan de realización del proceso. 7. Seguir las acciones correctivas hasta su cierre. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Seleccionar del conjunto de procesos estándar de la organización aquellos procesos que cubran el área de proceso y que mejor satisfagan las necesidades del proyecto o función de la organización. 2. Establecer el proceso definido adaptando los procesos seleccionados de acuerdo con las guías de adaptación de la organización. 3. Asegurar que los objetivos del proceso de la organización se tratan de forma apropiada en el proceso definido. 4. Documentar el proceso definido y los registros de la adaptación. 5. Modificar la descripción del proceso definido según sea necesario. |
| 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. Almacenar medidas del proceso y del producto en el repositorio de mediciones de la organización. 2. Remitir la documentación para su inclusión en la biblioteca de activos de proceso de la organización. 3. Documentar las lecciones aprendidas del proceso para su inclusión en la biblioteca de activos de proceso de la organización. 4. Proponer mejoras a los activos de proceso de la organización. |

1. **Preguntas de Auditoría para la Definición del Proceso**

|  |
| --- |
| Temática: Definición y documentación del Proceso |
| La evaluación de la definición del proceso en Seguridad en el Desarrollo y Adquisición de Software es un componente esencial para asegurar la efectividad y la solidez de las prácticas de seguridad implementadas en la implementación, el desarrollo y la evaluación del software. Este proceso se enfoca en examinar y validar la claridad, coherencia y cumplimiento de los procedimientos y políticas de seguridad establecidos en una organización, asegurando que estén alineados con estándares reconocidos y las mejores prácticas del sector. La importancia de esta auditoría radica en su capacidad para identificar posibles brechas o deficiencias en la definición del proceso, lo que podría generar un mal uso e instalación de un software el cual no cumpla los parámetros de seguridad o resulta del todo eficiente para las actividades que quiera realizar la empresa con este.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe un plan documentado para llevar a cabo el proceso de seguridad en el desarrollo y adquisición de software?   + ¿El plan establece claramente los objetivos, alcance y actividades del proceso?   + ¿Se ha asignado responsabilidad para la ejecución del plan?   + ¿El plan incluye un cronograma y recursos necesarios para la implementación efectiva del proceso? * ¿Existe una descripción detallada del proceso de seguridad en el desarrollo y adquisición de software?   + ¿La descripción del proceso abarca todas las fases, desde el diseño hasta la implementación y el mantenimiento?   + ¿Se han identificado y documentado los controles de seguridad específicos incorporados en cada fase del desarrollo de software?   + ¿La descripción del proceso incluye pautas claras para la gestión de riesgos y la respuesta a incidentes de seguridad? * ¿Se ha llevado a cabo una revisión del plan con las partes interesadas relevantes?   + ¿Se ha obtenido el acuerdo de las partes interesadas respecto al plan?   + ¿Existe un registro documentado de la revisión y el acuerdo de las partes interesadas?   + ¿Hay un proceso establecido para modificar el plan según sea necesario?   + ¿Se han documentado los cambios realizados en el plan después de la revisión?   + ¿Se asegura de que todas las partes interesadas relevantes estén informadas sobre las modificaciones realizadas en el plan? * ¿Se ha llevado a cabo una identificación exhaustiva de todas las partes interesadas relacionadas con el proceso de Seguridad en el Desarrollo y Adquisición de Software?   + ¿Se han considerado tanto las partes internas como externas que puedan tener impacto o ser impactadas por las prácticas de seguridad?   + ¿Existe un proceso establecido para evaluar la relevancia y nivel de influencia de cada parte interesada en el contexto de la seguridad del software?   + ¿Se ha documentado y comunicado claramente a las partes interesadas relevantes la planificación y ejecución del proceso de seguridad en el desarrollo y adquisición de software?   + ¿Existe un método efectivo para la comunicación bidireccional con las partes interesadas, permitiendo la retroalimentación y la actualización de información relevante?   + ¿Se informa de manera regular y oportuna a las partes interesadas sobre cambios en los procedimientos, políticas o enfoques de seguridad?   + ¿Se ha desarrollado un plan detallado que describa cómo y cuándo se involucrará a cada parte interesada relevante en el proceso de seguridad?   + ¿Existe evidencia de que las partes interesadas pertinentes están participando activamente según lo planificado en la definición y ejecución del proceso de seguridad?   + ¿Hay un sistema para evaluar la satisfacción y la percepción de valor por parte de las partes interesadas respecto a su participación en el proceso de seguridad? * ¿Se realiza una evaluación periódica del progreso real del proceso de Seguridad en el Desarrollo y Adquisición de Software en comparación con el plan establecido?   + ¿Existen métricas definidas y utilizadas para medir el rendimiento del proceso en términos de eficacia y eficiencia?   + ¿Se documentan y comunican claramente los resultados de la evaluación del progreso a todas las partes interesadas relevantes?   + ¿Se realiza una revisión detallada de los logros y resultados obtenidos en relación con los objetivos establecidos en el plan de realización del proceso?   + ¿Se identifican y evalúan las desviaciones significativas entre el progreso real y el plan de realización del proceso?     - ¿Se establecen umbrales claros para determinar qué desviaciones se consideran significativas?     - ¿Se documentan las acciones tomadas en respuesta a desviaciones significativas y se comunican a las partes interesadas pertinentes? * ¿Se lleva a cabo una revisión regular para identificar problemas tanto en el plan de realización del proceso como en la ejecución del proceso?   + ¿Existen mecanismos para documentar y abordar los problemas identificados de manera proactiva?   + ¿Se ajusta el plan de realización del proceso según sea necesario para abordar los problemas detectados durante la ejecución? * ¿Se realiza una evaluación exhaustiva para seleccionar procesos estándar que aborden de manera efectiva las necesidades específicas de seguridad en el desarrollo y adquisición de software?   + ¿Se documentan las razones para la selección de procesos específicos y cómo satisfacen las necesidades particulares?   + ¿Existe un mecanismo formal para ajustar y personalizar los procesos estándar de acuerdo con las características únicas de la organización?   + ¿Se documentan las modificaciones realizadas durante el proceso de adaptación y se asegura de que estén alineadas con las prácticas y estándares de seguridad?   + ¿Se garantiza que los objetivos específicos del proceso de seguridad en el desarrollo y adquisición de software se aborden de manera adecuada en el proceso definido? * ¿Existe un proceso para revisar y alinear continuamente los objetivos del proceso con las necesidades cambiantes de la organización?   + ¿Se asegura de que las adaptaciones realizadas no comprometan la integridad y efectividad del proceso?   + ¿Se documenta de manera clara y detallada el proceso definido y los registros de todas las adaptaciones realizadas?   + ¿Los documentos son accesibles para todas las partes interesadas relevantes y se mantienen actualizados?   + ¿Se documentan y comunican las modificaciones de manera efectiva a todas las partes interesadas?   + ¿Existe un mecanismo para evaluar el impacto de las modificaciones en los resultados y objetivos del proceso? * ¿Se sigue un procedimiento definido para almacenar medidas del proceso y del producto en el repositorio de mediciones de la organización?   + ¿Se asegura la integridad y confidencialidad de las medidas almacenadas en el repositorio?   + ¿Existen controles para garantizar la precisión y actualización constante de las medidas almacenadas?   + ¿Se documenta y remite la información pertinente para su inclusión en la biblioteca de activos de proceso de la organización?   + ¿Se comprueba la calidad y relevancia de la documentación antes de su inclusión en la biblioteca?   + ¿Existe una revisión regular de los documentos almacenados para garantizar su actualización y pertinencia?   + ¿Se documentan de manera sistemática y detallada las lecciones aprendidas durante el proceso? * ¿El equipo responsable del proceso propone mejoras identificadas durante la ejecución del proceso?   + ¿Se documentan y explican las razones detrás de cada propuesta de mejora?   + ¿Existe un mecanismo para evaluar y priorizar las propuestas de mejora antes de su implementación?   + ¿Las mejoras implementadas se documentan y se incorporan de manera efectiva a los activos de proceso de la organización? |