

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

**Preguntas de Auditoría**

**Implementación de Entornos Seguros**

**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 la adopción de medidas integrales para salvaguardar la integridad, confidencialidad y disponibilidad de los sistemas. Este proceso abarca desde la fase inicial de diseño hasta la adquisición de soluciones externas, asegurando la incorporación de prácticas de desarrollo seguro, pruebas exhaustivas de seguridad y la aplicación de controles adecuados en la infraestructura tecnológica. Se requiere una evaluación constante de las amenazas cibernéticas y la actualización de las políticas de seguridad para mantener la resiliencia del entorno. Además, la colaboración entre equipos de desarrollo, auditoría especializada y la conformidad con estándares y regulaciones son aspectos cruciales para garantizar la eficacia y sostenibilidad de entornos seguros en el ciclo completo de vida del software.

**1.1 Desarrollo Seguro de Software:**

La implementación de entornos seguros en el desarrollo de software inicia con la integración de prácticas de desarrollo seguro. Esto implica la aplicación de metodologías y buenas prácticas que aborden las vulnerabilidades desde las primeras etapas del ciclo de vida del software, asegurando la creación de aplicaciones resistentes a amenazas cibernéticas.

**1.2 Evaluación Continua de Amenazas Cibernéticas:**

La visión general también incluye la necesidad de una evaluación constante de las amenazas cibernéticas. Esto implica monitorear y analizar las tendencias de seguridad, adaptando proactivamente las defensas para hacer frente a las amenazas emergentes y mantener la seguridad del entorno de desarrollo y adquisición.

**1.3 Colaboración Interdisciplinaria:**

La implementación exitosa de entornos seguros requiere una colaboración efectiva entre equipos de desarrollo, operaciones, auditoría y seguridad. Esta sinergia asegura la alineación de objetivos, la comunicación eficiente y la aplicación coherente de medidas de seguridad en todo el ciclo de vida del software.

**1.4 Cumplimiento con Estándares y Regulaciones:**

La conformidad con estándares y regulaciones de seguridad es esencial para garantizar la adopción de mejores prácticas y la mitigación de riesgos legales y regulatorios. Asegurarse de que el entorno cumpla con normativas específicas contribuye a robustecer la postura de seguridad global.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Utilizar autenticación multifactor basada en riesgos y acceso condicional para cada entorno. 2. Utilizar segmentación de red y controles de acceso para separar entornos y componentes para reducir riesgos y privilegios de atacantes. 3. Hacer cumplir la autenticación y restringir estrictamente las conexiones que entran y salen de cada entorno de desarrollo de software. 4. Minimizar el acceso humano directo a sistemas de la cadena de herramientas y monitorear intentos de acceso y uso privilegiado. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Configurar cada punto final de desarrollo según guías aprobadas, como el cifrado de datos confidenciales y la mínima funcionalidad necesaria.  2. Supervisar continuamente la seguridad de los puntos finales de desarrollo, incluyendo el seguimiento de todo uso de acceso privilegiado.  3. Requerir autenticación multifactor para todos los accesos a puntos finales de desarrollo y recursos. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Minimizar el uso de software y servicios del entorno de producción desde entornos que no son de producción. 2. Registrar, monitorear y auditar periódicamente las relaciones de confianza para autorización y acceso entre entornos y componentes. 3. Monitorear continuamente el software implementado en cada entorno para detectar nuevas vulnerabilidades y responder adecuadamente. 4. Configurar medidas para asegurar las infraestructuras de alojamiento de los entornos siguiendo una arquitectura de confianza cero. 5. Proporcionar puntos finales de desarrollo dedicados en redes que no sean de producción y configurar cada punto final siguiendo una arquitectura de confianza cero. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles |  |
| 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. **Preguntas de Auditoría para Implementación de Entornos Seguros**

|  |
| --- |
| Temática: Autenticación Multifactor |
| Implica un análisis exhaustivo de los mecanismos de autenticación implementados para garantizar un nivel adecuado de protección de acceso. Este proceso incluye la revisión detallada de las políticas y controles de autenticación multifactor, evaluando su efectividad para mitigar riesgos asociados con accesos no autorizados. La auditoría se centra en verificar la implementación adecuada de factores de autenticación adicionales, como códigos temporales, tokens o biometría, y en asegurar que se integren de manera coherente en el flujo de trabajo del software en desarrollo. Además, se busca confirmar la adaptabilidad de los mecanismos de autenticación multifactor a las mejores prácticas de seguridad y a las regulaciones específicas, garantizando la resistencia del sistema ante posibles amenazas de compromiso de credenciales.  Este levantamiento puede incluir análisis específicos tales como:   * **¿**Cómo se configuran y gestionan los factores de autenticación adicionales en el sistema?   + ¿Se han definido claramente los requisitos de seguridad para la configuración de factores de autenticación?   + ¿Se revisan regularmente las configuraciones para asegurar que se mantienen actualizadas y efectivas?   + ¿Existen procedimientos documentados para la gestión de factores de autenticación, incluyendo la adición, eliminación y actualización de estos? * ¿Cómo se realiza la integración de la autenticación multifactor en el flujo de trabajo del software en desarrollo?   + ¿Se ha asegurado que la autenticación multifactor no interfiere con la experiencia del usuario?   + ¿Está la autenticación multifactor implementada en todos los puntos críticos del flujo de trabajo?   + ¿Se han realizado pruebas de integración para verificar que la autenticación multifactor funciona correctamente en todos los escenarios del software? * ¿Cómo se verifica la adaptabilidad de los mecanismos de autenticación multifactor a las mejores prácticas de seguridad?   + ¿Se comparan regularmente los mecanismos de autenticación multifactor con los estándares de la industria y las mejores prácticas?   + ¿Se actualizan los mecanismos de autenticación multifactor para abordar nuevas amenazas y vulnerabilidades?   + ¿Existe un proceso de revisión para adaptar los mecanismos de autenticación a los cambios en el entorno de amenazas? * ¿Cómo se realizan pruebas de robustez y resistencia de la autenticación multifactor?   + ¿Se llevan a cabo pruebas de carga para verificar la capacidad del sistema de manejar grandes volúmenes de autenticaciones?   + ¿Se realizan simulaciones de ataques para evaluar la resistencia de los mecanismos de autenticación multifactor?   + ¿Los resultados de las pruebas se utilizan para mejorar la robustez del sistema? * ¿Cómo se gestiona el ciclo de vida de los dispositivos y tokens utilizados en la autenticación multifactor?   + ¿Existen procedimientos claros para la emisión, mantenimiento y revocación de dispositivos y tokens?   + ¿Se realiza un seguimiento de todos los dispositivos y tokens activos para asegurar su correcta gestión?   + ¿Se implementan medidas de seguridad para garantizar que los dispositivos y tokens retirados no puedan ser reutilizados de manera no autorizada? |

|  |
| --- |
| Temática: Segmentación de Red |
| Implica realizar una evaluación detallada de la arquitectura de red para garantizar la implementación efectiva de medidas de segmentación. Este proceso abarca la revisión de la configuración de firewalls, switches y routers para confirmar que se establezcan zonas seguras, restringiendo el tráfico entre diferentes segmentos de la red. La auditoría se enfoca en verificar que la segmentación se haya diseñado de manera coherente con los requisitos de seguridad y las políticas de acceso, asegurando que la comunicación entre sistemas y servicios esté limitada según los principios de menor privilegio. Además, se evalúa la resistencia a posibles ataques de lateralidad, asegurando que la segmentación de la red contribuya eficazmente a la mitigación de riesgos y a la protección de activos críticos durante el desarrollo y la adquisición de software.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo se configuran y gestionan los firewalls para implementar la segmentación de red?   + ¿Se han establecido reglas de filtrado específicas que restrinjan el tráfico entre segmentos de red?   + ¿Se revisan regularmente las configuraciones de los firewalls para asegurar que cumplen con las políticas de seguridad establecidas?   + ¿Existen procedimientos documentados para la actualización y gestión de las reglas de los firewalls? * ¿Cómo se aplican los principios de menor privilegio en la segmentación de la red?   + ¿Se limita la comunicación entre segmentos de red únicamente al tráfico necesario?   + ¿Las excepciones a las reglas de acceso siguen un proceso formal de revisión y aprobación?   + ¿Se auditan regularmente las políticas de acceso para asegurar que se mantenga el principio de menor privilegio? * ¿Cómo se gestionan las políticas de segmentación en switches y routers?   + ¿Las configuraciones de switches y routers están alineadas con las políticas de segmentación de la red?   + ¿Se han implementado controles para evitar configuraciones que puedan comprometer la seguridad de la segmentación?   + ¿Existen procedimientos para revisar y actualizar las políticas de segmentación en estos dispositivos de red? * ¿Cómo se garantiza la resistencia ante posibles ataques de lateralidad en la red segmentada?   + ¿Se realizan pruebas de seguridad, como simulaciones de ataques de lateralidad, para evaluar la efectividad de la segmentación?   + ¿Las medidas de segmentación incluyen controles específicos para contener movimientos laterales en caso de un compromiso de seguridad?   + ¿Se revisan y actualizan regularmente las estrategias de segmentación para mejorar la resistencia a ataques de lateralidad? * ¿Cómo se documenta y gestiona la topología de red y la segmentación implementada?   + ¿La documentación de la red, incluyendo diagramas y políticas de segmentación, está actualizada y refleja con precisión la configuración real?   + ¿Existen procesos establecidos para mantener la documentación al día, especialmente después de cambios significativos en la red?   + ¿Se revisa la documentación durante las auditorías para asegurar que sea precisa y útil para la gestión de la red? |