

Plan de Auditoría de Seguridad en TI para el Área de Desarrollo de Software

Introducción

La auditoría de seguridad en TI tiene como objetivo evaluar y mejorar las medidas de seguridad implementadas en el área de desarrollo de software, asegurando la protección de los datos y el cumplimiento de las políticas de seguridad. Este plan de auditoría se enfoca en revisar el control de acceso, la protección de datos, la gestión de vulnerabilidades y la adherencia a las políticas de desarrollo seguro, considerando las diferentes jerarquías y roles dentro del equipo de trabajo.

Detalles de la Auditoría

Entidad Auditada	INNOVAHTEC SOLUTIONS
Dirección	Alfonso Ugarte #651
Responsable	Miguel Vilcherrez
Auditor(es)	Brayan Rojas Freyre
DNI del Auditor	74473887
Email del Auditor	rfreyrebrayaned@gmail.com
Teléfono del Auditor	998511769
Fecha del Informe	05/07/2024
Motivo de la Auditoría	Evaluar y fortalecer los controles de seguridad de TI para proteger activos críticos y datos sensibles en el entorno de desarrollo.

Resumen Auditoria

Número Total de Controles Auditados	14
Número de Controles Cumplidos	12
Número de Controles No Cumplidos	2
Porcentaje de Cumplimiento	85.71%

Auditoría General

Código	Área de Seguridad	Descripción del Control	Estado	Evidencia	Observaciones
DS-001	Desarrollo Seguro	Adherencia a la política de desarrollo seguro	No Cumple	Sin evidencia	
SED-001	Seguridad en el Entorno de Desarrollo	Separación de entornos de desarrollo y producción	Cumple	Sin evidencia	
CA-003	Control de Acceso	Repositorios y Proyectos	Cumple	Sin evidencia	
CA-004	Protección de Datos	Protección de Proyectos y Repositorios	Cumple	Sin evidencia	
SA-008	Seguridad de Aplicaciones	Este control garantiza que se realicen pruebas exhaustivas de seguridad, como pruebas de penetración y análisis estático de código, para identificar y mitigar vulnerabilidades antes de que las aplicaciones sean desplegadas en un entorno operativo.	Cumple	Sin evidencia	
SA-009	Seguridad de Aplicaciones	Este control asegura que las API sean desarrolladas y configuradas con medidas de seguridad adecuadas, protegiendo contra accesos no autorizados y asegurando la integridad y disponibilidad de los datos intercambiados.	Cumple	Sin evidencia	
GI-011	Gestión de Incidentes	Este control establece la documentación adecuada y la generación de reportes detallados sobre los incidentes de seguridad ocurridos en el entorno de desarrollo, facilitando la revisión y mejora continua de las medidas de seguridad implementadas.	Cumple	Sin evidencia	

DS-014	Desarrollo Seguro	Este control asegura que el personal de desarrollo reciba formación continua sobre buenas prácticas de seguridad, promoviendo una cultura de desarrollo seguro dentro de la organización.	Cumple	Sin evidencia	
GV-016	Gestión de Vulnerabilidades	Este control establece procesos para asegurar una comunicación efectiva y colaboración entre equipos, facilitando la identificación y resolución rápida de vulnerabilidades críticas en el entorno de desarrollo.	Cumple	Sin evidencia	
PD-018	Protección de Datos	Este control asegura que se implementen y mantengan medidas de cifrado robustas para proteger datos sensibles contra acceso no autorizado y cumplir con regulaciones de protección de datos aplicables.	No Cumple	Sin evidencia	
PD-020	Protección de Datos	Este control asegura que se sigan procedimientos definidos para la eliminación segura de datos sensibles al final de su vida útil, minimizando el riesgo de exposición accidental o maliciosa.	Cumple	Sin evidencia	
CA-021	Control de Acceso	Este control asegura que se establezcan y mantengan políticas claras y procedimientos para gestionar los accesos de usuarios, garantizando que solo personal autorizado tenga acceso a sistemas y datos críticos.	Cumple	Sin evidencia	

CA-022	Control de Acceso	Este control asegura que se establezcan y mantengan políticas claras y procedimientos para gestionar los accesos de usuarios, garantizando que solo personal autorizado tenga acceso a sistemas y datos críticos.	Cumple	Sin evidencia	
CA-024	Control de Acceso	Este control asegura que se implementen medidas físicas y lógicas para proteger dispositivos que contienen acceso a sistemas de desarrollo, minimizando el riesgo de acceso no autorizado en caso de robo o pérdida.	Cumple	Sin evidencia	

Detalles de Auditoría por Sección

Código	DS-001
Área de Seguridad	Desarrollo Seguro
Descripción del Control	Adherencia a la política de desarrollo seguro
Estado	No Cumple
Evidencia	
Observaciones	
Recomendaciones	

Código	SED-001
Área de Seguridad	Seguridad en el Entorno de Desarrollo
Descripción del Control	Separación de entornos de desarrollo y producción
Estado	Cumple
Evidencia	
Observaciones	
Recomendaciones	

Código	CA-003
Área de Seguridad	Control de Acceso
Descripción del Control	Repositorios y Proyectos
Estado	Cumple
Evidencia	
Observaciones	
Recomendaciones	

Código	CA-004
Área de Seguridad	Protección de Datos
Descripción del Control	Protección de Proyectos y Repositorios
Estado	Cumple
Evidencia	
Observaciones	
Recomendaciones	

Código	SA-008
Área de Seguridad	Seguridad de Aplicaciones
Descripción del Control	Este control garantiza que se realicen pruebas exhaustivas de seguridad, como pruebas de penetración y análisis estático de código, para identificar y mitigar vulnerabilidades antes de que las aplicaciones sean desplegadas en un entorno operativo.
Estado	Cumple
Evidencia	
Observaciones	
Recomendaciones	

Código	SA-009
Área de Seguridad	Seguridad de Aplicaciones
Descripción del Control	Este control asegura que las API sean desarrolladas y configuradas con medidas de seguridad adecuadas, protegiendo contra accesos no autorizados y asegurando la integridad y disponibilidad de los datos intercambiados.
Estado	Cumple
Evidencia	
Observaciones	
Recomendaciones	

Código	GI-011
Área de Seguridad	Gestión de Incidentes
Descripción del Control	Este control establece la documentación adecuada y la generación de reportes detallados sobre los incidentes de seguridad ocurridos en el entorno de desarrollo, facilitando la revisión y mejora continua de las medidas de seguridad implementadas.
Estado	Cumple
Evidencia	
Observaciones	
Recomendaciones	

Código	DS-014
Área de Seguridad	Desarrollo Seguro
Descripción del Control	Este control asegura que el personal de desarrollo reciba formación continua sobre buenas prácticas de seguridad, promoviendo una cultura de desarrollo seguro dentro de la organización.
Estado	Cumple
Evidencia	
Observaciones	
Recomendaciones	

Código	GV-016
Área de Seguridad	Gestión de Vulnerabilidades
Descripción del Control	Este control establece procesos para asegurar una comunicación efectiva y colaboración entre equipos, facilitando la identificación y resolución rápida de vulnerabilidades críticas en el entorno de desarrollo.
Estado	Cumple
Evidencia	
Observaciones	
Recomendaciones	

Código	PD-018
Área de Seguridad	Protección de Datos
Descripción del Control	Este control asegura que se implementen y mantengan medidas de cifrado robustas para proteger datos sensibles contra acceso no autorizado y cumplir con regulaciones de protección de datos aplicables.
Estado	No Cumple
Evidencia	
Observaciones	
Recomendaciones	

Código	PD-020
Área de Seguridad	Protección de Datos
Descripción del Control	Este control asegura que se sigan procedimientos definidos para la eliminación segura de datos sensibles al final de su vida útil, minimizando el riesgo de exposición accidental o maliciosa.
Estado	Cumple
Evidencia	
Observaciones	
Recomendaciones	

Código	CA-021
Área de Seguridad	Control de Acceso
Descripción del Control	Este control asegura que se establezcan y mantengan políticas claras y procedimientos para gestionar los accesos de usuarios, garantizando que solo personal autorizado tenga acceso a sistemas y datos críticos.
Estado	Cumple
Evidencia	
Observaciones	
Recomendaciones	

Código	CA-022
Área de Seguridad	Control de Acceso
Descripción del Control	Este control asegura que se establezcan y mantengan políticas claras y procedimientos para gestionar los accesos de usuarios, garantizando que solo personal autorizado tenga acceso a sistemas y datos críticos.
Estado	Cumple
Evidencia	
Observaciones	
Recomendaciones	

Código	CA-024
Área de Seguridad	Control de Acceso
Descripción del Control	Este control asegura que se implementen medidas físicas y lógicas para proteger dispositivos que contienen acceso a sistemas de desarrollo, minimizando el riesgo de acceso no autorizado en caso de robo o pérdida.
Estado	Cumple
Evidencia	
Observaciones	
Recomendaciones	