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%

Auditoria General

Código	Área de Seguridad	Descripción del Control	Estado	Evidencia	Observaciones
DS-001	Desarrollo Seguro	Este control verifica que la organización tenga una política de desarrollo seguro bien definida y estructurada. La política debe incluir los principios, prácticas y procedimientos necesarios para garantizar la seguridad en todas las etapas del ciclo de vida del desarrollo de software.	No Cumple	- -	Existen vulnerabilidades de la informacion, ya que las politicas no incluyen a los freelancers.
SED-001	Seguridad en el Entorno de Desarrollo	Este control garantiza que existan medidas claras y efectivas para separar los entornos de desarrollo, prueba y producción. La separación de estos entornos es fundamental para evitar la contaminación de datos, proteger la integridad del sistema y minimizar los riesgos de acceso no autorizado o cambios no intencionados en el entorno de producción.	Cumple	- -	Se asegura una separación efectiva mediante un proceso formal de gestión de cambios y control de acceso. La firma de un documento de desvinculación por parte de los empleados al dejar la empresa es una buena práctica para prevenir accesos no autorizados.
CA-003	Control de Acceso	Este control verifica que la organización implemente medidas adecuadas para gestionar y supervisar el acceso a los repositorios de proyectos. Esto incluye definir niveles de acceso basados en roles y responsabilidades, así como implementar mecanismos de monitoreo para detectar y responder a accesos no autorizados o actividades sospechosas.	Cumple	- -	El acceso a los repositorios de proyectos en GitHub se controla mediante la asignación de permisos según el rol de cada desarrollador. Se implementan políticas claras de acceso y uso, y se registran actividades para auditoría.

CA-004	Protección de Datos	Este control verifica que la organización haya establecido políticas y procedimientos claros para prevenir la clonación no autorizada de proyectos. Estas medidas son esenciales para proteger la propiedad intelectual y la integridad de los proyectos almacenados en los repositorios.	Cumple	- -	Los productos están protegidos mediante patentes registradas, y se están evaluando opciones adicionales para fortalecer esta protección, como acuerdos de confidencialidad más estrictos y tecnologías de gestión de derechos digitales (DRM).
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	- -	Solo el personal autorizado y capacitado puede realizar las acciones de despliegue a producción, asegurando que se realicen las pruebas de seguridad correspondientes.
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	- -	Todas las APIs están protegidas mediante seguridad de token según su lenguaje de programación, y los archivos de entorno de desarrollo que especifican las APIs externas están siempre encriptados.
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	- -	Los incidentes de seguridad se documentan y reportan mediante la generación de tickets de atención, que alertan al líder de área para su verificación posterior.

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	- -	Se proporcionan capacitaciones internas y se adquieren cursos en la plataforma Udemy para mejorar la seguridad a nivel de base de datos y obtener conocimientos sobre buenas prácticas de seguridad.
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	- -	Se realizan reuniones semanales entre equipos de desarrollo y seguridad para definir acuerdos y fechas de conclusión. Además, se utiliza la plataforma Notion para registrar y verificar el estado de los pendientes.
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	- -	Actualmente no se ha implementado el cifrado de datos en los entornos de desarrollo, a pesar de manejar credenciales de acceso sensibles.
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	- -	Existe un procedimiento para encriptar la información de votaciones para mantener el anonimato.
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	- -	Se utilizan roles de usuario tanto en GitHub como en bases de datos para gestionar el acceso a proyectos y recursos.

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	- -	Se crean credenciales de acceso individuales para cada programador, lo que permite monitorear y registrar el acceso a servidores y bases de datos, incluyendo detalles como hora y dirección IP.
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	- -	La empresa administra de manera eficiente su inventario de bienes, así como la información asociada a cada uno de ellos.

Detalles de Auditoría por Sección

Código	**DS-001**
Área de Seguridad	Desarrollo Seguro
Descripción del Control	Este control verifica que la organización tenga una política de desarrollo seguro bien definida y estructurada. La política debe incluir los principios, prácticas y procedimientos necesarios para garantizar la seguridad en todas las etapas del ciclo de vida del desarrollo de software.
Estado	No Cumple
Observaciones	Existen vulnerabilidades de la informacion, ya que las politicas no incluyen a los freelancers.
Recomendaciones	Incluir a todos los freelancers bajo las mismas políticas de seguridad que los empleados.

Código	**SED-001**
Área de Seguridad	Seguridad en el Entorno de Desarrollo
Descripción del Control	Este control garantiza que existan medidas claras y efectivas para separar los entornos de desarrollo, prueba y producción. La separación de estos entornos es fundamental para evitar la contaminación de datos, proteger la integridad del sistema y minimizar los riesgos de acceso no autorizado o cambios no intencionados en el entorno de producción.
Estado	Cumple
Observaciones	Se asegura una separación efectiva mediante un proceso formal de gestión de cambios y control de acceso. La firma de un documento de desvinculación por parte de los empleados al dejar la empresa es una buena práctica para prevenir accesos no autorizados.
Recomendaciones	Implementar herramientas automatizadas de control de versiones y despliegue continuo (CI/CD) para mejorar la gestión de cambios y asegurar aún más la separación de entornos.

Código	**CA-003**
Área de Seguridad	Control de Acceso
Descripción del Control	Este control verifica que la organización implemente medidas adecuadas para gestionar y supervisar el acceso a los repositorios de proyectos. Esto incluye definir niveles de acceso basados en roles y responsabilidades, así como implementar mecanismos de monitoreo para detectar y responder a accesos no autorizados o actividades sospechosas.
Estado	Cumple
Observaciones	El acceso a los repositorios de proyectos en GitHub se controla mediante la asignación de permisos según el rol de cada desarrollador. Se implementan políticas claras de acceso y uso, y se registran actividades para auditoría.
Recomendaciones	Implementar un sistema de alertas en tiempo real para detectar y notificar actividades sospechosas o no autorizadas en los repositorios.

Código	**CA-004**
Área de Seguridad	Protección de Datos
Descripción del Control	Este control verifica que la organización haya establecido políticas y procedimientos claros para prevenir la clonación no autorizada de proyectos. Estas medidas son esenciales para proteger la propiedad intelectual y la integridad de los proyectos almacenados en los repositorios.
Estado	Cumple
Observaciones	Los productos están protegidos mediante patentes registradas, y se están evaluando opciones adicionales para fortalecer esta protección, como acuerdos de confidencialidad más estrictos y tecnologías de gestión de derechos digitales (DRM).
Recomendaciones	Acelerar la implementación de tecnologías de gestión de derechos digitales (DRM) y reforzar los acuerdos de confidencialidad.

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
Observaciones	Solo el personal autorizado y capacitado puede realizar las acciones de despliegue a producción, asegurando que se realicen las pruebas de seguridad correspondientes.
Recomendaciones	Integrar herramientas automatizadas de pruebas de seguridad (como SAST y DAST) en el pipeline de CI/CD para realizar pruebas continuas durante el desarrollo y antes del despliegue.

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
Observaciones	Todas las APIs están protegidas mediante seguridad de token según su lenguaje de programación, y los archivos de entorno de desarrollo que especifican las APIs externas están siempre encriptados.
Recomendaciones	Implementar herramientas de monitoreo y auditoría continua para las APIs, que permitan detectar y responder a actividades sospechosas o inusuales en tiempo real.

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
Observaciones	Los incidentes de seguridad se documentan y reportan mediante la generación de tickets de atención, que alertan al líder de área para su verificación posterior.
Recomendaciones	Implementar un sistema de gestión de incidentes más robusto que incluya la clasificación de incidentes, seguimiento del estado, análisis post-incidente y lecciones aprendidas.

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
Observaciones	Se proporcionan capacitaciones internas y se adquieren cursos en la plataforma Udemy para mejorar la seguridad a nivel de base de datos y obtener conocimientos sobre buenas prácticas de seguridad.
Recomendaciones	Diversificar las fuentes de capacitación incluyendo programas certificados de seguridad (como CISSP, CISM, o cursos específicos de seguridad de aplicaciones) y realizar talleres prácticos regulares.

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
Observaciones	Se realizan reuniones semanales entre equipos de desarrollo y seguridad para definir acuerdos y fechas de conclusión. Además, se utiliza la plataforma Notion para registrar y verificar el estado de los pendientes.
Recomendaciones	Implementar una plataforma de gestión de vulnerabilidades dedicada (como JIRA, Bugzilla, o una solución específica de seguridad) que incluya seguimiento de estado, asignación de prioridades y notificaciones automáticas.

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
Observaciones	Actualmente no se ha implementado el cifrado de datos en los entornos de desarrollo, a pesar de manejar credenciales de acceso sensibles.
Recomendaciones	Implementar el cifrado de datos tanto en reposo como en tránsito en todos los entornos de desarrollo. Utilizar herramientas y protocolos estándar de la industria, como TLS/SSL para datos en tránsito y AES para datos en reposo.

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
Observaciones	Existe un procedimiento para encriptar la información de votaciones para mantener el anonimato.
Recomendaciones	Desarrollar y documentar procedimientos específicos para la eliminación segura de datos sensibles al final de su ciclo de vida. Esto puede incluir el borrado seguro de datos de todas las bases de datos y sistemas, y la destrucción física de medios de almacenamiento si es necesario.

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
Observaciones	Se utilizan roles de usuario tanto en GitHub como en bases de datos para gestionar el acceso a proyectos y recursos.
Recomendaciones	Implementar auditorías regulares y automatizadas de los accesos de usuarios a sistemas y recursos. Utilizar herramientas que generen informes detallados de accesos y actividades sospechosas.

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
Observaciones	Se crean credenciales de acceso individuales para cada programador, lo que permite monitorear y registrar el acceso a servidores y bases de datos, incluyendo detalles como hora y dirección IP.
Recomendaciones	Implementar un sistema automatizado de monitoreo y alertas en tiempo real para detectar y responder rápidamente a actividades sospechosas. Utilizar herramientas de seguridad que integren análisis de comportamiento de usuarios (UBA) y generación de alertas automáticas.

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
Observaciones	La empresa administra de manera eficiente su inventario de bienes, así como la información asociada a cada uno de ellos.
Recomendaciones	Implementar medidas adicionales como el cifrado completo de disco en todos los dispositivos y el uso de autenticación multifactor (MFA) para acceder a sistemas críticos. También, considerar soluciones de gestión de dispositivos móviles (MDM) para rastrear y controlar dispositivos de forma remota.