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:	HTEC
Dirección:	Alfonso Ugarte 6
Responsable:	Henry Percial
Auditor:	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 mejorar las medidas de seguridad implementadas.

Auditoria General

Código	Área de Seguridad	Descripción del Control	Estado	Evidencia	Observaciones
PD-002	Protección de Datos	Accesos y Permisos	Pendiente	Sin evidencia	
GV-001	Gestión de Vulnerabilidades	Análisis de vulnerabilidades periódicos	Pendiente	Sin evidencia	
DS-001	Desarrollo Seguro	Adherencia a la política de desarrollo seguro	Pendiente	Sin evidencia	
SED-001	Seguridad en el Entorno de Desarrollo	Separación de entornos de desarrollo y producción	Pendiente	Sin evidencia	
CA-003	Control de Acceso	Repositorios y Proyectos	Pendiente	Sin evidencia	
CA-004	Protección de Datos	Protección de Proyectos y Repositorios	Pendiente	Sin evidencia	
SED-005	Seguridad en el Entorno de Desarrollo	Este control asegura que solo personal autorizado tenga acceso a los entornos de desarrollo, con medidas de autenticación y monitoreo continuo para detectar y responder a intentos de acceso no autorizados.	Pendiente	Sin evidencia	
SED-006	Seguridad en el Entorno de Desarrollo	Este control establece políticas y procedimientos para la gestión segura de credenciales y claves de acceso, minimizando el riesgo de compromiso de información sensible y asegurando la integridad del entorno de desarrollo.	Pendiente	Sin evidencia	
SA-007	Seguridad de Aplicaciones	Este control asegura que las aplicaciones sean desarrolladas utilizando metodologías y herramientas que incorporen prácticas de seguridad desde el diseño, minimizando vulnerabilidades y asegurando la robustez del código.	Pendiente	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.	Pendiente	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.	Pendiente	Sin evidencia	
GI-010	Gestión de Incidentes	Este control asegura que se tenga un procedimiento claro y efectivo para la detección temprana, respuesta y manejo de incidentes de seguridad, minimizando el impacto en las operaciones y asegurando la recuperación rápida de los sistemas afectados.	Pendiente	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.	Pendiente	Sin evidencia	

GI-012	Gestión de Incidentes	Este control asegura que se implementen acciones correctivas para abordar las causas raíz de los incidentes de seguridad, así como medidas preventivas para evitar que ocurran nuevamente en el futuro.	Pendiente	Sin evidencia	
DS-013	Desarrollo Seguro	Este control asegura que se sigan prácticas de desarrollo seguro, como revisión de código, pruebas de seguridad y análisis estático de código, para identificar y remediar vulnerabilidades antes de que el software sea desplegado.	Pendiente	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.	Pendiente	Sin evidencia	
GV-015	Gestión de Vulnerabilidades	Este control asegura que se realicen evaluaciones regulares de vulnerabilidades utilizando herramientas y metodologías adecuadas, priorizando y mitigando las vulnerabilidades identificadas de manera oportuna.	Pendiente	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.	Pendiente	Sin evidencia	

GV-017	Gestión de Vulnerabilidades	Este control asegura que se sigan procedimientos definidos para la gestión de parches de seguridad, garantizando que las vulnerabilidades sean corregidas de manera efectiva y sin afectar la estabilidad de los sistemas.	Pendiente	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.	Pendiente	Sin evidencia	
PD-019	Protección de Datos	Este control establece medidas para asegurar que los datos sensibles no sean alterados o comprometidos, garantizando su disponibilidad para usuarios autorizados y sistemas internos.	Pendiente	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.	Pendiente	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.	Pendiente	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.	Pendiente	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.	Pendiente	Sin evidencia	

Detalles de Auditoría por Sección

Código	PD-002
Área de Seguridad	Protección de Datos
Descripción del Control	Accesos y Permisos
Estado	Pendiente
Evidencia	
Observaciones	
Recomendaciones	

Código	GV-001
Área de Seguridad	Gestión de Vulnerabilidades
Descripción del Control	Análisis de vulnerabilidades periódicos
Estado	Pendiente
Evidencia	
Observaciones	
Recomendaciones	

Código	DS-001
Área de Seguridad	Desarrollo Seguro
Descripción del Control	Adherencia a la política de desarrollo seguro
Estado	Pendiente
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	Pendiente
Evidencia	
Observaciones	
Recomendaciones	

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

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

Código	SED-005
Área de Seguridad	Seguridad en el Entorno de Desarrollo
Descripción del Control	Este control asegura que solo personal autorizado tenga acceso a los entornos de desarrollo, con medidas de autenticación y monitoreo continuo para detectar y responder a intentos de acceso no autorizados.
Estado	Pendiente
Evidencia	
Observaciones	
Recomendaciones	

Código	SED-006
Área de Seguridad	Seguridad en el Entorno de Desarrollo
Descripción del Control	Este control establece políticas y procedimientos para la gestión segura de credenciales y claves de acceso, minimizando el riesgo de compromiso de información sensible y asegurando la integridad del entorno de desarrollo.
Estado	Pendiente
Evidencia	
Observaciones	
Recomendaciones	

Código	SA-007
Área de Seguridad	Seguridad de Aplicaciones
Descripción del Control	Este control asegura que las aplicaciones sean desarrolladas utilizando metodologías y herramientas que incorporen prácticas de seguridad desde el diseño, minimizando vulnerabilidades y asegurando la robustez del código.
Estado	Pendiente
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	Pendiente
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	Pendiente
Evidencia	
Observaciones	
Recomendaciones	

Código	GI-010
Área de Seguridad	Gestión de Incidentes
Descripción del Control	Este control asegura que se tenga un procedimiento claro y efectivo para la detección temprana, respuesta y manejo de incidentes de seguridad, minimizando el impacto en las operaciones y asegurando la recuperación rápida de los sistemas afectados.
Estado	Pendiente
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	Pendiente
Evidencia	
Observaciones	
Recomendaciones	

Código	GI-012
Área de Seguridad	Gestión de Incidentes
Descripción del Control	Este control asegura que se implementen acciones correctivas para abordar las causas raíz de los incidentes de seguridad, así como medidas preventivas para evitar que ocurran nuevamente en el futuro.
Estado	Pendiente
Evidencia	
Observaciones	
Recomendaciones	

Código	DS-013
Área de Seguridad	Desarrollo Seguro
Descripción del Control	Este control asegura que se sigan prácticas de desarrollo seguro, como revisión de código, pruebas de seguridad y análisis estático de código, para identificar y remediar vulnerabilidades antes de que el software sea desplegado.
Estado	Pendiente
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	Pendiente
Evidencia	
Observaciones	
Recomendaciones	

Código	GV-015
Área de Seguridad	Gestión de Vulnerabilidades
Descripción del Control	Este control asegura que se realicen evaluaciones regulares de vulnerabilidades utilizando herramientas y metodologías adecuadas, priorizando y mitigando las vulnerabilidades identificadas de manera oportuna.
Estado	Pendiente
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	Pendiente
Evidencia	
Observaciones	
Recomendaciones	

Código	GV-017
Área de Seguridad	Gestión de Vulnerabilidades
Descripción del Control	Este control asegura que se sigan procedimientos definidos para la gestión de parches de seguridad, garantizando que las vulnerabilidades sean corregidas de manera efectiva y sin afectar la estabilidad de los sistemas.
Estado	Pendiente
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	Pendiente
Evidencia	
Observaciones	
Recomendaciones	

Código	PD-019
Área de Seguridad	Protección de Datos
Descripción del Control	Este control establece medidas para asegurar que los datos sensibles no sean alterados o comprometidos, garantizando su disponibilidad para usuarios autorizados y sistemas internos.
Estado	Pendiente
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	Pendiente
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	Pendiente
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	Pendiente
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	Pendiente
Evidencia	
Observaciones	
Recomendaciones	