Carrera: Certificación

Asignatura: Integridad y autenticidad de la información

NAO ID: 3111

Nombre: Geovanna Estefanía Pincay Arreaga

Fecha de Entrega: 1 de Serptiembre del 2024.

Sprint 2

Historias de Usuario

--Como usuario de ToCupboard, quiero poder realizar compras de productos de primera necesidad de forma segura, para proteger mis datos personales y financieros durante el proceso de compra.

Criterios de Aceptación:

- La plataforma debe usar cifrado HTTPS para todas las transacciones.
- Deben implementarse medidas de seguridad para proteger datos personales y financieros.
- Debe haber opciones de autenticación de dos factores para usuarios.

--Como pequeño comerciante, quiero que la información de mis productos y transacciones esté segura en la plataforma, para evitar pérdidas por fraude o ataques cibernéticos.

Criterios de Aceptación:

- Los datos de los productos deben estar cifrados.
- Se deben implementar controles de acceso basados en roles para proteger la información del comerciante.
- La plataforma debe ofrecer notificaciones de actividad sospechosa.

--Como desarrollador del equipo de ToCupboard, quiero tener acceso a herramientas de análisis de código y escaneo de vulnerabilidades, para detectar y corregir problemas de seguridad antes de que el sitio esté en producción.

Criterios de Aceptación:

- La integración de herramientas de análisis de código debe estar completa.
- Las vulnerabilidades detectadas deben ser documentadas y priorizadas para su corrección.

--Como administrador de ToCupboard, quiero implementar controles de acceso y cifrado de datos, para garantizar que solo el personal autorizado pueda acceder a la información sensible.

Criterios de Aceptación:

- Los controles de acceso deben estar basados en roles y ser configurables.
- Todos los datos sensibles deben estar cifrados tanto en reposo como en tránsito.

--Como inversionista potencial, quiero asegurarme de que ToCupboard cumpla con los estándares de seguridad internacionales, para proteger mi inversión y garantizar la sostenibilidad a largo plazo del negocio.

Criterios de Aceptación:

- La plataforma debe cumplir con estándares como ISO 27001 y SOC 2.
- Se deben proporcionar informes de auditoría y certificación de seguridad.

Tablas de Registro

Tabla 1: Lista de Requerimientos

ID	**Descripción del Requerimiento**	**Prioridad**	**Responsable**	**Estado**
R1	Implementación de cifrado de datos para proteger información sensible.	Alta	Juan Carlos	En proceso
R2	Integración de herramientas de análisis de código automatizadas.	Alta	Equipo DevSecOps	Pendiente
R3	Configuración de controles de acceso para usuarios y administradores.	Media	Juan Carlos	En proceso
R4	Desarrollo de un sistema de monitoreo de eventos de seguridad.	Alta	Equipo de Seguridad	Pendiente
R5	Realización de pruebas de penetración (pentesting) periódicas.	Alta	Juan Carlos	Pendiente
R6	Creación de un informe detallado de hallazgos y recomendaciones.	Alta	Juan Carlos	Completado
R7	Cumplimiento de estándares y regulaciones de seguridad.	Alta	Equipo Legal/Seguridad	En proceso

Tabla 2: Registro de Actividades

ID	**Actividad**	**Fecha**	**Responsable**	**Notas**

A1	Análisis inicial de vulnerabilidades	2020-06-01	Juan Carlos	Identificadas varias vulnerabilidades críticas.
A2	Implementación de cifrado de datos	2020-06-15	Juan Carlos	Proceso de cifrado AES en curso.
A3	Integración de herramientas de análisis de código	2020-06-20	Equipo DevSecOps	Esperando aprobación para herramientas.
A4	Pruebas de penetración iniciales	2020-07-01	Juan Carlos	Resultados mostraron áreas para mejorar.
A5	Configuración de controles de acceso	2020-07-10	Juan Carlos	Acceso basado en roles configurado.
A6	Monitoreo de eventos de seguridad	2020-07-20	Equipo de Seguridad	Implementación de SIEM en progreso.

Roadmap de Protocolos de Seguridad

Trimestre	**Actividades**
Q2 2020	- Realizar análisis inicial de vulnerabilidades.
	- Implementar cifrado de datos en la plataforma.
Q3 2020	- Integrar herramientas de análisis de código y escaneo de vulnerabilidades.
	- Configurar controles de acceso para usuarios y administradores.
	- Desarrollar un sistema de monitoreo de eventos de seguridad.

Q4 2020	- Realizar pruebas de penetración completas y corregir las vulnerabilidades encontradas.
	- Generar y revisar informes detallados de hallazgos y recomendaciones.
	- Asegurar el cumplimiento de estándares y regulaciones de seguridad.
Q1 2021	- Revisar y mejorar los protocolos de seguridad según los resultados de las pruebas de penetración.
	- Expandir las capacidades de monitoreo y respuesta ante incidentes.