Documento de requerimientos de software

Sistema de gestión de transacciones - SecuraBank

Fecha: [28/10/2024]

Tabla de contenido

Historial de Versiones

Fecha	Versión	Autor	Organización	Descripción
22 de octubre de 2024	1	David Aucancela	Aplicaciones 2	Definición del perfil, alcance, objetivo del proyecto.
29 de octubre de 2024	2	David Aucancela	Aplicaciones 2	Documento de los requisitos y requerimientos

Información del Proyecto

Empresa / Organización	Escuela superior politécnica de Chimborazo
Proyecto	SecuraBank
Fecha de preparación	22/10/2024
Cliente	
Patrocinador principal	
Gerente / Líder de Proyecto	David Aucancela
Gerente / Líder de Análisis de negocio y requerimientos	David Aucancela

Aprobaciones

Nombre y Apellido	Cargo	Departamento u Organización	Fecha	Firma
Ing. Julio Santillán				

1. Propósito

El sistema transaccional web está diseñado para proporcionar una plataforma robusta y segura que permita a los usuarios gestionar sus operaciones bancarias de forma confiable y eficiente. Su propósito principal es garantizar la protección de la información sensible y la integridad de las transacciones mediante el uso de medidas de seguridad avanzadas, como la autenticación multifactorial (MFA) en el inicio de sesión. Además, ofrece un panel de administración intuitivo, que permite a los administradores monitorear accesos, configurar políticas de seguridad, y gestionar usuarios y roles de forma centralizada.

Con herramientas como el historial de auditoría y el seguimiento detallado de actividades, el sistema facilita la identificación y mitigación de actividades sospechosas, proporcionando transparencia y control sobre todas las operaciones realizadas. Asimismo, el simulador de transacciones permite a los usuarios experimentar diferentes tipos de operaciones, como transferencias y pagos, en un entorno controlado, lo que asegura un mejor manejo y conocimiento de los procesos internos.

2. Alcance del producto / Software

El sistema transaccional web tiene como propósito la creación de una plataforma segura que cumpla con las normativas y mejores prácticas de seguridad web establecidas en OWASP. Este sistema implementará categorías avanzadas de seguridad, integrando un modelo de segmentación de redes para proteger la información sensible y minimizar riesgos. El enfoque se centra en ofrecer una aplicación web capaz de resistir las amenazas más comunes a través de una arquitectura robusta, que permite la verificación y control de vulnerabilidades a lo largo de todo el proceso de interacción de los usuarios.

El sistema incluirá funcionalidades clave, como autenticación multifactorial, gestión de roles y permisos, y auditoría de actividad en tiempo real. Además, la plataforma garantizará que todas las operaciones y transacciones bancarias sean seguras, proporcionando un entorno controlado donde se aplicarán los controles específicos de seguridad recomendados por OWASP. Este enfoque permite a los administradores implementar parámetros de seguridad y políticas avanzadas, asegurando que el software no solo cumpla con estándares de integridad y protección de datos, sino que también se adapte a las amenazas emergentes del entorno digital.

3. Referencias

- Pérez, J. (2024). *Documento de visión y definición de alcance del sistema de seguridad transaccional web* (Versión 1.0). Repositorio interno de la organización, Documentación técnica.
- Departamento de Seguridad IT. (2023). *Políticas y procedimientos de seguridad de la información* (Versión 2.3). Intranet de la organización, Políticas de Seguridad.

- OWASP Foundation. (2023). *OWASP Top Ten: Amenazas y prácticas de seguridad para aplicaciones web* (Versión 2023). Recuperado de https://owasp.org/www-project-top-ten/
- Equipo de Desarrollo. (2024). *Especificación de requerimientos de software del sistema transaccional web* (Versión 1.5). Repositorio interno de la organización, Especificaciones técnicas.
- Martínez, L. (2024). *Flujogramas de procesos para la gestión de roles y transacciones* (Versión 1.2). Documentación del proyecto, Diagramas de flujo.

4. Funcionalidades del producto

1. Inicio de sesión seguro con autenticación multifactorial (MFA).
2. Panel de administración para monitoreo y configuración de seguridad.
3. Gestión de usuarios y roles con permisos específicos.
4. Auditoría y registro de actividad detallado.
5. Gestión de dispositivos y sesiones activas.
6. Configuración avanzada de políticas de seguridad.
7. Simulador de transacciones para operaciones bancarias seguras.
8. Generación de reportes de actividad y cambios en seguridad.
9. Monitoreo y cierre remoto de sesiones no autorizadas.
10. Filtrado de historial de auditoría por fechas, usuarios, dispositivos y eventos.
11. Alertas de seguridad ante actividad sospechosa.
12. Ajustes de autenticación y duración de sesiones.

5. Clases y características de usuarios

1. Administrador: Usuario con acceso completo al sistema y privilegios elevados. Utiliza el sistema de forma frecuente para administrar y monitorear la seguridad,

2. Usuario Estándar: Usuario con acceso a funcionalidades básicas de transacciones bancarias. Utiliza el sistema de forma moderada, especialmente para realizar consultas de saldo y efectuar operaciones como transferencias y pagos.

3. Supervisor de Seguridad: Usuario con privilegios intermedios enfocados en el monitoreo de seguridad. Utiliza el sistema para revisar y responder a incidentes de seguridad, verificar actividad y generar reportes de auditoría.

4. Usuario Invitado (opcional): Usuario con permisos limitados para acceder a funciones restringidas. Generalmente no realiza operaciones bancarias, pero puede consultar información pública o limitada del sistema según políticas de acceso.

6. Entorno operativo

Plataforma de Hardware: Servidores de alta disponibilidad y estaciones de trabajo para usuarios administrativos. Compatible con dispositivos móviles y computadoras de escritorio.

Sistema Operativo: Compatible con versiones actualizadas de Windows Server, Linux (distribuciones basadas en Ubuntu y CentOS), y sistemas operativos de cliente Windows 10 y macOS para usuarios.

Base de Datos: MySQL para almacenamiento de datos transaccionales, configuración de políticas y registro de auditoría.

Infraestructura de Red: Segmentación de red basada en el modelo de seguridad Zero Trust, con VPN y firewalls configurados para limitar el acceso según roles y dispositivos.

Servidores Web y Aplicaciones: Apache para el manejo de solicitudes HTTP, y un entorno de ejecución backend basado en Django para los servicios transaccionales.

Compatibilidad con Navegadores: El sistema funcionará en los navegadores principales, incluidos Chrome, Firefox, Edge y Safari, priorizando el acceso seguro mediante HTTPS.

Integración con Herramientas de Seguridad Externas: Soporte para integrarse con sistemas de autenticación multifactorial (MFA) y sistemas de monitoreo de eventos de seguridad (SIEM) como Splunk o Elastic Stack.

7. Requerimientos funcionales

cada funcionalidad:

- Autenticación mediante MFA para todos los usuarios.
- Creación, edición y eliminación de usuarios por el administrador.
- Asignación de roles y permisos basados en políticas configurables.
- Visualización de gráficos de control y estadísticas de acceso.
- Registro de dispositivos permitidos y bloqueados.
- Monitoreo de sesiones activas y cierre remoto de sesiones no autorizadas.
- Simulación de transacciones bancarias (transferencias, pagos y consultas de saldo).
- Generación de alertas por actividades sospechosas.
- Registro y auditoría de todas las transacciones y actividades.
- Filtros de auditoría por usuario, fecha, dispositivo o evento.

8. Reglas de negocio

Reglas de acceso: Solo los administradores pueden asignar o modificar roles y permisos. Los usuarios regulares no pueden acceder a funciones de auditoría.

Reglas de transacción: Antes de completar una transacción, el sistema verifica permisos y cumplimiento de políticas de acceso (ubicación, dispositivo, etc.).

Política de auditoría: Todas las actividades relevantes deben ser registradas y accesibles solo para administradores y auditores.

9. Requerimientos de interfaces externas

Interfaces de usuario

- Interfaz de inicio de sesión con campo de usuario, contraseña y código MFA.
- Panel de administración intuitivo para monitoreo, gestión de usuarios y auditoría.
- Simulador de transacciones con opciones para transferencias y pagos.

Interfaces de hardware

- Requisitos mínimos de hardware en dispositivos de los usuarios, como acceso a SMS o correo para MFA.
- Equipos de red y dispositivos seguros en los puntos de acceso.

Interfaces de software

- Integración con una base de datos SQL para almacenamiento de usuarios, roles, transacciones, y auditorías.
- Comunicación con API de autenticación (SMS o correo) para MFA.

Interfaces de comunicación

- Protocolos HTTPS para asegurar la comunicación de datos sensibles.
- Soporte para envío de mensajes de texto y correos electrónicos como segundo factor de autenticación.

identificación	Sub identificación	Descripción del requisito	Versión	Estado actual	Última fecha estado registrado	Criterios de aceptación	Nivel de complejidad	Nec oportu objet ne
RF-001	RF-001-1	Autenticación mediante MFA para todos los usuarios.	1.0	En desarrollo	29/10/2024	MFA funcionando y autenticación exitosa de usuarios	Alta	Asegur seguro p
RF-002	RF-002-1	Creación, edición y eliminación de usuarios por el administrador.	1.0	En desarrollo	29/10/2024	CRUD de usuarios funcionando correctamente	Media	Administ segú per
RF-003	RF-003-1	Asignación de roles y permisos basados en políticas configurables.	1.0	En desarrollo	29/10/2024	Roles y permisos configurados exitosamente	Alta	Control funcio segú
RF-004	RF-004-1	Visualización de gráficos de control y estadísticas de acceso.	1.0	Planificado	29/10/2024	Gráficos generados con datos correctos	Media	Facilitar decisione análisis
RF-005	RF-005-1	Registro de dispositivos permitidos y bloqueados.	1.0	Planificado	29/10/2024	Lista de dispositivos actualizada correctamente	Alta	Asegura dispositi accedan
RF-006	RF-006-1	Monitoreo de sesiones activas y cierre remoto de sesiones no autorizadas.	1.0	En desarrollo	29/10/2024	Función de monitoreo y cierre funcionando	Alta	Aumenta mediante ses

RF-007	RF-007-1	Simulación de transacciones bancarias (transferencias, pagos y consultas de saldo).	1.0	Planificado	29/10/2024	Simulador funcionando y generando datos correctos	Alta	Probar l y funcio trans
RF-008	RF-008-1	Generación de alertas por actividades sospechosas.	1.0	En desarrollo	29/10/2024	Alertas generadas correctamente	Alta	Notificar inu
RF-009	RF-009-1	Registro y auditoría de todas las transacciones y actividades.	1.0	Planificado	29/10/2024	Registro de auditoría completo	Alta	Mant historia para a
RF-010	RF-010-1	Filtros de auditoría por usuario, fecha, dispositivo o evento.	1.0	En desarrollo	29/10/2024	Filtros funcionando correctamente	Media	Facilitar en a

10. Otros requerimientos

Requisitos de Seguridad

Protección de Datos: Encriptación de datos sensibles, protección de sesiones, y políticas de privacidad.

Autenticación Avanzada: Implementación de MFA, configuración de restricciones por ubicación y dispositivo.

Control de Acceso: Políticas basadas en roles y permisos, y acceso restringido a datos sensibles.

Gestión de Riesgos y Alertas: Notificación de actividades sospechosas, generación de alertas y prevención de fraude.

Requisitos de Usabilidad

Interfaz de Usuario (UI): Diseño intuitivo y amigable del sistema, con fácil navegación entre opciones de administración y simulación.

Accesibilidad: Adaptación de la interfaz para ser accesible en diferentes dispositivos (desktop, tablet, móvil).

Experiencia de Usuario (UX): Procesos simplificados para realizar transacciones, auditoría y configuraciones, además de soporte en caso de problemas.

Requisitos de Rendimiento

Tiempo de Respuesta: Respuesta rápida para consultas de saldo y procesamiento de transacciones.

Escalabilidad: Capacidad de manejar múltiples transacciones y usuarios simultáneos sin comprometer el rendimiento.

Disponibilidad: Alta disponibilidad del sistema para garantizar el acceso en todo momento.