Documento de requerimientos de software

Sistema de gestión de transacciones - SecuraBank

Fecha: [28/10/2024]

Tabla de contenido

1. 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

2. 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

3. Aprobaciones

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

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. Requerimientos funcionales

Funcionalidad 1: Inicio de sesión seguro con autenticación multifactorial (MFA)

- **REQ-1**: El sistema debe permitir a los usuarios autenticarse mediante nombre de usuario y contraseña.
- **REQ-2**: El sistema solicitará un segundo factor de autenticación (MFA) para verificar la identidad del usuario.
- **REQ-3**: Si el segundo factor de autenticación es inválido, el sistema mostrará un mensaje de error y permitirá reintentos limitados.

Funcionalidad 2: Panel de administración para monitoreo y configuración de seguridad

- **REQ-4**: El sistema debe permitir a los administradores visualizar el estado de seguridad en tiempo real.
- **REQ-5**: El sistema permitirá configurar y personalizar políticas de seguridad según las necesidades organizativas.
- **REQ-6**: Al ingresar configuraciones incorrectas, el sistema debe mostrar advertencias y sugerencias de corrección.

Funcionalidad 3: Gestión de usuarios y roles con permisos específicos

- **REQ-7**: El sistema permitirá al administrador crear, editar y eliminar usuarios y asignarles roles.
- **REQ-8**: Los roles deberán tener permisos específicos para acceder a ciertas áreas del sistema.
- **REQ-9**: Si un usuario intenta acceder a una sección sin los permisos necesarios, el sistema deberá bloquear el acceso y mostrar un mensaje informativo.

Funcionalidad 4: Auditoría y registro de actividad detallado

- **REQ-10**: El sistema debe registrar automáticamente todas las actividades relevantes para auditoría y revisión.
- **REQ-11**: El sistema permitirá a los administradores consultar y exportar el historial de actividad.
- **REQ-12**: Si una consulta de auditoría no encuentra registros, el sistema debe informar que no hay datos disponibles para el período seleccionado.

Funcionalidad 5: Gestión de dispositivos y sesiones activas

- **REQ-13**: El sistema permitirá a los usuarios verificar y gestionar los dispositivos conectados a su cuenta.
- **REQ-14**: Los usuarios podrán cerrar sesiones activas en dispositivos no autorizados.
- **REQ-15**: En caso de que el usuario intente cerrar una sesión que ya no está activa, el sistema debe mostrar un mensaje indicando que la sesión ya fue finalizada.

Funcionalidad 6: Configuración avanzada de políticas de seguridad

- **REQ-16**: El sistema permitirá al administrador configurar parámetros de seguridad avanzados como la duración de sesiones y requisitos de contraseña.
- **REQ-17**: Al realizar cambios en las políticas, el sistema debe aplicar y guardar los cambios de inmediato.
- **REQ-18**: Si se ingresan configuraciones que no cumplen los estándares, el sistema mostrará una advertencia y solicitará corrección.

Funcionalidad 7: Simulador de transacciones para operaciones bancarias seguras

- **REQ-19**: El sistema permitirá simular transacciones bancarias de manera segura y controlada.
- **REQ-20**: El sistema debe validar todos los datos ingresados en la simulación para evitar errores.
- **REQ-21**: Si se detectan datos incompletos o inválidos, el sistema mostrará un mensaje de error y solicitará corrección.

Funcionalidad 8: Generación de reportes de actividad y cambios en seguridad

- **REQ-22**: El sistema permitirá a los administradores generar reportes de actividad de seguridad en formato PDF o CSV.
- **REQ-23**: El sistema debe ofrecer opciones de filtro para personalizar los reportes según el período o tipo de actividad.
- **REQ-24**: En caso de que no haya datos para el período seleccionado, el sistema debe notificar que no se encontraron registros.

Funcionalidad 9: Monitoreo y cierre remoto de sesiones no autorizadas

- **REQ-25**: El sistema debe monitorear todas las sesiones activas y alertar sobre actividades sospechosas.
- **REQ-26**: Los administradores podrán cerrar sesiones sospechosas de manera remota para proteger el sistema.
- **REQ-27**: Si una sesión ya ha sido cerrada previamente, el sistema debe notificar que no está activa actualmente.

Funcionalidad 10: Filtrado de historial de auditoría por fechas, usuarios, dispositivos y eventos

- **REQ-28**: El sistema permitirá a los administradores filtrar el historial de auditoría por fechas, usuarios, dispositivos y eventos específicos.
- **REQ-29**: El sistema debe actualizar y mostrar solo los registros que coincidan con los filtros aplicados.
- **REQ-30**: En caso de que los filtros aplicados no devuelvan resultados, el sistema debe informar que no se encontraron coincidencias.

Funcionalidad 11: Alertas de seguridad ante actividad sospechosa

- **REQ-31**: El sistema debe monitorear y detectar patrones inusuales de acceso o intentos de acceso.
- **REQ-32**: Al detectar actividad sospechosa, el sistema enviará una alerta a los administradores.

- **REQ-33**: Si una alerta es generada por error, el sistema debe permitir marcarla como "falsa alarma" para no afectar futuras decisiones.

Funcionalidad 12: Ajustes de autenticación y duración de sesiones

- **REQ-34**: El sistema permitirá configurar la duración máxima de las sesiones de usuario.
- **REQ-35**: Los administradores podrán habilitar o deshabilitar la autenticación multifactorial (MFA) para diferentes roles.
- **REQ-36**: Si el usuario intenta iniciar sesión después de la expiración de su sesión, el sistema deberá redirigirlo al inicio de sesión y mostrar una advertencia sobre la duración de la sesión.

11. 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.

12. Otros requerimientos

Requisitos no funcionales

- El sistema debe responder a las solicitudes de inicio de sesión en un tiempo máximo de dos segundos, garantizando una experiencia fluida para el usuario.
- La interfaz de usuario debe ser intuitiva y consistente en todo el sistema, con una distribución de elementos y estilo que facilite la navegación tanto para usuarios finales como para administradores.

- La aplicación debe ser accesible a través de navegadores modernos como Chrome, Firefox, Safari, y Edge, y debe mantener su funcionalidad en dispositivos móviles, tabletas y escritorios.
- El sistema debe estar diseñado para soportar un crecimiento gradual de usuarios y transacciones sin comprometer el rendimiento, permitiendo futuras expansiones de capacidad sin modificaciones sustanciales en la arquitectura.
- El sistema debe garantizar la protección de datos confidenciales mediante técnicas de encriptación en todas las comunicaciones entre el cliente y el servidor, utilizando protocolos como HTTPS y TLS.
- La aplicación debe incluir una auditoría de seguridad interna periódica, revisando configuraciones de seguridad, registros y el cumplimiento de políticas, para detectar y corregir posibles vulnerabilidades.
- Todas las transacciones sensibles deben requerir autenticación multifactorial (MFA) para confirmar la identidad del usuario y prevenir accesos no autorizados.
- El sistema debe almacenar todos los registros de actividad en un formato seguro y debe ser capaz de mantener estos registros por un periodo mínimo de dos años, con opciones de filtrado y búsqueda avanzadas para facilitar la auditoría.

Requisitos de seguridad

- Los datos sensibles, tales como contraseñas y detalles de transacciones, deben almacenarse cifrados en la base de datos utilizando estándares de encriptación robustos como AES-256.
- El sistema debe detectar automáticamente intentos de acceso no autorizados y notificar a los administradores en tiempo real, permitiéndoles tomar medidas preventivas de manera inmediata.
- La aplicación debe permitir el control de acceso basado en roles (RBAC) de forma detallada, asegurando que cada usuario tenga acceso solo a la información y funciones que le corresponden según su rol.
- Las configuraciones de seguridad del sistema deben ser flexibles y permitir personalización, de modo que se puedan ajustar a las necesidades

específicas del entorno de uso y a cambios en las políticas de la organización.

- El sistema debe ser resistente a ataques de inyección **de SQL, Cross-Site Scripting (XSS) y Cross-Site Request Forgery (CSRF),** entre otros ataques comunes, para proteger la integridad de los datos y la seguridad de los usuarios.
- La arquitectura del sistema debe soportar una infraestructura distribuida, permitiendo que los servicios se ejecuten en múltiples servidores o nodos para mejorar la disponibilidad y la recuperación ante fallos.
- La autenticación y el acceso al sistema deben gestionarse de acuerdo con las normas ISO 27001:2020, cumpliendo con las prácticas de seguridad reconocidas a nivel internacional.
- El sistema debe ser auditable en términos de cambios en políticas de acceso, configuraciones de seguridad y cualquier modificación significativa, garantizando la trazabilidad de los cambios.
- El sistema debe soportar el bloqueo automático de cuentas tras múltiples intentos fallidos de inicio de sesión, protegiéndose contra ataques de fuerza bruta y asegurando que solo usuarios autorizados accedan a la información.