Plan de Gestión de Riesgos

Sistema de gestión de transacciones - SecuraBank

Fecha: [05/11/2024]

Tabla de contenido

Información del Proyecto

Empresa / Organización	Escuela superior politécnica de Chimborazo
Proyecto	SecuraBank
Fecha de preparación	05/11/2024
Cliente	
Patrocinador principal	
Gerente / Líder de Proyecto	David Aucancela

Metodología

Se utilizará el método de identificación, evaluación, mitigación y monitoreo de riesgos siguiendo las pautas de la norma ISO 31000. Los riesgos se evaluarán y clasificarán según su probabilidad e impacto, con controles diseñados para reducir vulnerabilidades y asegurar la integridad del sistema de transacciones.

Etapas del Proceso de Gestión de Riesgos:

1. **Identificación de Riesgos:** Identificación de posibles amenazas que puedan afectar la seguridad y operatividad del sistema.
2. **Análisis y Evaluación de Riesgos:** Análisis del impacto y la probabilidad de cada riesgo. Clasificación de los riesgos según niveles de prioridad.
3. **Desarrollo de Estrategias de Mitigación:** Creación de planes específicos para mitigar, transferir o aceptar riesgos.
4. **Monitoreo y Revisión:** Seguimiento continuo para evaluar la efectividad de las medidas de mitigación y actualización de la matriz de riesgos.

Roles y Responsabilidades

1. **Gerente de Proyecto:** Supervisar el proceso general de gestión de riesgos y coordinar con el equipo de seguridad y desarrollo.
2. **Oficial de Seguridad de la Información (ISO):** Identificación y análisis de riesgos relacionados con la seguridad. Responsable de la implementación de controles y políticas de seguridad.
3. **Analista de Riesgos:** Realizar evaluaciones de probabilidad e impacto, y apoyar en la generación de informes de riesgo.

4. **Desarrolladores y Equipo Técnico:** Implementar y mantener medidas de mitigación en el sistema.
5. **Stakeholders:** Revisar y aprobar la tolerancia al riesgo, y participar en la evaluación de impacto.

Presupuesto

Categoría	Detalle	Costo Estimado (USD)
1. Licencias de Software y Herramientas		
Autenticación Multi-factor (MFA)	Software de autenticación, tokens físicos o biométricos	$10,000
Sistema de Gestión de Identidad y Acceso (IAM)	Implementación de un sistema de acceso basado en roles	$8,000
Herramientas de Encriptación	Licencias para herramientas de encriptación de datos (ej., AES-256)	$5,000
Firewall de Aplicaciones Web (WAF)	Configuración de firewall específico para aplicaciones web	$7,000
Subtotal		**$30,000**
2. Infraestructura en la Nube		
Servidores Virtuales	Infraestructura para procesamiento y alojamiento seguro en la nube	$15,000
Almacenamiento Seguro de Datos	Espacio de almacenamiento en la nube con encriptación	$5,000
Redes Virtuales Privadas (VPN)	Configuración de VPN para comunicación segura	$3,000
Subtotal		**$23,000**
3. Consultoría y Certificación		
Consultoría en Seguridad (Zero Trust e ISO 27001)	Servicios de consultoría para implementación y conformidad con ISO 27001	$12,000
Auditoría para Certificación ISO 27001	Evaluación por una entidad certificadora	$10,000
Subtotal		**$22,000**
4. Capacitación y Entrenamiento		

Capacitación en Zero Trust	Capacitación del equipo técnico y de seguridad en el modelo Zero Trust	$5,000
Entrenamiento en ISO 27001	Formación para cumplir con la normativa ISO 27001	$4,000
Subtotal		**$9,000**
5. Desarrollo y Configuración del Sistema		
Desarrollo de Aplicaciones Seguras	Programación y desarrollo de la aplicación con enfoque en seguridad	$15,000
Integración de Sistemas de Seguridad	Configuración de autenticación, encriptación, y acceso seguro	$10,000
Pruebas de Penetración y Evaluación de Vulnerabilidades	Evaluación de seguridad mediante pruebas de intrusión simuladas	$6,000
Subtotal		**$31,000**
6. Mantenimiento y Monitoreo		
Monitoreo Continuo de Seguridad	Software y servicios de monitoreo de seguridad	$5,000
Actualizaciones y Parches de Seguridad	Implementación de actualizaciones periódicas de seguridad	$3,000
Subtotal		**$8,000**
7. Contingencias	Fondo para imprevistos o emergencias	**$10,000**
Total Estimado		**$133,000**

Calendario

Evento o Hito	Descripción	Fecha Estimada
Inicio del Proyecto	Inicio oficial del proyecto con revisión inicial de los objetivos y el alcance	01/01/2025
Fase de Identificación de Requisitos	Reunión con stakeholders para identificar y documentar requisitos específicos del sistema	08/01/2025

Análisis de Riesgos	Realización de la primera evaluación de riesgos, identificando amenazas y vulnerabilidades principales	15/01/2025
Diseño de la Arquitectura de Seguridad	Diseño del sistema basado en el modelo Zero Trust, incluyendo la arquitectura de autenticación y encriptación	01/02/2025
Implementación Inicial del Sistema	Desarrollo e integración inicial del sistema con controles de acceso y autenticación	01/03/2025
Capacitación en Zero Trust e ISO 27001	Capacitación del equipo de desarrollo y administración sobre las políticas y controles de seguridad	15/03/2025
Auditoría de Seguridad y Pruebas de Penetración	Ejecución de pruebas de intrusión para evaluar posibles vulnerabilidades	01/04/2025
Evaluación de Conformidad ISO 27001	Auditoría para la certificación ISO 27001 por una entidad externa	15/04/2025
Implementación Completa del Sistema	Integración final de todas las funciones de seguridad y revisión de controles	01/05/2025
Fase de Pruebas de Aceptación del Usuario (UAT)	Pruebas de aceptación con usuarios simulados para validar funcionalidad y seguridad	15/05/2025
Certificación ISO 27001	Recepción oficial de la certificación ISO 27001 tras cumplir con todos los requisitos	01/06/2025
Lanzamiento del Sistema	Implementación final del sistema en el entorno simulado	15/06/2025
Revisión Post-Implementación	Evaluación de la efectividad de la implementación y ajustes finales según el feedback de stakeholders	15/07/2025
Monitoreo Continuo de Seguridad	Inicio de monitoreo y mantenimiento constante para asegurar la integridad y seguridad del sistema	16/07/2025 y en adelante

Categorías de Riesgo

- Riesgos Técnicos: Vulnerabilidades en el software, fallos de autenticación, acceso no autorizado.
- Riesgos Operacionales: Fallos en procesos de seguridad, errores de configuración.
- Riesgos Financieros: Costos elevados en implementación de seguridad y mitigación de riesgos.
- Riesgos Legales y Regulatorios: Incumplimiento de ISO 27001 o leyes de protección de datos.
- Riesgos Humanos: Falta de capacitación en seguridad de personal clave o negligencia en el manejo del sistema.

Estructura de Desglose de Riesgos (RBS)

	Riesgo	Descripción del Riesgo	Estrategia de Mitigación
1	**Vulnerabilidades en el código**	Errores como inyecciones SQL, XSS o CSRF pueden permitir que atacantes accedan o manipulen datos críticos del sistema.	Implementar un enfoque de Zero Trust en la validación de usuarios y solicitudes. Aplicar el Estándar de Verificación de Seguridad de Aplicaciones (OWASP ASVS) para guiar el desarrollo seguro.
2	**Configuración insegura del servidor**	Configuraciones incorrectas en el servidor o en la red pueden abrir brechas de seguridad y facilitar accesos no autorizados.	Emplear un diseño en capas (defensa en profundidad) que limite el acceso mediante la segmentación de redes y políticas de acceso por capa. Revisar y endurecer configuraciones de servidores y redes.
3	**Manejo inadecuado de datos sensibles**	Almacenar datos sin cifrado o inadecuadamente puede llevar a filtraciones y exposición de datos confidenciales.	Usar técnicas de tokenización y cifrado simétrico para proteger datos sensibles tanto en tránsito como en reposo, siguiendo el principio de “mínimo privilegio” en el acceso a los datos.
4	**Falta de cifrado en la comunicación**	La falta de cifrado en las comunicaciones permite que datos importantes, como credenciales, sean	Implementar HTTPS en todo el sitio y establecer un cifrado TLS de extremo a extremo para la protección de datos en tránsito entre cliente y servidor.

		interceptados fácilmente.	
5	**Autenticación y autorización débiles**	Métodos de autenticación sin controles fuertes permiten accesos no autorizados a usuarios y transacciones.	Incorporar autenticación multifactorial (MFA) y usar RBAC para limitar el acceso de usuarios según sus roles. Revisar regularmente permisos y roles asignados.
6	**Fallas en la autenticación de transacciones**	La falta de validación adecuada en transacciones críticas puede comprometer la integridad del sistema y permitir fraudes.	Utilizar firmas digitales o hash para validar la integridad de las transacciones. Emplear patrones de verificación de integridad en cada paso transaccional.
7	**Deficiencias en la validación de datos**	Entradas no validadas correctamente pueden permitir ataques como inyección de código y manipulación de datos.	Usar validación y sanitización de entradas en todas las capas (cliente y servidor). Aplicar un firewall de aplicaciones web (WAF) para detectar y bloquear inyecciones en tiempo real.
8	**Inconsistencias en transacciones concurrentes**	La concurrencia no controlada puede generar conflictos, errores en los datos y pérdida de transacciones.	Utilizar bases de datos que soporten propiedades ACID para mantener la integridad de las transacciones. Implementar bloqueos de registros y transacciones atomizadas.
9	**Caídas del sistema bajo alta carga**	Un diseño no escalable puede causar caídas en el sistema al enfrentar altos volúmenes de transacciones, afectando su disponibilidad.	Adoptar patrones de arquitectura de microservicios y balanceo de carga para distribuir la carga y manejar el tráfico de manera eficiente.
10	**No cumplimiento de regulaciones de seguridad**	El incumplimiento de normas como PCI-DSS y GDPR puede resultar en sanciones legales y dañar la reputación del sistema.	Establecer un sistema de monitoreo continuo de conformidad y realizar auditorías regulares para asegurar el cumplimiento con estándares regulatorios y de privacidad.

Matriz de Probabilidad e Impacto

Riesgo	Descripción	Probabilidad	Impacto
1. Vulnerabilidades en el código	Errores como inyecciones SQL, XSS o CSRF pueden permitir que atacantes accedan o manipulen datos críticos del sistema.	Alta	Muy Alto (0.80)
2. Configuración insegura del servidor	Configuraciones incorrectas en el servidor o en la red pueden abrir brechas de seguridad.	Media	Alto (0.40)
3. Manejo inadecuado de datos sensibles	Almacenar datos sin cifrado puede llevar a filtraciones de datos confidenciales.	Alta	Muy Alto (0.80)
4. Falta de cifrado en la comunicación	Permite que datos importantes, como credenciales, sean interceptados fácilmente.	Alta	Alto (0.40)
5. Autenticación y autorización débiles	Métodos de autenticación sin controles fuertes permiten accesos no autorizados.	Alta	Muy Alto (0.80)
6. Fallas en la autenticación de transacciones	La falta de validación adecuada en transacciones críticas puede comprometer la integridad del sistema.	Media	Alto (0.40)
7. Deficiencias en la validación de datos	Entradas no validadas correctamente permiten ataques como inyección de código.	Media	Medio (0.20)

8. Inconsistencias en transacciones concurrentes	La concurrencia no controlada puede generar conflictos y errores en los datos.	Baja	Medio (0.20)
9. Caídas del sistema bajo alta carga	Un diseño no escalable puede causar caídas en el sistema, afectando su disponibilidad.	Alta	Alto (0.40)
10. No cumplimiento de regulaciones de seguridad	El incumplimiento de normas como PCI-DSS y GDPR puede resultar en sanciones legales.	Media	Muy Alto (0.80)

Amenazas (Riesgos)

Impacto / Probabilidad		Muy Bajo	Bajo	Medio	Alto	Muy Alto
		0,05	0,10	0,20	0,40	0,80
Muy Alta	0,90					
Alta	0,70					
Media	0,50					
Baja	0,30					
Muy Baja	0,10					

Oportunidades

Impacto / Probabilidad		Muy Alto	Alto	Medio	Bajo	Muy Bajo
		0,05	0,10	0,20	0,40	0,80
Muy Alta	0,90					
Alta	0,70					
Media	0,50					
Baja	0,30					
Muy Baja	0,10					

Revisión de la tolerancia de los interesados (Stakeholders)

Formatos de los Informes

- Informe de Identificación de Riesgos: Detalle de cada riesgo identificado y su categoría.
- Matriz de Evaluación de Riesgos: Documento donde se registra la probabilidad, el impacto y la prioridad de cada riesgo.
- Plan de Mitigación de Riesgos: Estrategias definidas para reducir la probabilidad o impacto de riesgos específicos.
- Informe de Monitoreo de Riesgos: Actualización periódica de los riesgos y la efectividad de las medidas implementadas.

Seguimiento

El seguimiento de riesgos se realizará de forma continua con revisiones trimestrales. Las evaluaciones se llevarán a cabo mediante revisiones de auditoría y con el uso de herramientas de monitoreo en tiempo real. Esto permitirá hacer ajustes en las estrategias de mitigación y asegurará que el sistema mantenga altos niveles de seguridad conforme a la normativa ISO 27001 y el modelo Zero Trust.

Aprobaciones

Aprobador	Fecha	Firma
David Aucancela	06/11/2024