

# Estudio de factibilidad

*Sistema de gestión de transacciones - SecuraBank*

*Fecha: [05/11/2024]*

## Tabla de contenido

Historial de Versiones .....	3
Información del Proyecto.....	3
Resumen Ejecutivo .....	3
Antecedentes del proyecto .....	3
El proyecto y su contexto .....	4
Descripción del proyecto.....	4
Objetivos .....	4
Contexto del proyecto .....	4
Alcance del estudio de factibilidad .....	5
Factibilidad técnica.....	5
Factibilidad económica.....	5
Factibilidad legal.....	6
Factibilidad de recursos .....	7
Factibilidad de mercado .....	8
Factibilidad operacional.....	8
Factibilidad de tiempo .....	8
Recomendaciones y aprobación .....	9

## 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
05 de noviembre de 2024	3	David Aucancela	Aplicaciones 2	Primera actualización del documento de factibilidad y elaboración de la gestión de riesgos.

## 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

## Resumen Ejecutivo

Evaluar la viabilidad de implementar un sistema de transacciones web seguro, centrado en el modelo Zero Trust y la norma ISO 27001:2020. Este sistema estará diseñado para entornos bancarios simulados y controlará vulnerabilidades mediante controles de autenticación y acceso.

## Antecedentes del proyecto

El proyecto surge de la creciente necesidad de fortalecer la seguridad en los sistemas de transacciones web, especialmente en el ámbito bancario, frente a amenazas cibernéticas en constante evolución. Este sistema de seguridad basado en el modelo Zero Trust e ISO 27001:2020 tiene como objetivo implementar controles de autenticación y segmentación de redes para mitigar vulnerabilidades. La iniciativa fue impulsada por el departamento de TI de la universidad, con la participación de estudiantes y profesores de la facultad de

Ingeniería de Software. Antes del estudio de factibilidad, se realizaron actividades preliminares, como la evaluación de tecnologías de seguridad y el análisis de mejores prácticas en entornos simulados, para fundamentar la propuesta del proyecto.

## El proyecto y su contexto

### Descripción del proyecto

Este proyecto busca implementar un sistema de transacciones web centrado en seguridad, aplicando el modelo Zero Trust y cumpliendo con los estándares de la norma ISO 27001:2020. El propósito principal es reducir vulnerabilidades y mejorar el control de acceso y autenticación en entornos bancarios simulados. Los entregables incluyen un sistema funcional de transacciones, un panel de monitoreo de seguridad y documentación detallada del proceso y resultados.

### Objetivos

- Desarrollar un sistema de autenticación multifactorial para garantizar un acceso seguro para los usuarios, reduciendo riesgos de accesos no autorizados y fortaleciendo la confianza del cliente.
- Implementar segmentación de redes basada en Zero Trust para proteger los activos críticos del sistema limitando el acceso solo a usuarios verificados, lo que incrementa la protección contra posibles ataques internos.
- Mejorar la visibilidad y control de las acciones dentro del sistema, lo cual ayuda en la detección de actividades sospechosas y en la toma de decisiones informadas.

### Contexto del proyecto

Este estudio se realiza en el contexto de una universidad, donde se requiere una solución de seguridad avanzada para simular escenarios bancarios para lo cual se establecieron las etapas previas: estudio de factibilidad, consultas con expertos y sesiones informativas con estos interesados para alinear la visión y asegurar que el enfoque propuesto satisfaga las necesidades de seguridad tanto internas como usuarios.

## Alcance del estudio de factibilidad

- Interfaz de inicio de sesión con autenticación multifactorial (MFA).
- Panel administrativo con herramientas de monitoreo de seguridad.
- Gestión integral de usuarios, dispositivos y políticas de acceso.
- Aseguramiento del cumplimiento de políticas robustas de seguridad y monitoreo en tiempo real.

## Factibilidad técnica

- **Recursos tecnológicos:** El proyecto se desarrollará con herramientas educativas y software gratuito.
- **Infraestructura:** Requiere una infraestructura de red segura, servidores de autenticación y segmentación de red.
- **Capacidades:** Se dispone de frameworks y tecnologías (como MFA, bases de datos seguras, y protocolos de encriptación) que soportan un desarrollo seguro que permitan una implementación simulada de Zero Trust y MFA.

## Factibilidad económica

### Costos Iniciales:

- **Licencias de Software:** Costos de software para autenticación, control de acceso, encriptación y gestión de identidades.
- **Infraestructura en la Nube:** Costos de almacenamiento, procesamiento y escalabilidad en una plataforma cloud segura.
- **Capacitación del Personal:** Inversión en formación del equipo técnico y administrativo sobre el modelo Zero Trust y la norma ISO 27001.

### Costos de Mantenimiento:

- **Actualizaciones y Parches de Seguridad:** Necesarios para mitigar nuevas vulnerabilidades.

- **Soporte Técnico Continuo:** Contratación de servicios de soporte técnico y especialistas en ciberseguridad para el mantenimiento del sistema.

### ROI (Retorno de Inversión):

- **Beneficios Potenciales:** Un sistema seguro basado en Zero Trust reduce significativamente los riesgos de brechas de seguridad, lo cual disminuye posibles pérdidas por fraudes o ataques cibernéticos.
- **Atractivo para Instituciones Bancarias Simuladas:** Puede atraer usuarios de simulaciones bancarias o de capacitaciones financieras.

Concepto	Año 1	Año 2	Año 3	Año 4	Año 5
<b>Ingresos</b>					
Ventas de productos	\$0	\$0	\$0	\$0	\$0
Ventas de servicios	\$0	\$0	\$0	\$0	\$0
<b>Costos</b>					
Personal	\$5,000	\$5,500	\$6,000	\$6,500	\$7,000
Materiales	\$1,000	\$1,100	\$1,200	\$1,300	\$1,400
Recursos informáticos	\$2,000	\$2,100	\$2,200	\$2,300	\$2,400
Entrenamiento	\$1,500	\$500	\$500	\$500	\$500

## Factibilidad legal

El proyecto se alinea con los estándares de seguridad de la norma ISO 27001:2020 y no enfrenta restricciones legales significativas, ya que se implementará en un entorno educativo controlado. Esto minimiza riesgos relacionados con el cumplimiento legal, ya que el entorno simulado no involucra datos reales de clientes bancarios, sino datos de prueba, lo cual facilita la adhesión a las regulaciones de protección de datos y privacidad.

### Cumplimiento Normativo:

- **ISO 27001:2020:** La normativa ISO 27001:2020 establece los requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI), asegurando que la implementación del sistema cumpla con altos estándares de seguridad.

- **Regulaciones de Protección de Datos (GDPR/LGPD):** Dependiendo de la ubicación geográfica de los usuarios simulados, se requiere cumplir con normativas de protección de datos.

### Requisitos Legales para Datos Sensibles:

- **Control de Información Personal:** Dado que se maneja información sensible en un entorno bancario simulado, el sistema debe implementar políticas de privacidad y proteger los datos de manera rigurosa.
- **Auditoría y Documentación:** Implementación de procesos de auditoría y documentación continua que respalden el cumplimiento con la ISO 27001.

## Factibilidad de recursos

La universidad cuenta con recursos de hardware y software necesarios para desarrollar el sistema, incluyendo infraestructura de red y servidores para pruebas. Además, dispone de personal técnico y estudiantes en formación que pueden apoyar en la implementación. No obstante, el éxito del proyecto depende de la disponibilidad de tiempo y dedicación del equipo, ya que se debe completar en un plazo de cuatro meses.

### Recurso Humano:

- **Especialistas en Seguridad Informática:** Expertos en Zero Trust e ISO 27001.
- **Desarrolladores de Software:** Ingenieros con experiencia en aplicaciones web seguras y gestión de identidades.

### Recursos Técnicos:

- **Servidores y Almacenamiento en la Nube:** Necesarios para el procesamiento y la gestión de transacciones de alta seguridad.
- **Herramientas de Monitoreo y Detección de Vulnerabilidades:** Esenciales para una respuesta proactiva a posibles amenazas de seguridad.

## Factibilidad de mercado

El proyecto tiene potencial de aplicabilidad en el sector bancario y en organizaciones interesadas en la ciberseguridad, aunque en este contexto específico es educativo. La implementación del modelo Zero Trust dentro de un entorno simulado puede servir como experiencia práctica para estudiantes, preparando a futuros profesionales en un área de alta demanda en el mercado de la ciberseguridad.

### **Demanda en el Mercado de Simulación Bancaria:**

- **Uso Educativo y Capacitaciones:** Este tipo de sistema podría ser útil para instituciones educativas y corporativas en la capacitación en ciberseguridad bancaria.
- **Interés en Simulaciones Seguras:** La creciente demanda de sistemas de simulación bancaria confiables podría abrir oportunidades de negocio para la plataforma.

### **Competencia en el Mercado:**

- **Sistemas Similares:** Existen otros sistemas de simulación bancaria, pero pocos implementan un enfoque robusto como Zero Trust con ISO 27001, lo cual representa una ventaja competitiva.

## Factibilidad operacional

- **Capacitación del personal:** Los operadores deberán recibir formación en Zero Trust y la norma ISO 27001.
- **Facilidad de implementación:** El sistema debe ser compatible con las operaciones bancarias estándar, y su interfaz será intuitiva para los administradores de seguridad.

## Factibilidad de tiempo

### **Tiempo de Implementación:**

- **Fase de Desarrollo:** Estimación de 6-12 meses para completar el desarrollo del sistema de transacciones y las pruebas de seguridad en un entorno bancario simulado.



- **Certificación ISO 27001:** Dependiendo de la madurez del SGSI, obtener la certificación puede requerir entre 3 y 6 meses adicionales.

### Lanzamiento y Evaluación:

- **Tiempo de Pruebas y Evaluación:** Se sugiere una fase de pruebas de 3 meses para la detección y mitigación de posibles vulnerabilidades.
- **Revisión Continua:** La implementación de Zero Trust requiere una revisión constante para asegurar la efectividad de los controles.

## Recomendaciones y aprobación

- La factibilidad técnica es alta, pero se necesitará asegurar la implementación correcta de Zero Trust y el cumplimiento con ISO 27001:2020 mediante auditorías internas.
- La factibilidad económica es media-alta, con una inversión inicial significativa, pero con un potencial de retorno debido a la seguridad que ofrece en el entorno bancario simulado. El proyecto es viable económicamente, siempre que se mantenga dentro de un presupuesto ajustado y controlado.
- La factibilidad de recursos es alta siempre que se cuente con un equipo capacitado y acceso a tecnología avanzada.
- La implementación es operativamente viable; se recomienda establecer un protocolo de capacitación para el personal.
- La factibilidad legal es alta siempre que se adhiera estrictamente a los estándares de ISO 27001 y se consideren las leyes de protección de datos.
- La factibilidad de tiempo es moderada-alta, con una línea de tiempo proyectada de 9-15 meses, dependiendo de las certificaciones y los recursos.

Aspecto de Factibilidad	Puntaje
Factibilidad técnica	8
Factibilidad económica	9
Factibilidad legal	10
Factibilidad de recursos	11
Factibilidad de mercado	12
Factibilidad operacional	13
Factibilidad de tiempo	8

Con un puntaje promedio alto en los diferentes aspectos de factibilidad, el análisis muestra que el proyecto de implementación de un sistema de transacciones web seguro, basado en el modelo Zero Trust y en la norma ISO 27001:2020, es viable.

Este estudio de factibilidad indica que el sistema de transacciones web seguro es viable en términos técnicos, económicos, legales, de recursos, mercado, operacional y de tiempo. Sin embargo, se recomienda realizar una inversión inicial importante en infraestructura, formación y certificaciones para asegurar el cumplimiento de los estándares de Zero Trust e ISO 27001.

**Link del repositorio:** <https://github.com/DavidAucancela/SecuraBank.git>