Escuela Superior de Guerra ‘General Rafael Reyes Prieto’

Estudio de caso “Cooperativa de ahorro en transición a convertirse en Banco”

Grupo

My. Andres Camilo Aguilar Villamil

My. Elkin Fabian Cubides Puentes

My. John Alexander Serrano Parra

My. Yerson Enrique Suarez Rojas

Gestión de Riesgos

Docente

Dr. Jaider Ospina Navas

Curso de Estado Mayor 2025 – Aula R

marzo de 2025

Estudio de caso “Cooperativa de ahorro en transición a convertirse en Banco”

Introducción

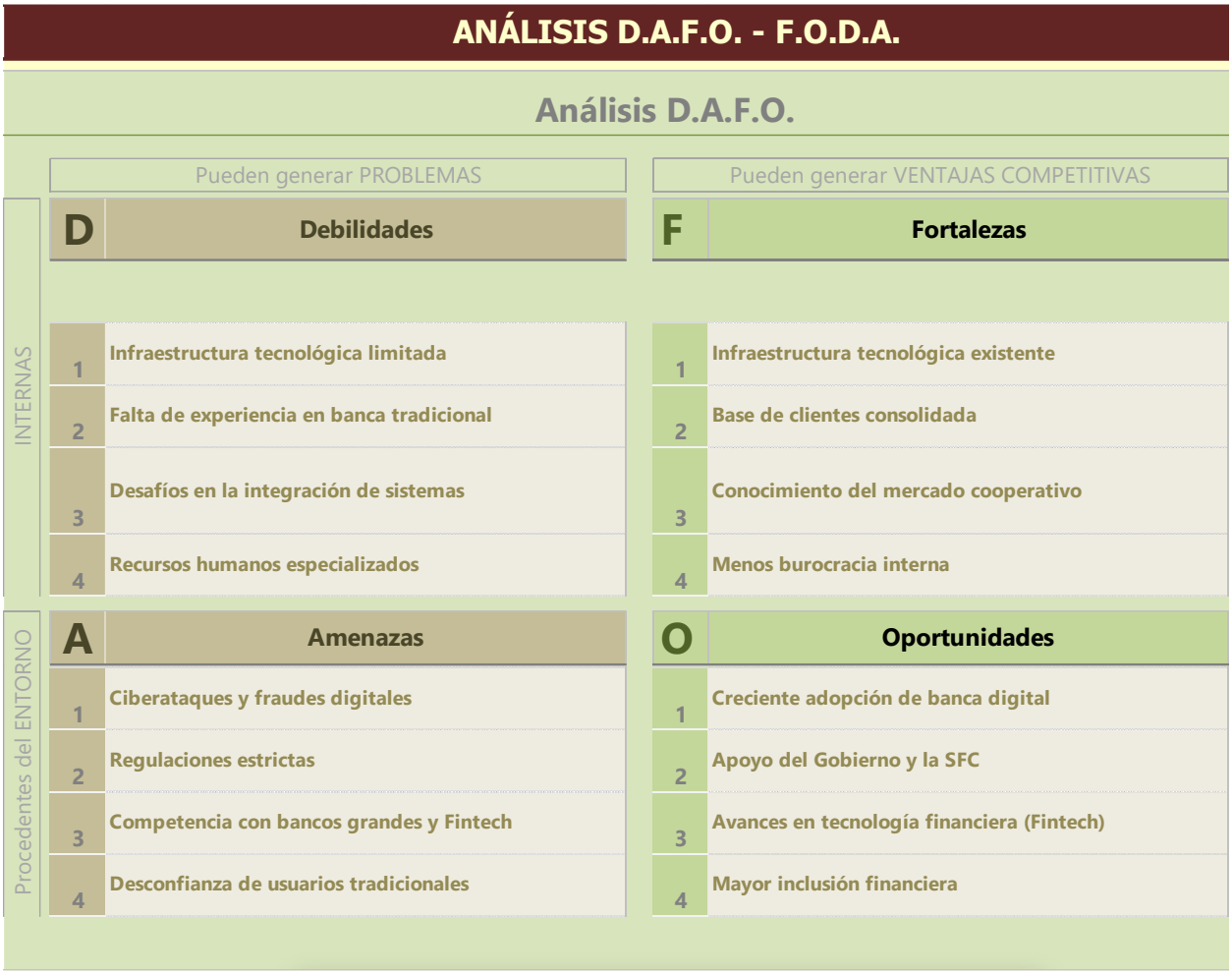
Al definir el escenario se establece que tenemos una cooperativa bajo el nombre de “Cooperativa de modelado de sueños”, organismo mediante el cual se ahorra y se brinda crédito a estudiantes con proyectos justificados que requieran inversión. En su visión de ampliación contempla la posibilidad de evolucionar desde una cooperativa de ahorro hacia una entidad bancaria en Colombia. La República de Colombia y específicamente la Superintendencia Financiera establece que para constituir un banco en Colombia, es necesario cumplir con requisitos establecidos en el Estatuto Orgánico del Sistema Financiero (EOSF) y las directrices de la Superintendencia Financiera de Colombia (SFC) (Superintendencia Financiera, s.f.). Así mismo, referiré que dicho “banco” debe constituirse como una sociedad anónima mercantil o una asociación cooperativa. Esta cooperativa y sus directivos al estar interesados, presentaron una solicitud ante la Superintendencia Financiera, donde fue manifestado dentro de muchas consideraciones, siendo mandatorio y una de las más importantes, la siguiente, “**… deberá demostrarse** la viabilidad del proyecto, respecto a infraestructura tecnológica, esto específicamente enfocado al funcionamiento adecuado de la aplicación móvil, que permita mitigar los potenciales ataques cibernéticos, generar tranquilidad en los usuarios y demostrar una adecuada gestión de riesgos…”

Corolario de lo anterior, se determinó como primera medida realizar una lluvia de ideas o brainstorming entre el equipo de trabajo del CSIRT FINANCIERO y directivos para permitir realizar una determinación del análisis FODA como elemento para evaluar potenciales mejoras en la aplicación móvil.

Desarrollo

1. Diagrama FODA

Producto derivado del brainstorming se obtienen las cuatro (04) principales fortalezas, oportunidades debilidades y amenazas, así:



Fuente: Elaboración propia a partir de tabla suministrada por el Doctor Jaider Ospina

Mediante el cruce de las variables cruzadas, se procede a establecer estrategias ofensivas, defensivas, de reorientación y de supervivencia que permitan cumplir ante la Superintendencia Financiera y ante los clientes, con el propósito de implementar una aplicación viable para la bancarización de la cooperativa, así:

Estrategias - MATRIZ DAFO / FODA

DAFO	Oportunidades	Amenazas
	Creciente adopción de banca digital	Ciberataques y fraudes digitales
	Apoyo del Gobierno y la SFC	Regulaciones estrictas
	Avances en tecnología financiera (Fintech)	Competencia con bancos grandes y Fintech
	Mayor inclusión financiera	Desconfianza de usuarios tradicionales
Fortalezas	**Estrategias OFENSIVAS**	**Estrategias DEFENSIVAS**
Infraestructura tecnológica existente	1 Generar un plan de gestion de infraestructura	1 Generar verificación con consultores respecto a la infrestructura requerida
Base de clientes consolidada	2 Difusión en medios de comunicación de la gestión a realizar para generar tranquilidad	2 Realizar escaneo y verificación al sistema existente
Conocimiento del mercado cooperativo	3 Utilizar metodos agiles de gestion de proyectos para evaluar el seguimiento dedicado al mismo	3 Creación y evolución del plan de gestion de riesgos
Menos burocracia interna	4 Usar recursos de la aplicación para la parte administrativa	4 Establecer nuevas regulaciones que completen las existentes en ciberseguridad
Debilidades	**Estrategias REORIENTACIÓN**	**Estrategias SUPERVIVENCIA**
Infraestructura tecnológica limitada	1 Compra de hardware requerido	1 Actualizar permanentemente los incidentes y ataques de acuerdo a factores publicos; realizar simulaciones de actuacion ante ataques
Falta de experiencia en banca tradicional	2 Capacitación respecto a condiciones requeridas en banca tradicional	2 Estudiar las memorias anuales de ataques e incidentes de las CSIRT FINANCIERAS publicas y desarrollar un modelo de Gestion del Conocimiento
Desafíos en la integración de sistemas	3 Estudio de activos informaticos respecto a la posible adaptacion de lo existente	3 Seguimiento al plan de gestion y actualizacion de hardware
Baja difusión y promoción de políticas de gestión de la información / comunicaciones	4 Elaborar un plan de gestion de las comunicaciones	4 Realizar actualizaciones permanentes de acuerdo al plan de gestion del conocimiento.

Fuente: Elaboración propia a partir de tabla suministrada por el Doctor Jaider Ospina

1. Identificación de las amenazas.

Derivado de las estrategias implementadas como son el escaneo periódico al sistema existente, asesoría por parte de la Superintendencia Financiera, otros consultores contratados para tal fin y el estudio de las memorias anuales de ataques e incidentes proporcionados por la ASOBANCARIA, se determinó que la aplicación móvil contaba con siete (7) potenciales amenazas con incidencias medias y altas, que representan restricciones hacia la certificación.

Ataque de ransomware
Robo de credenciales
Accesos no autorizados a datos sensibles
Interrupción del servicio por ataques DDoS

Fuga de información por mala configuración de hardware y software

Fallas en la integración con otros sistemas bancarios

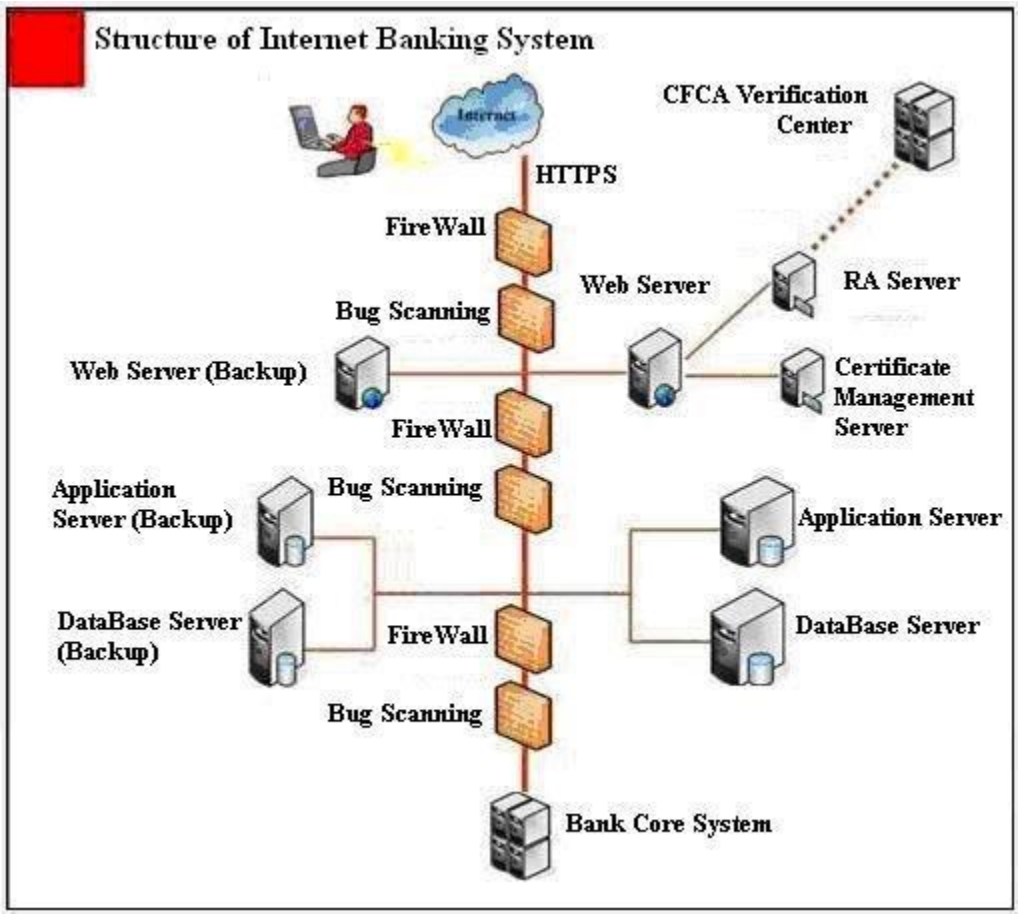
Suplantación de identidad en transacciones

2. Matriz de riesgos (amenaza, probabilidad, impacto, mitigación).

Amenaza	Probabilidad	Impacto	Mitigación
Ataque de malware o ransomware	Alta	Crítico	Implementación de firewalls y antivirus avanzados, copias de seguridad frecuentes.
Phishing y robo de credenciales	Media	Alto	Autenticación multifactor (MFA) y educación en ciberseguridad para los usuarios.
Accesos no autorizados a datos sensibles	Media	Alto	Cifrado de datos, control de acceso y monitoreo en tiempo real.
Interrupción del servicio por ataques DDoS	Alta	Crítico	Sistemas de prevención de DDoS y monitoreo de tráfico en servidores.
Fuga de información por mala configuración	Media	Alto	Configuración segura en bases de datos y políticas de acceso restringido.
Suplantación de identidad en transacciones	Alta	Crítico	Validaciones avanzadas de identidad y alertas en transacciones sospechosas.
Fallas en la integración con sistemas bancarios	Media	Medio	Monitoreo de integraciones, redundancia y validaciones en APIs bancarias.

Fuente: Elaboración propia a partir de tabla suministrada por el Doctor Jaider Ospina

3. Diagramas de arquitectura de seguridad.



Fuente: (Gong, 2011)

4. Identificación de las amenazas.

Posterior a las primeras verificaciones por parte de personal recientemente contratado para la gestión del riesgo y la evolución de la aplicación se determinó mediante el Scanner del sistema que las amenazas eran mas delicadas de lo diagnosticado en un primer momento, para lo cual se estableció mediante el modelo STRIDE el modelado e identificación de amenazas, así:

Categoría STRIDE	Amenaza	Probabilidad	Impacto	Mitigación	Estado actual
Spoofing (Suplantación de identidad)	Suplantación de identidad en transacciones	Media-Alta	Crítico	Autenticación multifactorial (MFA), validaciones avanzadas de identidad	Se encontraba implementándose autenticación únicamente mediante usuario y contraseña
Tampering (Alteración de datos)	Vulnerabilidad en la aplicación móvil	Media-Alta	Crítico	Pruebas de seguridad, auditorías de código, actualizaciones frecuentes	Al utilizar técnicas y herramientas de Scanner se detectó problemas en las generaciones de código al olvidar la contraseña
Repudiation (Repudio de transacciones)	Falta de trazabilidad en transacciones electrónicas	Media	Alto	Registro detallado de transacciones, mecanismos de auditoría	La migración de datos era transferida a archivos. XLSx en un sistema externo que evidenciaba vulnerabilidades en la transferencia y perdida de datos

Information Disclosure (Divulgación de información)	Fuga de información por mala configuración	Media	Alto	Configuración segura en bases de datos, cifrado de datos sensibles	Se tenían diferentes versiones en las actualizaciones de software propio y problemas de parches.
Denial of Service (Denegación de servicio)	Interrupción del servicio por ataques DDoS	Media	Media	Sistemas de prevención de DDoS, monitoreo de tráfico	Eran públicas las direcciones IP de los firewalls físicos del componente de red.
Elevation of Privilege (Elevación de privilegios)	Accesos no autorizados a datos sensibles	Media-Baja	Alto	Cifrado de datos, control de acceso, monitoreo en tiempo real	Problemas en el cifrado de datos desde la aplicación.

Fuente: Elaboración propia

5. Políticas de seguridad propuestas y controles a implementar.

Gestión de Accesos y Control de Identidad: Se deben implementar mecanismos de autenticación robustos, como la autenticación multifactor (MFA), para prevenir accesos no autorizados (ISO/IEC 27001, 2022). Mitigación: Reduce riesgos de suplantación de identidad y accesos indebidos.

Cifrado de Información: Se deben cifrar datos en tránsito y en reposo mediante protocolos como AES-256 y TLS 1.2 o superior (ISO/IEC 27001, 2022). Mitigación: Previene la divulgación de información en caso de interceptación o robo de datos.

Seguridad en Aplicaciones: Implementación de pruebas de seguridad en el desarrollo de software, como análisis de vulnerabilidades y pruebas de penetración periódicas (ISO/IEC 27001, 2022). Mitigación: Reduce el riesgo de explotación de fallas en la aplicación móvil y los sistemas informáticos.

Protección contra Malware: Se deben instalar y mantener actualizados sistemas de detección de malware y antivirus en todos los dispositivos y servidores (ISO/IEC 27001, 2022). Mitigación: Previene ataques de malware y ransomware que puedan comprometer la operatividad de la entidad.

Gestión de Incidentes de Seguridad de la Información: Se debe establecer un proceso de respuesta ante incidentes, incluyendo monitoreo en tiempo real y análisis forense posterior (ISO/IEC 27001, 2022). Mitigación: Mejora la capacidad de detección y respuesta ante ataques cibernéticos.

Continuidad del Negocio y Respaldo de Datos: Implementación de planes de recuperación ante desastres (DRP) y respaldo de información en múltiples ubicaciones seguras (ISO/IEC 27001, 2022). Mitigación: Asegura la recuperación rápida de los servicios en caso de fallas o ataques.

Adicionalmente se propone dentro del plan de gestión del riesgo vincular una serie de actividades complementarias generales, que sean aplicables permanentemente como políticas establecidas para fortalecer la ciberseguridad. Donde destacan el utilizar hardware independiente de otros dispositivos de procesamiento de información, generar informes de vulnerabilidades al menos dos veces al año, remediar las vulnerabilidades detectadas proponiendo plazos cortos, analizar las vulnerabilidades y compararlas con informes anteriores, utilizar herramientas homologadas por el CVE, contar con sistemas de detección de incendios en la infraestructura de hardware y por último cumplir con la regulación PCI DSS.

Conclusiones

La implementación de controles de seguridad basados en la normatividad ISO/IEC 27001 y 27002, se establece junto con los marcos NIST y CIS, que combinados proporcionan una base sólida para proteger la infraestructura tecnológica de la cooperativa en su transición a banco.

De lo anteriormente expuesto, la gestión de accesos y autenticación robusta garantiza que solo usuarios autorizados accedan a los sistemas como el mecanismo mas importante que brinda garantías a los usuarios, lo cual es complementado con el cifrado de información en las diferentes capas de la red, lo cual protege los datos sensibles de estos clientes contra aquellos accesos no autorizados.

Es complementario a lo anterior definir, el protocolo, horarios, y otros factores que conlleven a conducir las pruebas de seguridad en aplicaciones, permitiendo detectar y corregir vulnerabilidades antes de que sean explotadas. Dichas protecciones, brindan protección contra malware y el potencialmente más peligroso randsomware el cual previene infecciones que podrían comprometer la operatividad del banco.

Como recomendación final, se acentúa la idea de evaluar constantemente la gestión de incidentes mejorando la capacidad de respuesta ante ataques, reduciendo el impacto en la continuidad del negocio y ejerciendo desde el CSIRT financiero juegos y desafíos que aseguren la continuidad del negocio, con respaldo suficiente que asegure la recuperación rápida de la información y de los sistemas ante desastres tecnológicos.

Recomendaciones

Para fortalecer la seguridad de la información en la cooperativa es vinculante resaltar la importancia de implementar programas de formación en ciberseguridad para todos los empleados, realizar auditorías regulares de seguridad de la información, propender por implementar herramientas que permitan el monitoreo continuo y respuesta automatizada ante incidentes, colaborar con expertos en ciberseguridad para mantenerse actualizado en las mejores prácticas y amenazas emergentes.

Adicionalmente es sugerido, implementar una matriz RACI que complemente el Plan de Gestión de Riesgos y el Plan de Gestión de las Comunicaciones basados en el marcos de Gestión de proyectos, bajo un esquema general como el siguiente.

Control de Seguridad	Responsable (R)	Aprobador (A)	Consultado (C)	Informado (I)
Gestión de Accesos	Seguridad TI	CIO	Auditoría	Usuario

Cifrado de Datos	Seguridad TI	CIO	Cumplimiento	Auditor
Seguridad en App	Desarrollo TI y CSIRT Financiero	CIO	Seguridad TI	Auditor
Protección Malware	Seguridad TI	CIO	Cumplimiento	Usuario
Gestión de Incidentes	Seguridad TI	CIO	Auditoría	Toda la organización
Continuidad del Negocio	Seguridad TI	CIO	Cumplimiento	Toda la organización

Referencias

CIS. (2021). CIS Controls v8. Center for Internet Security.

Gong, X. (2011). Application of PKI in Encrypting Communications and Verifying Identities of Users in the Internet Banking. *International Journal of Wireless and Microwave Technologies*.

ISO/IEC 27001. (2022). Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos. International Organization for Standardization.

ISO/IEC 27002. (2022). Tecnología de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información. International Organization for Standardization.

NIST. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5). National Institute of Standards and Technology.

Superintendencia Financiera. (s.f.). Superfinanciera.

Superintendencia Financiera de Colombia. (s.f.). Taxonomia Unica de Incidentes Ciberneticos.