**Informe de Seguridad: Plataforma Digital Bancaria**



**Alumnos**

My. Andres Camilo Cotes Cadena

My. Miguel David Giraldo Gaitan

My. Danilo Saba Corredor

My. Diego Hernando Rivas Camacho

**Docente**

Jaider Ospina Navas

**Gestión de Riesgos Cibernéticos**

**Escuela Superior de Guerra**

**Bogotá D.C 25 de febrero 2025**

**Introducción**

En la era digital, los bancos han evolucionado significativamente, adoptando plataformas digitales para ofrecer servicios bancarios a sus clientes. Esta evolución ha facilitado el acceso a las finanzas, ha mejorado la eficiencia operativa y ha proporcionado una experiencia de usuario más fluida. Sin embargo, esta digitalización también ha traído consigo una serie de riesgos cibernéticos que deben ser analizados y gestionados adecuadamente

La presente evaluación de seguridad establece el alcance del análisis, situando el estudio en el contexto de la seguridad de una infraestructura digital critica, como es el caso de una plataforma bancaria.

Se destaca la importancia de la seguridad en el sector financiero, donde la confianza de la información es fundamentales para el funcionamiento de la economía y la protección de datos sensibles de los clientes. Además, se menciona la metodología STRIDE, lo cual es crucial ya que este modelo permite identificar de forma sistémica las amenazas en seis categorías (Spoofing, Tampering, Repudiation, Información Disclosure, Denia lof Service y Elevation of Privilege). Esta aproximación estructurada no solo facilita la detección de vulnerabilidades, sino que también ayuda a priorizar las acciones de mitigación. En este sentido, la introducción podría ampliarse resaltando la relevancia del análisis en el contexto actual, donde los ciberataques a las instituciones financieras están aumentando y la ciberseguridad se ha convertido en una prioridad estratégica.

1. **Identificación de Amenazas**

A continuación, se detallan las amenazas identificadas en cada una de las categorías de STRIDE para un banco de plataforma digital:

**a. Spoofing (Suplantación de Identidad)**

**Descripción:** La suplantación ocurre cuando un atacante engaña a un sistema para que crea que un usuario es alguien a quien no debería permitir el acceso.

**Ejemplos de Amenazas:**

* + Acceso no autorizado mediante el uso de credenciales robadas.
  + Uso de técnicas de phishing para obtener datos de inicio de sesión de clientes.
  + Creación de cuentas falsas que parecen legítimas.

**b. Tampering (Manipulación de Datos)**

**Descripción:** La manipulación involucra la modificación no autorizada de datos.

**Ejemplos de Amenazas:**

* + Alteración de transacciones financieras durante la transmisión.
  + Modificación de la información de las cuentas de los usuarios en la base de datos.
  + Inserción de código malicioso en las aplicaciones móviles o web.

**c. Repudiation (Repudio)**

**Descripción:** El repudio se produce cuando un usuario niega haber realizado una acción, lo que puede complicar la identificación de responsabilidades.

**Ejemplos de Amenazas:**

* + Un usuario legítimo niega haber realizado una transacción, argumentando que su cuenta fue comprometida.
  + Falta de registros de auditoría o logs que muestren claramente las acciones realizadas por los usuarios.

**d. Information Disclosure (Divulgación de Información)**

**Descripción:** La divulgación involucra la exposición de datos sensibles a individuos no autorizados.

**Ejemplos de Amenazas:**

* + Acceso indebido a datos personales de los clientes, como números de tarjetas de crédito o información de cuentas.
  + Vulnerabilidades en la aplicación que permiten la filtración de información.
  + Ataques de inyección SQL que permiten a los atacantes extraer datos de la base de datos.

**e. Denial of Service (Denegación de Servicio)**

**Descripción:** La denegación de servicio se refiere a ataques diseñados para hacer que un servicio no esté disponible para los usuarios legítimos.

**Ejemplos de Amenazas:**

* + Ataques DDoS (Distributed Denial of Service) que sobrecargan los servidores del banco.
  + Fallos en el sistema o caídas del servidor que impiden a los clientes acceder a sus cuentas.
  + Ataques que provocan tiempos de inactividad en los servicios de la aplicación.

**f. Elevation of Privilege (Elevación de Privilegios)**

**Descripción:** La elevación de privilegios ocurre cuando un usuario obtiene acceso no autorizado a recursos que normalmente estarían restringidos.

**Ejemplos de Amenazas:**

* + Un atacante que explota una vulnerabilidad para obtener permisos de administrador.
  + Uso indebido de privilegios por parte de empleados del banco, lo que lleva a accesos no autorizados a datos sensibles.
  + Código malicioso que permite a los atacantes ejecutar acciones que normalmente están restringidas.

1. **Matriz De Riesgos**

A continuación, se presenta un formato estructurado para la evaluación de riesgos en un banco de plataforma digital, que incluye un resumen de las amenazas, probabilidades, impactos, medidas de mitigación y un análisis general. Esta evaluación servirá como guía para priorizar acciones de seguridad y para la gestión de riesgos en ciberseguridad.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Amenaza | Probabilidad | Impacto | Modificación | Índice de Riesgo | Mitigación |
| Suplantación de identidad | Alta | Alto | Alto | Alto | Implementar autenticación multifactor (MFA), educación sobre phishing, y monitoreo continuo de acceso. |
| Manipulación de datos | Media | Alto | Alto | Alto | Usar conexiones seguras (SSL/TLS), realizar auditorías y validar las transacciones. |
| Repudio | Media | Medio | Medio | Medio | Mantener registros de auditoría claros y seguros, implementar soluciones de trazabilidad. |
| Divulgación de información | Alta | Alto | Alto | Alto | Establecer controles de acceso, encriptar datos sensibles y realizar pruebas de seguridad periódicas. |
| Denegación de servicio | Alta | Alto | Alto | Alto | Implementar soluciones anti-DDoS y garantizar redundancia de servicios y servidores. |
| Elevación de privilegios | Media | Alto | Alto | Alto | Realizar auditorías de accesos, aplicar el principio de menor privilegio y monitorear el acceso a datos sensibles. |

**Índice de Riesgo**: Se asigna un índice que puede ser **Bajo**, **Medio** o **Alto** según la combinación de la probabilidad y el impacto de la amenaza. Esto ayuda a priorizar la atención y los recursos para la mitigación.

La evaluación de riesgos es una parte crucial del proceso de gestión de ciberseguridad para un banco digital. La identificación de amenazas específicas, junto con sus probabilidad e impacto, permite a la organización priorizar la mitigación de riesgos y asignar recursos de manera más efectiva. Implementar medidas de mitigación proactivas no solo protegerá los activos de información del banco, sino que también contribuirá a mantener la confianza de los clientes en una era donde las amenazas cibernéticas están en constante evolución.

La periodicidad de la revisión y actualización de esta evaluación es fundamental para adaptarse a nuevos desafíos y amenazas emergentes.

1. **Análisis DREAD**

Como Complemento a la matriz de riesgo, se ha implementado el análisis DREAD, el cual permite asignar una puntuación a cada amenaza en función de cinco dimensiones criticas. Cada dimensión se puntúa de 1 a 10, sumándose para obtener un valor total que ayuda a priorizar la mitigación.

* Damage Potencial (Potencial de Daño): Evalua el impacto que tendría la amenaza sobre la confidencialidad, integridad y disponibilidad del sistema.
* Reproducibility (Reproducibilidad): Mide la facilidad con la que un atacante puede repetir el ataque.
* Exploitability (Explotabilidad): Determina la facilidad de la explotación de la vulnerabilidad.
* Affected Users (Usuarios afectados): Considera el numero de usuarios que podrían verse comprometidos.
* Discoverability (Facilidad de Descubrimiento): Mide la facilidad con la que se pueden detectar la vulnerabilidad.

Ejemplo para la amenaza Spoofing

* Damage Potential: 8
* Reproducibility: 6
* Exploitability: 7
* Afected Users: 8
* Discoverability: 8
* Puntuación Total: 8+6+7+8+8=37/50

Este puntaje indica que el riesgo de Spoofing es critico y requiere medidas de mitigación urgentes. Se aplicara un énfasis similar para cada amenaza (Tampering, Repudiation, Information Disclosure, Denia of service y Elevation of Privilege), lo que me permite priorizar los riesgos de manera objetiva y ajustar las estrategias de mitigación según la criticidad evaluada.

1. **Diagrama de Arquitectura de Seguridad General**

**Descripción:**  
Este diagrama proporciona una visión general de los componentes del sistema y su interconexión, así como las capas de seguridad implementadas.



**Componentes Clave:**

* **Aplicación Móvil/Web:** Interfaz a través de la cual los usuarios interactúan con el banco.
* **API Gateway:** Punto de acceso para las solicitudes y respuesta entre cliente y servicios.
* **Servidor de Seguridad:** Firewalls, sistemas de detección y prevención de intrusos (IDS/IPS).
* **Sistema de Monitoreo de Seguridad (SIEM):** Herramienta para la recolección y análisis de eventos de seguridad.

**Diagrama de Flujo de Datos**

**Descripción:**  
Este diagrama ilustra cómo fluyen los datos a través del sistema del banco digital y los procesos involucrados en la interacción del usuario.



**Componentes Clave:**

1. **Validación de Usuario:** Proceso donde se verifica la identidad del usuario a través de la autenticación.
2. **Acceso a Datos:** Las solicitudes de datos se dirigen al servidor de bases de datos.
3. **Acceso a Servicios:** Los servicios del banco se invocan y se procesan.
4. **Salida de Datos:** Las respuestas se envían de vuelta al usuario.

**Políticas de Seguridad Propuestas**

**Política de Autenticación y Control de Acceso**

**Objetivo:** Garantizar que solo los usuarios autorizados puedan acceder a sistemas y datos críticos.

**Directrices:**

* + Implementar autenticación multifactor (MFA) para todos los accesos a sistemas sensibles.
  + Aplicar el principio de menor privilegio, asegurando que los usuarios solo tengan acceso a los recursos necesarios para realizar sus funciones.
  + Revisar periódicamente los permisos de acceso y realizar auditorías de cuentas de usuario.

**Política de Protección de Datos**

**Objetivo:** Proteger la información sensible de clientes y empleados contra fugas o accesos no autorizados.

**Directrices:**

* + Encriptar datos sensibles tanto en reposo como en tránsito.
  + Implementar controles de acceso basado en roles para asegurar que solo el personal autorizado pueda acceder a datos críticos.
  + Realizar backups regulares y mantener un plan de recuperación ante desastres.

**Política de Respuesta a Incidentes**

**Objetivo:** Establecer un marco para la respuesta efectiva a incidentes de seguridad cibernética.

**Directrices:**

* + Crear un equipo de respuesta a incidentes (IRT) responsable de manejar y mitigar incidentes de seguridad.
  + Desarrollar procedimientos claros para la identificación, contención, erradicación y recuperación de incidentes.
  + Realizar simulaciones de incidentes y entrenamientos regulares para asegurar la preparación del equipo.

1. **Política de Seguridad de la Red**

**Objetivo:** Proteger la infraestructura de red y los sistemas de información contra ataques y accesos no autorizados.

**Directrices:**

* + Implementar firewalls, sistemas de detección y prevención de intrusos (IDS/IPS) y segmentación de red.
  + Monitorear y registrar el tráfico de la red en tiempo real para detectar actividades sospechosas.
  + Establecer conexiones seguras (VPN) para acceso remoto a la red interna.

**Política de Educación y Concienciación en Seguridad**

**Objetivo:** Cultivar una cultura de seguridad entre todos los empleados y usuarios del banco.

**Directrices:**

* + Proporcionar capacitación regular sobre amenazas cibernéticas, mantenimiento de la seguridad de la información y mejores prácticas.
  + Realizar campañas de concienciación sobre phishing y otras técnicas de ingeniería social.
  + Evaluar el conocimiento de los empleados a través de simulaciones y evaluaciones periódicas.

**Política de Evaluación y Gestión de Riesgos**

**Objetivo:** Identificar, evaluar y gestionar riesgos cibernéticos en un enfoque continuo.

**Directrices:**

* + Realizar evaluaciones de riesgos periódicas para identificar nuevas amenazas y vulnerabilidades.
  + Desarrollar un plan de acción para mitigar los riesgos identificados y evaluar la efectividad de las medidas implementadas.
  + Documentar y revisar la política de gestión de riesgos anualmente, actualizando las estrategias según sea necesario.

Estas políticas de seguridad son fundamentales para establecer una base sólida en la estrategia de ciberseguridad de un banco de plataforma digital. La implementación efectiva y el cumplimiento de estas políticas ayudarán a proteger al banco y a sus clientes contra una amplia variedad de amenazas cibernéticas. Además, es recomendable revisar y actualizar estas políticas regularmente para garantizar que sigan siendo efectivas ante un panorama de amenazas en constante cambio.

**Diseño de Controles de Seguridad**

**Controles de Acceso**

**Autenticación Multifactor (MFA):**

* + **Descripción:** Requiere que los usuarios proporcionen al menos dos formas de verificación para acceder a los sistemas.
  + **Implementación:** Utilizar métodos como contraseñas, tokens de hardware o autenticación biométrica.

**Control de Acceso Basado en Roles (RBAC):**

* + **Descripción:** Asigna permisos de acceso a usuarios según su rol en la organización.
  + **Implementación:** Crear perfiles de usuario y asignar privilegios mínimos necesarios para realizar funciones específicas.

**Revisión y Auditoría de Accesos:**

* + **Descripción:** Monitorear y revisar los accesos a los sistemas críticos.
  + **Implementación:** Realizar auditorías trimestrales de los accesos y permisos de cuentas de usuario.

**Controles de Protección de Datos**

**Cifrado de Datos:**

* + **Descripción:** Protege datos sensibles mediante encriptación tanto en reposo como en tránsito.
  + **Implementación:** Utilizar algoritmos de cifrado robustos (como AES) para proteger bases de datos y comunicaciones.

**Clasificación de Datos:**

* + **Descripción:** Categorizar la información según su sensibilidad y riesgo asociado.
  + **Implementación:** Establecer un esquema de clasificación que determine qué datos requieren mayor protección.

**Política de Retención de Datos:**

* + **Descripción:** Define períodos de retención y eliminación de datos conforme a regulaciones y prácticas necesarias.
  + **Implementación:** Establecer procesos automáticos para la eliminación segura de información obsoleta.

**Controles de Red**

**Firewalls y Sistemas de Detección/Prevención de Intrusos (IDS/IPS):**

* + **Descripción:** Filtrar tráfico malicioso y detectar actividades sospechosas.
  + **Implementación:** Configurar firewalls en perímetro y en capas internas, junto con IDS/IPS para monitorear el tráfico de red.

**Segmentación de Red:**

* + **Descripción:** Dividir la red en segmentos para mejorar la seguridad y limitar el movimiento lateral de ataques.
  + **Implementación:** Crear zonas DMZ para servidores públicos y redes internas para sistemas críticos.

**VPN para Acceso Remoto:**

* + **Descripción:** Proporcionar una conexión segura para el acceso remoto a la red interna.
  + **Implementación:** Implementar soluciones VPN que requieran autenticación robusta y cifrado.

**Controles de Monitoreo y Respuesta**

**Sistema de Monitoreo de Seguridad (SIEM):**

* + **Descripción:** Centralizar la recolección y análisis de eventos de seguridad.
  + **Implementación:** Implementar un SIEM para detectar patrones anómalos y alertar a los equipos de seguridad.

**Plan de Respuesta a Incidentes:**

* + **Descripción:** Establecer un protocolo claro para la identificación y manejo de incidentes de seguridad.
  + **Implementación:** Diseñar un plan que incluya roles, responsabilidades y procedimientos para cada etapa de respuesta.

**Simulaciones de Incidentes:**

* + **Descripción:** Realizar pruebas regulares para medir la efectividad del plan de respuesta.
  + **Implementación:** Conducir simulaciones de ataques cibernéticos para evaluar la preparación y mejorar el plan.

**Controles de Educación y Concienciación**

**Capacitación Regular en Seguridad:**

* + **Descripción:** Educar a empleados y usuarios sobre amenazas y buenas prácticas de seguridad.
  + **Implementación:** Proporcionar sesiones de formación semestrales y materiales de referencia.

**Campañas de Concienciación:**

* + **Descripción:** Aumentar la concienciación sobre técnicas de ingeniería social y amenazas emergentes.
  + **Implementación:** Realizar campañas a través de correos electrónicos, carteles y recordatorios en la intranet.

El diseño de controles de seguridad propuesto crea una defensa en profundidad para un banco de plataforma digital. Implementar estos controles ayudará a proteger la infraestructura crítica, asegurará la confidencialidad, integridad y disponibilidad de los datos, y mitigará los riesgos asociados a las amenazas cibernéticas. Es fundamental revisar y actualizar continuamente estos controles según evolucione el entorno de amenazas y se introduzcan nuevas tecnologías.

1. **Matriz DAFO**

Para complementar el análisis de riesgos y controles, se presenta una matriz DAFO que evalua el entorno interno y externo de la plataforma digital Bancaria:

|  |  |
| --- | --- |
| **DAFO** | **ASPECTOS IDENTIFICADOS** |
| Fortalezas | * Infraestructura tecnológica y robusta segmentada * Herramientas de monitoreo avanzadas (Zabbix, SIEM) * Políticas de autenticación y cifrado ya implementadas |
| Debilidades | * Dependencia de sistemas heredados o Software desactualizado * Falta de capacitación continua en ciberseguridad para ciertos empleados * Brechas en la gestión de parches y actualizaciones |
| Oportunidades | * Crecimiento en inversión en seguridad a nivel global. * incorporación de nuevas tecnologías (IA, ML) para mejorar la detección y respuestas de amenazas. * Fortalecimiento de la imagen y confianza mediante certificaciones (ISO 27001). |
| Amenazas | * Aumento en la sofisticación de ataques cibernéticos (Phishing, DDOS, inyecciones). * Amenazas internas derivadas en fallos en la gestión de accesos. * Evolución constante de vulnerabilidades y presión de actores maliciosos. |

Este análisis revela que aunque la base tecnológica y las políticas existentes ofrecen un solida línea de defensa que corresponden a las fortalezas. Es crucial mantener la actualización constante, ya que las limitaciones en capacitación y en la actualización de sistemas pueden generar vulnerabilidades que requieren una estrategia de modernización continua, lo que hace referencia a las debilidades. Además, la integración de tecnologías emergentes y el cumplimiento de estándares internacionales representan oportunidades que pueden mejorar la resiliencia y la confianza en la plataforma, mientras que en el entorno de amenazas, dinámico y en constante evolución, demanda revisión periódicas y un enfoque proactivo en la mitigación de riesgos.

1. **Conclusiones**

La implementación de un sistema de seguridad robusto y efectivo es esencial para la operación de un banco de plataforma digital en el contexto actual, donde las amenazas cibernéticas son cada vez más sofisticadas. A lo largo de este informe, se han identificado y analizado diversas amenazas cibernéticas utilizando el marco STRIDE, se ha elaborado una matriz de riesgos para evaluar la probabilidad, impacto y medidas de mitigación, y se han propuesto políticas y controles de seguridad que abordan de manera integral estos riesgos.

**Identificación de Amenazas:** Se identificaron amenazas críticas, como la suplantación de identidad, la manipulación de datos y la divulgación de información, que presentan altos riesgos para la seguridad del banco digital.

**Evaluación de Riesgos:** La matriz de riesgos permite priorizar acciones de mitigación, destacando áreas donde la probabilidad e impacto de las amenazas son elevados y donde se requiere una atención inmediata.

**Diseño de Controles de Seguridad:** Se presentaron controles de seguridad estratégicos que, al ser implementados, contribuirán a crear un entorno más seguro para las operaciones bancarias digitales y protegerán la información sensible de los clientes.

**Importancia de la Concienciación:** La educación y sensibilización de los empleados y usuarios son fundamentales para prevenir ataques basados en ingeniería social y para fomentar una cultura de seguridad dentro de la organización.

**Recomendaciones**

Con base en las conclusiones anteriores, se proponen las siguientes recomendaciones para fortalecer la seguridad en un banco de plataforma digital:

**Implementar Políticas de Seguridad Efectivas:**

Asegurarse de que todas las políticas de seguridad estén documentadas, comunicadas y sean de obligatorio cumplimiento para todos los empleados y partes interesadas.

**Actualizar y Revisar Regularmente las Evaluaciones de Riesgos:**

Realizar evaluaciones de riesgos periódicas para identificar nuevas amenazas y vulnerabilidades. Esto debe incluir la revisión de controles existentes y la mejora continua de las prácticas de seguridad.

**Fortalecer el Programa de Capacitación en Seguridad:**

Desarrollar programas de capacitación en seguridad más dinámicos y relevantes, incluyendo simulaciones de ataques y talleres prácticos, para preparar mejor a los empleados frente a amenazas.

**Monitoreo y Respuesta a Incidentes:**

Establecer un sistema de monitoreo 24/7 y un equipo de respuesta a incidentes bien entrenado, preparado para abordar y mitigar incidentes de seguridad de manera rápida y eficiente.

**Adoptar Nuevas Tecnologías de Seguridad:**

Considerar la implementación de tecnologías emergentes, como inteligencia artificial y aprendizaje automático, para mejorar la detección de amenazas y la respuesta ante incidentes.

**Fomentar una Cultura de Seguridad:**

Promover una mentalidad de seguridad entre todos los empleados mediante campañas regulares de concienciación y incentivos para aquellos que reporten incidentes o sugieran mejoras.

**Colaborar y Compartir Información:**

Establecer alianzas con otras organizaciones y participar en foros de ciberseguridad para compartir información sobre amenazas y mejores prácticas.

**Conclusión Final**

La seguridad cibernética en un banco de plataforma digital no es solo una responsabilidad del departamento de TI, sino un esfuerzo conjunto que involucra a toda la organización. La implementación de controles robustos, junto con una cultura de seguridad y educación continua, será clave para proteger el patrimonio del banco y mantener la confianza de los clientes en un entorno digital cada vez más complejo.

**Referencias Bibliográficas**

1. **Stallings, W. & Brown, L. (2012).** *Computer Security: Principles and Practice* (3rd ed.). Pearson.
2. **Shostack, A. (2014).** *Threat Modeling: Designing for Security.* Wiley.
3. **NIST (National Institute of Standards and Technology). (2018).** *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1). NIST.
4. **ISO/IEC 27001:2013.** *Information technology — Security techniques — Information security management systems — Requirements.*
5. **OWASP (Open Web Application Security Project). (2021).** *OWASP Top Ten: 2021.* OWASP Foundation.