Estrategias Contra el Fraude Electrónico

Darlin Carolina López Gutiérrez ID 823332

Corporación Universitaria Minuto de Dios

Rectoría Sede Principal

Sede Bogotá D.C. - Sede Principal

Programa Administración de Empresas

agosto de 2024

Estrategias Contra el Fraude Electrónico

Darlin Carolina López Gutiérrez ID 823332

Sistematización presentado como requisito para optar al título de Administrador de Empresas

Asesor(a)

Manuel Ricardo Rey Romero

Docente

Corporación Universitaria Minuto de Dios

Rectoría Virtual y a Distancia

Sede Bogotá Sur

Programa Administración de Empresas

agosto de 2024

Dedicatoria

Este trabajo está dedicado a mi familia, en reconocimiento a su invaluable apoyo y amor incondicional a lo largo de todo el proceso. Su constante motivación y confianza en mis capacidades fueron fundamentales para la realización de este proyecto.

Agradecimientos

En este espacio quiero expresar mi más sincero agradecimiento al docente Manuel Ricardo Rey Romero, cuya guía y asesoría fueron fundamentales para alcanzar este logro. Su paciencia y dedicación han sido invaluables en todo el proceso.

Finalmente, quiero reconocer el apoyo de compañeros cercanos y familiares, así como la ayuda recibida en la toma de datos, el préstamo de literatura y equipo, la preparación de tablas y figuras, las sugerencias útiles, las ideas que ayudaron a interpretar los resultados, y la colaboración en la lectura crítica y corrección del documento.

Contenido

Lista de tablas

Lista de figuras

Lista de anexos

Resumen

Este proyecto aborda el problema de robos en línea que afecta a los clientes del banco AV Villas. Su propósito fue analizar esta problemática y desarrollar un plan de mejora. Se utilizaron encuestas para recolectar datos de los clientes, permitiendo entender mejor el problema. Las principales lecciones aprendidas incluyen la necesidad de fortalecer las medidas de seguridad y educar a los clientes sobre prácticas seguras en línea para reducir el riesgo de robos y aumentar la confianza en los servicios del banco.

Palabras clave:

Seguridad en línea, robos bancarios, encuestas, banco AV Villas, plan de mejora.

Abstract

1. INTRODUCCIÓN

Este documento presenta un proyecto de mejora dirigido a enfrentar una preocupación creciente relacionada con la seguridad en línea de los clientes del Banco AV Villas. En los últimos tiempos, se ha registrado un aumento en los casos de fraude electrónico, que han resultado en transacciones no autorizadas y pérdidas financieras significativas para los clientes. Esta problemática ha puesto de manifiesto vulnerabilidades en la protección de la información confidencial, lo que ha generado una urgente necesidad de revisar y fortalecer las medidas de seguridad del banco.

El objetivo principal de este proyecto es analizar en profundidad los problemas actuales relacionados con la seguridad cibernética y proponer estrategias efectivas para mitigar los riesgos de fraude electrónico. Para lograr esto, el documento se estructura en varias secciones clave:

1. Reseña General de la Organización
2. Área Organizacional de la Propuesta
3. Descripción de la Problemática
4. Pregunta de Investigación
5. Objetivo General
6. Objetivos Específicos
7. Marco Conceptual
8. Marco Legal
9. Árbol de Problemas
10. Estrategia Actual del Banco

Este documento tiene como finalidad no solo identificar y analizar los problemas actuales, sino también ofrecer soluciones prácticas y efectivas para mejorar la seguridad en línea del Banco AV Villas y proteger la información de sus clientes de manera más eficiente.

1.1 Planteamiento del problema

En el Banco AV Villas, se ha observado un preocupante aumento en los casos de fraude electrónico, donde los clientes se convierten en víctimas de robos en línea. La raíz de este problema radica en la divulgación involuntaria de información confidencial por parte de los clientes. Los delincuentes obtienen acceso a datos sensibles, como: Contraseñas y números de tarjeta y códigos CVV (código de valor de verificación)

Entre estos métodos, se incluyen llamadas telefónicas engañosas y sitios web falsos que aparentan ser legítimos. En estas situaciones, los clientes son engañados para que proporcionen su información personal bajo la falsa afirmación de una comunicación oficial o de una oferta atractiva.

Este tipo de fraude ocurre frecuentemente debido a la falta de precaución de los usuarios al manejar su información financiera. Los errores comunes incluyen:

- Proporcionar Información en Respuesta a Llamadas Sospechosa
- Acceder a Sitios Web Falsos
- Desconocimiento de Medidas de Seguridad

Figura 1

Causas y efectos de la problemática

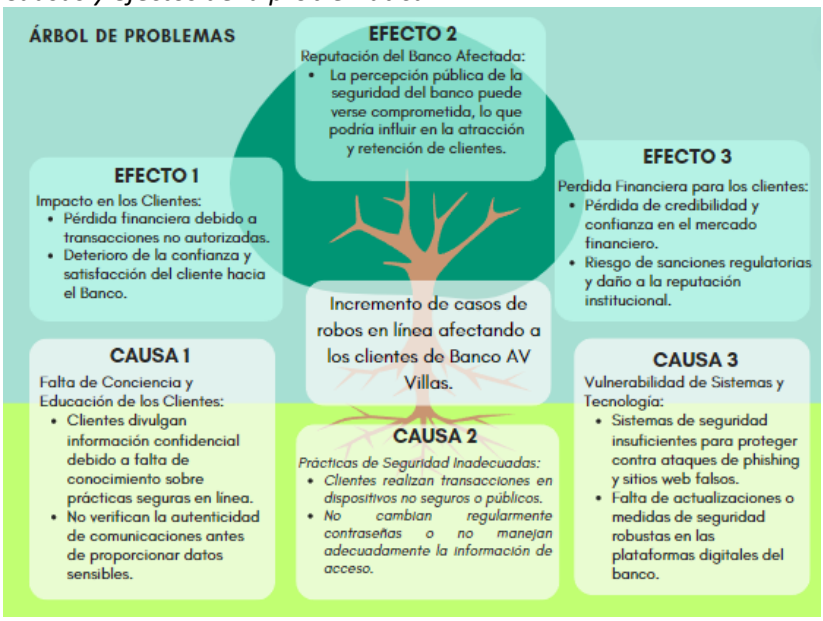

Figura 1. Árbol de Problemas que ilustra las causas y efectos de los robos en línea. El diagrama visualiza las principales causas que conducen a incidentes de fraude electrónico y los efectos resultantes en los clientes y la seguridad financiera.

1.2 Objetivos

Objetivo General

Fortalecer la posición de Banco AV Villas como una entidad financiera confiable y segura, reforzando las medidas de seguridad cibernética y promoviendo la concienciación entre los usuarios sobre prácticas seguras en el uso de servicios bancarios virtuales.

Objetivos Específicos

- Diagnosticar las vulnerabilidades actuales en las medidas de seguridad cibernética del Banco AV Villas para identificar áreas críticas que requieren mejora.
- Analizar las necesidades y comportamientos de los clientes en relación con la protección de datos, para diseñar estrategias efectivas de seguridad y educación.
- Estructurar e implementar medidas de seguridad avanzadas y actualizadas, incluyendo la adopción de tecnologías emergentes y procedimientos mejorados para proteger la información confidencial de los clientes.
- Validar la efectividad de las nuevas medidas de seguridad y programas educativos mediante pruebas y evaluaciones continuas, asegurando que cumplen con los objetivos de reducción de fraudes y fortalecimiento de la confianza del cliente.

1.3 Justificación

La sistematización de este proyecto aborda la creciente problemática de robos en línea que afecta a los clientes del banco AV Villas. Su propósito es mejorar la seguridad bancaria y proteger a los usuarios contra fraudes. El proyecto beneficia directamente a los clientes al proporcionar soluciones para mitigar riesgos, y a la institución al fortalecer sus medidas de seguridad.

La investigación se basa en encuestas para identificar vulnerabilidades y desarrollar estrategias preventivas. Este enfoque garantiza que las soluciones sean efectivas y respondan a las necesidades reales de los clientes.

2. MARCO CONCEPTUAL

Glosario

Se destaca la necesidad de un glosario que facilite la comprensión de la terminología y lenguaje financiero utilizado en el proyecto.

- **Fraude en línea**
- **Phishing:** Los delincuentes intentan obtener información confidencial de los usuarios, como contraseñas o números de tarjeta haciéndose pasar por entidades de confianza a través de correos electrónicos, llamadas mensajes de texto o sitios web falsos.
- **CVV (Código de Valor de Verificación**): Número de tres o cuatro dígitos impresos en las tarjetas de crédito o débito, utilizado como medida de seguridad adicional en transacciones en línea.
- **Pharming:** Técnica de fraude que redirige a los usuarios a sitios web falsos sin su conocimiento.
- **Seguridad Cibernética: Seguridad Cibernética:** Conjunto de tecnologías, procesos y prácticas diseñadas para proteger sistemas, redes y datos contra ataques, daños o acceso no autorizado.
- **Token:** Dispositivo físico o aplicación móvil que genera códigos temporales y únicos utilizados como parte del proceso de autenticación de dos factores.
- **Suplantación de identidad:** Hacerse pasar por otra persona o entidad con el fin de obtener beneficios fraudulentos.
- **Biometría:** Autenticación basada en características físicas o comportamentales únicas de una persona como huellas dactilares, reconocimiento facial o voz.
- **Criptografía:** Técnica matemática utilizada para proteger la información mediante el cifrado de datos para que solo los destinatarios autorizados puedan descifrarlos.
- **URL:** Dirección web que identifica una página específica en internet, utilizada para acceder a sitios web, incluidos los sitios seguros de bancos.
- **UPAC:** Unidad de Poder Adquisitivo Constante es un sistema utilizado para ajustar créditos a la inflación, protegiendo así el poder adquisitivo de los deudores.

3. METODOLOGÍA

Selección de Experiencias: La selección de las experiencias sistematizadas se basó en la identificación de problemas recurrentes en la seguridad en línea del Banco AV Villas, específicamente en los casos de robos electrónicos reportados por clientes. Se optó por esta experiencia debido a su relevancia en el contexto digital actual y su impacto directo en la confianza de los clientes. El proyecto se desarrolló durante un periodo de seis meses, involucrando a diferentes actores clave del banco, lo que permitió un análisis integral del problema y sus consecuencias.

Recopilación de Información: Para recolectar la información necesaria, se emplearon encuestas y entrevistas dirigidas a dos perfiles dentro del banco, como asesores comerciales y subgerentes. Las encuestas se llevaron a cabo los días 8 y 9 de julio de 2024 mediante Google Formularios, permitiendo recopilar datos cuantitativos sobre las percepciones de seguridad. Posteriormente, el 23 de julio de 2024, se realizaron entrevistas más profundas con subgerentes para obtener un análisis cualitativo. Estas herramientas fueron seleccionadas por su eficacia en captar tanto datos estadísticos como impresiones más detalladas sobre el problema.

Análisis de Datos: Los datos recopilados fueron analizados mediante la identificación de patrones y tendencias en las respuestas. Se prestó especial atención a los factores de preocupación, las medidas preventivas propuestas, y las percepciones sobre la información brindada a los clientes. El análisis permitió extraer lecciones clave, como la necesidad de mejorar la educación del cliente y la implementación de sistemas de seguridad más robustos. Las conclusiones generales se centraron en la necesidad de una estrategia integral que abarque tanto la tecnología como la formación del cliente para abordar eficazmente los problemas de seguridad identificados.

4. DESCRIPCIÓN DE LAS EXPERIENCIAS SISTEMATIZADAS

Contexto: En los últimos meses de 2024, la oficina principal del Banco AV Villas en Villavicencio priorizó la seguridad en línea debido a la creciente vulnerabilidad de los clientes ante fraudes electrónicos.

Actores Involucrados: Asesores comerciales y subgerentes participaron en el proceso.

Condiciones Sociales y Económicas: La creciente dependencia de servicios bancarios digitales aumentó los riesgos de fraude, afectando la confianza en el sistema bancario.

Desarrollo y Resultados: Encuestas e entrevistas en julio de 2024 revelaron preocupaciones sobre phishing y la falta de concienciación de los clientes. Se recomendaron mejoras en autenticación y educación para reforzar la seguridad y restaurar la confianza de los clientes.

Tabla 1

Factor preocupante de robos en linea.

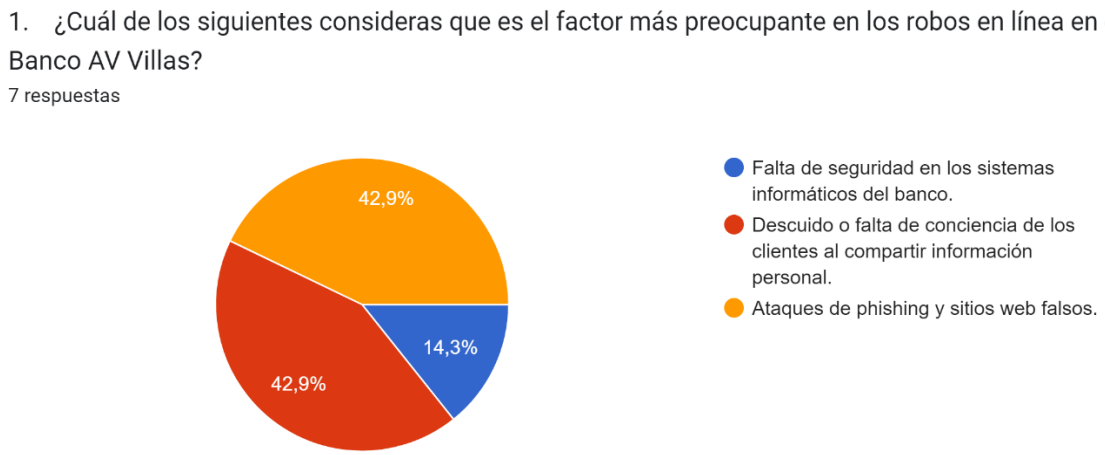

Tabla 1. La encuesta revela que los encuestados están divididos en cuanto a los factores más preocupantes en los robos en línea. Un 42.9% considera que los ataques de phishing y sitios web falsos son la principal preocupación, mientras que otro 42.9% señala el descuido de los clientes al compartir información personal como un factor de gran preocupación. En contraste, solo un 14.3% menciona la falta de seguridad en los sistemas informáticos del banco como un factor principal de inquietud.

Tabla 2

Medidas más efectivas para prevenir robos en línea.

Tabla 2. La mayoría de los encuestados (71.4%) cree que implementar sistemas de autenticación más robustos y medidas de seguridad adicionales sería la medida más efectiva para prevenir robos en línea en Banco AV Villas. Un 14.3% sugiere mejorar la educación de los clientes sobre prácticas seguras en línea, mientras que otro 14.3% considera crucial reforzar la vigilancia y detección de actividades fraudulentas por parte del banco.

Tabla 3

Nivel de información para protegerse contra fraudes en línea en Banco AV Villas.

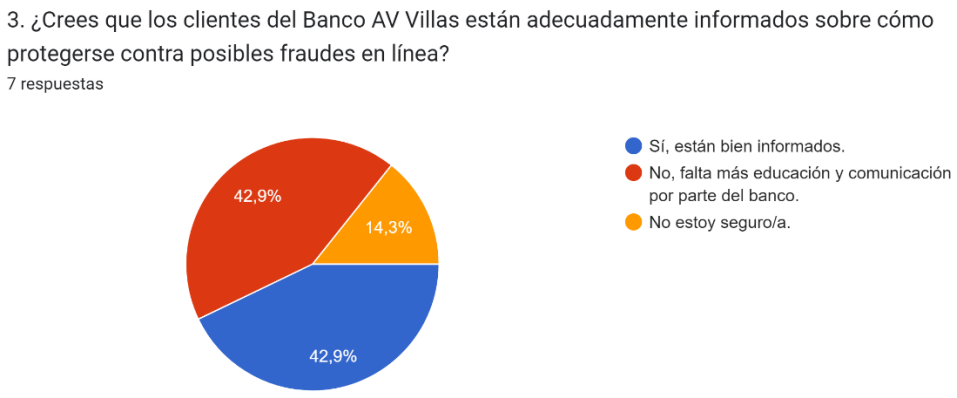

Tabla 3. Los resultados muestran que hay opiniones divididas: el 42.9% cree que los clientes del Banco AV Villas están adecuadamente informados sobre cómo protegerse contra fraudes en línea, otro

42.9% considera que falta más educación y comunicación por parte del banco, y un 14.3% no está seguro/a sobre el nivel de información de los clientes.

Tabla 4

Opiniones de los clientes sobre la respuesta del Banco AV Villas ante casos de fraude reportados.

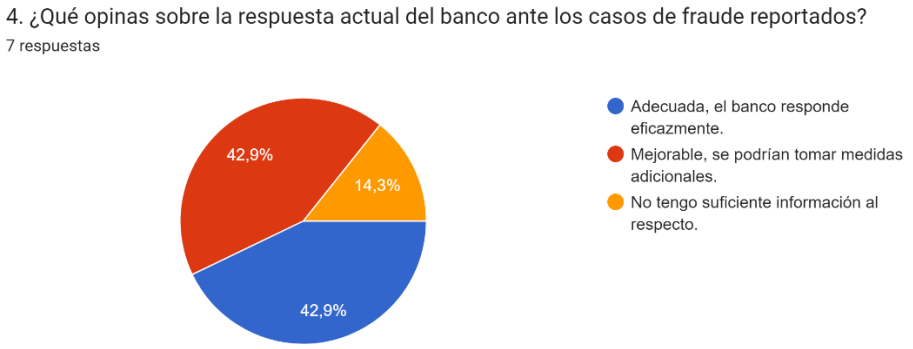

Tabla 4. Los resultados muestran opiniones divididas: el 42.9% está satisfecho con la respuesta actual del Banco AV Villas ante casos de fraude, otro 42.9% sugiere tomar medidas adicionales para mejorarla, y un 14.3% no tiene suficiente información para evaluarla.

Tabla 5

Propuestas de los clientes para mejorar la seguridad y prevenir fraudes en línea.

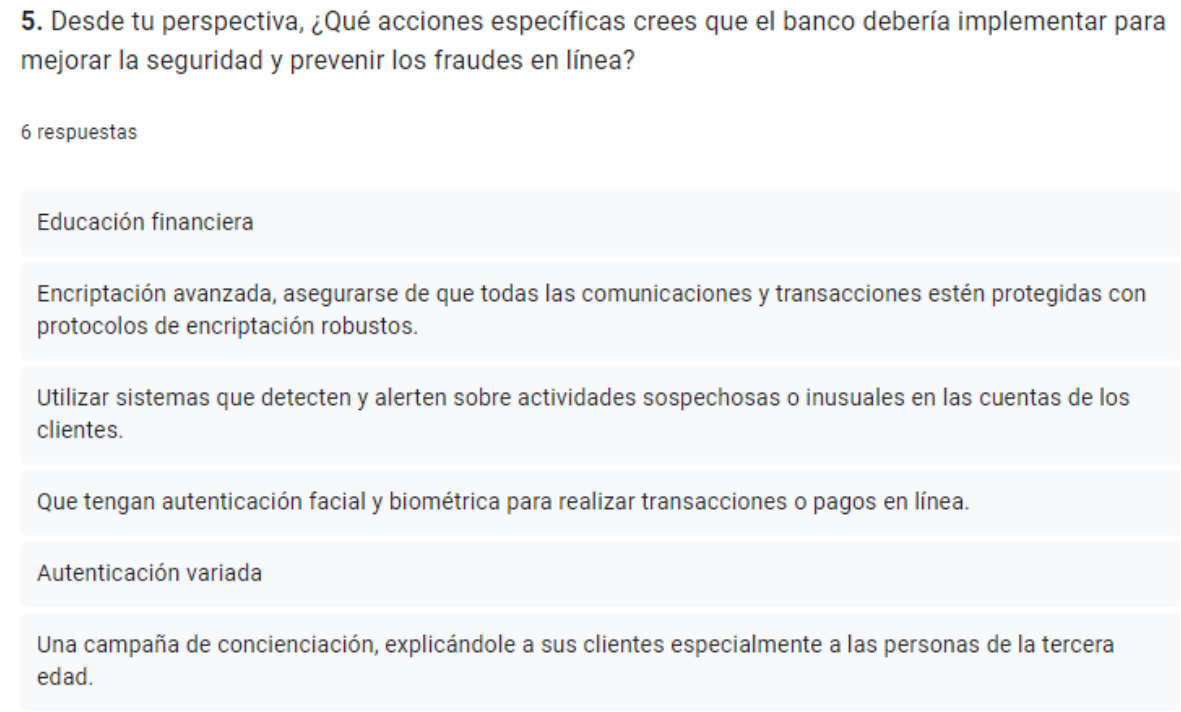

Tabla 5. Los encuestados proponen varias acciones para mejorar la seguridad y prevenir fraudes en línea en Banco AV Villas: educación financiera, encriptación avanzada, sistemas de detección de actividades sospechosas, autenticación biométrica, autenticación variada y una campaña de concienciación dirigida a personas mayores.

Tabla 6

Impacto percibido de los robos en línea y fraudes financieros en la confianza de los clientes hacia Banco AV Villas

6.En tu opinión, ¿Qué impacto crees que tienen los robos en línea y los fraudes financieros en la confianza de los clientes hacia el Banco AV Villas?

6 respuestas

Desconfianza a su sistema
Daño a la reputación, los incidentes de fraude pueden dañar la reputación del banco, afectando no solo a los clientes actuales, sino también a potenciales nuevos clientes que pueden optar por otros bancos con mejores registros de seguridad.
Además de la pérdida directa de fondos, los bancos pueden enfrentar costos adicionales relacionados con la investigación del fraude, la compensación a los clientes afectados y la implementación de nuevas medidas de seguridad.
Grande porque las personas dicen que el banco es quien se roba el dinero.
Mala reputación
Se pierde credibilidad cuando un funcionario del banco llama para ofrecer los productos, debido a que las personas que han sido víctimas cuentan su experiencia y mala fama de la entidad financiera.

Tabla 6. Según las personas encuestadas dicen que los robos en línea y los fraudes financieros tienen un efecto significativo en la confianza hacia el Banco AV Villas. Estos incidentes pueden generar desconfianza generalizada en el sistema bancario, afectar negativamente la reputación del banco y resultar en una pérdida de credibilidad entre los clientes, especialmente aquellos que han sido directamente afectados por fraudes.

Figura 2

Factores Clave en el Incremento de Casos de Robos en Línea.

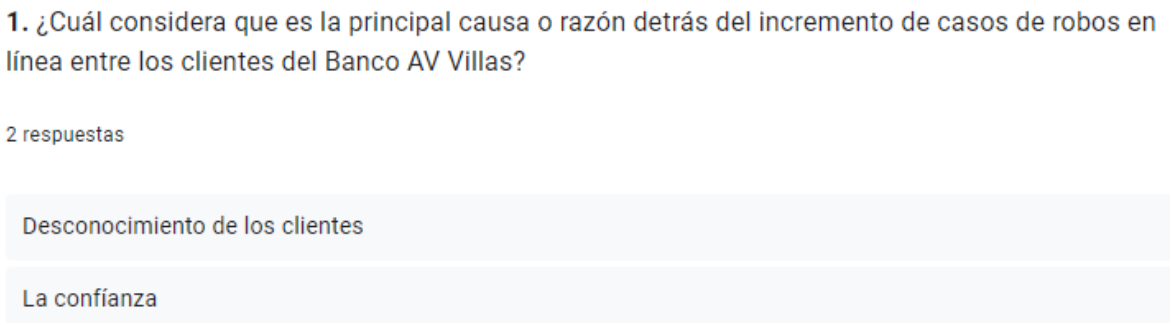

Figura 2. La figura ilustra las opiniones de dos encuestados sobre las principales causas del incremento de casos de robos en línea entre los clientes del Banco AV Villas. Según un encuestado, la principal causa es el desconocimiento de los clientes acerca de las medidas de seguridad y buenas prácticas en línea. El otro encuestado identifica como causa principal la confianza excesiva de los clientes en la seguridad del banco, lo que podría llevar a una menor precaución y vulnerabilidad ante ataques cibernéticos.

Figura 3

Principales Desafíos en la Protección contra Fraudes en Línea.

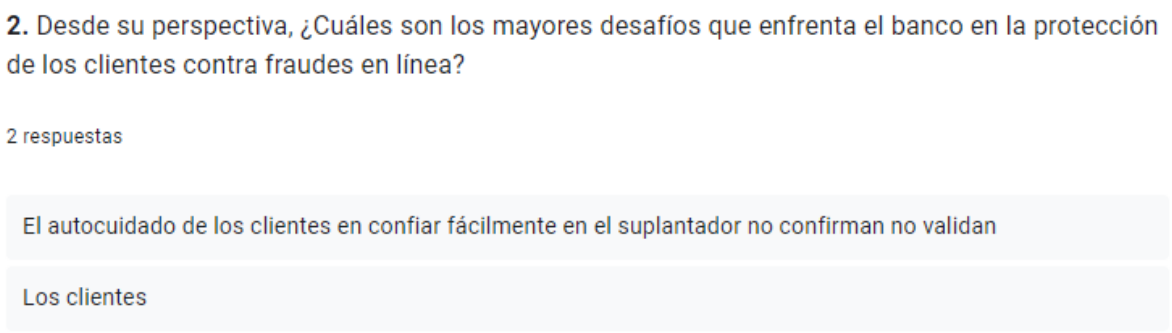

Figura 3. Muestra los desafíos identificados por los encuestados respecto a la protección de clientes del Banco AV Villas contra fraudes en línea. Un encuestado menciona el autocuidado inadecuado de los clientes, quienes confían fácilmente en suplantadores sin verificar la autenticidad. El otro encuestado resalta la falta de verificación y validación por parte de los clientes como un desafío clave.

Figura 4

Recomendaciones para Mejorar la Seguridad y Prevenir Robos en Línea.

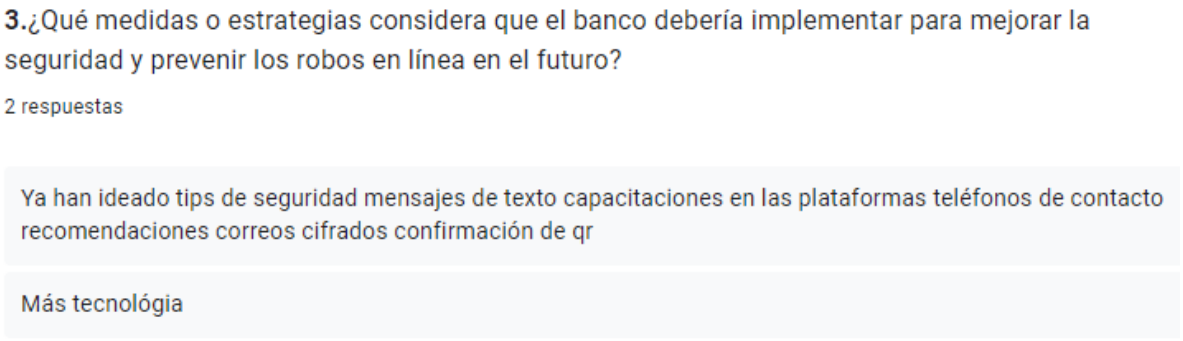

Figura 4. Un encuestado sugiere que el banco debería implementar medidas ya existentes como tips de seguridad, mensajes de texto, capacitaciones, y recomendaciones, junto con tecnologías adicionales como correos cifrados y confirmaciones de QR. El otro encuestado destaca la necesidad de más tecnología para fortalecer la protección en línea.

Figura 5

Estrategias para Fortalecer la Concienciación sobre la Protección de Información Personal.

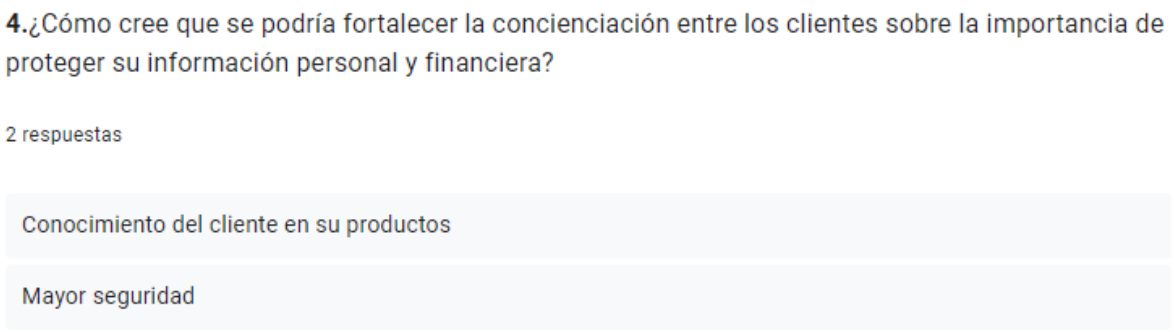

Figura 5. Un encuestado sugiere mejorar el conocimiento del cliente sobre los productos y servicios del banco, mientras que el otro propone aumentar la seguridad general para sensibilizar a los clientes sobre la importancia de proteger su información.

Figura 6

Acciones para Aumentar la Confianza y Satisfacción de Clientes Afectados por Robos en Línea.

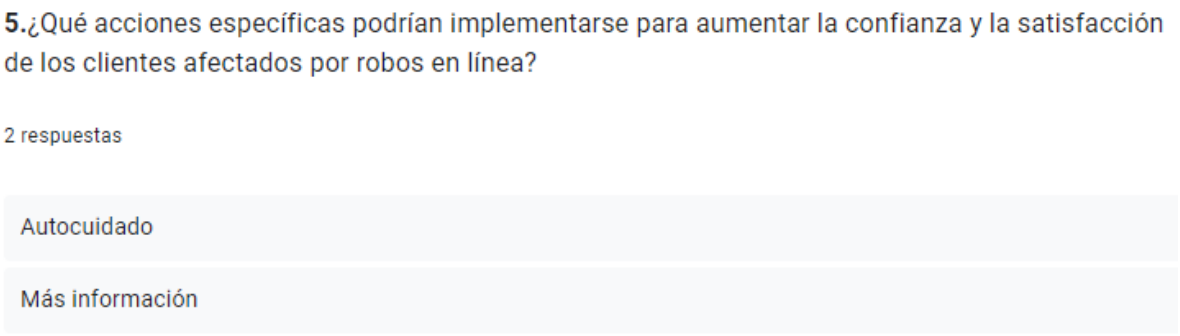

Figura 6. Un encuestado sugiere fomentar el autocuidado entre los clientes, mientras que el otro recomienda proporcionar más información para gestionar mejor las situaciones de fraude y fortalecer la confianza.

5. ANALISIS

Patrones Identificados:

1. **Falta de Concienciación de los Clientes:** La mayoría de los participantes señaló la insuficiente educación financiera y digital como un factor clave en la vulnerabilidad a fraudes.
2. **Confianza Excesiva en la Seguridad Bancaria:** Los clientes confían demasiado en la seguridad del banco, lo que les hace descuidar su autocuidado.

Contribución al Conocimiento y la Práctica:

Estas lecciones destacan la necesidad de mejorar la educación y la comunicación con los clientes en temas de seguridad, lo que es esencial para la práctica profesional en el sector bancario.

Relación con el Proceso Formativo y Desarrollo Profesional:

La experiencia subraya la importancia de un enfoque integral que combine conocimientos técnicos con habilidades de comunicación, vital para el desarrollo en el ámbito financiero.

Lecciones Aprendidas:

- La educación del cliente es crucial para prevenir fraudes.
- Es necesario mejorar la comunicación bancaria para informar sobre amenazas.
- Las soluciones tecnológicas deben ir acompañadas de estrategias educativas.

6. CONCLUSIONES

La sistematización de las experiencias revela que los principales desafíos en la seguridad cibernética del Banco AV Villas incluyen ataques de phishing, sitios web falsos y falta de conciencia entre los clientes. Las medidas más efectivas para combatir estos problemas incluyen la implementación de tecnologías avanzadas como la autenticación biométrica y la encriptación, junto con una robusta capacitación para empleados y clientes.

Estas conclusiones aportan una comprensión más clara sobre la importancia de combinar tecnología con educación para mejorar la seguridad en línea. Además, subrayan la necesidad de un enfoque integral que integre recursos tecnológicos, humanos y financieros para abordar de manera efectiva las amenazas cibernéticas y restaurar la confianza del cliente en los servicios bancarios.

7. RECOMENDACIONES

Para fortalecer la seguridad cibernética del Banco AV Villas, se recomiendan las siguientes acciones:

Nombre: Seguridad Integral Bancaria

Objetivo: Reforzar la seguridad cibernética del Banco AV Villas para:

- Reducir el fraude electrónico
- Proteger la información confidencial de los clientes
- Aumentar la confianza en los servicios bancarios en línea.

Recursos

Tecnológicos: Autenticación biométrica, encriptación avanzada, firewalls, sistemas de detección de intrusiones, análisis de vulnerabilidades, almacenamiento en la nube seguro.

Humanos: Equipo de ciberseguridad (analistas, ingenieros, especialistas), personal de equipo de tecnología, consultores externos, equipo de capacitación.

Financieros: Presupuesto para tecnologías de seguridad, capacitación del personal y consultores externos.

Infraestructura: Espacios seguros para servidores, redes seguras, centros de datos con alta disponibilidad.

Personal Requerido

Equipo de Ciberseguridad: Jefe de Seguridad Informática, Analistas, Ingenieros, Especialistas en Respuesta a Incidentes, Administradores de Sistemas y Redes.

Consultores Externos: Expertos en Ciberseguridad, Auditores, Especialistas en Legislación.

Equipo de Capacitación: Instructores, Coordinadores, Diseñadores de Material Didáctico.

Acciones Para Realizar

Evaluación Inicial

- Implementación de Tecnologías de Seguridad
- Capacitación y Sensibilización

- Área de Monitoreo y Respuesta a Incidentes
- Revisión y Mejora Continua

Capacitaciones Requeridas

Para Empleados: Seguridad cibernética, uso de nuevas tecnologías, respuesta a incidentes.

Para Clientes: Protección de información personal, uso seguro de servicios en línea, material educativo en línea.

Referencias

Conoce nuestra historia y compromiso - Tradicional - Banco AV Villas. (s. f.). Tradicional. https://www.avvillas.com.co/productos-en-oficina/acerca-de-avvillas/#historia

Políticas de protección de datos personales - tradicional - Banco AV Villas. (s. f.). Tradicional. https://www.avvillas.com.co/productos-en-oficina/politicas-de-proteccion-de-datos-personales

Superfinanciera. (2024) Regulación.Superfinanciera.Recuperado de: https://www.superfinanciera.gov.co/publicaciones/10114691/innovasfcfinanzas-abiertasfinanzas-abiertas-colombiaparticipantesnormas-10114691/

Encuesta de Percepción y Seguridad en Transacciones en Línea. (s. f.). Google Docs. Recuperado de: https://docs.google.com/forms/d/1fGwQ3gtX81QsnQhsw9RdvlS65EozW8XK4Je6z6pNOGc/viewform?edit_requested=true#responses

Protege tus transacciones y datos - Tradicional - Banco AV Villas. (s. f.). Tradicional. Recuperado de: https://www.avvillas.com.co/productos-en-oficina/seccion-seguridad

Encuesta sobre Seguridad y Experiencia del Cliente. (s. f.). Google Docs. Recuperado de: https://docs.google.com/forms/d/1W6GDA5qf0wC6-lsuCTJ4zc2tt1YY3Jb9CZTXzslYtzM/viewform?edit_requested=true

https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

https://www.ccit.org.co/articulos-tictac/ciberseguridad-en-el-sistema-financiero-colombiano-entre-la-amenaza-y-la-resiliencia/

https://veridas.com/es/autenticacion-biometrica-que-es-tipos/

https://seon.io/es/recursos/glosario/autenticacion-biometrica/

https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-Metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf