Riesgos cibernéticos en el sector financiero colombiano
situación actual y tendencias.

César Oswaldo Nieto Rodríguez[1], Angie Liliana Sánchez Rojas[2]

Resumen

La ciberseguridad en Colombia es un tema de alta importancia que cada vez adquiere mayor relevancia a nivel empresarial, gubernamental y social. El país ha experimentado un aumento significativo en la cantidad de ataques cibernéticos en los últimos años, lo que ha llevado a la necesidad de mejorar la seguridad de la información y las redes.

Para abordar este problema, el gobierno colombiano ha promulgado una serie de leyes y regulaciones, incluyendo la Ley de Protección de Datos Personales y la Ley de Ciberseguridad. Además, varias empresas han implementado medidas de seguridad cibernética, como la capacitación del personal en seguridad de la información, la implementación de soluciones de seguridad de red y la realización de pruebas de penetración. Sin embargo, aún hay grandes retos para la implementación efectiva de la ciberseguridad en Colombia. Uno de los principales problemas es la falta de conciencia de los usuarios sobre los riesgos de seguridad y la necesidad de proteger la información.

Bajo el escenario descrito, existe un problema de dimensiones considerables que requiere atención continua y un enfoque proactivo por parte de todos los individuos. La implementación efectiva de medidas de seguridad cibernética y la educación de los usuarios son esenciales para mitigar los riesgos y el mantenimiento de la protección de la información.

Palabras clave

Riesgo, ciberseguridad, finanzas, internet

[1] Estudiante especialización gerencia financiera, Fundación Universitaria del Área Andina, Bogotá, Colombia, cnieto12@estudiantes.areandina.edu.co

[2] Estudiante especialización gerencia financiera, Fundación Universitaria del Área Andina, Bogotá, Colombia, asanchez192@estudiantes.areandina.edu.co

Introducción

La masificación del uso de internet y los servicios que allí se encuentran, han generado un *boom* sin límites que día tras día obliga a la humanidad a estar interconectada y funcionalmente interactuando con las diversas opciones disponibles en la red: correo electrónico, redes sociales, aplicaciones de software (*apps*), etc. En este marco digital, el sector financiero ha tenido que experimentar una transformación constante para garantizar su operatividad y disponibilidad, descentralizando las actividades que normalmente se realizaban en las oficinas físicas de las diversas entidades que prestan sus servicios. De esta manera tal como se define en el prólogo del libro *La reinvención financiera en la era digital, "*Las experiencias sensoriales han migrado a escenarios digitales; en la misma línea, los servicios y desarrollo de mercados se ejecutan en espacios virtuales diseñados para tal fin. Estos espacios, considerados como metaversos, condensan gran parte de la experiencia humana de forma virtual; es un nuevo escenario de comportamientos económicos que requieren de una banca organizada y segura para la confianza en este nuevo entorno social y financiero". R

Pero no todo es color rosa en el mundo digital, ya que en la medida en que la evolución de los sistemas genero mayor crecimiento de almacenamiento de datos, creció también el riesgo de seguridad asociado a la información allí contenida. Es así como en los años 70 surgen los primeros ciberdelincuentes y el *malware (*cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario*)*. Actualmente los ciberataques se están especializando y existen organizaciones criminales estructuradas para la creación y propagación de *ransomware* (es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción)

Definición del problema

Los riesgos cibernéticos se han convertido en un problema de tipo estratégico para las empresas, ya que vulneran la confidencialidad e integridad de la información, como sucedió en el reciente caso en la organización multinacional Keralty, que afecto la operación de los servicios de la EPS Sanitas y Colsanitas.

Para los usuarios del sistema financiero son un latente dolor de cabeza ante las posibilidades de sufrir una experiencia nada grata respecto a las incidencias que se puedan presentar en el ciclo

transaccional en el uso de las plataformas digitales, muchos de estos casos requieren de engorrosos procesos de reclamación y respuestas en contra del cliente.

Objetivo

Analizar el escenario actual de riesgos cibernéticos en el sector financiero en Colombia y las tendencias para establecer mejores prácticas en ciberseguridad.

Justificación

Consideramos importante el desarrollo de la investigación con el objeto de analizar la situación actual y las tendencias relacionadas con la ciberseguridad y la mitigación de los riesgos cibernéticos en el sector financiero Colombiano, ya que es una problemática que ha adquirido relevancia tanto para las entidades financieras como para los usuarios de los servicios financieros a todo nivel.

Antecedentes

La creación de internet surge como resultado de las necesidades de comunicación que se generaron durante la guerra fría en los años 60 para el servicio de defensa de Estados Unidos. La primera definición conocida se identifica como ARPANET, por las siglas de Advanced Researchs Projects Agency, en donde científicos desarrollaron mecanismos entre computadores para compartir bases de datos. Entre 1974 a 1982 con el éxito obtenido por ARPANET se crearon varias redes entre las cuales se destacan: Usenet (1979) , Bitnet(1981) y Eunet(1982) todas enfocadas en la posibilidad de unir sistemas independientes con orígenes descentralizados.

En 1983 se adapta el protocolo TCP/IP desarrollado en los años 70 por Robert Kahn y Vinton Cerf a los servicios de ARPANET. Este fue un acontecimiento importante para la expansión del internet, ya que la cantidad de usuarios se incrementó exponencialmente y su uso se internacionalizo. Para ese momento el principal servicio de internet fue el intercambio de emails y almacenamiento de documentos a nivel global. En 1989 se presentó el lenguaje HTML (Lenguaje de Marcado de Hipertexto) utilizado para la estructuración y despliegue de una página web con todos sus contenidos (texto, imágenes y video).

Durante todo este tiempo internet fue solo una herramienta de uso para los usuarios en modo consulta, permitiendo la búsqueda de datos para acceso a la información sin la posibilidad de interactuar con el sistema a este escenario se le conoció como web 1.0. Ya para el año 2000, internet se transforma a la llamada web social o 2.0, en la que la interactividad entre los usuarios y el sistema transformó los servicios estáticos a un dinamismo de intercambio multimedia. En esta instancia surgen también las primeras redes sociales, Facebook, Twitter, Whatsapp, Youtube, las más conocidas y que actualmente se mantienen en el entorno digital con sus diferentes servicios.

Para el 2010 y 2020 se evoluciona sobre tecnologías referidas al concepto de Inteligencia Artificial, que corresponden a la integración de sistemas y algoritmos para desarrollar maquinas que realizan tareas programadas, con el objeto de simular la inteligencia humana.

En la actualidad, como tendencia con mucho por descubrir y diversificar se tiene el metaverso, que surge como ecosistema virtual en 3D, para establecer una nueva funcionalidad del internet en la que se combina la realidad física con el mundo digital.

En cuanto a indicadores estadísticos, según el *Digital Report 2023*, realizado por We Are Social, el número de usuarios de internet en el mundo alcanzo los 5.160 millones de personas, lo que representa que el 64,4% de la población mundial, tiene cobertura de este servicio que cada vez es más incluyente en cuanto a las facilidades tecnológicas tanto de hardware como de software.

En la imagen que se presenta a continuación, se representa gráficamente la evolución del internet desde sus inicios hasta la actualidad.

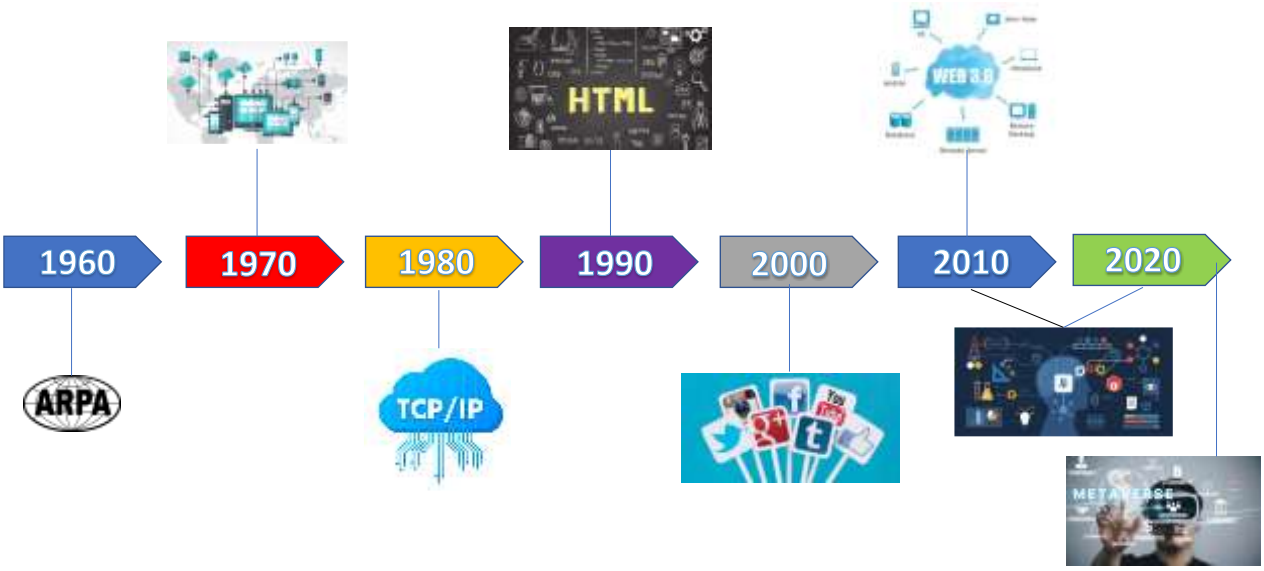


Figura 1. Evolución grafica del internet.

Fuente: Producción propia.

Tal cual evolucionaron las nuevas tecnologías y se alcanzaron grandes resultados para el establecimiento de la interconectividad a nivel mundial, surgieron también a principios de los años 70, los primeros ciberdelincuentes, es así como Bob Thomas desarrolló *Creeper* un programa que se replicaba por sí mismo y se difundía por toda la red con un mensaje que no era malicioso, sin embargo, fue el punto de partida para que a su vez también se desarrollara el primer antivirus comercial. A partir de este escenario siguieron apareciendo diferentes tipos de virus que generaban diversos tipos de incidentes en la operación del hardware y software de los sistemas informáticos y de allí la necesidad de contar con herramientas que solucionaran los efectos de los ataques, en teoría este es el principio origen de lo que a hoy conocemos como antivirus.

Con el paso del tiempo, ya a mediados del año 2000, las organizaciones criminales empezaron a financiar los ataques cibernéticos y surge la necesidad por parte de las empresas y gobiernos de actuar en contra de la ciberdelincuencia creando mecanismos más avanzados para mitigar los efectos de los ataques.

De acuerdo con Statista, plataforma online alemana especializada en datos de mercado y consumo, se pronostica que el tamaño del mercado mundial de Ciberseguridad crecerá a 345,4 mil millones de dólares para 2026.

Normatividad de la ciberseguridad financiera en Colombia

En Colombia, la ciberseguridad financiera está regulada por diferentes leyes y regulaciones que buscan proteger la integridad, confidencialidad y disponibilidad de la información financiera de las empresas y ciudadanos. A continuación, se relacionan algunas de las normas más relevantes:

NORMA	OBJETO	PRINCIPALES COMPONENTES
Ley 1266 de 2008 (Habeas Data)	Garantizar que los datos personales de los ciudadanos sean recopilados, almacenados, usados y divulgados de manera adecuada y segura, y proteger el derecho fundamental a la privacidad.	- Los titulares de los datos personales tienen derecho a conocer, actualizar, rectificar y eliminar su información personal. - Las empresas deben contar con medidas de seguridad adecuadas para evitar la pérdida, robo o uso no autorizado de la información. - La divulgación de información sin consentimiento está prohibida, excepto en los casos en los que la ley lo permita. - Sanciones para las empresas y entidades que violen los derechos de los titulares de datos personales.
Decreto 1078 de 2015	Establece medidas y procedimientos para garantizar la protección de los sistemas de información y la infraestructura crítica del país, con el fin de prevenir y mitigar riesgos y amenazas cibernéticas.	- Creación de una política nacional de ciberseguridad: Fomentar la colaboración entre entidades y sectores. - Creación de un Comité Intersectorial de Ciberseguridad: Coordinar y articular las acciones de los diferentes actores en materia de ciberseguridad. - Protección de la infraestructura crítica: protección de la infraestructura crítica del país, que incluye los sistemas financieros, de transporte, energía, entre otros. - Establecimiento de medidas de seguridad: Creación de planes de contingencia y la implementación de medidas de seguridad técnicas y organizativas.
Decreto ley 1950 de 2019	Establecer medidas para garantizar la seguridad y protección de la información en el ámbito digital. Protección de los sistemas informáticos y de la información que se maneja a través de ellos.	- Protección de la integridad, disponibilidad y confidencialidad de la información. Estas medidas deben ser proporcionales al riesgo y la criticidad de la información. - Medidas de protección de los datos personales de los usuarios que se manejan en los sistemas informáticos - Creación de un Sistema Nacional de Ciberseguridad: Conformado por diferentes entidades públicas encargadas de velar por la ciberseguridad en el país. - Las entidades públicas y privadas deben reportar a la autoridad competente cualquier incidente de seguridad informática que afecte la disponibilidad, integridad o confidencialidad de la información.

NORMA	OBJETO	PRINCIPALES COMPONENTES
Circular Básica Jurídica de la Superintendencia Financiera de Colombia	Establece los lineamientos que deben seguir las entidades financieras del país en materia de ciberseguridad. Proteger la información de los clientes y usuarios de los servicios financieros, así como garantizar la estabilidad del sistema financiero colombiano.	- Las entidades financieras deben implementar medidas de seguridad tecnológicas y organizacionales para proteger sus sistemas y datos de posibles ataques cibernéticos. Designar a un funcionario responsable de la seguridad de la información, establecer políticas y procedimientos de seguridad de la información, realizar auditorías y pruebas de seguridad periódicas, y reportar cualquier incidente de seguridad. - Necesidad de colaboración entre las entidades financieras y las autoridades en materia de ciberseguridad.
Decreto 620 de 2020	Establecer las normas y medidas de ciberseguridad que deben ser implementadas en el país. El objetivo de este decreto es mejorar la seguridad en línea y proteger la información personal y empresarial de los ciudadanos.	-Creación de un comité encargado de coordinar y ejecutar acciones en materia de ciberseguridad, integrado por representantes de diferentes entidades gubernamentales. -Se establece la obligación de las empresas y organizaciones de identificar y evaluar los riesgos en materia de ciberseguridad y establecer medidas de protección adecuadas. -Implementar medidas de protección, adoptar políticas de seguridad, realizar auditorías de seguridad, entre otras. -Se establece la obligación de las empresas y organizaciones de notificar cualquier incidente de seguridad que afecte a sus sistemas o información. -Sanciones para las empresas y organizaciones que no cumplan con las medidas de ciberseguridad establecidas, incluyendo multas y clausura de operaciones.
Circular externa 052 de 2017	Establecer lineamientos y recomendaciones en materia de ciberseguridad para las entidades financieras que operan en el país.	- Necesidad de adoptar medidas de seguridad de la información y ciberseguridad adecuadas, que permitan la protección de los datos de los clientes y la continuidad del negocio en caso de incidentes cibernéticos. - Obligación de establecer un plan de respuesta a incidentes que permita a las entidades financieras responder de manera efectiva ante cualquier eventualidad relacionada con la seguridad de la información. - Importancia de tener en cuenta los estándares y buenas prácticas internacionales en materia de ciberseguridad, como el Marco de Ciberseguridad del NIST (National Institute of Standards and Technology) y la norma ISO 27001. - Necesidad de contar con políticas y procedimientos de seguridad de la información que estén actualizados y que sean conocidos por todo el personal de la entidad financiera. -Importancia de realizar pruebas de vulnerabilidad y evaluaciones de riesgos de manera periódica, con el fin de identificar posibles brechas de seguridad y tomar medidas para mitigar los riesgos.

NORMA	OBJETO	PRINCIPALES COMPONENTES
Circular externa 038 de 2021	Establece medidas para fortalecer la ciberseguridad en el sector financiero colombiano. Proteger la información y los activos de las entidades financieras del país, y garantizar la continuidad de sus operaciones en caso de posibles incidentes cibernéticos.	- Las entidades financieras deben establecer políticas y procedimientos de seguridad cibernética adecuados y eficaces para minimizar los riesgos de seguridad de la información. - Evaluar y gestionar los riesgos asociados a la seguridad de la información de manera periódica y establecer medidas de mitigación adecuadas. - Las entidades financieras deben implementar medidas de seguridad física y lógica para proteger la información de los clientes y de la propia entidad financiera. - Implementar herramientas y tecnologías de monitoreo de amenazas para detectar y prevenir posibles incidentes cibernéticos. - Contar con planes de contingencia y respuesta para gestionar los incidentes cibernéticos de manera eficaz
Circular externa 052 de 2020	Directriz emitida por la Superintendencia Financiera de Colombia, la cual tiene como objetivo establecer medidas de seguridad y prevención en materia de ciberseguridad para las entidades vigiladas por dicha superintendencia, tales como bancos, cooperativas financieras, aseguradoras, entre otros.	- Implementación de medidas de seguridad informática para prevenir y detectar ataques cibernéticos. - Establecimiento de protocolos de respuesta ante incidentes de seguridad informática. - Designación de un responsable de seguridad de la información y ciberseguridad en la entidad. - Realización de pruebas periódicas de vulnerabilidad y auditorías de seguridad informática. - Establecimiento de políticas y procedimientos de seguridad informática para el personal de la entidad. La circular también hace énfasis en la importancia de mantenerse actualizado respecto a las nuevas amenazas en materia de ciberseguridad y en la necesidad de implementar medidas de seguridad adicionales en caso de ser necesario.

Cuadro 1. Comparativo normatividad Colombiana en ciberseguridad.

Fuente: Producción propia

En conclusión, empresas y gobierno en Colombia han sido consecuentes con la definición e implementación de políticas que minimicen los riesgos derivados del uso, ajustados a los lineamientos que a nivel mundial se han desarrollado en la búsqueda del aseguramiento de los sistemas informáticos. No obstante, toda esta infraestructura se ha dispuesto con el fin de blindar la operación, siguen existiendo vulnerabilidades que continúan generando alto impacto.

Principales riesgos en la ciberseguridad financiera colombiana

La ciberseguridad financiera en Colombia enfrenta diversos riesgos que pueden afectar la seguridad de los sistemas financieros, la privacidad y la protección de los datos de los clientes y la integridad de las transacciones financieras. A continuación, se describen algunos de los principales riesgos:

1. Ataques cibernéticos: Los ataques cibernéticos son uno de los principales riesgos en la ciberseguridad financiera colombiana. Estos ataques pueden ser realizados por ciberdelincuentes que intentan obtener información confidencial, realizar fraudes financieros, robar identidades o sabotear los sistemas financieros.
2. Phishing: El phishing es una técnica de ingeniería social que consiste en enviar correos electrónicos falsos o mensajes de texto con el fin de obtener información confidencial, como contraseñas o datos de tarjetas de crédito. Los ciberdelincuentes pueden utilizar esta técnica para engañar a los usuarios y acceder a sus cuentas bancarias o tarjetas de crédito.
3. Malware: El malware es un software malicioso que se utiliza para infectar sistemas informáticos y obtener información confidencial. Los ciberdelincuentes pueden utilizar diferentes tipos de malware, como virus, troyanos, spyware, ransomware, etc. para infectar sistemas financieros y obtener acceso a la información confidencial.
4. DDoS: Los ataques de denegación de servicio (DDoS) son otra forma de ataque cibernético que se utiliza para interrumpir el servicio de los sistemas financieros. Los ciberdelincuentes utilizan múltiples dispositivos para inundar los servidores de los sistemas financieros con solicitudes de tráfico, lo que provoca una sobrecarga y hace que el servicio sea inaccesible.
5. Vulnerabilidades de seguridad: Las vulnerabilidades de seguridad en los sistemas financieros pueden ser explotadas por los ciberdelincuentes para acceder a información confidencial o realizar fraudes financieros. Es importante que los sistemas financieros estén actualizados y protegidos para evitar la explotación de estas vulnerabilidades.
6. Uso inadecuado de dispositivos móviles: El uso inadecuado de dispositivos móviles por parte de los usuarios puede aumentar el riesgo de ciberataques y la exposición de información confidencial. Los usuarios deben ser conscientes de las prácticas seguras en el uso de sus dispositivos móviles y proteger su información personal y financiera.

7. Accesos no autorizados: Los empleados y contratistas con acceso a los sistemas financieros de Colombia pueden ser un riesgo para la ciberseguridad. Los accesos no autorizados pueden permitir el acceso a información financiera confidencial, lo que podría dar lugar a fraude y robo de identidad.
8. Falta de conciencia sobre ciberseguridad: La falta de conciencia sobre ciberseguridad puede hacer que los usuarios y empleados de las instituciones financieras sean vulnerables a ataques de phishing y malware. La educación y la concienciación sobre ciberseguridad son esenciales para mitigar los riesgos de seguridad.

Estos son solo algunos de los riesgos en la ciberseguridad financiera colombiana. Para reducir el riesgo de ciberataques, es importante que las instituciones financieras implementen medidas de seguridad efectivas y que los usuarios adopten prácticas seguras en el uso de los servicios financieros en línea.

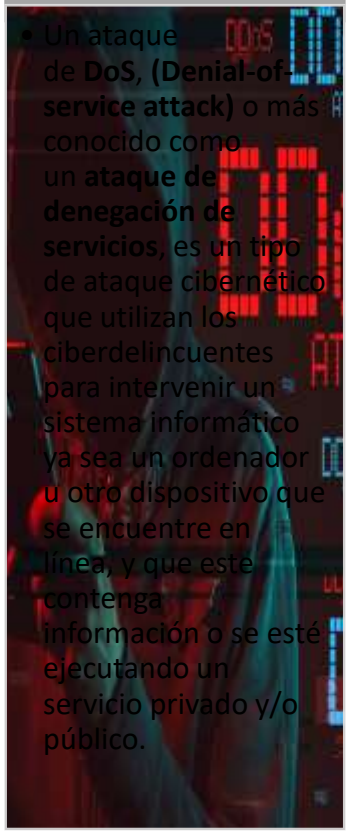
Vulnerabilidades de la ciberseguridad en los sistemas financieros de Colombia.

La ciberseguridad es un tema crítico para los sistemas financieros de Colombia, ya que los ataques cibernéticos pueden comprometer la integridad de los datos financieros de las instituciones, la privacidad de los clientes y la estabilidad del sistema financiero en general. Algunas de las vulnerabilidades de la ciberseguridad en los sistemas financieros de Colombia incluyen:

Phishing	¿Qué es?	¿Cómo funciona?	¿Cómo cuidarse?
	• El pishing es una técnica que utilizan los ciberdelincuentes para **engañar y conseguir información sensible** como contraseñas, número de cuentas bancarias, datos de tarjetas de crédito e infomración confidencial entre otros. Se considera un tipo de ataque de ingenieria social porque se basa en errores humanos.	•Los ciberdelincuentes intentan suplantar a una entidad legítima(entidad financiera, entidad pública o privada, servicio técnico, entre otros). •La mayoria de los ataques comienzan con la recepción de un correo electrónico o un mensaje directo. •Los correos incluyen enlaces a sitios web preparados por los atecantes en los que solicitan información. •Otros medios de propagación son: mensajería instantánea, redes sociales y SMS.	• sí, desconfia de un correo o de su origen, nunca lo abra. • Evite hacer clic en links no confiables y nunca los reenvíe • Ante cualquier sospecha de pishing, repórtelo al area de seguridad en la información o elimine el correo de su bandeja personal.

Cuadro 2. Phishing. Definición, funcionamiento y cuidados.

Fuente: Producción propia

Ataque de denegación de servicios (DoS)	¿Qué es?	¿Cómo funciona?	¿Cómo cuidarse?
	• Un ataque de **DoS**, **(Denial-of-service attack)** o más conocido como un **ataque de denegación de servicios**, es un tipo de ataque cibernético que utilizan los ciberdelincuentes para intervenir un sistema informático ya sea un ordenador u otro dispositivo que se encuentre en línea, y que este contenga información o se esté ejecutando un servicio privado y/o público.	• Se puede dar de diferentes maneras **para determinar cómo funciona un ataque DoS,** pero todas tienen como finalidad el mismo propósito que es **"tumbar"** un sitio web o un servicio, así: • Realizar tantas peticiones al tiempo que los recursos del sistema no den abasto y colapse. • Obstruir el medio de comunicación entre un usuario y un servicio • Alterar la información alojada	• Contar con dispositivos que analicen en tiempo real el trafico en la red y el volumen de datos • Tener un servidor de respaldo • Tener dispositivos que detecten y desvíen el trafico cuando detecte comportamientos atípicos • IPS sistema de prevención de intrusiones. • Segmentar las redes

Cuadro 3. DoS. Definición, funcionamiento y cuidados.

Fuente: Producción propia

Falta de actualizaciones de seguridad	¿Qué es?	¿Cómo funciona?	¿Cómo cuidarse?
	• La falta de actualizaciones de seguridad se refiere a la falta de actualizaciones o parches que se emiten para corregir vulnerabilidades o brechas de seguridad en un software, sistema operativo o dispositivo.	• Estas actualizaciones son críticas para garantizar que el software o dispositivo esté protegido contra ataques cibernéticos y que la información y los datos almacenados estén seguros. La falta de actualizaciones de seguridad puede dejar un software o dispositivo expuesto a ataques, lo que podría comprometer la privacidad y seguridad de los usuarios y exponerlos a posibles ataques de piratas informáticos.	•Es importante mantener actualizado el software y los dispositivos para garantizar su seguridad y privacidad. Utilice contraseñas seguras, y únicas para cada una de sus cuentas en línea. Evite utilizar contraseñas fáciles de adivinar, como "123456" o "contraseña" Haga copias de seguridad de sus datos regularmente en caso de que algo salga mal con su dispositivo. Séa cuidadoso con los correos electrónicos: son una forma común para que los hackers intenten infectar su dispositivo con malware. Asegúrese de no abrir correos electrónicos sospechosos y de no descargar archivos adjuntos de remitentes extraños.

Cuadro 4. Falta de actualizaciones de seguridad. Definición, funcionamiento y cuidados.

Fuente: Producción propia.

Frente a los diversos tipos de ciberataques, surgen mecanismos de seguridad para contrarrestar los efectos que pueden afectar la seguridad cibernética de cada organización por esto cada una deberá implementar medidas adicionales para adaptar sus necesidades a los riesgos específicos.

Tipos de seguridad	Descripción	Ejemplo
Contraseñas seguras	Utilizar contraseñas fuertes y únicas para cada cuenta. Evitar contraseñas fáciles de adivinar, como "123456" o "contraseña".	"H*2k9j#L$m!"
Autenticación de dos factores	Añadir una capa adicional de seguridad al requerir un segundo método de autenticación, como un código enviado al teléfono del usuario, además de la contraseña.	Google Authenticator
Actualización del software	Mantener actualizado el software y aplicaciones, ya que las actualizaciones pueden incluir parches de seguridad importantes.	Actualizar el sistema operativo de Windows
Firewall	Un firewall protege la red bloqueando el acceso no autorizado desde Internet u otras redes.	Firewall de hardware
Seguridad de la red	La seguridad de la red se enfoca en proteger la infraestructura de red, incluyendo routers, switches, servidores y otros dispositivos.	Configuración de VLAN
Encriptación	Encriptar datos sensibles para protegerlos de accesos no autorizados.	Encriptación de archivos con AES-256
Conciencia de seguridad	Educación y concientización de los usuarios sobre la importancia de la seguridad en línea y cómo protegerse.	Capacitación en ciberseguridad para empleados
Uso de VPN	Utilizar una VPN para cifrar la conexión a Internet y proteger la privacidad.	Servicio de VPN de pago

Cuadro 5. Mecanismos de ciberseguridad.

Fuente: Producción propia.

Las vulnerabilidades de ciberseguridad son un riesgo importante para los sistemas financieros de Colombia. Es importante que las instituciones financieras implementen medidas de seguridad efectivas, actualicen regularmente su software y fomenten la conciencia sobre ciberseguridad entre los empleados y los clientes.

Los ciberataques son una amenaza cada vez más frecuente y grave en todo el mundo, y el sector financiero es un objetivo especialmente atractivo para los ciberdelincuentes debido a la gran cantidad de datos sensibles y valiosos que manejan. En Colombia, se han presentado casos de ciberataques a bancos y otras instituciones financieras en los últimos años.

Para mitigar estos riesgos, las instituciones financieras en Colombia y en todo el mundo suelen invertir en medidas de seguridad cibernética, como firewalls, detección de intrusiones, autenticación de usuarios y cifrado de datos. También es importante que los usuarios de servicios financieros sean conscientes de los riesgos de seguridad y tomen medidas para proteger sus propios datos, como utilizando contraseñas seguras y actualizadas, evitando compartir información confidencial en línea y verificando la autenticidad de los correos electrónicos y los sitios web antes de compartir información personal.

Hasta este punto todo el contexto detallado respecto a los antecedentes, identificación de amenazas, políticas y normativa relacionada con los riesgos cibernéticos, ha estado enfocado en las empresas y el Gobierno, dos de los tres componentes de los agentes económicos en cualquier sociedad. ¿Y las familias, que papel desempeñan en todo este escenario? La respuesta a este interrogante está abierta a lo que cada uno como usuario ha tenido frente a la interacción con los servicios financieros digitales, que parecen operar con normalidad pero que, según datos de la Asobancaria, durante el año 2022 en Colombia se registraron más de 54.000 denuncias por delitos cibernéticos, dato que revela una situación anormal que no es de conocimiento público y al cual se le da baja importancia.

La realidad muy seguramente es otra, son muchos más los eventos en que los usuarios tienen experiencias que generan reclamos ante los entes financieros y comúnmente lo que se encuentra en primera instancia frente a un problema que genera angustia y ansiedad, es una máquina que responde bajo los lineamientos de la inteligencia artificial y no brinda las soluciones puntuales que se requieren tener. De entrada, la impersonalización prima sobre las necesidades del cliente. Posteriormente al establecer contacto para atención personalizada u obtener instrucciones más puntuales de cómo proceder frente al problema, el usuario se encuentra con una nueva barrera, la de la tramitología para atención de su reclamo. Finalmente transcurre el tiempo y en la mayoría de los casos a pesar del tiempo invertido, la consecución de pruebas y documentos y los engorrosos procedimientos que conllevan todos estos incidentes la respuesta es en contra del

cliente. Este es el ciclo real del proceso de atención de un reclamo, que por lo general toma entre 20 a 30 días y que finalmente se archiva como otros tantos en el olvido.

Las entidades financieras promulgan a diestra y siniestra que sus sistemas y servicios están garantizados bajo estrictas normas de seguridad y venden además de sus productos, ideas de confianza que en la mayoría de los casos no son más que falacias para lograr sus objetivos comerciales. Entonces, ¿Que nos espera a corto, mediano y largo plazo?, ¿De qué otras formas se puede abordar esta problemática?

En principio las entidades financieras manejan planes de mitigación de riesgos cibernéticos, en los que se tiene como referente cuatro actores principales (personas, procesos, información y tecnología) que se integran en pro de alcanzar los objetivos de la ciberseguridad informática: prevenir, detectar, responder y recuperar, acorde a lo que se especifica en la siguiente imagen:

Figura 2. Implementación de un Modelo de Prevención de Fraude Cibernético

Fuente: producción propia basado en un Marco de Trabajo Estándar. José marangunich.

Propuesta de mejores prácticas

No solo las acciones relacionadas con la implementación de sistemas de seguridad y normativas que en la mayoría de los casos se quedan en el papel, van a dar una solución al problema. Por ello se plantean tres ideas focalizadas en las posibles soluciones, que de forma integral para los componentes de los agentes económicos, permitan constituir alternativas más afianzadas hacia el futuro de mediano y largo plazo.

1. Programas de capacitación multinivel

Nelson Mandela promulgó la frase célebre “La educación es el arma más poderosa que puedes usar para cambiar el mundo”. A través de la educación como eje motor se proyecta concientizar desde la escuela hasta los programas más avanzados en la educación superior los principales aspectos relacionados con ciberseguridad, esto como principio básico de conocimiento respecto al correcto uso de los recursos informáticos, de la falta de contenidos a nivel educativo en la enseñanza básica primaria y secundaria en la que los contenidos de los programas solo tratan temas de programas y sus usos y aplicaciones pero no se abordan temas relacionados con los riesgos de los sistemas, ni mucho menos como será la futura interacción de los jóvenes con el sistema financiero.

En cuanto a la educación universitaria con visión profesional se propone difundir con mayor interés los programas educativos que ofrecen algunas universidades con relación al tema y así continuar ampliando la oportunidad del aprendizaje y conocimiento en este tema.

2. Estandarización de métodos de ciberseguridad a nivel financiero

Si bien es cierto todas las entidades financieras tienen en sus modelos operativos incluidos programas, estrategias, procesos y procedimientos encaminados a la ciberseguridad, no son comunes y aplican de la misma forma entre una y otra. Es necesario que los entes de control que regulan el funcionamiento del sector establezcan los lineamientos generales y obligatorios para todos, propendiendo por un modelo de mejores y mayores garantías para los usuarios.

Es incomprensible que algunas entidades cobren ofreciendo productos y seguros para garantizar ciertos tratamientos especiales que le den mayores garantías al dinero depositado por los clientes.

En otros escenarios hasta ahora se estén constituyendo áreas enfocadas en el análisis y control de posibles fraudes cuando diario millones de personas generan transacciones en las diferentes plataformas que en la actualidad operan en la prestación de estos servicios.

3. Integración de estrategias en ciberseguridad a nivel internacional

En apartes del articulo *Globalización, ciberseguridad y estrategia* publicado en "The economy journal.com" se indica… "Hoy la seguridad de cada país y la paz mundial están amenazadas por peligros económicos, ecológicos, tecnológicos, sociales o institucionales en similar medida que a peligros militares. Entre los peligros tecnológicos están los riesgos y amenazas en el ciberespacio, campo de la ciberseguridad que requiere de su propia estrategia". Por esto y por la imperiosa necesidad del trabajo cooperativo, el gobierno Colombiano en conjunto con las empresas debe estar a la vanguardia participando activamente para garantizar que la vida cotidiana de la sociedad en conjunto permita continuar generando oportunidades de uso adecuado en el internet y se mitiguen los nuevos riesgos que surjan deben ser neutralizados.

Conclusiones

La ciberseguridad es un tema cada vez más relevante en Colombia debido al aumento del uso de tecnologías de la información y comunicación en todos los ámbitos, incluyendo el empresarial, gubernamental y social.

La seguridad de la información y la protección de datos personales son dos aspectos clave de la ciberseguridad, ya que un fallo en cualquiera de estos aspectos puede tener graves consecuencias, como el robo de información confidencial o el acceso no autorizado a sistemas y redes.

El aumento de los ciberataques en Colombia, así como la sofisticación y complejidad de los mismos, evidencian la necesidad de implementar medidas de seguridad cada vez más robustas para proteger los sistemas y redes de empresas, organizaciones y particulares.

La implementación de políticas públicas que promuevan la ciberseguridad, la concienciación de la población sobre la importancia de proteger su información y la colaboración entre empresas y organismos estatales son fundamentales para mejorar la ciberseguridad en Colombia.

La ciberseguridad es importante para el crecimiento económico y la competitividad de Colombia en el contexto global, ya que un buen nivel de seguridad de la información y de protección de datos personales aumenta la confianza de los inversores y de los consumidores en el país.

La capacitación y actualización constante de los profesionales de la ciberseguridad es fundamental para mantener un nivel adecuado de seguridad en el país, y para enfrentar los desafíos que suponen los ciberataques cada vez más sofisticados y complejos.

La ciberseguridad es un tema que debe ser abordado de manera multidisciplinaria, involucrando no solo a expertos en tecnología de la información, sino también a abogados, psicólogos, sociólogos y otros profesionales que puedan aportar su conocimiento para lograr una estrategia integral de protección.

Referencias bibliográficas

ACIS (marzo, 2021). Empresas financieras en Colombia gastan US$180 millones al año para prevenir delitos financieros. https://bit.ly/3m6DiYO

AdolfoManaure. (27 de marzo de 2023). *Digital Too*. Obtenido de incremento de ciberataques en latinoamérica exige un cambio de estrategia: https://www.digitaltoo.com/2017/12/05/2017-kaspersky-mas-25-ataques-ransomware-fue-dirigido-empresas/

Amaya, J. (2014). El sistema financiero y la seguridad informática. Universidad Piloto de Colombia. [Tesis, Universidad Piloto de Colombia]. Repositorio institucional https://bit.ly/3iUvBTu

Asobancaria (2022). Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina. https://bit.ly/3yYMG4a

Asobancaria (Septiembre de 2022). La reinvención financiera en la era digital. (p.8). https://asobancaria.com/wp-content/uploads/La_reinvencion_financiera_en_la_era_digital-2022.pdf. Recuperado abril 2023.

Axess. (2020). Ciberseguridad & Big Data: la conectividad satelital y la fábrica inteligente 4.0. https://axessnet.com/ciberseguridad-big-data-la-conectividad-satelital-y-la-fabrica-inteligente-4-0/

Banco Interamericano de Desarrollo & Organización de Estados Americanos (2016). Perfiles de países: Colombia, Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? (p. 64), https://publications.iadb.org/en/ cybersecurity-are-we-ready-latin-america-and-caribbean. Recuperado marzo 2023.

Catarina Sá Couto (EC Young Leader Class de junio de 2018). https://cartadelatierra.org/la-educacion-es-el-arma-mas-poderosa-para-lograr-la-sostenibilidad/. *Recuperado abril de 2023*

Ceballos A., Bautista F. y Mesa L. (2020). Ciberseguridad en entornos cotidianos. TicTac. Cámara Colombiana de informática y telecomunicaciones (CCIT). https://www.ccit.org.co/wp-content/uploads/ciberseguridad-en-entornos-cotidianosvfene-1.pdf

Circular externa 052 de 2017. La cual se refiere a los Riesgos potenciales asociados a las operaciones realizadas con "Monedas Electrónicas- Criptomonedas o Monedas Virtuales.22 de junio de 2017

CONPES 3995 (1 de julio de 2020). Política Nacional de Confianza y Seguridad Digital. Consejo Nacional de Política Económica y social. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Decreto 620 de 2020. Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011. los literales e. j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales. Mayo 02 de 2020.

Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. 26 de mayo de 2015

Decreto ley 1950 de 2019. Por medio de la cual se aprueba el «Acuerdo sobre los términos de la adhesión de la República de Colombia a la Convención de la Organización para la Cooperación y el Desarrollo Económicos», suscrito en París, el 30 de mayo de 2018 y la «Convención de la Organización para la Cooperación y el Desarrollo Económicos», hecha en París el 14 de diciembre de 1960.

IBM. (2020). Inteligencia artificial en ciberseguridad. https://www.ibm.com/co-es/security/artificial-intelligence

Infobae (29 de abril de 2021). Web del Congreso de la República fue objeto de ciberataques. https://www.infobae.com/america/colombia/2021/04/29/web-del-congreso-de-larepublica-fue-objeto-de-ciberataques

InfoSecurity México. (2021). Ciberseguridad: una guía completa de conceptos, tipos, amenazas y estrategias. https://www.infosecuritymexico.com/es/ciberseguridad.html

ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. En *COBIT 5 AN ISACA FRAMEWORK* (pág. 31 a 31).

Kaspersky. (2023). *¿Qué son los ataques DDoS?* Obtenido de https://latam.kaspersky.com/resource-center/threats/ddos-attacks

Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.31 de diciembre de 2008.

Línea, G. e. (s.f.). *Manual para la implementación de la Estrategia de Gobierno en línea en las entidades del orden nacional de la República de Colombia – Estrategia 2012-2015 para el Orden Nacional, Estrategia 2012-2017 para el Orden Territorial.* Bogotá, Colombia.

MinTIC, Colombia, Boletín Trimestral de las TIC - tercer trimestre, 2020.

Molina M. (2022) Globalización, ciberseguridad y estrategia: especial consideración a la estrategia de la información. https://www.theeconomyjournal.com/texto-diario/mostrar/939724/globalizacion-ciberseguridad-estrategia-especial-consideracion-estrategia-informacion. Recuperado Abril de 2023.

Portafolio. (2021). Bancos aumentaron en un 64% gastos de ciberseguridad. https://www.portafolio.co/economia/finanzas/bancos-aumentaron-64-gastos-en-ciberseguridad-553594

https://worldcampus.saintleo.edu/noticias/historia-de-la-ciberseguridad#:~:text=A%20partir%20del%202021%2C%20la,millones%20de%20d%C3%B3lares%20para%202026.

Superintendencia Financiera de Colombia (C.E. 029/14), https://www.superfinanciera.gov.co/inicio/normativa/normativa-general/circular-basica-juridica-ce----10083443. Recuperado abril de 2023

Superintendencia Financiera de Colombia (2007). Octubre 2007, Circular Externa 038 de 2021, https://www.superfinanciera.gov.co/publicacion/20072. Recuperado marzo, 2023.

Superintendencia Financiera de Colombia (2012). Octubre 2012, Circular Externa 052 de 2020, https://www.superfinanciera.gov.co/publicacion/61268. Recuperado abril, 2023.

TechTarget. (2021). Autenticación multifactor o MFA. https://searchdatacenter.techtarget.com/es/definicion/Autenticacion-multifactor-MFA

Technology, I. (Septiembre de 2021). *Así funciona un ataque de DoS: Ataque de denegación de servicio*. Obtenido de Nsit: https://www.nsit.com.co/asi-funciona-un-ataque-de-dos-ataque-de-denegacion-de-servicio/

We are social (2023) https://wearesocial.com/es/blog/2023/01/digital-2023/. Recuperado marzo, 2023.