# Importancia De La Seguridad Informática En La Labor Del Contador Como Asesor Financiero

ANGIE MARCELA ÁVILA BELTRÁN & ERIKA MAYERLY SÁNCHEZ QUINTERO

Marzo 2024.

Universidad de Cundinamarca
Extensión Facatativá
Contaduría Pública

2024.

## Contenido

## Índice de tablas



## Índice de figuras

# Dedicatorias

**Erika Mayerly Sánchez Quintero**

Dedico este trabajo, en primer lugar, a Dios, por ser mi fortaleza en los momentos difíciles, por darme la luz y la esperanza cuando sentí que ya no podía continuar. Sin Su guía, este camino habría sido mucho más difícil.

A mi padre, Armando Sánchez, quien nunca dejó de creer en mí. A pesar del cansancio y las dificultades, siempre estuvo ahí, esperándome al final de cada jornada con palabras de ánimo y fe. Él ha sido mi mayor inspiración para alcanzar este sueño que alguna vez fue también el suyo.

A mi madre, Yolanda Quintero, por su valentía, su amor incondicional y su ejemplo de lucha constante. Gracias a ella aprendí a no rendirme, incluso cuando todo parecía cuesta arriba.

A mis hermanos y sobrinos, quienes celebraron cada uno de mis logros como propios y estuvieron presentes con su apoyo y cariño en cada etapa de este proceso.

A mi pareja, por ser mi impulso en los momentos de duda, por creer en mí cuando yo misma lo dudaba, y por motivarme a seguir adelante hasta alcanzar esta meta.

A todos ustedes, les dedico este trabajo. No fue un camino fácil, pero hoy estoy a un paso de cumplir este gran sueño, gracias al amor, la fe y el apoyo que me brindaron.

**Angie Marcela Ávila Beltrán**

Quería expresar mis agradecimientos principalmente a Dios, quien fue mi fuente de sabiduría y fortaleza, por guiarme en este camino académico y brindarme el entendimiento y la sabiduría necesaria para alcanzar esta meta, él es quien me ha bendecido con la capacidad de aprender y tener este logro que para mí era algo imposible de cumplir.

Con profunda gratitud y amor, agradezco este logro a mis padres por su inquebrantable apoyo, sacrificio y amor incondicional, han sido la luz que me han guiado a lo largo de este camino académico. Cada éxito que alcanzo es también suyo. Ya que su constante aliento y ejemplo han sido mi mayor inspiración.

Gracias por ser mis pilares en los momentos más desafiantes y por celebrar conmigo cada triunfo. Este logro lleva su nombre y dedicación y es en honor a ustedes que continuo esforzándome por alcanzar mis metas. Con todo mi cariño esta monografía lleva grabado su nombre en cada página.

Gracias a nuestra tutora Ángela Duarte, por la paciencia y dedicación en orientarme en forma positiva en mi trabajo de grado.

**Resumen**

La seguridad informática en el sector financiero es un aspecto fundamental para la protección de datos, la prevención de fraudes y la confianza de los clientes. Esta monografía analiza la importancia de implementar estrategias y tecnologías avanzadas para mitigar riesgos cibernéticos en entidades financieras.

Los resultados evidencian que, aunque la inversión en seguridad informática ha aumentado, las amenazas siguen evolucionando, lo que obliga a las entidades a adoptar enfoques de seguridad más proactivos, como la autenticación multifactorial, el uso de inteligencia artificial y blockchain. Sin embargo, aún existen brechas en la implementación de estas tecnologías, especialmente en instituciones de menor tamaño.

**Palabras clave:** ciberseguridad, ciberdelincuentes, ciberdelitos, IA

**Abstract**

Cybersecurity in the financial sector is a fundamental aspect of data protection, fraud prevention, and customer trust. This monograph analyzes the importance of implementing advanced strategies and technologies to mitigate cyber risks in financial institutions. The results show that although investment in cybersecurity has increased, threats continue to evolve, forcing institutions to adopt more proactive security approaches, such as multi-factor authentication, the use of artificial intelligence, and blockchain. However, there are still gaps in the implementation of these technologies, especially in smaller institutions.

Key Words: Cybersecurity, Cybercriminals, Cybercrimes, AI

## Introducción

Siempre, desde que la vida se vislumbró en la Tierra, la comunicación entre seres vivos ha sido fundamental. Las especies, han evolucionado y con ellas su capacidad de crear, transmitir y guardar mensajes.

En los años 50's los sistemas de comunicación comenzaron a extenderse, dándole así importancia a elementos como el teléfono, que funcionaba para el intercambio de información a distancia, sin embargo, la información allí dicha podía ser escuchada y/o intervenida en cualquier momento, sin ningún tipo de seguridad, visibilizando un quiebre en la confidencialidad del sistema.

Ya en los años 80's, los llamados actualmente hackers empezaron a aparecer, ya que, los sistemas informáticos cobraron mayor fuerza y por ende el estudio de estos también, haciendo que los hackers, pudieran comenzar a explorar la intromisión en aquellos sistemas.

Es por ello por lo que, a partir de aquí, se empezaron a presenciar las amenazas que siempre han puesto vulnerables a las empresas: los virus, los ataques cibernéticos, códigos maliciosos y entre otros, los cuales han venido evolucionado de la mano con la tecnología (Hernández, 2017). Según Benz y Chatterjee, (2020), la exposición a vulnerabilidades informáticas es un fenómeno que ha venido presentando gran relevancia en las organizaciones debido a la creciente interconexión global. Por lo anterior, puede iniciarse un cambio en esta manipulación de la información y se logra la creencia de que el proceso de nuevos modelos y de innovación tecnológica, como por ejemplo el uso de la ciberseguridad, siendo este un término actual, que tiene como objetivo principal disminuir en gran proporción los riesgos anteriormente mencionados, tratando de mitigar de diferentes

maneras todos los riesgos posibles que puedan llegar a afectar la información condensada de manera virtual (Fereira y Torres, 2017).

También, y no menos importante, se ha posicionado de manera muy rápida, el concepto y la utilización de programas relacionados con la Inteligencia Artificial (IA), quien se ha ocupado de la generación de prácticas, enfocadas a la seguridad y confiabilidad a nivel de hardware y software, teniendo en cuenta que, al día de hoy, el lugar donde se archive la información no es problema para quienes quieren obtenerla o dañarla.

Por todo lo anterior, esta monografía busca profundizar acerca de la importancia de la seguridad informática en el sector financiero, ya que ha sido evidente, que es un sector sensible a delitos informáticos, que puede ocasionar graves consecuencias. Busca aportar información valiosa, que permita dar una visión más clara de la importancia de la utilización de recursos TICS para fortalecer la seguridad.

# Problema De Investigación

## Planteamiento Del Problema.

### Síntesis del problema

Antes de la pandemia, se consideraba que la labor del contador público se limitaba a un área contable y financiera, la cual se debía realizar netamente desde la empresa, aun en algunas organizaciones se maneja de esta manera; sin embargo se dio también a la oportunidad de trabajo en casa para optimizar los tiempos y adaptarse a los cambios ambientales del momento, a raíz de esto, las empresas se vieron en la obligación de adquirir sistemas contables que permitan que los colaboradores, contadores y usuarios de la información puedan tener acceso desde cualquier medio ya sea un teléfono inteligente, computador, tableta, entre otros.

En todo el mundo, los contadores y profesionales financieros demostraron que eran los "asesores más confiables". A través de la satisfacción de las demandas de un mundo disruptivo y en constante cambio, la profesión cumplió su propósito de promover la prosperidad y las oportunidades para quienes cuentan con los contadores públicos, cómo la profesión se unió a las personas, empresas y comunidades que luchaban contra los efectos económicos de la pandemia (Instituto Americano De Contadores Públicos Aicpa, 2023)

Con la implementación de nuevas tecnologías, se corre el riesgo de filtración de información debido también a los diversos programas que se ha creado con el fin de intervenir los sistemas y solicitar dinero a cambio de liberar la información que es relevante para el cumplimiento de los objetivos organizacionales o el funcionamiento

adecuado, es por esto que para implementar nuevas tecnologías, se requiere no solamente efectividad en conectividad sino eficiencia en la limitación de acceso a la información mediante software con niveles de seguridad altos con el fin de prevenir estos riesgos.

Es por esto que mediante la presente investigación, se busca comprender la importancia de la seguridad informática en la labor del contador público desde el asesoramiento financiero, la importancia de conocer los posibles riesgos informáticos, con la implementación de nueva tecnología y la Inteligencia Artificial, analizar los posibles riesgos a los que se expone las organizaciones al brindar información importante y confidencial a diversas entidades y sobre todo el nivel de confianza que puede generar esta implementación, si en un futuro este tipo de avances puede reemplazar el trabajo del contador público o por el contrario mejora el desarrollo de las actividades, optimizando los tiempos de revisión y generando de manera sistemática la información adecuada que facilita a la industria en general el crecimiento sostenible a través del tiempo.

**Formulación del Problema**

¿Por qué es importante la seguridad informática en la labor del contador público como asesor financiero en los últimos cinco años?

**Sistematización del Problema**

¿Cuáles son los riesgos se puede presentar en las áreas contables por la falta de implementación o falta de actualización de las tecnologías?

¿De qué manera afecta la implementación de nuevos softwares contables frente a la seguridad de la información?

¿Qué efectos tiene la verificación y tratamiento de información confidencial de las organizaciones?

## Justificación

En una era digital como lo actual, en la que empresas, personas e incluso gobiernos poseen información importante y/o clasificada en dispositivos digitales (fijos o móviles), se hace de vital importancia conocer los riesgos existentes ya sea de ataques, espionajes o actos delictivos de los cuales se puede ser víctima, así como de las herramientas existentes para detectarlos, prevenirlos y contrarrestarlos. Si bien es cierto que con el paso del tiempo los ciberataques y delincuencia cibernética han evolucionado, no en menor medida los programas y herramientas para evitar ser víctima de dichos ataques también han evolucionado, por ello es importante mantenerse al día sobre la seguridad informática, ya sea mediante reseñas, cursos (online o presencial), lecturas autodidactas, o cualquier otro método de aprendizaje, lo importante es estar actualizado sobre las tendencias y métodos de protección de información digital.

Esta monografía, busca precisamente brindar información que permita a cualquier tipo de profesional y/o empresa tener conocimiento de cuáles son los riesgos informáticos existentes y por supuesto como prevenirlos o en su defecto solucionarlos.

# Objetivos

## Objetivo General

Analizar la relevancia de la seguridad informática en el ejercicio profesional del contador público como asesor financiero.

## Objetivos Específicos

- Identificar los principales delitos informáticos y financieros que impactan el área contable, en relación con las responsabilidades del contador como asesor financiero.
- Determinar la relevancia de la seguridad informática en la prevención de delitos informáticos en Colombia, desde el rol del asesor financiero.
- Analizar métodos efectivos para proteger la información organizacional y la adaptación profesional ante los avances tecnológicos.

# Línea de Investigación

## Línea de investigación translocal

Gestión, emprendimiento, organizaciones sociales del conocimiento y aprendizaje.

## Línea de investigación complementaria

Gestión contable y financiera.

# Metodología

## Enfoque de la Investigación

Este estudio tiene este enfoque ya que buscó identificar la importancia que tiene la seguridad informática en el sector financiero, y el impacto que tiene sobre temas como protección de datos y fraudes en micro y macroempresas.

Vera (2015) menciona que este tipo de investigación permite analizar la calidad de las actividades o instrumentos necesarios para una determinada situación o problema, obteniendo resultados que permitan dar solución a la temática a tratar.

Por su parte, Hernández y otros (2010) mencionan que este tipo de investigación se basa en descripciones y observaciones. Por todo lo anterior, en esta investigación busca la comprensión del fenómeno social, su incidencia y la influencia que tiene sobre un área específica, que en este caso sería contable y financiera.

## Tipo de Investigación

Se hizo una investigación documental y exploratoria. Se recopiló información de fuentes académicas, normativas, y artículos científicos para construir un marco teórico sólido.

## Métodos de Recolección de Información

Para desarrollar la monografía, se utilizaron los siguientes métodos:

### Revisión bibliográfica

Para el desarrollo de esta monografía se utilizó el método de revisión bibliográfica, basado en la recopilación, análisis y síntesis de fuentes importantes y relacionadas al tema de estudio. De esta manera, se pudo construir una base teórica sólida y relacionarla con el problema de investigación en cuestión.

Se consultaron libros de contaduría pública e informática, artículos científicos, tesis académicas, y documentos digitales publicados en bases de datos con alta confiabilidad como Scielo, Redalyc, Science Direct y Google académico.

La selección de dichas fuentes, se hizo a partir de su actualidad, relevancia temática y rigurosidad académica. Se tuvieron muy en cuenta, los documentos publicados en los últimos cinco años, para corresponder con el objetivo del trabajo.

**Análisis de Datos**

Los datos obtenidos serán analizados mediante un enfoque cualitativo, categorizando la información en temas clave como amenazas cibernéticas y estrategias de seguridad.

Para ello, se realizó una técnica de análisis de contenido, donde se identificaron temáticas en común en las fuentes revisadas.

En cada revisión bibliográfica, se realizó una lectura crítica de las fuentes seleccionadas, priorizando las principales posturas teóricas en torno al tema. Esta información fue contrastada y relacionada con el marco teórico. El análisis permitió, obtener conclusiones basadas en la comprensión del fenómeno estudiado, problemáticas y soluciones a las mismas.

# Marcos de Referencia

## Estado del Arte

Según Gamboa (2020) en una era digital como lo actual, en la que empresas, personas e incluso gobiernos guardan información importante y/o clasificada en dispositivos digitales (fijos o móviles), se hace muy importante conocer los riesgos existentes ya sea de ataques, espionajes o actos delictivos de los cuales se puede ser víctima, así como de las herramientas existentes para detectarlos, prevenirlos y contrarrestarlos. Con el paso del tiempo los ciberataques y delincuencia cibernética han venido creciendo, por ello es importante mantener una actualización sobre la seguridad informática, debido a la importancia que esta tiene.

La seguridad informática, se trata sobre la protección de información de índole personal, empresarial o gubernamental contenida no solo en la red, sino también en los dispositivos de uso diario como teléfonos celulares, tabletas, computadoras de escritorio, laptop o cualquier dispositivo digital, de amenazas que puedan poner en riesgo la información almacenada o transportada en alguno de los dispositivos antes mencionados. Una buena Ciberseguridad no solo se debe basar en la prevención de ataques, sino también detección y corrección de estos, reduciendo los riesgos de exposición de la información, brindando confianza a los usuarios (Peña,2019).

Y es que, en definitiva, la era digital ha traído con ella una enorme transformación para el funcionamiento de las empresas, abarcando desde la gestión administrativa hasta la toma de decisiones estratégicas. Lo que implica, que la ciberseguridad se ha convertido en un aspecto fundamental, ya que el aumento del uso de plataformas digitales, sistemas contables en la nube y transacciones electrónicas, expone una vulnerabilidad en las organizaciones a múltiples riesgos informáticos, como el robo de datos financieros, fraudes o pérdida de información contable sensible (Peña,2019).

De este modo, la labor del contador público no solo debe centrarse en el registro y análisis financiero tradicional, sino también de ser proactivo en la protección de la información contable. Es decir, el profesional contable debe tener conocimientos básicos de seguridad informática, para así mismo, poder identificar vulnerabilidades en los sistemas contables y accionar frente a ellos (Salas, 2010).

Lo anterior deja entrever, que la era digital, definitivamente no reemplaza al contador, sino que lo reconfigura, lo prepara para asumir nuevos retos que crecen a medida que pasan los años.; aportando así, un novedoso desarrollo empresarial e integral.

## Marco teórico

### Importancia De La Seguridad Informática en las Organizaciones

Según Jaimovich (2018), en latino américa, aproximadamente 10 bancos fueron víctimas de ataques cibernéticos, viéndose perjudicados datos y por supuesto capitales; confirmando que año tras año la vulnerabilidad respecto a este tema va en aumento.

Aunque la implementación de IA, ha traído muchas ventajas, es importante mencionar que tiene algunas desventajas (Mayorga, 2019). La alimentación de la Inteligencia Artificial en el sector financiero hace que haya recolección de información personal para entrenamiento de modelos y generación de predicciones, las cuales toman el historial crediticio del cliente y diferentes transacciones, para filtrar según el índice de búsqueda y posterior envió del servicio que se quiere ofrecer. Sin embargo, con la adecuada selección y utilización de modelos de IA, los resultados, serán más precisos y seguros, cumpliendo, con las expectativas (Bryson, 2018).

Según Duque (2019) en Colombia aún no se cuenta con regulaciones estipuladas sobre el uso y regulación de la IA, ni la regulación de los datos que se emplean con la misma, aunque sí se cuenta con políticas de transformación y desarrollo que permiten mejorar, en cuenta para el

buen uso de las tecnologías. Se ha sugerido, que se debe implementar unos lineamientos éticos para el manejo de la información, que garantice la seguridad (Gobierno Nacional De Colombia - MARCO ÉTICO IA, 2021).

Según Salas (2010), deben existir ciertos parámetros mínimos de seguridad:

• **Autenticidad:** Reconocer quienes son los autores de páginas web y los servicios que ofrecen, Por ejemplo, entidades como bancos utilizan contraseñas, preguntas de seguridad, tarjetas de coordenadas, claves de seguridad, entre otros.

- **Privacidad:** Los bancos deben ofrecer servicios óptimos para que la comunicación interna de su plataforma sea segura, auditando constantemente.
- **Integridad:** Los bancos deben verificar la información para que la integridad de la misma sea óptima. Por ello debe llevar un proceso que garantice, emisión, recepción y respuesta.

## Marco Conceptual

Zunzunegui, (2018) asegura, que la seguridad informática ha sido un aspecto muy importante en el desarrollo del sector financiero a lo largo de la historia. A medida que la tecnología ha ido avanzando y las instituciones bancarias se han actualizado, adquiriendo sistemas digitales, también nace la necesidad de proteger los datos y las transacciones financieras. A continuación, se presentan los antecedentes más relevantes que han marcado la importancia de la seguridad informática en este sector.

Desde la década de 1970, se introdujeron los sistemas informáticos en las instituciones financieras, y la banca comenzó a migrar de procesos manuales a sistemas digitales. Esta transformación permitió una mayor eficiencia en la gestión de transacciones, pero también trajo consigo vulnerabilidades que podían ser explotadas por actores malintencionados. La necesidad

de implementar protocolos de seguridad se hizo evidente para proteger los datos y evitar fraudes (Zunzunegui, 2018).

Cuando el internet en la década de 1990 tuvo un boom importante, la banca electrónica se popularizó, permitiendo que los usuarios pudieran acceder a sus cuentas y realizar transacciones de manera remota. Sin embargo, estas nuevas actividades originaron nuevos tipos de amenazas, como el phishing y el robo de identidad. Como respuesta, se desarrollaron mecanismos de autenticación más avanzados y cifrado de datos para proteger la información financiera (Peña,2019).

En los primeros años del siglo XXI, el cibercrimen incrementó y así mismo se popularizó, convirtiéndose en una amenaza global para el sector financiero (Santos, 2022). Comenzó a evidenciarse el malware y técnicas de hacking para infiltrarse en sistemas bancarios y robar grandes sumas de dinero. Sin embargo, para contrarrestar estas amenazas, se aplicaron normas con estándares estrictos para la protección de datos financieros (García, 2017).

A partir del año 2010, los ataques cibernéticos dirigidos a grandes empresas como bancos y sistemas de pago electrónico aumentaron considerablemente. Es evidente, que la mayoría de empresas a nivel de Latino América desde esta fecha, han sido vulnerables a los ataques cibernéticos, ya que el 93% reflejan ser vulnerables a estos ataques, según el estudio de la CISCO, revela que el 40% de los ataques son a pequeñas y medianasempresas (PYMES), siendo esta la mayor amenaza el phishing; sin embargo, el 83% de las PYMES reconocen estar preparadas, y apenas el 9% de estas ha contratado un seguro de ciber responsabilidad que les permita recuperarse después de algún delito informático (Peña, 2019).

Dentro de las vulnerabilidades que según Delgado y Diaz (2021) se evidencian en mayor porcentaje, el 85% fue por la intervención de personas con fácil acceso al manejo de la información y, el 61% fue porque las contraseñas eran demasiado débiles (Ninja, 2024).

Este tipo de situaciones, son aquellas que afectan diversos aspectos en una empresa, pudiendo ser muy graves, debido a la información que allí se maneja. Hernández (2017), considera que 'Un sistema informático puede encontrarse en riesgo si este, está compuesto por la terna de activo, amenaza y vulnerabilidad', esto, relacionado con la siguiente fórmula:

$$\text{Riesgo (R)} = \text{amenaza (A)} + \text{vulnerabilidad (V)}$$

Así las cosas, se evidencia que las empresas suelen tener un conjunto de elementos que funcionan como estrategia para la conservación y protección de la información (los activos) ya que es información sensible que diariamente está expuesta.

Hoy en día, cuando la mayoría de las actividades son realizadas con tecnología, y así mismo nacen estrategias de seguridad, suele existir el riesgo de que en algún momento un computador no tenga las protecciones mínimas que deben tener (antivirus, actualizaciones del sistema operativo, etc.), pudiendo ocasionar el acceso no autorizado y tener así control total de la información o en su defecto la eliminación total o daño de los archivos allí existentes.

Por su parte, no solamente existe aquel riesgo empresarial de perder datos y/o que estos sean manipulados, sino que, además, los actualmente llamados ciberdelincuentes, aprovechan las ventajas actuales de pagos electrónicos para a través de PSE (Pagos Seguros en línea), con el propósito de robar contraseñas, números de documentos, información financiera, etc.

Coll (2020) afirma, que la revolución digital que se ha dado en los dos últimos siglos ha sido un avance fundamental para la humanidad, ya que involucra temas sociales, económicos y culturales trayendo consigo ventajas y desventajas.

En cuanto a las ventajas, encontramos la facilidad que la tecnología brinda para facilitar la comunicación pudiendo hacer la mayoría de las actividades de manera virtual.

Según Branch (2021) en nuestro país Colombia el porcentaje de personas que han optado por el uso de las TIC es de aproximadamente un 4% del 2020 al 2021, donde cerca de 1.3 millones de personas se convirtieron en ciberusuarios en todo el territorio.

Este incremento del uso de las tecnologías hace que los riesgos también aumenten, pues se crea, una dependencia que puede hacer que la incidencia de hackers aumente, con el fin de buscan dañar o beneficiarse económicamente en base a terceros e intentan penetrar en las redes para extraer información, plantar virus, hackear mails, etc. (Saín, 2015).

**Figura 1 Crecimiento digital en Colombia**


Fuente: Clay (2021)

En el año 2021, se registraron aproximadamente 46.500 denuncias por múltiples delitos cibernéticos, evidenciándose un incremento del 21% con respecto al año 2020 (ElTiempo, 2021). Esto, demuestra que los ciberataques son más persistentes que en otros años, un acelerador de este fenómeno fue el inicio de la pandemia, ya que en este periodo las personas se vieron obligadas a compartir información importante por internet, y realizar varias actividades virtuales tales como el comercio electrónico, haciendo un mayor uso de tarjetas, posibilitando a los delincuentes acaparar un área específica criminal, que tiene múltiples vacíos y desventajas (ElTiempo, 2021).

En el contexto actual 9 de cada 10 bancos en América latina y el caribe sufrieron algún tipo de ataque cibernético durante en los últimos 4 años (Fortinet. 2023), lo cual es una evidencia de que en el sector financiero las bases de datos están expuestas a su vulneración, siendo una problemática que se ha acrecentado año tras año. De acuerdo con cifras del Laboratorio de Inteligencia de Amenazas Fortinet, en la primera mitad del 2023 Colombia tuvo más de 5.000 millones de intentos de ciberataques, ubicándose en el cuarto lugar a

nivel regional. En comparación al 2022, que tuvo una caída de casi mil intentos pues fueron6. 300 millones de intrusión. Significando un aumento del 70% (Fortinet, 2023).
Según el Boletín Oficial de Delitos Cibernéticos proporcionado por la INTERPOL y el Centro Cibernético Policial los sitios web sin protección alguna son explotados para estafas de pishing, colocando páginas falsas, aparentando ser sitios importantes, y a través de eso, recopilan datos privados y bancarios para robar dinero.
Se dice, que los países, preparados actualmente para proteger y hacer uso de la IA son Chile, Brasil, Uruguay y en el puesto número seis está Colombia (Bnamericas, 2023).

**Factores De Riesgos En La Seguridad Informática:** Hay 3 factores de riesgo definidos y que son considerados fundamentales.

- **Factor ambiental:** Hace referencia a las lluvias, terremotos, inundaciones, rayos, calor humedad y otro factor externo.

· **Factor Tecnológico:** se refiere a daños de software y/o hardware, que se evidencian a través de ataque por virus informáticos, entre otros, etc.

· **Factor Humano:** Hace referencia a los fraudes, modificaciones, sabotaje, crackers, vandalismo, hackers, falsificación de información, contraseñas robadas, intrusión no autorizada, entre otros, etc**.**

## Marco Legal

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

**Artículo 269A: Acceso Abusivo a Un Sistema Informático:** Acceso sin autorización a un sistema informático configurado con una medida de seguridad, o en contra de la voluntad del

legítimo propietario, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

**Artículo 269B: Obstaculización Ilegítima De Sistema Informático o Red De Telecomunicación.** Cualquiera que impida el funcionamiento o el acceso a un sistema informático, o a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

**Artículo 269C: Interceptación De Datos Informáticos:** La interceptación de datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

**– Artículo 269D: Daño Informático:** La destrucción, daño, deterioro, alteración o que suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

**Artículo 269E: Uso De Software Malicioso:** Quién produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

**Artículo 269F: Violación De Datos Personales:** Quien con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases

de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

La Ley 1266 de 2008 definió el término dato personal como "cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica". Este artículo, obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien "sustraiga" e "intercepte" dichos datos a pedir autorización al titular de los mismos.

**Artículo 269G: Suplantación De Sitios Web Para Capturar Datos Personales:** Cualquiera que, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

**Artículo 269I: Hurto Por Medios Informáticos y Semejantes:** Cualquiera que realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.

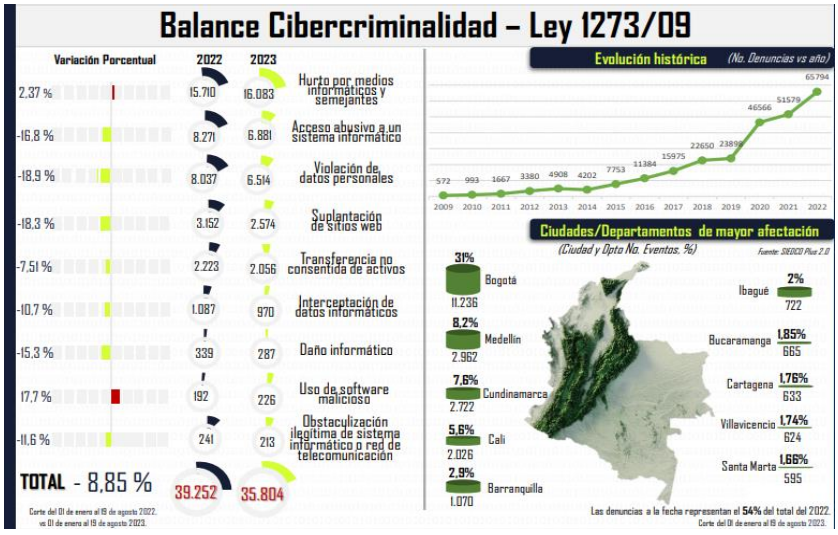
**Artículo 269J: Transferencia No Consentida De Activos:** Quien, valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

## Tipos De Delitos Informáticos y Financieros Más Comunes a los que están Expuestas Las Empresas En el Área Contable y Financiera

Wang (2019) a través de un análisis, se estudiaron los modelos de infiltración o ingreso de los atacantes de empresas en Latinoamérica, entre los cuales se encontraron rasonware, denegación de servicios DDoS, duplicidad de información, spam, cryptohacking, malware, los cuales interrumpen el proceso natural de un sistema, afectando su funcionamiento.

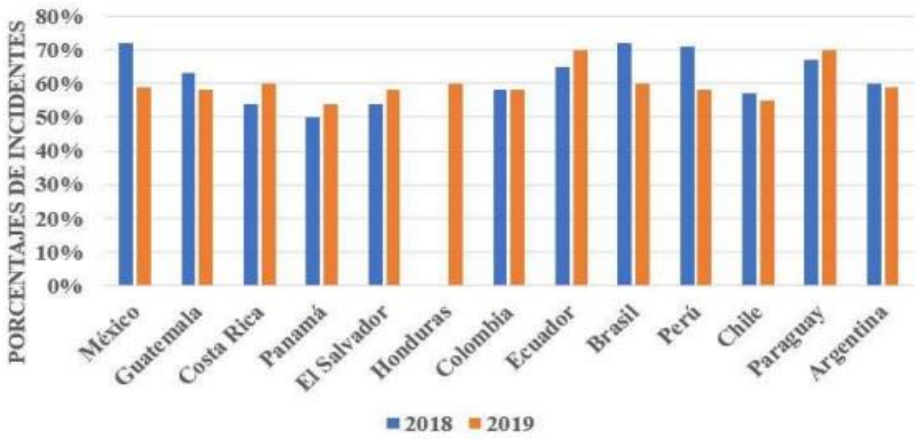
Por ese motivo, estos países comenzaron a utilizar Blockchain para la seguridad de la información y las transacciones. A continuación, se muestran los porcentajes de incidentes registrados mayormente en organizaciones públicas de cada país.

**Figura 2 Criminalidad en Colombia año 2023**




Fuente: *CAI Virtual (2022)*

**Figura 3 Incidentes cibernéticos en los últimos años en países de Latinoamérica**




Fuente: Wang (2019)

1. **Ataques que se producen contra el derecho a la intimidad:** Delito de descubrimiento y relevación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos (artículo del 197 al 201 del código penal).
2. **Infracciones a la propiedad intelectual a través de la protección de los derechos de autor:** Cuando se realiza la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas (artículos 270 y otros del código penal).
3. **Falsedades:** Documentos soporte materiales que exprese o incorpore datos relacionados con débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad. (artículos 386 y ss. Del código penal).
4. **Sabotajes informáticos:** Se provoca la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (artículo 263 y otros del código penal).

5. **Fraudes informáticos**: Se realizan estafas a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (artículos 248 y ss. Del código penal).
6. **Amenazas:** Realizadas por cualquier medio de comunicación. (artículos 169 y ss. Del código penal).
7. **Calumnias e injurias:** Difusión por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (artículos 205 y ss. Del código penal).
8. **Ciberinducción al daño físico:** Para este tipo de delito, la población infantil y juvenil es la más vulnerable. Ya que estos, tienen cada vez más interacciones en el mundo digital. Entre algunos hallazgos detectados, se identificaron 15 grupos delictivos a nivel mundial en la red de Facebook (ballena azul, reto del hada de fuego), 3 grupos eliminados en Colombia (Facebook), 4123 usuarios que se les impidió el acceso a estos grupos, 1 alerta mundial INTERPOL (circular morada), y muchos más, sin embargo, las redes sociales son un tema muy complejo de frenar debido a la cantidad de usuarios que a ellas ingresan diariamente (Karpensky, 2017).
9. **Estafa por suplantación de simcard:** Esta modalidad criminal se presenta cuando el titular del dispositivo está ausente, se solicita una nueva sim para suplantarlo, sincronizando todo lo que a ella está ligada, aplicaciones, contactos, correos y por ende cuentas bancarias.
10. **Vishing o tráfico de datos personales:** Socialmente, los delincuentes buscan obtener información personal (Karpensky, 2017).
11. **Ciberpirámides:** El desconocimiento sobre la moneda virtual o criptomoneda hace que esto sea motivo de engaños donde se piden inversiones con la finalidad de retener dineros y desaparecer (Karpensky, 2017).

12. **Ransomware: WannaCry y Petya:** Los hackers utilizan esta técnica para bloquear dispositivos y exigir un rescate a cambio de recuperar el acceso. En Colombia este ataque impacto principalmente a las pymes vinculadas al sector productivo del país (Karpensky, 2017).
13. **Ataques a entes gubernamentales:** Durante muchos años, se han presentado este tipo de delitos donde las entidades fueron atacadas por un malware y la utilización de la técnica RAT (Remote Access Tool), el cual permite la entrada de un software malicioso que transfiere dinero, información del sector público, bases de datos, etc. L es una de las modalidades de ciberdelitos más costosas debido a su dificultad y nivel de consecuencias (Cibernético Policial, 2017)
14. **Carding:** Por medio de esta modalidad los ciberdelincuentes comercializan los datos de tarjetas de crédito y débito, cuentas bancarias e información financiera. Los primordiales tipos de ataques de carding son skimming (clonación de tarjetas), intercambio de tarjetas (cambiazo), ataques en atm, phishing (suplantación de sitios web para capturar datos personales) y vishing (falsos call center) (Cibernético Policial, 2017).

A continuación, se condensa en una tabla planteada por Cisco (2020), los delitos informáticos que han sido más comunes en los últimos años.

**Tabla 1**
**Ciberataques más comunes**

| CIBERDELITO | DESCRIPCIÓN |
|---|---|
| **Malware o software malintencionado** | Se camufla tras otros programas o datos, los hackers, sacan provecho de los virus para acceder a los equipos o |

| | |
|---|---|
| | redes. Este provoca la alteración de las redes de Tecnología de Información TI. Los más conocidos son: troyanos, spyware, gusanos, virus y adware**.** |
| **Scripting entre sitios (XSS)** | Ataque que se realizan por medio de "scrpi insertado", que actúa por un vínculo de sitio web o spam que llega a la bandeja de entrada, y cuando este es abierto, el delincuente tiene acceso a la información. |
| **Redes de robots (botnets)** | Varios equipos que se conectan a una red, se infectan por un virus a través de mensajes emergentes o spam. |
| **Ataque de denegación de servicio distribuido (DDoS)** | Sucede cuando varios equipos están pirateados y se dirigen a un sitio o red. |
| **Suplantación de identidad o "phishing"** | Correos electrónicos fraudulentos con nombre falsificado de empresas importantes, que buscan obtener datos de una persona o empresa**.** |
| **Ransomware** | Malware que bloquea o destruye el acceso a sistemas o datos, hasta que se pague una recompensa. |
| **Ataques por inyección de código SQL** | Se realiza a través de un código SQL, y |

| | |
|---|---|
| | el delicuente aprovecha de este software para ingresar a las aplicaciones y robar, o eliminar datos (Likedln, target). |
| **Ataques de intermediarios (MitM)** | Ataques de secretos que ocurren cuando se insertan transacciones entre dos partes. Una vez que el delincuente vulnera el dispositivo se instala un software y se procesa la información de la víctima. |

Fuente: (CISCO, 2020).

**Importancia de la seguridad informática frente a la confidencialidad de la información para prevención de delitos informáticos desde la perspectiva del asesor financiero.**

Las instituciones de servicios financieros son las más vulnerables a los ciberataques, ya que son el objetivo principal de los cibercriminales. La industria de los servicios financieros es de las más susceptible en recibir email malicioso, así como sus clientes (Deloitte, 2014). A continuación, se muestra un mapa de calor que explica el impacto en el sector bancario.

**Tabla 2**

**Mapa de calor de actores e impactos de ciberataques en sector bancario**

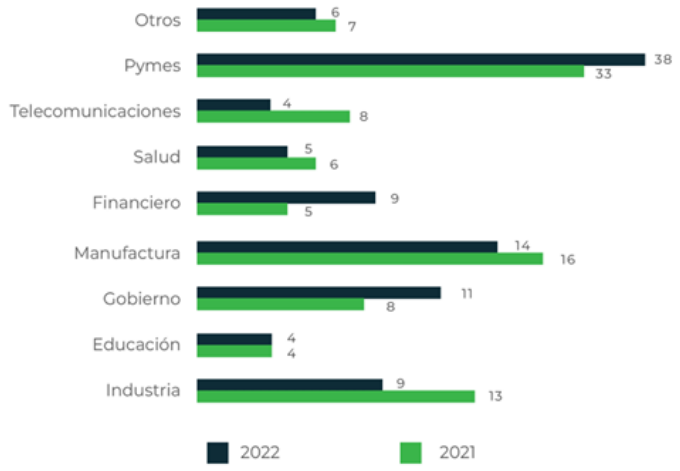
| | IMPACTS | | | | | | |
|---|---|---|---|---|---|---|---|
| **ACTORS** | Financial theft/ fraud | Theft of intellectual property on strategic plans | Business disruption | Destruction of critical infrastructure | Reputation damage | Threats to life/ safety | Regulatory |
| Organised criminals | ↑↑ | → | ↓ | ↓ | ↑↑ | ↓ | ↑↑ |
| Hacktivists | ↑ | → | ↑↑ | ↑ | ↑↑ | ↓ | ↑ |
| Nation-states | ↑ | ↑ | ↑↑ | ↑↑ | ↑↑ | ↓ | ↑↑ |
| Insiders | ↑↑ | ↑ | ↑ | ↑ | ↑ | → | ↑ |
| Third parties | ↑ | → | → | → | ↑↑ | ↓ | ↑↑ |
| Skilled individual hackers | ↑↑ | ↑ | ↑ | ↑ | ↑ | ↓ | ↑ |

↑↑ Very high ↑ High → Moderate ↓ Low

Fuente: (Deloitte, 2014).

Fortinet.( 2022) afirma, que en la primera mitad de 2022, la región de América Latina y el Caribe sufrió 137 mil millones de intentos de ciberataques, lo que representa un aumento del 50% en comparación con el mismo período del año anterior. Para el caso de Colombia según (TicTac, 2023) en su informe de anual de ciberseguridad, las denuncias de ciberdelitos aumentaron un 26 % en el año 2022 comparado al año anterior, aproximadamente cada 8 minutos se registra una denuncia, este mismo informe muestra cuales fueron los sectores más afectados del 2021-2022:

**Figura 4 Sectores afectados en años del 2020-2022**



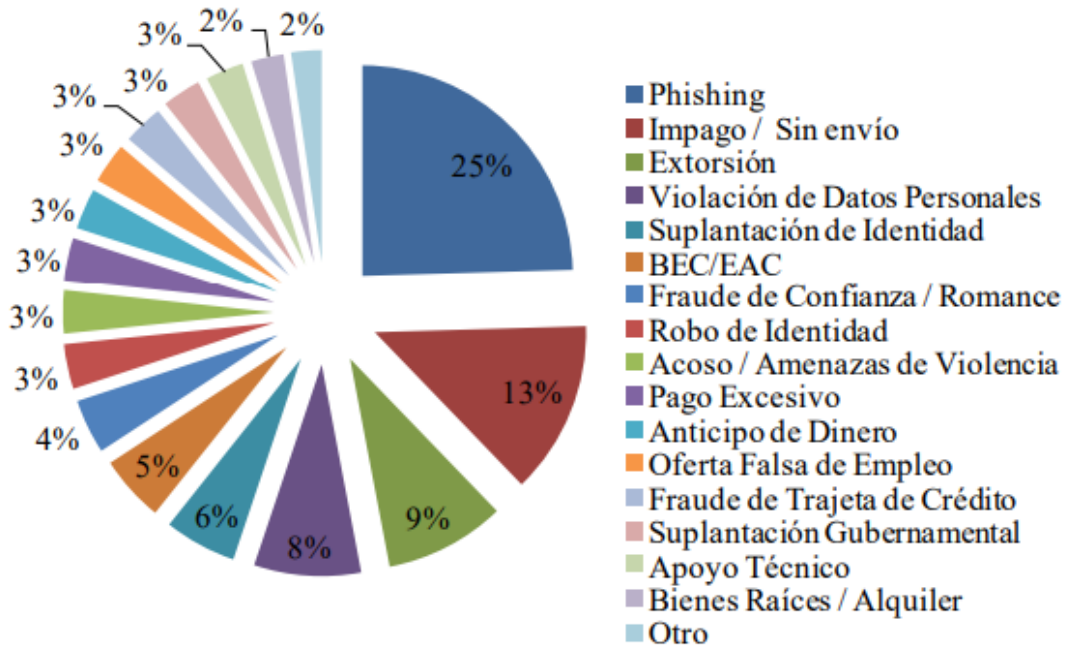

Fuente: Tic Tac (2023)

Los sectores más afectados fueron los industriales, gobierno, educación y salud, en el caso del sector financiero se presenta una disminución, sin embargo, estos datos demuestran la gravedad del problema de ciberdelito en Colombia y una clara necesidad de mejorar y fortalecer la ciberseguridad en todos los sectores (TicTac, 2023), también demuestran que los ciberdelincuentes no tienen preferencia por ningún sector económico, atacando instituciones grandes y medianas de todas las industrias y causando suspensión en el uso de sus sistemas, pérdidas financieras, económicas, pérdidas al no poder generar su operación de manera habitual y afectación de la buena reputación entres otras consecuencias, (Figueroa, 2022).

Según Figueroa (2022) , durante el año 2019, el Pishing ocupó el primer lugar con un mayor número de víctimas, enviando correos electrónicos haciéndose pasar por empresas o entidades bancarias, con la finalidad que los usuarios facilitaran información confidencial de sus cuentas bancarias, tarjetas de crédito upara obtener beneficios económicos. Este tipo de fraude electrónico representó el 25% del total de las denuncias de ciberataques mundiales.

A continuación, se visibilizan estadísticamente, la incidencia de los ciberdelitos en los últimos años.

**Figura 5 Distribución de ataques cibernéticos por tipo**




Fuente: Anton (2021)

Antón (2021), menciona que la implementación de la Inteligencia Artificial (IA), ha permitido que muchas de las actividades que antes eran tediosas y repetitivas, como la recopilación y archivo de datos, las cuentas, entre otras sean optimizadas, generando más cantidad de tiempo libre para que los trabajadores puedan realizar otras tareas importantes. menciona que, la inteligencia artificial es capaz de crear algoritmos que generen un aprendizaje automático, pudiendo analizar gran cantidad de datos de diferente origen e interpretación, detectando patrones y tendencias que ayudan en la toma de decisiones cruciales para una organización empresarial. Lo anterior, permite la reducción de datos y procesos errados, generando resultados más precisos y de calidad. Con esta herramienta, las empresas tienen la

ventaja de poder visualizar a futuro que tanta demanda puede haber, cuanto flujo de efectivo haciendo la empresa más competitiva y eficiente, generando proyecciones altamente confiables.

Sin embargo, aunque la inteligencia artificial sea una herramienta avanzada, es importante aclarar que no está exenta de cualquier delito informático, por lo tanto, los datos deben estar asegurados de tal manera que ningún error informático y del sistema perjudique el trabajo realizado.

Frías (2023) enfoca el uso de la inteligencia artificial, hacia el ejercicio del contador, mencionando que el uso de esta, colabora en un 85% en la reducción de las tareas usuales, independientemente del tamaño de la compañía; sin embargo eso no quiere decir que esta profesión esté cercana a desaparecer, sino que la IA es una herramienta que fortalezca el ejercicio de la misma para su eficiencia, llegando a reducir en un 30% las actividades repetitivas, siendo utilizado este tiempo para realizar otras tareas importantes.

Claudia (2019) hace una aclaración fundamental, sobre la implementación de la IA A pesar de los beneficios, es vital considerar las preocupaciones sobre la implementación de la IA en la contabilidad. La resistencia al cambio y el temor a la obsolescencia profesional son inquietudes comprensibles. Sin embargo, es importante comprender que la IA, mencionando que esta no reemplaza a los profesionales –ya que esta es una de las preocupaciones más latentes-, sino que los asiste.

La IA, tiene la capacidad de proteger la manipulación de datos financieros sensibles, por lo que es fundamental usarla contra amenazas cibernéticas para que toda la información esté salvaguardada (Flores, 2018).

La inteligencia artificial en la actualidad ha tenido una evolución muy grande, y por ende ha tenido una influencia importante en el sector financiero, ya que gracias a esta se han desarrollado

varios bots para poder agilizar los diferentes procesos en este sector (Colombia, 2015), específicamente en lo que tiene que ver con la protección de
datos los bancos los cuales tiene la obligación de velar por la buena administración de los mismos, cabe resaltar que además las bases de datos en Colombia obligatoriamente deben aparecer registradas en la página de la superintendencia de industria y comercio (Colombia, 2015), ya que la normativa vigente, menciona que las empresas en las que sus activos sean mayores a 100.000 UVT (Unidad de valor tributario) están
obligadas a reportar sus bases de datos sin falta alguna según lo estipulado por la ley (Colombia, 2015).

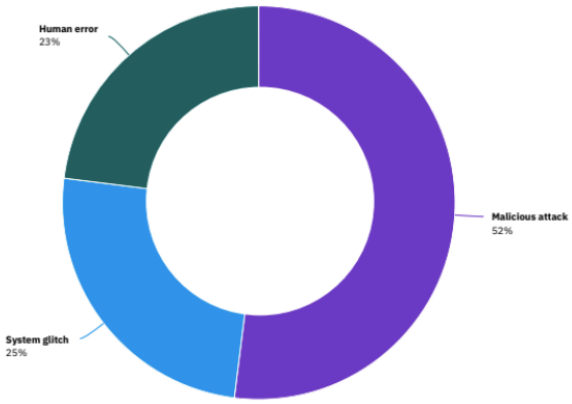
**Importancia De La Seguridad Informática Frente a La Confidencialidad De La Información Para Prevención De Delitos Informáticos Desde El Sector Financiero**

Según Eckenrode & Friedman, (2018) la mitad de las grandes empresas del sector financiero afirman que el gasto en gestión de riesgos cibernéticos considera un gasto de 20 millones de dólares o menos. Esto significa que la mitad de las empresas gastan un 1% o menos de sus ingresos en ciberseguridad. Lo anterior no es suficiente, teniendo en cuenta los riesgos de interrupción de las operaciones, la inversión y los posibles gastos de reparación.

Por ello, el desafío para las instituciones financieras es indudablemente, mejorar la rentabilidad mediante el uso seguro de las nuevas tecnologías. Ya que cada vez son más recurrentes los ciberataques y las pérdidas financieras relacionadas con robo de datos van en aumento a medida que pasan los años (Castellanos, 2019). Esto, gracias a que los cibercriminales han aumentado los objetivos potenciales y con ellos sus herramientas para ciberdelinquir. (IBM Security, 2020); por esto, es clave que se invierta en grandes cantidades en ciberdefensa, para así mismo lograr la ser prevención e inteligencia en materia de riesgos para construir una defensa en profundidad con diferentes capas de seguridad; además de que los sistemas de ciberseguridad

tienen que ser monitoreados, revisados y actualizados con regularidad, para lograr seguridad y resistencia (IBM Security, 2020). Es importante tener en cuenta el factor humano, ya que la falta de concienciación y capacitación fomenta procedimientos inadecuados. El error humano suele ser una causa común de filtraciones de datos en instituciones financieras (IBM Security, 2020). Por ello, las instituciones financieras tienen que considerar un sistema de formación a sus empleados para tratar de disminuir los errores humanos en sus organizaciones (IBM Security, 2020).

**Figura 6 Causas de filtración de datos**




Fuente: (IBM Security, 2020).

Colombia, cuenta con medidas que cooperan para que las empresas y las personas (comerciantes, empresarios, etc.) estén actualizadas sobre medidas para evitar situaciones de robo de información (Díaz, 2017). El Centro Cibernético Policial de la DIJIN, es un centro policial de denuncia virtual que busca brindar toda la información que sea necesaria para mantener en conocimiento a las empresas, personas y profesionales de informes sobre las modalidades más frecuentadas por los ciberdelincuentes, como medio de precaución y

prevención para que se tome como referencia las actuaciones que toman para delinquir virtualmente (Díaz, 2017). Además, se encarga de visualizar en tiempo real, Ciberincidentes, de los casos que se han presentado, dando la oportunidad de ver el tiempo en el que se evidenciaron, el tipo de robo de información o modalidad, el lugar y si fue a una persona o a una empresa, en este las personas se pueden dar cuenta que en años anteriores y actualmente en el país se evidenciaron muchos casos de vulnerabilidad y amenaza de la información. Todo lo anterior concuerda, con la modernización de las tecnologías ya habladas anteriormente, done las inteligencias artificiales cumplen su papel, a través de aplicaciones que permiten la disminución de estos delitos, como Polis, que está conectada directamente con la línea de emergencias de la Policía Nacional de Colombia 123, y A Denunciar, un sistema nacional de denuncia virtual, que proporciona agilidad para denunciar ataques cibernéticos (Ojeda, 2010).

Es importante tener en cuenta, que hoy en día se debe tener muy claras las implicaciones y los avances de estos temas, ya que la seguridad informática hace arte de un núcleo fundamental en las empresas. Puede dividirse en algunas categorías

**1) Seguridad de Red:** Protegen una red informática de malware oportunista. Utiliza el acceso a datos que se encuentran almacenados en la red, y pasan a ser controlados por un administrador.

**2) Seguridad de las Aplicaciones:** Proceso para hacer que las aplicaciones sean más seguras al encontrar, corregir y mejorar su seguridad.

**3) Seguridad de la información:** Medidas preventivas y reactivas que permiten resguardar o proteger la información, manteniendo la confidencialidad, integridad y la autenticación de los datos, tanto en el almacenamiento como en el tránsito.

**4) Seguridad Operativa:** Conjunto de procedimientos destinados a minimizar los riesgos a los que están expuestos la información, software y equipos, incluyendo los procesos y decisiones para manejar los recursos de datos.

Según Ojeda, (2010) para llevar a cabo una adecuada seguridad informática debe cumplirse lo siguiente:

- **Protección:** Configuración de software, sistema, aplicaciones y redes, desde su creación hasta su puesta en marcha para garantizar un perfecto funcionamiento.
- **Detección:** Identifica tiempo real si se ha cambiado la configuración de algún mecanismos o aspecto del sistema, equipo o si algún tráfico de red indica un problema.
- **Reacción:** una vez identificado los problemas rápidamente, responder de manera eficaz, eliminando la amenaza y regresar a un estado seguro de funcionamiento.
- **Confidencialidad:** el acceso a las redes, aplicaciones e información solo debe ser permitido a personal autorizado.
- **Autenticación:** la información procedente de un programa, aplicación, carpeta de red o usuario, debe verificada y se debe garantizar que el origen de los datos es correcto y fehaciente.

Por su parte, la DIJIN, también ofrece un mural de cibercrimen, que contiene información sobre modalidades que se vienen presentando como el Phishing, Malware, La carta nigeriana, La Estafa y Smishing, dando la facilidad de brindar ejemplos con imágenes de las estrategias que utilizan los delincuentes para obtener información de otras personas (Roa, 2013).

## Estrategias Para Mejorar La Seguridad Informática

**Inteligencia Artificial (Ventajas y Desventajas):** En la actualidad, los avances tecnológicos son impresionantes, uno de ellos, es la inteligencia artificial, que ha llegado a reemplazar el trabajo del ser humano, haciendo de ella una de las herramientas mas novedosas de todos nuestros tiempos. A continuación, se muestra una tabla que muestra los pros y contra que puede tener el uso de esta herramienta en el sector financiero (Romero, 2024).

**Tabla 3**

**Ventajas del uso de IA en el manejo de la información**

| VARIABLE | DEFINICIÓN CONCEPTUAL | DIMENSIONES |
|---|---|---|
| Aumento de Ataques Cibernéticos en Colombia | La IA ha acelerado la efectividad de las personas que realizan ataques cibernéticos, aún más, para lo nuevos hackers que no tienen experiencia en ello, ya que con herramientas como ChatGPT pueden facilitarles un punto de partida en sus esfuerzos. | Tipos de ataques: Malware - intermediario - inyecciones SQL - contraseñas - manipulación de URL - Phishing |
| Transformación digital en | Analizar la evolución del | 90% de los bancos en |

| | | |
|---|---|---|
| las entidades financieras | sector financiero respecto a la transformación digital. | Colombia aceleraron su transformación. |
| Cumplimiento normativo de protección de datos en el sector financiero | Validar como el sector financiero garantiza el consentimiento de esta norma. | Ley 1266 del 2008 Ley 1581 del 2012 |

Fuente: Romero (2024)

Por su parte, la OEA (Organización de los Estados Americanos) propone que no es suficiente con la utilización de herramientas como la IA, sino que, en definitiva, deben incorporarse métodos de ciberseguridad, donde debe tenerse en cuenta el tipo de empresa al que se le aplica, como se explica a continuación:

**Tabla 4**

**Ciberseguridad, según la empresa**

| **ENTIDADES FINANCIERAS GRANDES** | **ENTIDADES FINANCIERAS MEDIANAS** | **ENTIDADES FINANCIERAS PEQUEÑAS** |
|---|---|---|
| En el 33% solo hay un área responsable de seguridad digital. | El 85% es responsable de la seguridad digital, | El 82% es responsable de la seguridad digital, |
| En el 75% hay dos niveles | En el 80% hay dos niveles | En el 83% hay dos niveles |

| | | |
|---|---|---|
| jerárquicos entre el CEO y el máximo responsable de la seguridad digital. | jerárquicos entre el CEO y el máximo responsable de la seguridad digital | jerárquicos entre el CEO y el máximo responsable de la seguridad digital. |
| La mayoría de las entidades 50% cuenta con equipo de 16- 30 miembros. | La mayoría de las entidades 48% cuenta con equipo de 1- 5 miembros. | La mayoría de las entidades 85% cuenta con equipo de 1- 5 miembros |
| Son objeto de ataques de todo tipo de eventos de seguridad digital. | Son objeto de ataques de todo tipo de eventos de seguridad digital. | Son objeto de ataques de todo tipo de eventos de seguridad digital. |
| El 80% tienen incidencia de malware. | El 25% tienen incidencia de malware. | El 13% tienen incidencia de malware. |
| La mayoría detecta un 61% a 80% de eventos con sistemas propios. | La mayoría detecta un 31% a 80% y 100% de eventos con sistemas propios. | La mayoría detecta un 47% a 80% y 100% de eventos con sistemas propios. |
| El 83% realiza evaluación de madurez y realiza acciones correspondientes. | El 50% realiza evaluación de madurez y realiza acciones correspondientes. | El 50% realiza evaluación de madurez y realiza acciones correspondientes. |
| El 100% ofrece mecanismos para reportar incidencias. | El 88% ofrece mecanismos para reportar incidencias. | El 73% ofrece mecanismos para reportar incidencias. |
| El 50% reporta entre el 0% | El 42% reporta entre el 0% | El 40% ofrece |

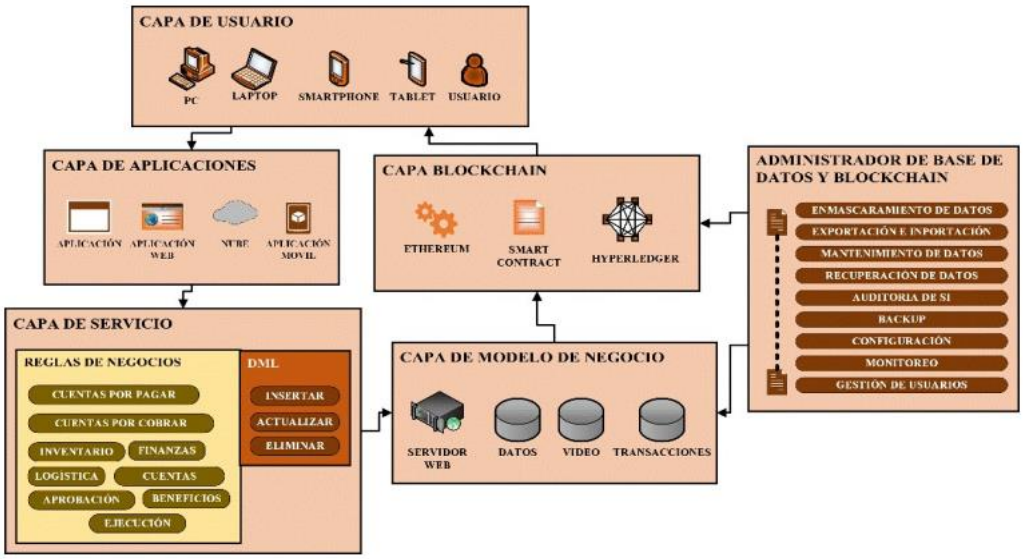
| | | |
|---|---|---|
| y el 20% reportados en la fiscalía general de la Nación. | y el 20% reportados en la fiscalía general de la Nación. | mecanismos para reportar incidencias. |

OEA (2020)

Escalante, (2021) menciona que el Blockchain es una metodología moderna, que permite mantener la seguridad en la información que se administra en algunas organizaciones, a través de un sistema de cinco capas, muy bien estructuradas y programadas para cumplir su finalidad, además contiene el sistema que gestiona la seguridad de los movimientos de la información dentro de la organización, manejando datos encriptados para envío o registro de información como se muestra a continuación:

- **Capa usuarios:** Se administran usuarios que ingresan al sistema de acuerdo con su rol, y deben ser internos de la organización, como trabajadores y usuarios externos como clientes o proveedores de servicios. Pueden acceder computadores, celulares inteligentes, tablets, entre otros.
- **Capa de aplicaciones: S**e identifican aplicaciones del sistema para usuarios públicos y privados, conectando con el servidor de la base de datos.
- **Capa de servicios:** Se establecen reglas de negocios que funcionan como procesos para interactuar negocio-aplicación, permitiendo procesos de manipulación de datos para el ingreso de información al servidor de almacenamiento.
- **Capa de modelo de negocio:** Es la base de datos transaccional que almacena los movimientos de los usuarios que se encuentran utilizando las aplicaciones.

**Figura 7 Prototipo de arquitectura de gestión de seguridad Blockchain**




Fuente: Escalante (2021*)*

**Antivirus:** Es muy importante mantener el software actualizado para obtener el mejor nivel de protección. El tipo de antivirus a utilizar depende de necesidades o requerimientos de cada usuario (Gorham, 2019).

**Cortafuegos:** Es un sistema que ejecuta una política de seguridad establecida, filtrando accesos de red y bloqueando la accesibilidad a personas no autorizadas (Hernández, 2020).

**Proxy:** Es un complemento del firewall ya que hace la función de intermediario, permitiendo el control de acceso, registro del tráfico, la mejora de rendimiento y el anonimato de la comunicación (Hernández, 2020) .

**Listas de control de acceso:** Estas listas permiten determinar los permisos de acceso apropiados a usuarios y grupos concretos (Gorham, 2019).

**Sistema de prevención de intrusos:** Es un sistema que soporta los dispositivos inalámbricos para evitar los puntos de acceso no autorizados y otras amenazas inalámbricas.

Estos métodos, son avalados por el Consejo Superior de Administración que permite el análisis y gestión de riesgos. Se verifica que sea funcional para todos aquellos que archivan su información de manera digital y permite saber cuánto valor está en juego y ayuda a protegerlo, dando a entender que conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos (Aguinaga, 2013).

Por lo tanto, se genera conciencia a las organizaciones sobre el riesgo que corre la información y la importancia de protegerla, a través de procesos sistemáticos que analizan los riesgos de las tecnologías de la información y comunicación (TIC). Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC); preparando indirectamente a cualquier empresa para procesos de evaluación, auditoría, certificación o acreditación (Aguinaga, 2013).

Bueno, (2022), dice que el concepto de ciberseguridad desde el siglo XX, la sociedad ha tenido una evolución tecnológica impactante, que ha estado relacionada con el aumento de las necesidades de la misma. Para el entendimiento de este término, se debe entender el concepto de 'ciberespacio', que es conjunto de sistemas de la información y telecomunicaciones que utilizan las TIC (Tecnologías de la Información y la Comunicación), es decir de redes de ordenadores, mucho más que Internet, más que los mismos sistemas y equipos.

De esta manera podemos decir que, este concepto está relacionado con todo lo que está dentro de los computadores y las redes, involucrando también a aquellos que navegan allí, llamados, cibernautas (Becerra, 2019).

Por su parte Acurio Del Pino (2016) se refiere a los delitos informáticos como actos asociados a los computadores, en los cuales, la victima sufre un daño o una pérdida y hay otros individuos beneficiados. Entonces, cuando se comete, una acción que involucre a un computador como

objeto, sujeto, instrumento o símbolo donde una persona tuvo una pérdida y otra tuvo una ganancia se clasifica como delito informático.

En los años 50, gracias a Alan Turing comenzaron las primeras apariciones de este término, gracias a que logró que una máquina simulara la inteligencia del ser humano. Sin embargo, solo fue en los inicios del siglo XXI, cuando se logró desarrollar con más amplitud alcanzando a realizar reconocimiento de imágenes, desarrollo de desafíos, transformación de lenguajes y construcción de redes neuronales profundas (Abeliuk & Gutiérrez, 2021). La IA es un término, que se refiere a la capacidad de las máquinas para recepcionar datos y a partir de ellos tomar decisiones, una acción muy similar a la de los seres humanos, pero con menos margen de error (Rouhiainen, 2018). Lo anterior sucede porque, la IA se basa en un aprendizaje automático y la toma de decisiones es sistemática; un ejemplo de ellas son Google y Facebook, aplicaciones que están dirigidas constantemente por IA, que mide algoritmos para ubicar y sugerir lo que la persona necesita (Luo, 2018). Por ello, es indiscutible, que la tecnología actual, se ajusta a los servicios y contenidos que se requieren en cada empresa o en cada usuario, generando servicios agradables y satisfactorias (Luo, 2018).

Hoy en día, es una herramienta que involucra muchos campos de acción, como las matemáticas, ingenierías, informática, biología, estadística, entre otras ciencias (Barrios et al., 2020).

Es importante que para que todas las herramientas anteriormente mencionadas tengan un efecto, debe cumplirse lo siguiente:

**Confidencialidad:** Hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos. Tiene como finalidad El objetivo de la confidencialidad es, entonces, prevenir la divulgación no autorizada de la información. En general, cualquier empresa

pública o privada y de cualquier ámbito de actuación requiere que cierta información no sea accedida por diferentes motivos (CCM, 2015).

**Integridad:** Hace referencia a la fidelidad de la información, su objetivo es prevenir modificaciones no autorizadas de la información (CCM, 2015).

Disponibilidad: Hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados. Su objetivo es prevenir interrupciones no autorizadas de los recursos informáticos (CCM, 2015).

## Referencias

Abeliuk. A, & Gutiérrez, C. (2021). History and evolution of artificial intelligence. Revista Bits de Ciencia.

Acurio Del Pino, S. (2016). Delitos informáticos: generalidades.

Aguinaga Espinoza, H. R. (2013). Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.

Antón Serrano F. (2021). Inteligencia artificial y administración tributaria: eficiencia administrativa y defensa de los derechos de los contribuyentes. ARANZADI / CIVITAS.Barrios, A., Díaz Pérez, V., & Guerra, Y. (2020). Subjetividades e inteligencia artificial: desafíos para ¨lo humano¨.

Becerra, J. et al. (2019). La seguridad en el ciberespacio. Un desafío para Colombia. Escuela Superior de Guerra.

Benz, M., y Chatterjee, D., (2020). Calculated risk A cybersecurity evaluation tool for SMEs,

Bongianino, C (2019). La aplicación de la inteligencia artificial en la contabilidad privada y en el sector gubernamental.

Bnamericas (2023). Los países de Latinoamérica más preparados para la IA.

Branch, A. (2021). Estadísticas de la situación digital de Colombia en el 2020-202.

Bryson Jonson. J. (2018). La última década y el futuro del impacto de la IA en la sociedad.

Bueno Munar, L (2022). Ciberseguridad en Colombia, avances y retos.

Castellanos, W (2019). Retos de gestión de riesgo cibernético en la Transformación Digital.

Cibernético Policial.

CISCO (2020) ¿Cuáles son los ciberataques más comunes? Recuperado el 1 de julio de 2024, CCM (2015). Introducción a la seguridad informática.

Clay, A (2021) Estadísticas de la situación digital de Colombia en el 2020-202.

Coll Morales, F (2020) Revolución Digital.

Colombia, G. d. (2015). Gobierno de la república de Colombia. Obtenido de Decreto 1074 de 2015 Sector Comercio, Industria y Turismo.

Delgado Olivera L., & Díaz Alonso L. (2021). Modelos de Desarrollo de Software. Revista Cubana de Ciencias Informáticas.

Deloitte. (2018). ¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?

Díaz, B, Tarapuez, E., & Hernández, R. (2017). Estrategia y calidad en empresas colombianas de servicios. Revista Venezolana de Gerencia.

Ferreira Barreto, J, & Torres, Petit, E (2017), Modelos explicativos del proceso de innovación tecnológica en las organizaciones. Revista Venezolana de Gerencia.

Eckenrode, J. & Friedman, S. (2018). The state of cybersecurity at financial institutions. There's no "one size fits all" approach. Deloitte Insights & Financial Services Information Sharing and Analysis Center.

El Tiempo (2021). Aeronáutica Civil recibió ataque cibernético. Recuperado de: https://www.elcolombiano.com/colombia/secuestro-a-informacion-del-dane-encolombia-IE16031966.

Escalante Quimis, O (2021). Prototipo de sistema de seguridad de base de datos en organizaciones públicas para mitigar ataques cibernéticos en Latinoamérica.

Flores Molina, F. & López Fernández, E (2018). La inteligencia artificial en el ámbito contable.

Fortinet (2022). Informe de amenazas cibernéticas de América Latina y el Caribe. Fortinet.

Fortinet (2023). Ciberseguridad en Colombia para el año 2023.

Figueroa Cubillos, T. (2022). Ciberataques, riesgos y consecuencias que han afectado a la población colombiana entre los años 2018 y 2020.

Frías, N. (2023). La era de la automatización y la inteligencia artificial en la contabilidad. 2023 Agencia de Noticias Panamá.

García Monje, R. (2017). *Seguridad informática y el malware* (Bachelor's thesis, Universidad Piloto de Colombia).

IBM Security (2020). Cost of a Data Breach Report.

Gobierno Nacional De Colombia - MARCO ÉTICO IA. (2021). MARCO ÉTICO. Bogotá. DC.

Gorham, M. (2019) Internet Crime Report", Federal Bureau of Investigation,

Hernández Martínez, R & Dopico, Blanco (2017). Gestión de riesgos: reflexiones desde un enfoque de gestión empresarial emergente. Revista Venezolana de Gerencia.

Hernández. (2020). Radiografía | Estos son los países más ciberseguros del mundo. [Online].

Hernández Fernández, J.y Baptista H. (2010) Metodología de la Investigación. Ediciones Mc Graw Hill. México.

INSTITUTO AMERICANO DE CONTADORES PÚBLICOS AICPA, Extraordinario ante el desafío: Barry Melancon reflexional sobre 2021.

Jaimovich, D. (2018). Infobae. Obtenido de Infobae: https://www.infobae.com/america/tecno/2018/09/25/cuentas-bancarias-en-la-mira-9-de cada-10-entidades-financieras-en-america-latina-fueron-blanco-de-ciberataques-en-el ultimo-ano/

Luo, J., Meng, Q., & Cai, Y. (2018). Analysis of the impact of artificial intelligence application on the development of accounting industry. Open Journal of Business and Management.

Mayorga Jácome , T., García Jiménez , M., Duret Gutiérrez, J., Carrión Jumbo, J., & Yarad Jeada, P. (2019). Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos.

Ninja, T. (2024). Estadísticas de ciberseguridad que toda PYME y MSP debe conocer en 2024.

Ojeda Pérez, J, Rincón Rodríguez, F., Arias Flórez, M. E., & Daza Martínez, L (2010), Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad.

Peña Jiménez, Y. (2019). Comercio electrónico ventajas y desventajas.

Ramírez Mesa, C., & González López, J (2020). Guía de Controles y Buenas Prácticas de Ciberseguridad para MiPymes.

Roa Buendía, J. (2013), Seguridad informática. Madrid, SPAIN: McGraw-Hill España. Semana. (2024), Así está Colombia en el ranking de ciberseguridad mundial.

Romero Barrero, R. Urrego Vergara, V. & Zamora Chaves, N. (2024). Impacto de la inteligencia artificial en la protección de datos en el sector financiero (Bachelor's thesis, Especialización en Administración Financiera Presencial).

Sain, K.. (2021). Equipos de trabajo de 110 empresas recibirán capacitación gratuita en ciberseguridad con el Ministerio TIC.

Santos Vidal, M. (2022). Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento: respuestas del Estado ecuatoriano en el período 2013-2022 (Master's thesis, Quito, EC: Universidad Andina Simón Bolívar, Sede Ecuador).

Universidad Estatal a Distancia (2019) Misión y visión de la UNED. San José, Costa Rica.

Vera; L (2015) La Investigación Cualitativa. Universidad Interamericana de Puerto Rico. Recinto de Ponce.

Wang, M., Cobeña, L, Gallegos, M.: Analysis of cyberattacks in public organizations in Latin America. Adv.

Zunzunegui, F. (2018). La digitalización de los servicios de pago (Open Banking). *Revista de Derecho del Mercado Financiero Working Paper*,