**TRABAJO DE GRADO**
**Opción Seminario-Diplomado.**

# Análisis De Amenazas Cibernéticas En Las Organizaciones Que Manejan Su Información Contable Y Financiera En La Nube

Corporación Universitaria Remington.
Facultad de Ciencias Contables
Contaduría Publica

Eliana Maritza Bohórquez Barinas[1]
Leydi Yohana López Cruz[2]
Shirley Johanna Rivillas Villamizar[3]
Opción de Trabajo de grado Seminario-Diplomado.
2024

[1] Estudiante decimo semestre de Contaduría Publica, Uniremington sede Sogamoso. E-mail: eliana.bohorquez.7184@miremington.edu.co
[2] Estudiante decimo semestre de Contaduría Pública, Uniremington sede Sogamoso. E-mail: leydi.loopez.6190@miremington.edu.co
3 Asesora Metodológico Seminario NIAS, Uniremington E-mail: srvillamizar@hotmail.com

## Tabla de Contenidos

**Resumen**

La ciberseguridad es un elemento importante en las organizaciones actuales, ya que la transformación digital y la adopción de la nube para procesos contables y financieros aumentan los riesgos de vulneración de información sensible. En este contexto, es fundamental proteger la información financiera y contable que se elabora y comparte en entornos digitales, garantizando su integridad, confidencialidad y disponibilidad. .

Por lo anterior, cobra especial importancia la seguridad cibernética de la información dentro de las organizaciones; en cualquier circunstancia que se presenten ataques cibernéticos que puedan afectar la economía de las organizaciones, por pérdida o robo de información generando riesgos a los recursos y/o activos económicos, disminuyendo la estabilidad y confianza de la organización.

Palabras Clave: Ciberseguridad, riesgos y ataques cibernéticos.

# Objetivos

## Objetivo General

Analizar las amenazas cibernéticas más comunes en las organizaciones que manejan su información contable y financiera en la nube a partir de una revisión de información secundaria.

## Objetivos Específicos

1. Revisión de conceptos básicos sobre riesgos cibernéticos más comunes en las organizaciones.
2. Identificar los riesgos cibernéticos más comunes y como afectan las organizaciones.
3. Concluir respecto a la importancia de la ciberseguridad en las organizaciones.

## Pregunta Orientadora De La Búsqueda

La ciberseguridad en las organizaciones es un proceso interno fundamental y de gran importancia para su desarrollo en la actualidad; ya que están siendo víctimas de ataques cibernéticos, donde su información contable y financiera sea perjudicada, lo cual puede generar pérdidas económicas y desconfianza para el desarrollo de las operaciones de los negocios en las organizaciones, para ello se debe tener en cuenta:

¿Cómo afectan los riesgos de ciberseguridad la información contable y financiera de las organizaciones?

## Metodología De Búsqueda De La Información

La metodología de investigación fue bajo revisión narrativa a partir de la búsqueda de información en artículos científicos y normatividad aplicable en documentos institucionales, sobre los riesgos de la ciberseguridad en las organizaciones

### Identificación De Bases De Datos Consultadas

Las bases de datos consultadas fueron principalmente las bibliotecas institucionales como Uniremington, elibro.net que es una biblioteca digital de gran proporción donde se encuentra la información con nuestro tema de ciberseguridad.

## Sustentación Teórica De La Pregunta

En las organizaciones a nivel mundial y en la actualidad la gran parte de la información económica de la empresa, específicamente la contable y financiera se maneja con sistemas informáticos en la nube, donde esta información se encuentra bajo el riesgo de cibercriminales afectando la reputación, crecimiento, confianza y economía de las organizaciones; siendo determinante preparar a los directivos, auditores y demás participantes de la información, para que amplíen sus conocimientos y capacidades para uso adecuado de la Tecnologías de la Información y la ciberseguridad de los datos que allí se comparten.

Para reconocer los riesgos a los que se enfrentan las organizaciones en ciberseguridad identifiquemos los siguientes conceptos:

1. **Malware:** Hace referencia a software malicioso propagado frecuentemente a través de correos electrónicos comúnmente con archivos de descargas existen varios tipos como virus que afectan todo el sistema informático, troyanos que se asemeja a un software legitimo robando información, spyware programa secreto que guarda la información para ser utilizada por los cibercriminales y los ransomware bloquea archivos y datos de usuario como amenaza para borrar información.
2. Phishing: Ataque a través de correos electrónicos mediante los cuales se solicita información confidencial suplantando empresas legitimas; por medio

de un clic motivan a los usuarios a ingresar datos sensibles y acceder a la información.

3. **Ataque "Man-in-the-middle":** Es una ciber amenaza donde interceptan la comunicación de varios individuos a través de las redes wi-fi abiertas no seguras, donde interceptan la transferencia de datos entre las víctimas y la red, donde pueden obtener información sensible.
4. **Ataque de negación de servicio (DoS Y DDoS):** Por medio de estos ataques los cibercriminales impiden que un sistema informático cumpla con solicitudes legitimas, sobrecargando redes y los servidores con tráfico, convirtiéndolo en un sistema inutilizable, impidiendo que se realicen funciones vitales.
5. **Ataques por fuerza bruta:** Por medio de estos ataques los cibercriminales intentan acceder a cuentas de usuario, ingresando con varios usuarios y claves que se ingresan en las diferentes aplicaciones o sitios web utilizados.
6. **Ataques de Reconocimiento:** Es un estudio preliminar que realizan los ciberdelincuentes o hackers para obtener información de forma encubierta toda la información posible sobre un sistema objetivo.
7. **Amenaza interna:** Es un riesgo de seguridad introducido por personal con malas intenciones dentro de la organización, teniendo acceso de alto nivel a los sistemas informativos, desestabilizando la seguridad de la infraestructura internamente.

Conociendo los probables riesgoscibernеticos mencionaos anteriormente, podemos a analizar a partir de ellos la importancia de la seguridad en las organizaiones de acurdo a la reviciona narrativa de estre trabajo, teniendo en cuenta:

Urcuqui, C. C. & Navarro Cadavid, A. (2022). Ciberseguridad: "**Ciberseguridad** es el área de las ciencias de la computación encargada de proponer mecanismos para la protección de los sistemas informáticos, redes de telecomunicaciones e información de posibles acciones maliciosas provenientes de cibercriminales." - "Ataques cibernéticos y amenazas cibernéticas: Un ataque informático es el resultado de la motivación de un individuo que aplica al menos un método sobre una o más vulnerabilidades de un objetivo; dependiendo del contexto, un atacante puede aplicar varios tipos de ataque informático, los cuales se pueden clasificar en: pasivos, activos, cercanos, con privilegios o distribuidos"

En las organizaciones el área de sistemas debe tener un proceso estandarizado de seguridad de la información, así como los sistemas, dispositivos y redes que se puedan manejar el personal de esta área estén respectivamente capacitados con el proceso cibernético y con los riesgos actuales que se pueden presentar utilizando las herramientas que estén implementadas para la reducción de los ataques cibernéticos a los que las organizaciones puedan verse expuestos en el momento de emitir, transmitir, reproducir y compartir la información en todos los sistemas informáticos internos y externos; cabe recalcar que todo este proceso puede ser auditable para verificar de forma efectiva las consecuencias y beneficios económicos, financieros y reputacionales para las organizaciones.

En las organizaciones donde se comparte la información económica, contable y financiera a través de tecnologías de información, el personal encargado de esta información deben estar capacitados en ciberseguridad, la protección, vulnerabilidad que representa el manejo información de acuerdo a los procesos internos que cada organización maneja; es importante que las áreas encargadas con la ciberseguridad de las organizaciones su labor sea desarrollada en conjunto con el área de sistemas para poder auditar y/o verificar de forma interna los procesos que allí se manejan y así salvaguardar los procesos en estas áreas generando seguridad y confiabilidad a la organización y su visualización para los clientes de la información compartida.

De acuerdo a Deutsch, V. E. (2022). “En la actualidad cada vez son más las empresas víctimas de ciberataques que generan graves daños para el negocio y ponen en entre dicho la reputación y confianza en ellas, reduciendo considerablemente su valor”; La mayoría de las organizaciones deberían interesarse de manera relevante para realizar auditorías internas focalizadas al sistema de seguridad de los sistemas informáticos para proteger toda la información que allí se emite, tramite y comparte, ya que en la actualidad los ciberdelincuentes están buscando herramientas para poder afectar las T.I. que se manejan en las organizaciones causando afectaciones en sus estructuras económicas y su nivel de confianza para los clientes de estas.

En las organizaciones de gran posicionamiento más allá de las afectaciones económicas existe un aspecto relevante: la reputación; convirtiéndose en un foco de gran

atención para los ciberdelincuentes, ya que muchos de estos buscan debilitar la confianza de las organizaciones, generando inestabilidad para los usuarios de la información.

## Conclusiones

En la actualidad, la ciberseguridad hace parte vital de las organizaciones, ya de acuerdo a los avances constantes del mundo hay mucha información que se comparten de ellas en los sistemas informáticos, pero sobre todo en la nube y que puede afectar de manera contundente la exposición económica de esta en niveles económicos, financieros y de confianza para los mercados.

Por lo que como directivos, auditores y coordinadores de todas las áreas en las organizaciones se deben conocer los riesgos cibernéticos por medio de la prevención para lograr seguridad y estabilidad en el tipo de información que las organizaciones emiten, comparten y transmiten atreves de dispositivos y demás herramientas tecnológicas.

Los directivos en las organizaciones deben generar respaldo y confianza sobre la información que se transmite por medio de las tecnologías informáticas, por medio de capacitaciones con procesos o sistemas que estén a la vanguardia junto con los colaboradores encargados de los sistemas de información y los encargados y transmitir esta información, para que la detección de riesgos y/o vulnerabilidades para la compañía sean detectables y reducidos a tiempo, para lograr que las compañías sean reconocidas y confiables dentro de los mercados y usuarios de su información.

## Bibliografía

Urcuqui, C. C. & Navarro Cadavid, A. (2022). *Ciberseguridad: los datos tienen la respuesta:* (1 ed.). Editorial Universidad Icesi. https://elibro.net/es/lc/remington/titulos/225844

Deutsch, V. E. (2022). *Ciberseguridad para directivos: riesgos, control y eficiencia de las tecnologías de la información:* (1 ed.). LID Editorial España. https://elibro.net/es/lc/remington/titulos/269669

Ramírez Pascual, B. (Coord.). (2023). *La ciberseguridad en la era de la Inteligencia Artificial: dilemas y retos empresariales:* (1 ed.). LA LEY Soluciones Legales S.A. https://elibro.net/es/lc/remington/titulos/248924