CIBERSEGURIDAD, RETO EMPRESARIAL PARA AFRONTAR LA ERA DE LA DIGITALIZACION ACTUAL.

William David Cano
Santiago Monsalve Machado

Docente

PhD. Ana María Vélez Evans

Universidad Pontificia Bolivariana
Facultad de Administración, Economía y Negocios
Investigación II
2023

CIBERSEGURIDAD, RETO EMPRESARIAL PARA AFRONTAR LA ERA DE LA DIGITALIZACION ACTUAL.

William David Cano
Santiago Monsalve Machado

Trabajo de grado para optar al título de Negocios Internacionales.

Docente

PhD. Ana María Vélez Evans

Universidad Pontificia Bolivariana
Facultad de Administración, Economía y Negocios
Investigación II
2023

Contenido

Lista de figuras

Tema: Inteligencia artificial.

Título: Ciberseguridad, reto empresarial para afrontar la era de la digitalización actual.

Problema de investigación: Las organizaciones presentan carencias en medidas tecnológicas destinadas a controlar su seguridad informática, generándoles perdidas de información por acceso de terceros o internos de la organización.

RESUMEN

El problema central abordado en este estudio se refiere las falencias en las medidas tecnológicas utilizadas por las organizaciones para controlar su seguridad informática; estas deficiencias se han traducido en la pérdida de información por accesos no autorizados, tanto de terceros como de empleados internos de la organización. Esta investigación se centra principalmente en la creciente necesidad de proteger la información y los activos digitales de las empresas en un mundo globalizado y de alta tecnología. La digitalización ha convertido a las organizaciones en blanco de ciberataques que buscan acceder ilegalmente a información confidencial, datos corporativos y recursos financieros.

La metodología utilizada en este estudio se basó en un enfoque cualitativo que se centró en una comprensión profunda y contextual del fenómeno de la ciberseguridad de las empresas actuales desde una perspectiva subjetiva. La atención se centró en la interpretación y significado de los factores mencionados en el estudio; Se trata de un estudio descriptivo que tuvo como objetivo describir y comprender las características y fenómenos relacionados con la ciberseguridad en la era digital, sin intentar establecer relaciones causales ni hacer predicciones.

Como hallazgo principal se presenta que la alta interconexión de los mundos digital y físico ha hecho de la seguridad digital una preocupación central. Las organizaciones necesitan proteger sus datos y sistemas contra amenazas como ciberataques y fraudes en línea. Las auditorías de seguridad, como la piratería ética, desempeñan un papel importante a la hora de identificar y remediar vulnerabilidades. La conciencia diaria sobre la higiene digital, la vigilancia contra posibles ataques y la aplicación de técnicas de aprendizaje automático para identificar patrones son prácticas importantes para mantener la seguridad de la red. Los autores enfatizan la necesidad de tomar medidas proactivas y utilizar tecnologías innovadoras como el aprendizaje automático para garantizar la seguridad de los datos y activos en el entorno digital. Y como conclusión se tiene que el papel fundamental de la inteligencia artificial (IA) en la seguridad cibernética, destaca su crecimiento explosivo y su contribución al fortalecimiento de la seguridad empresarial. Para prevenir amenazas, garantizar la precisión de los modelos de inteligencia artificial y abordar cuestiones relacionadas con la privacidad y las regulaciones legales, se enfatiza la necesidad de prestar atención a la seguridad en el uso de la inteligencia artificial en la ciberseguridad.

Palabras clave

- Ciberseguridad, Digitalización, Inteligencia artificial, Hackeos, Ciberataques.

INTRODUCCIÓN

En el contexto de una sociedad globalizada que se está desarrollando rápidamente a un nivel tecnológico sin precedentes, el mundo actual está siendo testigo de una confusión de los límites entre las esferas física, digital y biológica. El fenómeno ha provocado un cambio significativo en la dinámica empresarial y económica tanto a nivel empresarial como en la vida cotidiana de las personas. En este escenario, las empresas se ven obligadas a redefinir su visión técnica y metodológica para fortalecer su experiencia y seguir siendo competitivas en el mercado actual.

A medida que las organizaciones adoptan nuevas tecnologías, la necesidad de protegerse también explota, ya que los avances tecnológicos las convierten cada vez más en objetivos de ciberataques. La digitalización ha convertido a las empresas en blanco de ataques maliciosos destinados a vulnerar sus derechos de propiedad intelectual y acceder a información confidencial, desde la estructura interna hasta los datos personales y documentación confidencial de las personas vinculadas a la organización. A pesar de los esfuerzos de grandes corporaciones, pequeñas y medianas empresas y empresas multinacionales por implementar medidas de ciberseguridad, ninguna comunidad está exenta de ciberataques. Según datos publicados, el 57% de las empresas en países como el Reino Unido, Alemania y Estados Unidos sufrieron al menos un ciberataque, y el 42% de ellas enfrentó dos o más ataques en el último año (2019). Este panorama presenta un desafío importante para las empresas, generando incertidumbre y preguntas sobre las medidas necesarias para combatir la creciente amenaza cibernética.

En este contexto global, la pregunta central de esta investigación es: ¿Cuáles son los retos que la era digital impone a las empresas en el ámbito de la ciberseguridad? El propósito de este estudio es comprender los riesgos comerciales derivados de la digitalización, identificar la importancia de la ciberseguridad, analizar los riesgos internos y externos asociados a los ciberataques, definir las ciber herramientas necesarias para proteger los activos digitales e identificar los desafíos que enfrentan las empresas. implementar tecnología cibernética. seguridad mediciones

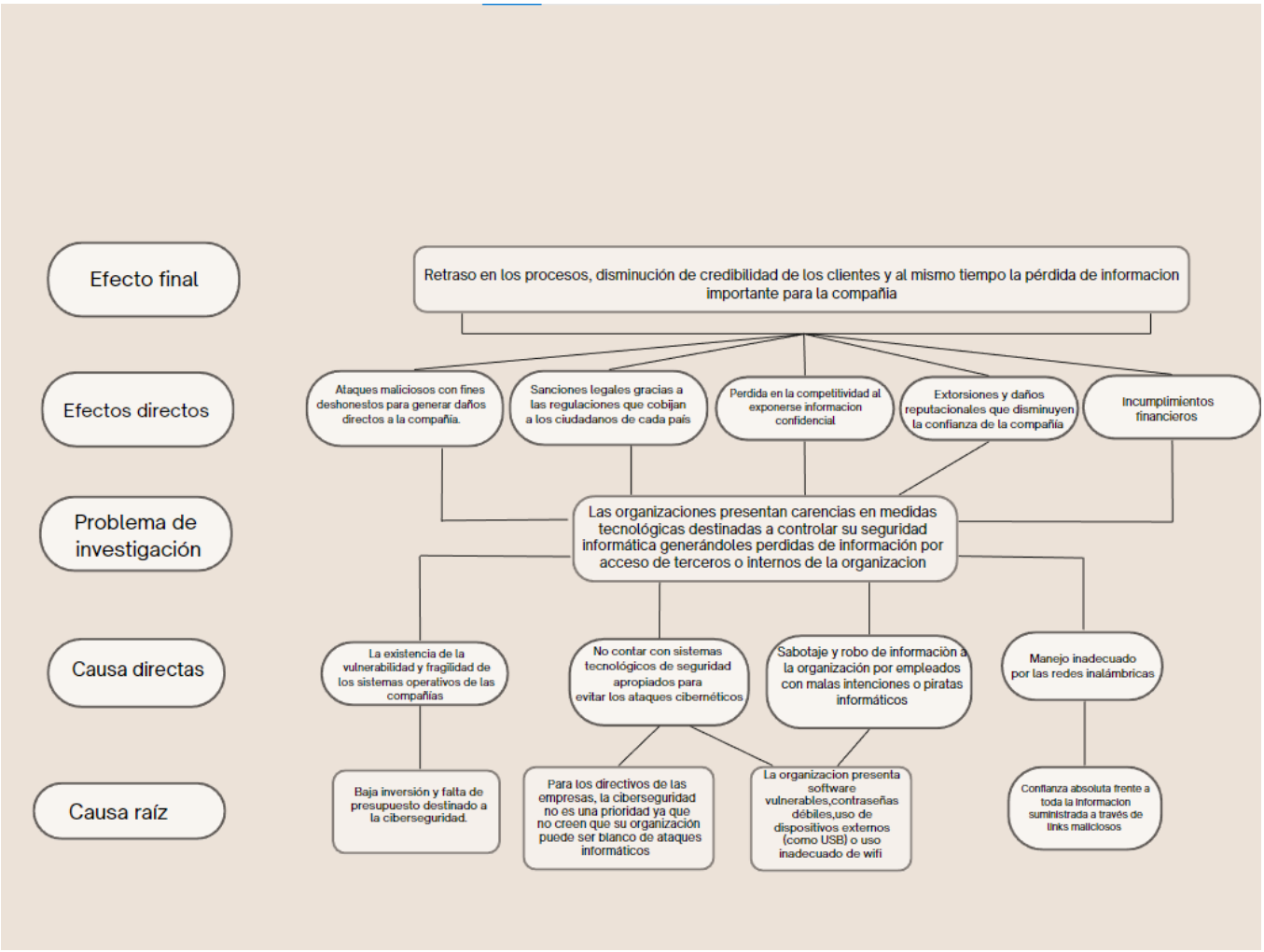
Este análisis en profundidad tiene como objetivo ayudar a comprender mejor cómo las empresas actuales pueden enfrentar y mitigar los riesgos cibernéticos mediante la implementación de medidas proactivas para garantizar la integridad de los datos, la confianza del cliente y la competitividad en la era digital.

1. DESCRIPCIÓN DEL PROBLEMA

1.1 Análisis del problema - Árbol de problemas

Con el propósito de identificar la naturaleza y contexto de la problemática que desarrolla la investigación y para dar mayor claridad y apreciación de esta se aplica la técnica de Árbol de problema para realizar un análisis problema – causa - efecto, que conduce a la construcción los aspectos que enmarcan la situación de estudio; los cuales serán expuestos y analizados posteriormente en los numerales 1.2, 1.3 y 1.4, que se presentan a continuación.

Figura 1. 1 Causas y efectos.



Fuente. Elaboración propia.

1.2. Situación actual del objeto de estudio

Se vive hoy por hoy en un mundo completamente globalizado el cual da pasos agigantados a niveles tecnológicos; un mundo que esta "borrando los límites entre las esferas físicas, digitales y biológicas" Y a su vez un mundo que obliga a un cambio en las relaciones comerciales y económicas tanto de las empresas como de las personas naturales, este nuevo escenario mundial exige completamente a las empresas una nueva visualización de carácter técnico y metodológico dentro de la organización para así generar unas competencias mejor estructuradas y una mayor competitividad en el mercado. (Echeverría Samanes & Martínez Clares, 2018)

Del mismo modo en que se incrementa la visión de incentivar nuevas tecnologías en las empresas, también se incrementa la necesidad de una protección para las mismas, dado que este avance tecnológico convierte a las empresas cada vez más en objetos de ataques cibernéticos con el fin de generar una violación en la propiedad inmaterial de la empresa. La digitalización ha hecho que las empresas se conviertan en foco de ataque malicioso con el fin de una obtención ilegitima de los secretos que a esta le pertenecen, tales como información reservada de la estructura de la empresa, referencias, datos y documentación de las personas vinculadas a la organización, como también bienes monetarios a nombre de dicha compañía.(Díaz, 2018)

Las grandes organizaciones han tratado de crear medidas para proteger sus activos cibernéticos e implementar programas de ciberseguridad para garantizar una solidez en el manejo de su información, pero esto no ha dado los mejores frutos. se conoce que desde las pymes (pequeñas y medianas empresas) hasta las grandes corporaciones son y han sido objetivo de ataques a su información y demás bienes digitales sin importar el sector de la economía en el cual labore la empresa; "El 57% de las empresas británicas, alemanas y estadounidenses han experimentado al menos un ataque cibernético y el 42% de esas organizaciones se han ocupado de dos o más ataques cibernéticos en el último año(2019)", esto nos deja ver que el panorama empresarial para tomar medidas en contra de aquellos personajes externos o internos que buscan la obtención ilegal de ciertos bienes digitales de una empresa, se tornan en una visión no muy positiva, generando incertidumbre en las empresas y a su vez cuestionamientos acerca de que se debería hacer para combatir con este tipo de criminalidad. (*Auditorías en Ciberseguridad*, s. f., p. 2)

La presidenta de la comisión europea, Úrsula von der Leyen citando un discurso sobre este tema deja expresado que: "No podemos hablar de defensa sin hablar de cibernética. En un mundo en el que todo está conectado, todo puede ser hackeado. Vista la escasez de recursos, debemos aunar nuestras fuerzas, y no darnos por satisfechos solamente con lidiar con la amenaza cibernética, sino que tenemos que trabajar para ser líderes en el ámbito de la ciberseguridad", dejando saber así, que dicha problemática es a nivel mundial y genera grandes complicaciones el no resguardarse o generar nuevas metodologías de seguridad para combatir estos atacantes.(*La ciberseguridad en la era de hipercompetitividad: ¿puede la UE afrontar l...: Discovery Service para Universidad Pontificia Bolivariana*, s. f.)

Por otra parte América latina no se queda atrás; al pasar de los años se ha visto de una manera muy directa las afectaciones que ha sufrido la región por dichos ataques que se ven más fortalecidos a causa de una vulnerabilidad mayor que tienen las empresas locales, "Se ha logrado evidenciar que para estos atacantes es posible obtener gran beneficio si el ataque consigue afectar a empresas o entidades de gobierno que aún no cuentan con planes de contingencia o contramedidas ante ataques cibernéticos de este tipo, ante los cual queda como única opción pagar el rescate de la información" lo cual genera pérdidas monetarias y de confiabilidad para la empresa.(Niño, 2023)
Dicha problemática actual de orden mundial hace que se genere un cuestionamiento a las empresas acerca de aquellas medidas que se deben tomar para atacar o defenderse de estos atacantes cibernéticos de desconocida procedencia; es una problemática que necesita ser tomada de manera muy seria buscando el contribuir a un buen manejo de la información de la compañía y así mismo generar una certeza organizacional por la seguridad que la empresa maneja, la tecnología y los conocimientos tecnológicos avanzan en gran escala con el pasar del tiempo, por ende las medidas que se tomen deben ser las más correctas para así poder generar una seguridad ante estos ataques que año tras año abren un campo de nuevas variables para combatir.

1.3 Momento y hechos que originaron el objeto de estudio

El problema de investigación que abarca este estudio, retraso en los procesos, disminución de credibilidad y perdida de patentes, refleja una lista de aspectos que han conducido a esta situación, los cuales se estarán analizando a continuación.

A. **Baja inversión y falta de presupuesto destinado a la ciberseguridad,** actualmente, el hecho de salvaguardar la información de todos los usurarios en una empresa, y de la empresa en general es indispensable y de vital importancia, tanto las pequeñas como las medianas empresas de Latinoamérica carecen de personal capacitado o apenas se encuentran en el proceso de implementación y desarrollo de un departamento de ciberseguridad, para evitar los ataques e infiltraciones no deseadas es imprescindible y necesario incrementar la inversión en medidas de seguridad y protección a la infraestructura tecnológica, en pocas palabras diseñar una intranet segura, cosa que solo se puede lograr haciendo un análisis detallado de todos los protocolos de seguridad, herramientas tecnológicas y aplicaciones informáticas (Rodrigo Cando-Segovia & Medina-Chicaiza, 2021).

B. **Para los directivos de las empresas, la ciberseguridad no es una prioridad, ya que no creen que su organización pueda ser blanco de ataques informáticos.** (Rea-Guaman et al., 2018) presenta que la ciberseguridad es un tema de actualidad y debe ser una de las principales preocupaciones de todas las organizaciones, esto debido a la constante y creciente adhesión de tecnologías en las mismas. Inicialmente, la ciberseguridad era un tema bastante simple, básicamente enfocada en virus y códigos maliciosos, algo relativamente fácil de

controlar, hablar de ciberseguridad hoy en día es cuestión de complejidad, es una actividad profunda que se caracteriza por ataques persistentes a gran escala que permiten tener acceso a las redes internas de las empresas (información de usuarios y datos privados de las empresas), generando grandes pérdidas en el sector económico, robos de la información crítica antes mencionada, caída de los servicios e incluso puede llevar a la perdida de la imagen y prestigio de la empresa que sufra este suceso.

El fenómeno de la ciberseguridad no se presenta únicamente para grandes corporaciones, sino también para la generalidad de las empresas, independientemente de su tamaño, que cada vez están más interconectadas en tiempo real, esto hace que estén cada vez más expuestas a todas aquellas amenazas cibernéticas que se presentan en la actualidad. Teniendo en cuenta lo antes mencionado, es válido decir que las pequeñas empresas también sienten la necesidad de considerar la ciberseguridad como un elemento indispensable e implementarla en su funcionamiento, ya que el no disponer ni de personal ni herramientas capacitadas y enfocadas en la ciberseguridad, para poder gestionar de manera eficaz y eficiente las amenazas que esta ofrece, significaría tener un nivel mayor de vulnerabilidad (Rea-Guaman et al., 2018)

C. **La organización presenta software vulnerable, contraseñas débiles, uso de dispositivos externos (memorias USB) o uso inadecuado de wifi.** (Jensen et al., 2022) Asegura que el riesgo que se corre en internet es alto, existen distintas técnicas para lograr el robo de datos como el Phishing, que quiere decir suplantación de identidad; es una práctica que usa la ingeniería social para robar/obtener datos sensibles y confidenciales engañando a los usuarios. (Jensen et al., 2022, p. 3)

   En esta técnica el cibercriminal se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial, por lo regular mediante correo electrónico, o algún sistema de mensajería instantánea e incluso utilizando también llamadas telefónicas o sitios falsos. De esta manera se otorgan deliberadamente datos ante un engaño. Un ejemplo de esto sería proporcionar datos de la tarjeta de crédito para una supuesta validación o el reclamo de un premio. (Jensen et al., 2022, p. 3)

   Desde que las oficinas se trasladaron a las casas con la crisis sanitaria (hablando en términos de la pandemia y el COVID 19), los límites entre lo profesional y lo personal se difuminaron y las empresas se vieron más vulnerables que nunca. («La ciberseguridad tiene mucho más que ver con psicología que con tecnología», 2021)

La incursión del teletrabajo significó la facilitación de los ciberataques, pueden saltar de un ordenador a un celular fácilmente, y el riesgo, por extensión, a todos los dispositivos de la casa. Metafóricamente, durante la pandemia, los hogares se convirtieron en fortalezas, pero al pasar más tiempo en ellos es mayor la exposición en el ámbito online, esto debido a toda la tecnología conectada entre sí, ya que fue la única manera de relacionarse con el mundo exterior, a través de lo digital (compras, comunicación, etc.,), esto llevó a todas las personas a salir de los perímetros de ciberseguridad que tenían las empresas, es aquí cuando cualquier persona es punto de vulnerabilidad para la empresa simplemente con el hecho de estar trabajado en línea. («La ciberseguridad tiene mucho más que ver con psicología que con tecnología», 2021).

D. Confianza absoluta frente a toda la información suministrada a través de links maliciosos.

Un sistema seguro depende de que los usuarios humanos hagan lo correcto de acuerdo con las políticas de ciberseguridad. Por lo tanto, es importante entender como los factores humanos crean debilidades en un sistema, debilidades que un atacante podría utilizar y aprovechar. La Asociación Internacional de Ergonomía define a los factores humanos como la "disciplina científica que se ocupa de la comprensión de la interacción entre humanos y elementos de un sistema". En este campo, las teorías, los principios, los métodos y los datos son aplicados para mejorar el bienestar humano y el rendimiento del sistema.

Los ataques de ciberseguridad pueden tener éxito porque los usuarios no son conscientes de sus vulnerabilidades y debido a su falta de conocimiento sobre las consecuencias y los riesgos. Con los usuarios de las redes sociales tratando de compartir una gran parte de sus vidas en línea, se facilita en gran parte para los atacantes encontrar formas de recopilar información sobre estos mismos usuarios y recopilarla para convencerlos de que su identidad e intenciones son legítimos (Desolda et al., 2022, p. 1,2,3)

1.4 Implicaciones

Las consecuencias de la carencia en las medidas tecnológicas destinadas a controlar la seguridad informática generándoles perdida de información por acceso a terceros o internos de la organización.

A) Ataques maliciosos con fines deshonestos para generar daños directos a la compañía

Ahora es una amenaza para los sistemas informáticos. Esto aumentado debido a la

creciente complejidad de las tecnologías. Además, hoy en día cualquier computadora conectada Internet lo que hace estar al frente de diferente amenaza cibernéticas.

Una manera de prevenir lo desactivar anticipadamente, detectando las vulnerabilidades potenciales que pueden ser aprovechada por las personas que están atacando la empresa, de esa manera se puede disminuir la probabilidad de éxito que tiene en los ataques que realicen.

B) No Sanciones legales gracias a las regulaciones que cobijan a los ciudadanos de cada país

Se pueden evidenciar los diferentes ataques que se hacen de manera sistemática a las diferentes empresas generando riesgos no solo para la misma sino para cada una de las personas que están en este momento registras con ellas, generando una exposición de la cual no hay una reversión ya que al sufrir un ataque contundente se expone toda la información de la empresa y sus clientes.

C) Las Perdida en la competitividad al exponerse información confidencial

Las empresas de hoy cuidan demasiado sus bases de datos, ya que estas son consideradas como los activos más preciados en esta nueva era a tal punto que esta información dándole un buen uso puede aumentar o disminuir su potencial. Cobo (2009) define el concepto TIC como "dispositivos tecnológicos (hardware y software) que permiten editar, producir, almacenar, intercambiar y transmitir datos entre diferentes sistemas de información que cuentan con protocolos comunes. Estas aplicaciones, que integran medios de informática, telecomunicaciones y redes, posibilitan tanto la comunicación y colaboración interpersonal (persona a persona) como la multidireccional (uno a muchos o muchos a muchos). Estas herramientas desempeñan un papel sustantivo en la generación, intercambio, difusión, gestión y acceso al conocimiento." (Niño, 2023)

D) Extorsiones y daños reputacionales que disminuyen la confianza de la compañía.

Las extorsiones y los daños reputacionales son dos problemas que pueden tener un gran impacto en la confianza de una compañía. En muchos casos, estos dos problemas están relacionados, ya que los extorsionadores pueden intentar dañar la reputación de la empresa como una forma de presionarla para que pague. La extorsión es un delito en el que una persona o grupo de personas amenaza con causar daño físico, económico o reputacional a alguien a menos que se cumpla con sus demandas. En el caso de las empresas, esto puede significar que los extorsionadores amenacen con publicar información confidencial o dañar la reputación de la compañía si no se les paga una suma de dinero.

Estas amenazas pueden ser muy efectivas porque la reputación es un activo importante para cualquier empresa. Si la reputación de una empresa se ve comprometida, esto puede disminuir la confianza de los consumidores y los inversores, lo que a su vez puede afectar las ganancias y la capacidad de la compañía para competir en el mercado; por ejemplo, si una empresa es víctima de una extorsión y paga para evitar que se revele información confidencial, los consumidores pueden perder la confianza en la empresa y su capacidad para proteger su información. Esto puede llevar a una disminución de las ventas y una pérdida de reputación a largo plazo. (Serrahima, 2009)

Además, si una empresa es víctima de un ataque reputacional, puede ser difícil recuperar la confianza de los consumidores e inversores. En algunos casos, la compañía puede tener que tomar medidas drásticas, como cambiar de marca o liderazgo, para recuperar su reputación.

E) Incumplimientos financieros, despachos inoportunos

Los ataques generan diferentes retardos inoportunos en las empresas generando tardanzas por sus problemas en los softwares y además disminuyen la competitividad de la empresa lo que generará los incumplimientos financieros, también las empresas pierden total credibilidad con sus clientes ya que quedan expuestas con toda información.

Los ataques cibernéticos pueden causar graves incumplimientos financieros a las empresas. Por ejemplo, un ataque de ransomware puede bloquear el acceso a los sistemas informáticos de una empresa y exigir un rescate para recuperar el acceso. Si la empresa no puede pagar el rescate o no puede recuperar sus datos, puede sufrir una interrupción significativa en sus operaciones, lo que puede llevar a pérdidas financieras y reputacionales.

Además, los ataques cibernéticos pueden exponer información confidencial de la empresa, como datos financieros, estrategias comerciales, propiedad intelectual y otra información importante. Si los datos de la empresa son robados o comprometidos, la empresa puede sufrir pérdidas financieras, multas regulatorias y daños a su reputación.

2. Formulación del problema.

¿Cuáles son los retos que la era digital les genera a las empresas frente al nuevo ámbito de la ciberseguridad?

3. Planteamiento del problema

3.1 Objetivo general

Determinar los retos que la era digital genera a las empresas frente al nuevo ámbito de la ciberseguridad.

3.2 Objetivos específicos

- Comprender los nuevos riesgos empresariales que surgen a partir de la digitalización y nuevas IA.
- Determinar la importancia de la ciberseguridad para las empresas contemporáneas.
- Especificar los riesgos internos y externos que se generan en torno a los ataques cibernéticos en las empresas contemporáneas.
- Definir en que herramientas cibernéticas deben invertir las empresas para la protección de sus activos digitales.
- Determinar los retos que tienen las empresas para implementar ciberseguridad.

3.3 Justificación

3.4 Contribución de la investigación

La siguiente investigación es de gran interés debido a que actualmente es un reto entender acerca de la ciberseguridad empresarial, ya que la mayoría de las empresas manejan información y datos confidenciales que pueden ser objeto de ataques informáticos. Dichos ataques pueden causar la pérdida de información importante, el robo de datos personales o financieros de los clientes, interrupción de los servicios, daño a la reputación de la empresa y en algunos casos, incluso pérdidas financieras. Además, el progreso tecnológico y la creciente interconexión de dispositivos y sistemas han aumentado la cantidad de

vulnerabilidades en las empresas y organizaciones, incrementando el riesgo de sufrir ataques cibernéticos. Es por ello que la presente investigación evidencia como las empresas pueden tomar medidas adecuadas para resguardar su información y sistemas, lo que incluye la implementación de políticas de seguridad, la capacitación de los empleados en prácticas seguras de navegación en internet y en el uso de dispositivos electrónicos, la realización de evaluaciones periódicas de seguridad, entre otras acciones.

La importancia de esta investigación de manera académica es relevante por varias razones; En primer lugar, permite comprender mejor las amenazas y los riesgos a los que se enfrentan las empresas y organizaciones en el mundo digital. Esto permite desarrollar soluciones más efectivas y adecuadas para proteger la información y los sistemas. Además, la investigación en ciberseguridad puede ayudar a identificar las tendencias y patrones de los ataques cibernéticos, lo que puede ayudar a prevenir futuros ataques y a mejorar la seguridad de los sistemas y dispositivos.

También es importante investigar sobre ciberseguridad para desarrollar nuevas tecnologías y herramientas que ayuden a mejorar la seguridad de la información y sistemas, y para entender cómo estas tecnologías pueden ser utilizadas de manera efectiva y responsable. Por último, esta investigación académica también puede ayudar a formar y capacitar a profesionales en esta área, lo que es vital para garantizar la seguridad en el mundo digital y para responder adecuadamente a las amenazas y los riesgos que se presentan en este entorno.

El aporte practico de esta investigación puede ser de suma importancia para las empresas de la actualidad debido a que se busca aportar a diferentes beneficios que puede traer el buen conocimiento de estos temas para el manejo de una empresa adiestrada en este mundo globalizado; tales aportes pueden ser la identificación de riesgos y como tomar medidas preventivas para evitar posibles ataques, a su vez desarrollar estrategias mas efectivas tomando las tendencias cibernéticas para lograr una buena seguridad en la información de la empresa, también hace un gran aporte a entender cómo se deben manejar las políticas de seguridad empresariales para así darle una protección mas amplia a sus datos y asimismo resguardar su reputación al minimizar la posibilidad de un ataque cibernético.

En resumen, investigar sobre la ciberseguridad como nuevo reto empresarial puede ayudar a las empresas a proteger su información, sus sistemas y su reputación. También les permite desarrollar políticas de seguridad más efectivas y mejorar la toma de decisiones en el área de ciberseguridad.

3.5 Conveniencia de la investigación

A continuación, se presentan los beneficios de la investigación frente a cada uno de los objetivos específicos propuestos.

Figura 2 1 Tabla 1: Beneficios de la investigación.

Objetivo especifico	Aporte significativo
• Comprender los nuevos riesgos empresariales que surgen a partir de la digitalización y nuevas IA.	Dar a conocer mediante un sustento teórico, los nuevos peligros que trae la eran de la digitalización y las tecnologías de IA, con el fin de incentivar tanto a las grandes compañías como las emergentes a que tengan un buen manejo de ciberseguridad para la protección de sus datos. Comprender que, durante la pandemia, el cambio masivo de miles de personas al trabajo remoto aceleró la implementación de la "nube" y provocó la necesidad de adoptar procesos de transformación digital para mantener la función empresarial. El ritmo al que esto sucedió dejó entrever que la ciberseguridad no se había contemplado adecuadamente.
• Determinar la importancia de la ciberseguridad para las empresas contemporáneas	Reducir al mínimo el riesgo de los problemas de accesos privilegiados, por lo general, las organizaciones renuncian a las mejores prácticas de acceso privilegiado, debido a la falta de recursos o a que se consideran de baja prioridad. Demostrar que la mayoría de las empresas emplean tres o más "nubes" públicas, lo que significa que tienen tres veces más el riesgo

	de seguridad. Por ello, garantizar la seguridad de los activos en la nube se puede lograr con una solución de gestión de accesos privilegiados. Esto puede ayudar a descubrir activos e instancias en la nube, incorporar y administrar cuentas privilegiadas, intermedias y auditar todos los accesos remotos. Así miso, hacer cumplir la verdadera restricción de privilegios, garantizar la infraestructura segura, supervisar y gestionar cada sesión privilegiada, tener una gestión unificada y evitar prácticas arriesgadas de contraseñas.
• Definir en que herramientas cibernéticas deben invertir las empresas para la protección de sus activos digitales.	La manera adecuada para saber cuáles son las herramientas en las que se deben invertir para mejorar la protección de los activos digitales es estando actualizado con todos los problemas que se están teniendo en los diferentes medios informáticos, sin embargo la única manera de hacerle frente a estos ataques que se reciben, es adelantando las investigaciones pertinentes con los desarrolladores para que a partir de estos fallos que se han tenido en el pasado se puedan mejorar y tener una respuesta clara de tal manera que los activos digitales queden protegidos. Las herramientas que nosotros recomendamos es empezar a tener un mecanismo de defensa para todo tipo de fraudes cibernéticos, desde el robo de las cédulas hasta las claves más importantes con las cuales proteges tus activos digitales, teniendo en cuenta esto se debe programar de diferentes maneras: Usando los diferentes antimalware, usar solo las herramientas que se diseñen para dicha empresa, no

	acceder a los diferentes links oficiales de las compañías con las que se colabora y muchas más.
• Especificar los riesgos internos y externos que se generan en torno a los ataques cibernéticos en las empresas contemporáneas.	Al estar en el medio cibernético nos exponemos a los diferentes ataques internos que poco tienen que ver con estar en la red, se debe a los malos manejos que pueden tener algunos funcionarios que solo buscan hacerle daño a la empresa filtrando la información y exponiendo los de diferente manera para que las personas mal intencionadas puedan ingresar al software y puedan romper toda su seguridad internamente lo que dejaría a merced de las personas que generan los fraudes cualquier empresa. Externamente la vulnerabilidad aumenta ya que las empresas contemporáneas no tienen la suficiente capacidad para detener todo tipo de ataque que recibe día a día, los hackers lo que hacen es debilitar el sistema de defensas de cualquier empresa y así aumentar su capacidad de información para contraatacarlo cada vez de manera más efectiva para poder filtrar toda su información, es por eso que las empresa que no están preparadas lo suficiente en este momento quedan demasiado expuestas para competir de la mejor manera. Los ciberdelincuentes siempre tienen en su punto de mira a las empresas y sus sistemas, con el objetivo de robar información (bancaria o de otra índole comercial o personal), tirar sus sistemas o utilizar sus recursos. Dos de las mayores amenazas que reciben las empresas hoy en día son ataques de denegación de servicio DDoS

	(inutilizan los sistemas informáticos de la empresa) o ataques con malware de tipo ransomware (encriptan los datos de la empresa, solicitando un rescate económico en criptomonedas para liberarlos)
• Determinar los retos que tienen las empresas para implementar ciberseguridad.	Los desafíos que enfrentan las empresas en la implementación de la ciberseguridad pueden tener varias contribuciones importantes, que incluyen: Identificar vulnerabilidades: Al investigar y analizar los desafíos que enfrentan las empresas al implementar la ciberseguridad, es posible identificar áreas o aspectos que son más vulnerables a posibles amenazas y ataques cibernéticos. Esto puede ayudar a las organizaciones a comprender las vulnerabilidades de seguridad existentes y tomar medidas para fortalecerlas, mejorando su postura de seguridad general. Planificación de una política de privacidad: Comprender los desafíos específicos que enfrentan las empresas al implementar la ciberseguridad puede ayudarlos a planificar y desarrollar estrategias de seguridad más efectivas. Por ejemplo, si la concienciación de los empleados se identifica como un desafío, se pueden implementar programas de formación y concienciación para mejorar la educación en seguridad. Si la falta de actualizaciones de software se identifica como un problema, se pueden establecer políticas y procedimientos para

	garantizar que se apliquen parches y actualizaciones regulares. Toma de decisiones mejorada: Conocer los desafíos de las implementaciones de ciberseguridad puede ayudar a las organizaciones a tomar decisiones más informadas sobre cómo asignar recursos y priorizar qué áreas de seguridad necesitan más atención. Esto puede permitir una asignación más eficiente de recursos y esfuerzos para implementar medidas de seguridad más apropiadas y efectivas para abordar los desafíos identificados. Conciencia y conciencia: Identificar los desafíos de implementación de la ciberseguridad puede ayudar a crear conciencia sobre la importancia de la seguridad de TI. Esto puede ayudar a comprender mejor las amenazas y los riesgos potenciales para que puedan priorizarse y comprometerse a implementar las medidas de seguridad adecuadas. Resiliencia de red mejorada: Comprender los desafíos de las implementaciones de seguridad cibernética y abordarlos de manera efectiva puede mejorar la resiliencia cibernética de una empresa. Al abordar las vulnerabilidades y vulnerabilidades identificadas, las organizaciones pueden prepararse mejor para hacer frente a posibles amenazas y ataques cibernéticos, reduciendo su impacto y la probabilidad de éxito de estos ataques.

	En conclusion, identificar los desafíos que enfrentan las empresas al implementar la ciberseguridad puede tener un impacto significativo en la mejora de la seguridad de la información de una empresa y la protección de los activos digitales. Al identificar y abordar desafíos específicos, las organizaciones pueden fortalecer su postura de seguridad y prepararse mejor para enfrentar las amenazas y los desafíos en el panorama actual de ciberseguridad.

Fuente. Elaboración propia.

4.0 MARCO REFERENCIAL

4.1. Estado del arte.

4.1.1. Rastreo bibliográfico.

Con el fin de identificar la producción académica existente en el tema, se realizó un rastreo bibliográfico tanto en el ámbito académico nacional como en los círculos internacionales en los últimos cinco (5) años. Esta revisión de antecedentes constituye un paso necesario para plantear la pregunta de investigación, construir una justificación pertinente, describir el estado del arte alrededor del tema y demostrar la viabilidad de esta propuesta investigativa.

Los insumos básicos para recopilar los aportes académicos y llevarlos a un espacio de discusión y análisis crítico fueron:

- Categorías teóricas-conceptuales: Era digital, ciberseguridad.
- Bases de datos: Google Scholar y Scielo.
- Revisores bibliográficos: Zotero.
- Bibliotecas: UPB y EAFIT.
- Autores corporativos

Con lo anterior, se obtuvo en la búsqueda libros, investigaciones, artículos científicos publicados
en revistas indexadas, trabajos de grado de estudios superiores, documentos y otras producciones académicas de fuentes confiables, rigurosas y de calidad que han desarrollado investigaciones relacionadas con el objeto de estudio.

Como producto de esta revisión bibliográfica, se presenta a continuación una tabla donde se
despliegan los autores más relevantes encontrados, con la producción académica que puede aportar a este trabajo de investigación, además de algunas ideas principales de cada fuente. En
esta tabla se presenta un total de quince (15) autores, desagregados en cinco (5) exponentes importantes, cinco (5) exponentes nacionales y cinco (5) exponentes internacionales.

Figura 3 1 Tabla 2: Rastreo Bibliográfico

#	Autor(es)	País	Título
Principales exponentes			
1	Pérez González Pablo (2014)	España	Ethical Hacking: Teoría y práctica para la realización de un pentesting.
2	Cebrián Alonso José María (Chema Alonso), (2020)	España	Metasploit para pentesters
3	Evans Lester (2018)	Inglaterra	Cybersecurity Lester Evans.
4	Diógenes Yuri (2022)	U.S.A (Texas)	Cybersecurity attack and defense strategies
5	Mitnick Kevin (2018)	U.S.A (L.A)	El arte de la invisibilidad.
Exponentes nacionales			
1	Cano Martínez Jeimy J. (2020)	Colombia	SISTEMAS "seguridad y ciberseguridad"
2	Serna Patiño Alexis Mauricio (2018)	Colombia	Análisis de la capacidad de ciberseguridad para la dimensión tecnológica en Colombia una mirada sistémica desde la organización
3	Molina Castaño, Stephannya (2021)	Colombia	Ciberseguridad de las empresas financieras
4	Olaya Oliveros Alexander (2021)	Colombia	Ataques cibernéticos
5	Nova Alarcón Michael	Colombia	Ciberestrategia Colombia

	Alejandro (2016)		
Exponentes internacionales			
1	Meraj Farheen Ansar (2022)	U.S.A(Kentucky)	The Impact and Limitations of Artificial Intelligence in Cybersecurity
2	Leong Chan (2019)	U.S.A(Atlanta)	Survey of AI in Cybersecurity for Information Technology Management
3	Alex Mathew (2021)	U.S.A(Bethany)	Artificial Intelligence for Offence and Defense - The Future of Cybersecurity
4	Xiaohua Feng (2020)	Canadá (Calgary)	Artificial Intelligence Cyber Security Strategy
5	Peter R.J. Trim (2021)	London (UK)	The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement

Fuente. Elaboración propia.

4.2. Análisis:

4.2.1. Análisis de literatura – Exponentes Principales

A continuación, se presentan las principales ideas de los autores/autores corporativos expuestos en la Tabla 2: Rastreo bibliográfico, que tienen una alta pertinencia en el tema, y que lideran la tendencia de publicaciones con relación a la investigación.

- **Pérez, González Pablo (2014):**

  El mundo digital y el mundo físico están más unidos cada día. Las organizaciones realizan más gestiones de manera electrónica y cada día más amenazas ponen en peligro los activos de estas. El mundo está interconectado, y por esta razón disciplinas como el hacking ético se hacen cada vez más necesarias para comprobar que la seguridad de los activos de una organización es la apropiada.

  El hacking ético es el arte que permite llevar a cabo acciones maliciosas envueltas en la ética profesional de un hacker que ha sido contratado con el fin de encontrar los agujeros de seguridad de los sistemas de cada organización. En este libro, el autor se enfoca en enseñar y mostrar los procedimientos, procesos, vectores de ataque, técnicas de hacking, teoría y práctica de este arte.

El autor propone un enfoque distinto a lo común, en el cual se guiará al lector por un conjunto de pruebas a realizar en auditorías técnicas. La auditoría perimetral y auditoría interna son el foco común en este tipo de procesos. Además, se añaden pruebas modernas, no tan comunes en los procesos de hacking ético. Los famosos APT, las pruebas de Dos o las simulaciones de fugas de información desde dentro de la organización son algunos de los ejemplos que se pueden encontrar en el libro.

- **Cebrián, Alonso José María (Chema Alonso), (2020):**

La seguridad de la información es uno de los mercados en auge en el mundo de la de informática hoy en día. Los gobiernos y empresas valoran sus acticos por lo que deben protegerlos de accesos ilícitos mediante el uso de auditorías que establezcan un status de seguridad a nivel organizativo. El pentesting forma parte de las auditorías de seguridad y proporciona un conjunto de pruebas que valoran el estado de la seguridad de la organización en ciertas fases.

Metasploit es una de las herramientas más utilizadas en procesos de pentesting ya que contempla distintas fases de un test de intrusión. Asimismo, el autor presenta una visión global de las fases en las que Metasploit puede ofrecer su potencia y flexibilidad al servicio del hacking ético.

Se presenta de una manera ordenada la organización un tanto caótica de la arquitectura de Metasploit que necesiten utilizar en framework. El enfoque eminentemente práctico, mediante la escenificación de pruebas de concepto, guía a los lectores a través de un gran número de posibilidades, para que de esta manera consiga asentar sus conocimientos en el framework y disponer así de distintos recursos para realizar distintas fases de un test de intrusión con la ayuda de Metasploit Framework.

- **Evans, Lester (2018):**

En el entorno digital, absolutamente todos estamos a un mal clic de algo que puede desbaratarnos la vida. Es claro que no hay que esperar a ser una víctima de un ciberataque para prevenir que pase. En un mundo tan tecnológico todos debemos preocuparnos por nuestra propia seguridad digital y las de las personas que nos rodean.

Contar con información y aplicar medidas contribuye a construir entornos digitales más seguros para exprimir el lado positivo de la tecnología y ponérselo más difícil a los cibercriminales que se mueven sigilosamente en la red con la única voluntad de causar el mayor daño posible. Asimismo, para el autor conviene adoptar las medidas de higiene digital en el día a día, y se deben reconocer las principales amenazas de seguridad en el internet como los hackeos y amenazas digitales actuales, para evitar engaños y poder ponerle cara a los principales riesgos digitales como la perdida de

datos importantes, el robo de infraestructura digital, la falsificación de documentación y el uso inadecuado de la información de una compañía, entre otras que se encuentran presentes en la red. El objetivo principal del autor es enseñar que las personas se inquietan muy pronto, pero olvidan lo fácil que es bajar la guardia en cuestiones de seguridad, y que si esto pasa en la red trae una cantidad de consecuencias.

- **Diógenes, Yuri (2022):**

El Machine Learning está revolucionando el mundo de la empresa y el día a día de la Sociedad gracias a infinidad de aplicaciones: sistemas predictivos, de soporte de decisión y recomendación, vehículos de conducción autónoma, agentes inteligentes de conversación, asistentes personales, visión artificial, detección de anomalías, procesamiento inteligente de textos, etc.

Las técnicas de Machine Learning consisten básicamente en automatizar, mediante distintos algoritmos, la identificación de patrones o tendencias que se "esconden" en los datos. En particular, "aprenden" de los datos para ir generando y ajustado, a partir de diferentes algoritmos, un modelo que resuelva un problema determinado sin tener que programar una solución de forma explícita. En el campo de la Seguridad Informática, en el que las ciberamenazas acechan tanto a particulares como a organizaciones en forma de fugas de información, robo y publicación de credenciales de clientes, uso no autorizado de marcas, noticias falsas etc.

- **Mitnick, Kevin (2018):**

Para el autor, Actualmente, cada uno de nuestros movimientos está siendo observado y analizado. Se roban las identidades de consumidores, y cada paso de la gente es rastreado y almacenado. Lo que en algún momento se pudo clasificar como paranoia, ahora es una dura realidad y la privacidad es un lujo que sólo unos pocos pueden entender y permitirse. Para esto el autor presenta que se debe utilizar tácticas como: contraseñas seguras, actualizaciones y parches; para mantener el software y los sistemas actualizados con las últimas actualizaciones y parches de seguridad, monitorización y detección de amenazas, entre otros y métodos como la conciencia de ingeniería social, la sensibilización del personal, la seguridad en redes y dispositivos y la protección de la información, tanto en la vida real como la virtual, para proteger las compañías. Estas técnicas de élite, usadas adecuadamente, pueden maximizar la privacidad. La invisibilidad no es sólo para los superhéroes, la privacidad es un poder que todos necesitamos y merecemos en esta era moderna.

- **Conclusión**

La seguridad digital es una preocupación creciente en el mundo actual, ya que el mundo digital y el mundo físico están cada vez más interconectados. Las organizaciones

necesitan proteger sus activos, incluidos sus datos y sistemas, de posibles amenazas. Las auditorías de seguridad, incluido el hacking ético o el pentesting, son herramientas importantes para identificar y corregir posibles vulnerabilidades.

Las principales amenazas a la seguridad en línea incluyen los ataques cibernéticos, que son intentos de dañar o robar información al atacar un sistema informático. Los expertos en ciberseguridad también advierten sobre los riesgos de fraude en línea, robo de identidad y otros delitos cibernéticos. Para mantenerse seguro en línea, es importante adoptar medidas de higiene digital a diario, estar alerta a posibles ataques cibernéticos y utilizar tecnología de aprendizaje automático para identificar patrones o tendencias en los datos.

Los autores destacan la importancia de ser consciente de la seguridad digital y tomar medidas proactivas para proteger la información y los activos en el entorno digital. Algunas técnicas innovadoras, como el aprendizaje automático, pueden ayudar a lograrlo.

4.2.2. Análisis de literatura – Exponentes Nacionales

Los estudios realizados a nivel nacional por diversos autores/autores corporativos aportan visiones interesantes sobre la temática. Estos son:

- **Cano, Martínez Jeimy J. (2020)**

Las organizaciones se esfuerzan por salvaguardar sus activos digitales y aplicar protocolos de seguridad cibernética, sin embargo, es inevitable que ocurran violaciones a la ciberseguridad y se ejecuten ataques informáticos. Por un lado, la vulnerabilidad informática se refiere a la carencia de medidas de seguridad apropiadas en un sistema, lo que lo convierte en blanco de ataques y violaciones a la seguridad. Esto puede ser causado por diversos factores, como la falta de actualizaciones de software, la falta de capacitación del personal en temas de seguridad digital, la carencia de controles de acceso efectivos, entre otros. Además, la vulnerabilidad informática también se refiere a la presencia de amenazas y ataques cibernéticos que buscan comprometer la seguridad de un sistema. Estas amenazas pueden originarse a través de hackers, malware, virus, phishing, y otros medios. Para proteger el sistema, es necesario tomar medidas importantes, lo que implica no solo la implementación de medidas de seguridad adecuadas en los sistemas informáticos, sino también estar al tanto de las últimas amenazas y vulnerabilidades digitales tomando medidas para prevenir su ocurrencia.

- **Serna Patiño, Alexis Mauricio (2018)**

La ciberseguridad se ha convertido en un concepto de gran relevancia en la actualidad, debido a su importancia estratégica para la ciudadanía, la sociedad, las empresas y el país en general. El rápido crecimiento de las Tecnologías de la Información y la Comunicación (TIC) ha generado nuevos desafíos en todos los aspectos de su gestión, y la ciberseguridad y la infraestructura que la sustenta son de vital importancia para garantizar el desarrollo sostenible de las organizaciones. En este sentido, este estudio, basado en el paradigma de simulación de la Dinámica de Sistemas, se enfoca en la dimensión tecnológica de la ciberseguridad, específicamente en la respuesta a incidentes y la protección de infraestructuras críticas. El objetivo es analizar la capacidad de la ciberseguridad en esta dimensión tecnológica, en lo que se refiere a la respuesta a incidentes y la protección de la infraestructura crítica en Colombia, desde una perspectiva sistémica. Se busca identificar los posibles escenarios y políticas que podrían mejorar el desempeño del sistema en la dimensión analizada, considerando la organización en su conjunto. De esta manera, se espera contribuir a un mejor entendimiento de la ciberseguridad en Colombia, y generar soluciones y medidas para fortalecer la seguridad digital en el país.

- **Molina Castaño, Stephannya (2021)**

El manejo de la información financiera en Colombia se ha vuelto cada vez más complejo debido al uso de tecnologías avanzadas. Por esta razón, es fundamental que las entidades financieras brinden un mejor soporte a sus clientes en cuanto a la seguridad de sus datos, teniendo en cuenta los riesgos que existen al realizar transacciones financieras en línea. Para lograr conservar la confidencialidad, disponibilidad e integridad de la información, es primordial analizar las amenazas y vulnerabilidades del sector financiero en Colombia en relación con el ciberdelito. Con este fin, se busca identificar los delitos y amenazas informáticas en el sector financiero, así como describir el tratamiento penal dentro del marco legal colombiano para los delitos informáticos financieros.
Este enfoque busca proporcionar una comprensión detallada de las políticas de ciberseguridad implementadas por las empresas del sector financiero en Colombia, y cómo estas políticas se relacionan con la vulnerabilidad en este ámbito. Además, se espera que este análisis proporcione una mayor claridad sobre el comportamiento de las empresas financieras y la manera en que los usuarios deben actuar en caso de enfrentar un ciberataque. Muchas personas no saben cómo solicitar medidas de seguridad para proteger su información financiera, lo que puede llevar a que les roben dinero en línea. Por lo tanto, es crucial que tanto las empresas financieras como los usuarios estén al tanto de las amenazas y vulnerabilidades del ciberdelito y tomen medidas adecuadas para salvaguardar la información financiera.

- **Olaya Oliveros, Alexander (2021)**

La dificultad para detectar los ataques cibernéticos y su origen representa un gran problema

ya que esto puede resultar en ataques a personas, empresas y corporaciones. Debido a que el ecosistema digital y su protección frente a acciones ilegales son temas globales, el cibercrimen se ha convertido en una realidad criminológica en todo el mundo. Aunque el cibercrimen se ha convertido en una realidad, a menudo se exagera la amenaza que representa o no se percibe el riesgo real asociado al uso de las TIC. La revolución de las TIC y las redes sociales son elementos clave en la ciberseguridad. El cibercrimen es un tema amplio y mundialmente relevante, por lo que es necesario conocer su caracterización y los ataques más comunes en cada país para comprender la importancia de la formación en cultura informática segura para los empleados de cualquier organización y minimizar los riesgos. Es importante entender cómo actúa un delincuente cibernético para comprender la problemática del cibercrimen y no confiar en todo lo que se encuentra en internet. Los delincuentes pueden engañar a sus víctimas con publicidades falsas o sitios web que los redirigen a páginas no auténticas, así como también pueden realizar ataques de malware o robo de información. Además, es crucial conocer las leyes que protegen y brindan apoyo a las víctimas de estos delitos, ya que penalizan las acciones ilegales de los delincuentes informáticos.

- **Nova Alarcón, Michael Alejandro (2016)**

Colombia trabaja en una política de Estado que aborda la ciberdefensa y la ciberseguridad nacional en conjunto con el desarrollo sostenible, con el objetivo de responder adecuadamente a las condiciones internas y externas necesarias para el país. Los modelos de seguridad cibernética están evolucionando, lo que implica nuevas funcionalidades y capacidades frente a arquitecturas de seguridad informática y conceptos nuevos en relaciones internacionales como el "ciberpoder". Con esto, se evalúa la estrategia nacional en el ciberespacio y sus impactos en la gestión del conocimiento, investigación, desarrollo e innovación del país, comparándola con los modelos de defensa establecidos conjuntamente con países aliados como Inglaterra, Israel y Estados Unidos, que son los principales socios en cooperación, capacitación y desarrollo militar.

El uso de tecnologías y la explotación del ciberespacio para la recolección de inteligencia, vigilancia, reconocimiento, orientación y ataque de la red se han convertido en una parte normal de la actividad militar. La guerra cibernética busca interrumpir los servicios esenciales de red, datos y la infraestructura crítica, generar incertidumbre y fomentar la duda entre los comandantes de oposición y líderes políticos. Los ataques cibernéticos pueden ser dirigidos a objetivos a distancias muy largas utilizando herramientas relativamente económicas.

- **Conclusión.**

Estos cinco autores coinciden en que la ciberseguridad es un tema muy relevante en la actualidad, debido a la creciente dependencia de las TIC en la sociedad, las empresas y el

país en su conjunto. Todos ellos enfatizan la importancia de proteger los activos digitales y aplicar protocolos de seguridad cibernética para protegerse contra amenazas y vulnerabilidades cibernéticas.
Las vulnerabilidades informáticas pueden ser causadas por una variedad de factores, como la falta de medidas de seguridad adecuadas, la falta de actualizaciones de software, la falta de capacitación en temas de seguridad digital y la falta de controles de acceso efectivos. Es importante estar al tanto de las últimas amenazas y vulnerabilidades en los sistemas informáticos y tomar medidas para evitar que sucedan.
Estos autores discuten la importancia de la respuesta a incidentes y la protección de infraestructuras críticas en la dimensión tecnológica de la ciberseguridad. Señalan que es importante analizar posibles escenarios y políticas que podrían mejorar el desempeño del sistema en su conjunto, considerando la organización en su conjunto.

Algunos autores enfatizan la importancia de preservar la confidencialidad, disponibilidad e integridad de la información financiera en el sector financiero colombiano, debido al creciente uso de tecnologías avanzadas en este campo. Resaltan la necesidad de identificar y analizar las amenazas y vulnerabilidades del ciberdelito en el sector financiero, así como el tratamiento penal dentro del marco legal colombiano para los delitos informáticos financieros.
El cibercrimen es una realidad a nivel mundial, y la revolución de las TIC y las redes sociales son componentes clave en la ciberseguridad. Existe la dificultad de detectar los ciberataques y su origen, y la importancia de percibir el riesgo real asociado al uso de las TIC; los autores coinciden en que la ciberseguridad es un tema importante en la actualidad y que debemos tomar medidas para protegernos de las amenazas y vulnerabilidades del mundo digital. También debemos ser conscientes de los peligros que representan los ciberdelincuentes y tomar medidas para evitar que dañen nuestros sistemas.

4.2.3 Análisis de literatura – Exponentes internacionales

- **Meraj Farheen, Ansar (2022)**

Para el autor, las explicaciones de Inteligencia artificial en ciberseguridad han tenido un crecimiento realmente exponencial a lo largo de estos años. Este factor ha requerido que las empresas y organizaciones exijan más medidas de seguridad. El intento de proteger los datos e información disponibles ha resultado en el crecimiento de la ciberseguridad, y se ha visto que la IA influye en la ciberseguridad a gran escala. Este factor ha hecho que el aprendizaje automático sea inducido significativamente en tecnologías recientes que apoyan la ciberseguridad.

- **Leong, Chan (2019)**

Los retos de ciberseguridad se han convertido en los últimos años en un desafío emergente para la gestión de la información empresarial. La Inteligencia Artificial (IA) se usa ampliamente en diferentes campos, pero aún es relativamente nueva en ciberseguridad. Sin embargo, las aplicaciones en ciberseguridad son cruciales para la vida diaria de todos. En este documento, presentamos el estado actual de la IA en el campo de la ciberseguridad y luego describimos varios estudios de casos y aplicaciones de la IA para ayudar a la comunidad, incluidos los gerentes y líderes de ingeniería, investigadores, educadores, innovadores, empresarios y estudiantes, a comprender mejor este campo, como los desafíos y cuestiones no resueltas de la IA en la ciberseguridad. Se proporcionan implicaciones de gestión y recomendaciones de políticas para las empresas y el gobierno.

También explica el autor detalladamente como los desarrolladores pueden darse el lujo de usar todas las tecnologías y empezar a emplear las IA de tal manera que se puedan ampliar todos los campos, desafíos y cuestiones que aun no se han explorado para determinar realmente el impacto que pueden tener estas tecnologías en el relacionamiento de los negocios en el futuro.

- **Alex, Mathew (2021)**

Según el autor, los ciber delincuentes empiezan a sofisticar la manera de intentar acceder a todas las bases de datos por medio de la inteligencia artificial que se está desarrollando, también se debe tener en cuenta de parte de la defensa como la inteligencia artificial se trata de las empresas e individuos y el uso de las herramientas para contrarrestar esos ciber ataques. Los sistemas de defensa se han vuelto mucho más robustos, eficientes y flexibles para disminuir los diferentes impactos asociados a las prácticas ciber ofensivas exitosas. Realmente este estudio ha revelado que el lenguaje de una máquina inteligencia artificial puede brindar diferentes beneficios para el presente y el futuro de la ciberseguridad adelante. Además, todos estos desarrollos que se están teniendo tan rápidamente en la seguridad informática, los empresarios tengan en cuenta la ciberseguridad como una prioridad para mejorar el cuidado de sus activos informáticos.

- **Xiaohua, Feng (2020)**

Bajo la crisis pandémica de COVID-19 de 2020, la enfermedad por coronavirus se extendió por todo el mundo en el que vivimos. Todos los gobiernos buscan consejos de científicos antes de hacer su plan estratégico. La mayoría de los países recopilan datos de hospitales (y hogares de ancianos, etc. en la sociedad), realizan análisis de datos, utilizan fórmulas para hacer algunos modelos de IA, para predecir los posibles patrones de desarrollo, con el fin de hacer su estrategia de gobierno. La seguridad de la IA se vuelve esencial. Si un ataque de seguridad hace que el patrón sea incorrecto, el modelo no es una predicción real, lo que

podría resultar en la pérdida de miles de vidas. La consecuencia potencial de este pronóstico inexacto sería aún peor. Por lo tanto, tener en cuenta la seguridad durante el modelado de IA de pronóstico, el gobierno de datos paso a paso, será significativo.
Un desarrollo futuro recomendado será un enfoque más apropiado para lograr una mejor compensación entre la IA y la seguridad cibernética y la opción del estado. Con el fin de obtener una mejor compensación entre los ciudadanos, el gobierno y las empresas comerciales. Se ocupará de la adquisición de datos con los múltiples problemas de diversidad, incluidos GDPR y PII, DP3T podría ser una de las soluciones ahora. Muchas investigaciones sobre privacidad y seguridad personal se han publicado en el pasado. Además, GDPR debe aplicarse para los estados de la UE y los relacionados. Por lo tanto, los requisitos de documentos legales deben ser la máxima prioridad. Lo mismo para encontrar una mejor compensación entre gobiernos, ciudadanos y organizaciones de IA y seguridad.

- **Trim, Peter R.J. (2021)**

Los altos directivos pueden utilizar el modelo global de seguridad cibernética para establecer un marco para hacer frente a una variedad de ataques de seguridad cibernética, así como para mejorar la base de conocimientos y habilidades de seguridad cibernética de las personas. Para que se establezca una mentalidad de ciberseguridad, los altos directivos deben asegurarse de que el personal se centre en la vulnerabilidad y la resiliencia de la organización, que exista un proceso de comunicación abierto y transparente y que el personal se comprometa a compartir conocimientos sobre ciberseguridad.
También el autor contribuye al área de la conciencia de seguridad cibernética, ya que proporciona información sobre por qué las estructuras y los sistemas organizacionales están interrelacionados y se utilizan para mejorar el desarrollo del conocimiento de seguridad cibernética de una organización. El modelo de seguridad cibernética global (GCS) descrito ayuda a los gerentes a visualizar cómo pueden establecer y administrar una estrategia con respecto a la mitigación de riesgos relacionada con la política de seguridad cibernética que hace que la organización sea más resistente.

Además, deben analizar cuidadosamente cómo la organización puede obtener una ventaja de la tecnología de seguridad cibernética, la IA y tipos específicos de modelos, de modo que los gerentes adopten un proceso estratégico de toma de decisiones de seguridad cibernética a lo largo del acuerdo de asociación.

- **Conclusión.**

Los autores coinciden en que la Inteligencia Artificial (IA) está jugando un papel importante en la ciberseguridad. Destacan que el crecimiento exponencial de la IA ha llevado a un aumento de las medidas de seguridad en las empresas y organizaciones, ya que la IA busca proteger la información y los datos disponibles. Se mencionan los beneficios de la IA en la

mejora de la eficiencia y robustez de los sistemas de defensa frente a ciberataques.

Se enfatiza la importancia de la seguridad al utilizar inteligencia artificial (IA) en ciberseguridad, con el fin de evitar posibles amenazas y asegurar la precisión y confiabilidad de los modelos de IA utilizados en la toma de decisiones estratégicas, durante una crisis pandémica, como la del COVID-19 pandemia.

Existe la necesidad de encontrar un equilibrio entre la inteligencia artificial y la ciberseguridad, dados los diferentes problemas relacionados con la privacidad, las regulaciones legales y el compromiso entre gobiernos, ciudadanos y organizaciones de seguridad.

Existe un acuerdo general entre los autores de que la IA está influyendo significativamente en la ciberseguridad y que es importante tener en cuenta la seguridad al desarrollar y aplicar la IA en este campo para garantizar una protección eficaz de la información y los datos. En el contexto actual de amenazas cibernéticas, se deben tomar las medidas de seguridad adecuadas para protegerse contra posibles ataques.

5.0 Marco Teórico:

Esta investigación está orientada por las categorías teóricos-conceptuales de: digitalización (era digital), Ciberseguridad y el hackeo empresarial. A continuación, se presentará el horizonte teórico que guiará el desarrollarlo de la temática que convoca.

5.1 Era digital

El categórico conceptual de digitalización, basado en las posturas de Evans (2018), plantea que la implementación de la digitalización en las empresas ofrece diversas oportunidades de mejora. Evans argumenta que la adopción de tecnologías digitales proporciona a las empresas alternativas para optimizar sus procesos, aumentar su eficiencia y ofrecer mejores productos o servicios a sus clientes. Al aprovechar las ventajas de la digitalización, las empresas pueden experimentar una mayor automatización de tareas, una gestión más eficiente de la información y una mayor agilidad en la toma de decisiones.

Sin embargo, el autor también destaca que la digitalización conlleva riesgos y desafíos

significativos. Una de las principales preocupaciones radica en la exposición a amenazas cibernéticas. En un mundo cada vez más conectado, las empresas se vuelven más vulnerables a ataques informáticos, robo de datos, sabotaje digital y otras formas de ciberdelincuencia. Las tecnologías digitales a las que las personas y las empresas tienen acceso brindan nuevas oportunidades a los delincuentes cibernéticos, lo que requiere un enfoque integral de seguridad digital.

Es crucial tener en cuenta que la responsabilidad de proteger a las empresas y a los ciudadanos de amenazas cibernéticas recae en gran medida en el Estado. Sin embargo, Evans argumenta que existe una limitada capacidad por parte del Estado para minimizar los riesgos a los que se enfrentan los ciudadanos en el ámbito digital. Para contrarrestar esta situación, es necesario que las empresas adopten medidas proactivas para garantizar la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales. Esto implica implementar sistemas de seguridad sólidos, capacitar al personal en cuestiones de ciberseguridad y establecer políticas y protocolos para prevenir y responder a posibles incidentes cibernéticos.

En el contexto de la digitalización, las empresas se ven inmersas en un entorno en constante evolución tecnológica. Aunque no están obligadas a adoptar nuevas tecnologías, la realidad es que los empresarios buscan maximizar sus recursos y mantenerse al día con la competencia. Evans subraya que, para sobrevivir y prosperar en la era digital, las empresas deben tener en cuenta múltiples aspectos. Además de protegerse de los ciberataques, también deben considerar factores como la gestión de datos, la privacidad del cliente, la transformación digital de sus procesos internos y la adaptación a las demandas cambiantes del mercado.

5.1.2 Ciberseguridad

El eje temático de la Ciberseguridad se abordará a partir de las posturas de Gonzales ~~Pérez-Pablo~~ (2014) y de Alfonso (2020). Para Gonzales (2014) la tecnología ha evolucionado a un ritmo vertiginoso, y con ella, las oportunidades en implementación de esta seguridad para las empresas y para la sociedad, asímismo el autor observa que estos avances también han traído consigo nuevos riesgos y amenazas como robos, extorciones, hackeos, facilidad de penetración en los datos importantes en el sector de la ciberseguridad. a lo largo de los últimos años el panorama de la ciberseguridad ha mostrado algunas tendencias, entre las cuales Gonzales señala:

- Toda empresa puede ser víctima de un incidente de seguridad. Es importante que la sociedad y las empresas tengan este hecho en mente y entenderlo. Implantar medidas de prevención como programas y softwares basados en seguridad informatica con el fin de disminuir el riesgo vital, ya que hoy en día existen empresas que dejan brechas

de seguridad de un tamaño exponencial, como por ejemplo Facebook, que expuso la información personal de mas de 50 millones de usuarios.

- La seguridad 100% no existe, por lo que se debe seguir trabajando de forma iterativa en la manera en la que las empresas se protegen, deben sumar medidas preventivas, alinear reactivas y crear una base en la que las personas de la organización queden involucradas en la seguridad de la organización.

La seguridad de la información es uno de los mercados en auge en el mundo de la informática de hoy en día, dado que los gobiernos y empresas conocen la importancia de sus activos por lo que deben protegerlos de accesos ilícitos mediante el uso de auditorías que establezcan un status de seguridad a nivel organizativo. Una herramienta para esto puede ser El pentesting, el cual forma parte de las auditorias de seguridad y proporciona un conjunto de pruebas que valoran el estado de la seguridad de las organizaciones en ciertas fases. El autor, afirma que junto a las nuevas tecnologías hay nuevas amenazas como robos, extorciones, hackeos, facilidad de penetración en los datos importantes tanto para las empresas como las personas naturales, y describe la ciberseguridad es el único recurso para evitar el phishing y el robo de datos vitales, concordando así con las afirmaciones de González (2014).

5.1.3 Hackeo empresarial

Esta temática se abordará desde la perspectiva de Kevin Mitnick (2018) quien define que, las empresas enfrentan amenazas persistentes y sofisticadas en el ciberespacio, y por esto tienen la necesidad de una protección eficaz contra la piratería, requiriendo una combinación de medidas técnicas, tecnología, capacitación, conciencia de la empresa, personal y políticas de privacidad adecuadas. El autor enfatiza la importancia de abordar la ingeniería social, las vulnerabilidades técnicas, las acciones internas de los empleados y los ataques cibernéticos avanzados como áreas importantes a considerar para proteger su negocio de las amenazas de ataques corporativos. También destaca la necesidad de tomar medidas proactivas, mantener los sistemas actualizados y seguros, y tomar decisiones informadas de asignación de recursos para mejorar la seguridad de las TIC y proteger los activos digitales, así como la información confidencial de la empresa.

Mitnick (2018),destaca; que las empresas son objetivos frecuentes de ataques cibernéticos debido a la valiosa información y activos digitales que manejan. los temas que el autor ha abordado para contrarrestar los hackeos empresariales los define como:

- Ingeniería social: muchos hackeos empresariales comienzan con la ingeniería social, que es una técnica utilizada por los atacantes para manipular a las personas y obtener información confidencial. Lo cual se puede contrarrestar generando la concienciación del personal y la capacitación en seguridad de las personas y las empresas para prevenir este tipo de ataques.

- Vulnerabilidades técnicas: Señala que las empresas a menudo tienen vulnerabilidades técnicas en sus sistemas y redes, como software desactualizado, configuraciones inseguras o falta de parches de seguridad, que pueden ser explotadas por los hackers. Por lo que se destaca la importancia de mantener los sistemas actualizados y protegidos con medidas de seguridad adecuadas.

- Amenazas internas: Habla sobre la amenaza que representan los empleados internos con acceso a información confidencial de las organizaciones, donde se pueden presentar riesgos asociados con la negligencia, la mala praxis o incluso la malicia de los empleados, lo que puede generar un uso inadecuado de la información.
- Ataques avanzados: se presetan diferentes formas de ataques avanzados como el phishing, el malware, el ransomware y otros tipos de ataques sofisticados que los hackers utilizan para infiltrarse en las redes empresariales y obtener acceso a datos valiosos o causar daños significativos.

- Protección y mitigación: Resalta la importancia de implementar medidas de protección y mitigación adecuadas en las empresas, como firewalls, sistemas de detección y respuesta de amenazas, políticas de acceso y autenticación seguras, y respaldos de datos efectivos, entre otros.

En general, Mitnick advierte sobre los peligros y las consecuencias de los hackeos empresariales y enfatiza la importancia de la concientización, la educación en seguridad, la seguridad profesional y las medidas apropiadas para reducir la inseguridad de los activos digitales y la información empresarial.

6. Metodología

6.1 Enfoque:

La presente investigación se basó un enfoque cualitativo el cual busco por medio del uso de métodos y técnicas textuales centrarse en la comprensión profunda y detallada de este fenómeno actual que ataca a las empresas contemporáneas desde una perspectiva subjetiva y contextual. Dicho enfoque cualitativo busco comprender la realidad social que viven las empresas actualmente ante la ciberseguridad y el reto que esta implica en la nueva era digital tomando principalmente la interpretación y significado que le atribuyen los autores anteriormente citados.

6.2 Alcance:

Esta investigación consto de un alcance descriptivo, interpretando un enfoque que busca describir y comprender las características, propiedades o fenómenos que ocurren en la realidad empresarial basados en el tema de la ciberseguridad en esta nueva era digital, sin

buscar establecer relaciones causales o hacer predicciones. El objetivo principal fue recopilar y analizar datos para proporcionar una descripción detallada y precisa de dicho fenómeno.

6.3 Tipo de Investigación:

El presente estudio abarco un tipo de investigación documental, que se basa principalmente en la revisión y análisis de documentos, escritos, registros o fuentes de información existentes, con el objetivo de obtener conocimiento, analizar, interpretar o describir el impacto que tiene la ciberseguridad en la era digital actual en este proyecto de investigación.

6.4 Fuentes de manejo de la información

Titulo investigación	Ciberseguridad, reto empresarial para afrontar la era de la digitalización actual

El presente trabajo se fundamentó en fuentes secundarias de información las cuales se tomaron para planteamientos narrativos y descriptivos

6.5 Técnicas de recolección de la información

Este estudio fue basado en la recolección de datos e información tomada de internet, libros, revistas y proyectos anteriormente realizados que abarcaban temas similares de investigación.

Tabla de contenido.

La siguiente tabla informa acerca de los instrumentos usados para la realización del presente documento.

Figura 4 1 Tabla 3: Contenido.

Pregunta	¿Cuáles son los retos que la era digital les genera a las empresas frente al nuevo ámbito de la ciberseguridad?
Objetivo general	Determinar los retos que la era digital genera a las empresas frente al nuevo ámbito de la ciberseguridad.

Objetivos específicos:

1. Comprender los nuevos riesgos empresariales que surgen a partir de la digitalización y nuevas IA.
2. Determinar la importancia de la ciberseguridad para las empresas contemporáneas.
3. Especificar los riesgos internos y externos que se generan en torno a los ataques cibernéticos en las empresas contemporáneas.
4. Definir en que herramientas cibernéticas deben invertir las empresas para la protección de sus activos digitales.
5. Determinar los retos que tienen las empresas para implementar ciberseguridad.

	APARTADO	**OBJETIVO ESPECIFICO**	**CONTENIDO**	**INSTRUMENTO**
1.	**Análisis de resultado- apartado 1.** **Riesgos empresariales generados por la nueva era de la digitalización.**	• Comprender los nuevos riesgos empresariales que surgen a partir de la digitalización y nuevas IA	• Párrafo introductorio acerca del tema. • Definición de digitalización y las nuevas IA. • Tipos de riesgos empresariales actuales que viven las empresas en un mundo globalizado. • Apreciación de las empresas sobre los nuevos retos que presentan en la actualidad. • Impactos generados por las nuevas tecnologías en las empresas.	• Análisis narrativo. • Tabla explicativa. • Explicación informativa. • Análisis narrativo.

			• Conclusiones y recomendaciones.	
2.	**Análisis de resultado – Apartado 2. Ciberseguridad, elemento indispensable para las empresas contemporáneas.**	• Determinar la importancia de la ciberseguridad para las empresas contemporáneas. • Especificar los riesgos internos y externos que se generan en torno a los ataques cibernéticos en las empresas contemporáneas.	• Iniciar con un párrafo que introduzca al lector en el tema. • Planteamiento del problema de seguridad virtual de las empresas • Especificar los principales puntos de vulnerabilidad de las empresas frente a los posibles ataques cibernéticos. • Determinar cómo está perjudicando a las empresas la carencia de ciberseguridad. • Determinar cuáles son los datos de vital importancia y enfocar los sistemas de ciberseguridad en estos. • Identificar las ventajas que trae la ciberseguridad y cómo usarlas	• **Infografía** • **Análisis narrativo y análisis comparativo** • **Análisis causa-efecto**

			para atacar las debilidades de las organizaciones. • Exponer todos los beneficios que trae y lo necesaria que es la ciberseguridad para las empresas • El apartado debe finalizar con un párrafo que concluya la información planteada anteriormente.	• **Análisis causa-efecto**
3.	**Análisis de resultado – Apartado 3. Inversiones y anticipos empresariales para aumentar su seguridad**	• Definir en que herramientas cibernéticas deben invertir las empresas para la protección de sus activos digitales. • Determinar los retos que tienen las empresas para implementar ciberseguridad.	• Iniciar con un párrafo que introduzca al lector en el tema. • Determinar cuales son los principales problemas en las empresas al no invertir en ciberseguridad. • Determinar en que deben invertir las empresas para poder desarrollar las estrategias que le permitan implementar una mayor	• **Análisis narrativo** • **Análisis narrativo – tabla comparativa** • **Infograma** • **Análisis**

			seguridad. • Determinar qué tan fácil es para las empresas implementar las acciones que la llevan al modelo de seguridad sugerido por las personas que tienen un mayor conocimiento en estas áreas específicas. • Problemas producidos por los múltiples ciberataques y hackeos que están en constantes desarrollo. • El apartado debe finalizar con un párrafo que concluya la información planteada anteriormente.	**narrativo**

Fuente. Elaboración propia.

7.0 Análisis de resultados

- **Comprender los nuevos riesgos empresariales que surgen a partir de la digitalización y nuevas IA**

Párrafo introductorio

En un mundo cada vez más interconectado y digitalizado, donde la tecnología ha tomado lugar desde la comunicación instantánea hasta la gestión empresarial y más allá, la ciberseguridad emerge como un faro de protección esencial en medio de la vastedad del mundo de la tecnología. Como un guardián virtual de nuestra presencia en línea y de los activos digitales que sustentan nuestra vida cotidiana, la ciberseguridad se ha levantado en una defensa crucial contra una cantidad de amenazas invisibles pero palpables.

La presencia constante de dispositivos inteligentes, la nube como almacén de información, y la automatización de procesos han dado lugar a un cambio en la forma en que las empresas y los individuos interactúan, colaboran y realizan transacciones. No obstante, esta transformación tecnológica también ha facilitado el camino para los ciberdelincuentes, quienes con ingenio y audacia esperan una oportunidad para sacar información valiosa de cuenta de la falta de ciberseguridad, listos para explotar cualquier brecha en las defensas digitales. En este panorama de paradojas digitales, es fundamental reconocer la ciberseguridad como el pilar fundamental que asegura nuestra información virtual. A medida que la información se convierte en moneda de cambio en esta economía digital, y las empresas almacenan no solo datos confidenciales, sino también su reputación y confianza, la ciberseguridad se erige como un centinela que resguarda la integridad y confidencialidad de todo lo que valoramos en el mundo virtual(Antonio, 2020).

En esta investigación, examinaremos en detalle las diferentes riesgos corremos todos en general, con el nacimiento de la ciberseguridad: desde las amenazas en constante evolución que se esconden en los bits y bytes, hasta las estrategias y medidas defensivas que permiten a las organizaciones reducir riesgos y mantener su fortaleza en el ciberespacio. Abordaremos la expansión de la superficie de ataque a medida que los dispositivos se conectan y las fronteras digitales se desvanecen, así como el papel crítico que desempeñan la educación y la concienciación en la creación de una cultura de seguridad resistente (*Las principales tendencias de seguridad y riesgos de Gartner para 2022*, s. f.).

Definición de digitalización y las nuevas IA

Digitalización:

La digitalización se refiere al proceso de convertir información, datos, objetos o procesos analógicos en formato digital. Implica la representación de elementos físicos o conceptuales

en forma de códigos binarios (0 y 1) que las computadoras y sistemas digitales pueden entender y procesar. La digitalización permite almacenar, manipular y transmitir información de manera eficiente, lo que ha llevado a una transformación significativa en diversos campos, desde la comunicación y el almacenamiento de datos hasta la automatización de procesos y la creación de nuevos modelos de negocio(*TFG-O-1891.pdf*, s. f.).

Nuevas Inteligencias Artificiales (IA):

Las nuevas inteligencias artificiales se refieren a las últimas y más avanzadas aplicaciones y sistemas basados en inteligencia artificial. La inteligencia artificial es una disciplina que busca crear máquinas y programas que puedan simular ciertos aspectos del pensamiento humano, como el aprendizaje, el razonamiento y la toma de decisiones. Las nuevas IA involucran enfoques como el aprendizaje profundo (Deep learning), el procesamiento del lenguaje natural, la visión por computadora y otros métodos avanzados para lograr resultados más precisos y sofisticados(García, 2018, s. f.)

Tipos de riesgos empresariales actuales que viven las empresas en un mundo globalizado

La digitalización ha revolucionado la forma en que las empresas operan, mejorando la eficiencia, la comunicación y el alcance global. Sin embargo, esta transformación también ha introducido una serie de nuevos riesgos empresariales en el ámbito de la ciberseguridad que requieren una comprensión profunda y una gestión adecuada. Para comprender y abordar estos riesgos, es esencial considerar los siguientes aspectos:

1. **Superficie de ataque ampliada**: Con la digitalización, las empresas han adoptado una variedad de tecnologías que incluyen dispositivos móviles, sensores IoT (Internet of things), sistemas de control industrial, servicios en la nube y más. Cada uno de estos puntos de conexión crea una posible entrada para los ciberdelincuentes. Comprender cómo estos dispositivos interactúan entre sí y con los sistemas empresariales es esencial para identificar y proteger posibles vulnerabilidades. Además, la expansión de la fuerza laboral remota también ha aumentado la exposición a riesgos, ya que los empleados acceden a la red corporativa desde diversas ubicaciones y dispositivos(Hernández García, 2014).

2. **Amenazas en constante evolución:** Los ciberdelincuentes están en constante búsqueda de nuevas formas de explotar vulnerabilidades. Desde ataques de "día cero" hasta malware altamente sofisticado, el panorama de las amenazas evoluciona rápidamente. Comprender las últimas tácticas, técnicas y procedimientos (TTP) utilizados por los atacantes, así como las tendencias emergentes en el mundo de la ciberdelincuencia, es fundamental para anticipar y contrarrestar estas amenazas de manera efectiva(Hernández García, 2014).

3. **Datos como activos críticos:** En la economía digital, los datos son un recurso valioso. Las empresas almacenan información sensible, desde datos personales de clientes hasta secretos comerciales. La pérdida o el robo de estos datos pueden tener graves consecuencias financieras y dañar la confianza del cliente. Comprender qué datos son críticos para la operación del negocio y cómo se deben proteger a lo largo de su ciclo de vida, incluyendo el almacenamiento, la transmisión y el procesamiento, es esencial para garantizar su integridad y confidencialidad(Hernández García, 2014).

4. **Cumplimiento normativo:** Con la creciente preocupación por la privacidad y la seguridad de los datos, los gobiernos y las autoridades reguladoras han implementado regulaciones estrictas para proteger la información. El incumplimiento de estas regulaciones puede resultar en multas significativas y daños a la reputación de la empresa. Comprender las regulaciones específicas que afectan a su industria y geografía, y adoptar medidas para cumplir con ellas, es esencial para evitar consecuencias legales y financieras adversas(Hernández García, 2014)

5. **Terceros y cadena de suministro:** Muchas empresas confían en terceros y proveedores para servicios clave, como proveedores de servicios en la nube, empresas de logística y otros socios comerciales. Sin embargo, estos terceros también pueden ser puntos débiles en la cadena de seguridad. Comprender cómo evaluar la postura de seguridad de los terceros, establecer requisitos de seguridad en los contratos y supervisar el cumplimiento de estas medidas es crucial para mitigar los riesgos que pueden surgir de la cadena de suministro(Hernández García, 2014)

6. **Cultura de seguridad:** Los empleados son una parte fundamental de la estrategia de ciberseguridad. La falta de conciencia y educación sobre las mejores prácticas de seguridad puede abrir la puerta a ataques. Fomentar una cultura de seguridad cibernética implica capacitar a los empleados en la identificación de correos electrónicos de phishing, el uso de contraseñas seguras, la autenticación de dos factores y la adopción de hábitos de trabajo seguros en línea (*6 Ways to Avoid a Ransomware Attack*, s. f.).

Apreciación de las empresas sobre los nuevos retos que presentan en la actualidad

Un aspecto importante a tener en cuenta a la hora de comprender los riesgos que trae la ciberseguridad es la naturaleza en constante evolución de las amenazas cibernéticas. La

ciberseguridad no es un desafío estático, sino que está en constante cambio debido a diversos factores, lo que requiere una comprensión dinámica y adaptativa por parte de las organizaciones y los profesionales de seguridad. La comprensión de esta dinámica implica varios aspectos clave, tales como:

1. **Tendencias y Tácticas Cambiantes:** Los atacantes cibernéticos constantemente buscan nuevas formas de explotar vulnerabilidades y evadir las medidas de seguridad. Comprender las últimas tendencias en tácticas y técnicas utilizadas por los ciberdelincuentes es esencial para anticipar posibles amenazas y fortalecer las defensas(Jeimy J. Cano M, 2020).

2. **Rápida Evolución de Normativas y Cumplimiento:** Las regulaciones y normativas relacionadas con la ciberseguridad también están en constante evolución. Comprender cómo estas regulaciones cambian y afectan a las prácticas de seguridad es crucial para evitar sanciones y garantizar el cumplimiento(M, 2020).

3. **Aprendizaje Continuo:** Dado que la ciberseguridad es un campo en constante cambio, es fundamental para los profesionales de seguridad mantenerse actualizados a través del aprendizaje continuo, la capacitación y la participación en comunidades de seguridad cibernética(M, 2020).

4. **Interconexión Global:** La interconexión global en la era digital significa que los riesgos pueden originarse en cualquier parte del mundo y propagarse rápidamente. Comprender cómo las amenazas pueden cruzar fronteras geográficas y afectar a una organización es vital(M, 2020).

En un mundo empresarial cada vez más digitalizado, la ciberseguridad se ha convertido en una prioridad estratégica inevitable. La comprensión de los riesgos emergentes es esencial para tomar medidas proactivas que protejan los activos y la reputación de una empresa. A medida que las organizaciones adoptan tecnologías de vanguardia para impulsar la innovación y la eficiencia, también deben reconocer la necesidad de construir una sólida defensa cibernética.

Impactos generados por las nuevas tecnologías en las empresas

Las nuevas tecnologías han traído consigo impactos significativos en el ámbito de la ciberseguridad en las empresas. Algunos de estos impactos incluyen:

- **Aumento de amenazas cibernéticas:** Con la adopción de nuevas tecnologías, las empresas se vuelven más propensas a una variedad de amenazas cibernéticas, como

ataques de phishing, malware, ransomware y ataques de denegación de servicio (DDoS). La expansión del panorama digital crea más puntos de entrada para los ciberdelincuentes(Antonio, 2020)

- **Mayor superficie de ataque:** La digitalización a menudo implica la conexión de más dispositivos y sistemas a la red, lo que amplía la superficie de ataque. Cada dispositivo conectado se convierte en un posible punto de acceso para los ciberatacantes si no está debidamente protegido(Saldaña Díaz, 2022).

- **Fugas de datos y brechas de seguridad:** Las empresas que manejan grandes cantidades de datos digitales están en riesgo de sufrir fugas de datos y brechas de seguridad. Los ciberatacantes pueden explotar vulnerabilidades en sistemas y aplicaciones para acceder a información confidencial y valiosa(Saldaña Díaz, 2022).

- **Desafíos de cumplimiento:** Las nuevas tecnologías a menudo vienen acompañadas de regulaciones y estándares de cumplimiento más estrictos en términos de seguridad de datos y privacidad. Las empresas deben asegurarse de cumplir con estas normativas, lo que puede requerir inversiones adicionales en seguridad cibernética(*Medida del nivel de seguridad informática de las pequeñas y medianas empres...*, s. f.).

- **Falta de conciencia y formación:** La rápida adopción de nuevas tecnologías puede llevar a una falta de conciencia y capacitación en ciberseguridad entre los empleados. La ingeniería social y los errores humanos pueden exponer a las empresas a riesgos cibernéticos(*Protecting Our Future*, s. f.).

- **Necesidad de soluciones de seguridad avanzadas:** Las empresas deben invertir en soluciones de seguridad cibernética más avanzadas para proteger sus activos digitales. Esto incluye firewalls avanzados, sistemas de detección de intrusiones, soluciones de seguridad para dispositivos móviles y análisis de amenazas en tiempo real(Saldaña Díaz, 2022).

- **Enfoque en la gestión de riesgos:** Las empresas deben adoptar un enfoque proactivo hacia la gestión de riesgos cibernéticos. Esto implica la identificación temprana de amenazas potenciales, la evaluación continua de vulnerabilidades y la implementación de medidas preventivas y correctivas(Saldaña Díaz, 2022)

- **Impacto en la reputación:** Las brechas de seguridad y los ciberataques exitosos pueden dañar la reputación de una empresa. La pérdida de la confianza del cliente y la mala publicidad pueden tener un impacto a largo plazo en los resultados financieros(Antonio, 2020).

Conclusión

En resumen, comprender los nuevos riesgos empresariales que trae la digitalización en relación con la ciberseguridad implica un enfoque completo que abarca la evolución de las amenazas, la protección de datos valiosos, el cumplimiento normativo, la gestión de terceros y proveedores, así como la promoción de una cultura de seguridad sólida. Abordar estos aspectos con diligencia y estrategia permitirá a las empresas enfrentar los desafíos de seguridad en la era digital y salvaguardar sus operaciones y activos de manera efectiva. La digitalización ofrece innumerables oportunidades para el crecimiento y la innovación empresarial, pero también trae consigo desafíos considerables en términos de seguridad cibernética. Al abordar estos desafíos de manera proactiva, educar a los empleados, implementar soluciones tecnológicas adecuadas y adoptar un enfoque global de la gestión de riesgos, las empresas pueden estar mejor preparadas para proteger sus activos, datos y operaciones en un mundo digital en constante evolución. La ciberseguridad ya no es simplemente una cuestión técnica, sino un componente esencial de la estrategia empresarial que requiere atención y acción continuas, en otras palabras, la integración acelerada de nuevas tecnologías en el entorno empresarial ha revolucionado la forma en que operan las organizaciones, pero este avance no está exento de desafíos en el ámbito de la ciberseguridad. La adopción de soluciones digitales y la interconexión de dispositivos han ampliado las posibilidades de ciberataques y fugas de datos. Las empresas se enfrentan a amenazas constantes como el phishing, el malware y el ransomware, que pueden tener consecuencias financieras y de reputación devastadoras. En este panorama, la concienciación de los empleados sobre la ciberseguridad se vuelve crucial, mientras que el cumplimiento normativo añade otra capa de responsabilidad. Para mantenerse protegidas, las empresas deben invertir en soluciones de seguridad avanzadas y adoptar estrategias de gestión de riesgos cibernéticos. A pesar de los desafíos, el aprovechamiento de las oportunidades de la digitalización y la inteligencia artificial puede lograrse con éxito al integrar medidas de seguridad sólidas en todas las etapas de la transformación digital. (*Protecting Our Future*, s. f.).

Ciberseguridad, elemento indispensable para las empresas contemporáneas.

Se puede evidenciar las diferentes interacciones que ha comenzado a generar la IA, el uso de aplicaciones en cualquier empresa es un reto desde un punto objetivo toda empresa quiere mejorar su eficiencia y eficacia al momento de estar compitiendo en cualquier mercado; no obstante todas las empresas tienen que aumentar su capacidad competitiva en la seguridad, no se trata solo de buscar la seguridad para evitar un ataque individual sino también para evitar el robo de información importante que puede ayudar a la competencia a tener una ventaja sobre el mercado.

El gran problema actual es el desconocimiento de todas las capacidades cibernéticas que hay en el medio, se busca cómo mejorar de una manera más óptima la vulnerabilidad que se tiene desde todos los aspectos al momento de intervenir e implementar tecnologías de IA. No es un secreto que la gran mayoría de empresas carecen actualmente de conocimiento de

la implementación sobre ciber seguridad al momento de competir con las diferentes ofertas que hay en los mercados, esto genera dificultad para las empresas. Realmente el uso de las tic y las redes sociales generan las alternativas necesarias para evidenciar falencias que tienen las compañías por la falta de capacitación al hacer uso en la WEB, no obstante, un sistema con falencia se muestra mucho más expuesto al momento de usarlo de manera incorrecta mostrando las personas que hacen ciber ataques no se pueden detectar con facilidad (Saldaña,Diaz 2022)

Hoy en día, las empresas utilizan diversas estrategias y tecnologías para guardar sus archivos digitales de manera segura y eficiente. Esto incluye el uso de servidores locales y en la nube. Muchas empresas implementan sistemas de gestión de documentos y almacenamiento en la nube, como Google Drive, Dropbox o Microsoft OneDrive, para almacenar y compartir archivos de manera colaborativa. Además, se realizan copias de seguridad regulares para garantizar la protección contra la pérdida de datos. También se aplican políticas de seguridad de datos y se utilizan medidas de cifrado para proteger la información sensible. En algunos casos, las empresas pueden utilizar servicios de almacenamiento en la nube privada o soluciones locales para un mayor control y seguridad de los datos.

El personal no capacitado es más propenso a caer en trampas de phishing y cometer errores que pueden resultar en ciberataques exitosos. El software no actualizado deja a la empresa vulnerable a vulnerabilidades conocidas. Estos problemas pueden llevar a la pérdida de datos, interrupciones en las operaciones, incumplimiento normativo y daños a la reputación. También existe un riesgo de filtraciones internas y violación de la privacidad. En resumen, la falta de capacitación y software actualizado puede tener graves consecuencias para la seguridad cibernética y la integridad de una empresa.

La IA tiene el potencial de mejorar la eficiencia operativa, la toma de decisiones y la personalización de servicios, lo que puede impulsar el crecimiento y la rentabilidad. No aprovechar esta tecnología puede significar quedarse atrás en un mercado cada vez más competitivo. Es claro la falta de inversión en IA puede limitar el potencial de las empresas para aprovechar al máximo las ventajas que esta tecnología puede ofrecer.

Las empresas tienen la responsabilidad de proteger una amplia variedad de datos al utilizar servicios de almacenamiento en la nube. Estos datos son cruciales para el funcionamiento y la reputación de la empresa, y su pérdida o exposición no autorizada puede tener consecuencias graves. Los tipos de datos que las empresas buscan proteger en la nube incluyen datos confidenciales de clientes, datos financieros, propiedad intelectual, información de empleados, datos de operaciones, datos de cumplimiento normativo, datos de análisis y marketing, así como copias de seguridad y registros.

Las consecuencias de no proteger adecuadamente estos datos en la nube pueden ser significativas e incluir brechas de seguridad, multas y sanciones por incumplimiento de regulaciones, pérdida de clientes, daño a la reputación, pérdida de propiedad intelectual, interrupción de negocios y costos significativos de recuperación.

Para mitigar estas consecuencias, las empresas deben implementar medidas de seguridad sólidas, como el cifrado de datos, el acceso basado en roles, la autenticación de dos factores y la supervisión continua de la actividad en la nube. Además, es esencial mantenerse actualizado sobre las regulaciones de privacidad de datos relevantes y cumplir con ellas

adecuadamente.

El COVID-19(SARS-CoV-2) tuvo un impacto sustancial en el ámbito de la ciberseguridad empresarial, entre ellos a combinación de rápidos cambios en los métodos de trabajo, la creciente dependencia de las herramientas digitales y la incertidumbre asociada a la pandemia crearon un entorno favorable para el crecimiento de las ciberamenazas y enfatizaron la importancia de la ciberseguridad en un mundo cada vez más digital. Las empresas tuvieron que adaptar y reforzar sus medidas de seguridad para afrontar estos nuevos retos. generando avances y transformaciones clave en la forma en que las organizaciones abordan la protección de sus activos digitales. Los cambios más destacados incluyeron un enfoque reforzado en la seguridad de las operaciones remotas, con la implementación de tecnologías como VPN, autenticación multifactor y políticas de acceso más rigurosas para salvaguardar las conexiones y dispositivos utilizados por los empleados que trabajan desde casa.

Además, se produjo un aumento significativo sobre la seguridad cibernética, con inversiones en programas de formación y campañas de sensibilización destinadas a educar a los trabajadores acerca de las amenazas en línea y las prácticas recomendadas de seguridad. La migración acelerada a entornos de nube también llevó a una mayor inversión en soluciones de seguridad específicas para la nube, como los servicios de seguridad de acceso a la nube (CASB) y la protección de datos en la nube.

Se hizo énfasis en la gestión de identidades y accesos (IAM), con la adopción generalizada de autenticación multifactor y soluciones IAM avanzadas para proteger las cuentas de usuario. Además, la aplicación de inteligencia artificial y análisis de amenazas permitió a las empresas identificar y mitigar proactivamente riesgos cibernéticos, a través de análisis de seguridad y la automatización de la detección de amenazas.

La continuidad del negocio y la recuperación ante desastres se volvieron fundamentales, con una revisión y mejora de los planes de respuesta a incidentes y la formulación de estrategias para mantener la operatividad en situaciones de crisis. Finalmente, se fomentó una mayor colaboración y compartición de información sobre amenazas entre organizaciones, fortaleciendo así la defensa colectiva contra los ataques cibernéticos.

En resumen, la pandemia de COVID-19 aceleró la evolución de la ciberseguridad empresarial, promoviendo avances en tecnología y prácticas para proteger los activos digitales en un entorno de trabajo cada vez más remoto y digitalizado. (Kevin Mitnick 2018)

La cita del autor Diogenes Yuri (2022) destaca la importancia de regulaciones efectivas en un mundo tecnológico en constante evolución. A medida que los avances revelan vulnerabilidades en sistemas empresariales, la falta de regulación adecuada amplía la brecha de seguridad. Las regulaciones bien diseñadas reducen costos de cumplimiento y permiten a las organizaciones fortalecer su resiliencia. Al adoptar estándares internacionales coherentes, las agencias reguladoras pueden evitar cargas innecesarias y la complejidad de la armonización. Sin embargo, es crucial reconocer que la educación en ciberseguridad y la preparación para la rápida proliferación de la IA son igualmente esenciales para garantizar que todos puedan acceder de manera segura a la tecnología en esta era de transformación digital (Diógenes Yuri 2022).

Conclusión

La creciente adopción de la inteligencia artificial (IA) en empresas de todo el mundo ha generado una serie de interacciones y desafíos significativos. En un mercado altamente competitivo, la eficiencia y la eficacia son imperativos para el éxito empresarial. Sin embargo, la seguridad cibernética se ha convertido en una preocupación crítica para las organizaciones, y no se limita solo a la prevención de ataques individuales, sino también a la protección de datos sensibles que podrían otorgar a la competencia una ventaja injusta. Un obstáculo importante en la actualidad es la falta de comprensión de las capacidades cibernéticas en constante evolución. Las empresas buscan constantemente mejorar su postura de seguridad, pero el desconocimiento de las amenazas potenciales puede llevar a vulnerabilidades inadvertidas al implementar tecnologías de IA. La mayoría de las empresas carecen de la capacitación necesaria en ciberseguridad para enfrentar eficazmente estos desafíos.

Las tecnologías de la información y la comunicación (TIC) y las redes sociales, aunque brindan oportunidades para identificar deficiencias en la seguridad, también exponen aún más a las organizaciones mal preparadas. Los ciberatacantes se benefician de esta falta de preparación y pueden operar de manera sigilosa, lo que hace que la detección sea una tarea ardua.

En conclusión, la IA y las TIC están transformando la forma en que las empresas compiten, pero también exponen sus debilidades en materia de seguridad. La falta de conocimiento y capacitación en ciberseguridad es un problema crítico que debe abordarse de manera urgente. Las empresas deben reconocer que la seguridad no es un lujo, sino una necesidad fundamental para garantizar la supervivencia y el éxito en un entorno empresarial cada vez más digital y competitivo. La inversión en educación y soluciones de ciberseguridad adecuadas es esencial para proteger los activos y la reputación de las empresas en esta era de IA y tecnología avanzada.

- **Especificar los riesgos internos y externos que se generan en torno a los ataques cibernéticos en las empresas contemporáneas.**

La seguridad cibernética se ha convertido en una preocupación crítica para las empresas en la era digital. La creciente dependencia de la tecnología y la información digital ha llevado a un aumento en las amenazas cibernéticas, lo que hace que la protección de los activos

digitales sea una prioridad indiscutible. En este contexto, la elección adecuada de herramientas cibernéticas es esencial para salvaguardar los datos y sistemas de una organización. Exploraremos las herramientas clave en las que las empresas deben invertir para fortalecer su seguridad cibernética y proteger sus activos digitales de manera efectiva.

En la era digital en la que vivimos, las organizaciones dependen en gran medida de la tecnología y la información en línea para operar de manera efectiva y competitiva. A medida que las empresas han adoptado cada vez más soluciones tecnológicas y han almacenado datos críticos en línea, también han aumentado sus vulnerabilidades a ciberataques. **(**Meraj Farheen, Ansar 2022)

En la era digital actual, las organizaciones dependen en gran medida de la información y la tecnología en línea para operar de manera eficiente y competitiva. A medida que las empresas adoptan soluciones tecnológicas y almacenan datos críticos en línea, aumenta su vulnerabilidad a los ciberataques. La falta de una ciberseguridad adecuada puede tener consecuencias inmediatas y perjudiciales para las empresas.

Uno de los problemas más destacados es el continuo desarrollo de ciberataques y piratas informáticos. Los adversarios están desarrollando métodos cada vez más sofisticados, lo que da como resultado un aumento en la frecuencia y variedad de las amenazas. Estos ataques pueden causar daños financieros a las organizaciones, incluidos enormes costos de recuperación y reparación del sistema, pérdida de datos importantes y propiedad intelectual, y posibles violaciones de la privacidad. Además de los problemas financieros, los ciberataques pueden afectar la reputación de una empresa y la confianza de sus clientes y socios comerciales. La interrupción de las operaciones comerciales normales y los costos de recuperación también pueden ser importantes. Las organizaciones pueden enfrentar desafíos legales y sanciones regulatorias si no cumplen con las regulaciones de ciberseguridad y protección de datos. (Kevin Mitnick 2018).

En resumen, la falta de una ciberseguridad adecuada puede tener una serie de consecuencias negativas, desde pérdidas financieras hasta problemas legales y daños a la reputación. Las organizaciones deben estar preparadas y tomar medidas proactivas para mitigar estos riesgos cibernéticos en un entorno digital en constante cambio.
La implementación efectiva de la ciberseguridad en las empresas es un desafío complejo y constante debido a diversos factores. En primer lugar, la falta de conocimiento y conciencia sobre la importancia de la ciberseguridad entre empleados y directivos puede poner en riesgo la protección de datos y sistemas. La educación y la concienciación son esenciales para abordar este problema.

Además, el rápido avance de las amenazas cibernéticas complica la tarea de mantenerse al día con las tácticas de ataque y vulnerabilidades emergentes. Esta evolución constante exige una vigilancia constante y adaptabilidad por parte de las empresas.

Un obstáculo crítico es la escasez de talento en ciberseguridad, lo que hace que sea difícil contratar y retener a expertos en este campo altamente demandado. Esto se agrava por los

costos asociados a la implementación de medidas de ciberseguridad sólidas, que incluyen inversiones en tecnología, capacitación y personal especializado.

La complejidad tecnológica también es un desafío importante, ya que muchas empresas gestionan una amplia variedad de sistemas y aplicaciones que deben protegerse. Además, el cumplimiento normativo puede requerir esfuerzos adicionales para garantizar el cumplimiento de estándares específicos.

Las amenazas internas, tanto accidentales como maliciosas, plantean un riesgo significativo para la seguridad de los datos y sistemas, lo que requiere un enfoque integral en la prevención y la detección.

La resistencia al cambio por parte de los empleados y la necesidad de integrar nuevas tecnologías, como la nube y el IoT, también son consideraciones importantes.

Por último, la comunicación efectiva entre los equipos de TI y la alta dirección es esencial para tomar decisiones informadas sobre la inversión en seguridad cibernética. En conjunto, estos desafíos subrayan la complejidad y la necesidad constante de adaptación en el ámbito de la ciberseguridad empresarial.

En la era digital interconectada, la ciberseguridad emerge como un elemento esencial para las empresas contemporáneas, independientemente de su tamaño o alcance. Este estudio profundiza en la relevancia de la ciberseguridad, abordando problemas de seguridad virtual, principales puntos de vulnerabilidad, cómo la ausencia de ciberseguridad perjudica a las empresas y los datos de vital importancia. Además, se exploran las ventajas de contar con un sólido sistema de ciberseguridad y cómo utilizarlo para abordar debilidades. **(**Meraj Farheen, Ansar 2022)

La ciberseguridad se convierte en un escudo esencial que protege las ambiciones, secretos comerciales y la confianza de los clientes. Tanto las empresas emergentes como las multinacionales comparten la dependencia de la tecnología y la conectividad, lo que subraya la importancia de la ciberseguridad en la estrategia de negocio.

Las empresas emergentes a menudo enfrentan recursos limitados, mientras que las multinacionales son objetivos atractivos para los ciberatacantes. Ambas pueden sufrir la pérdida de confianza y enfrentar desafíos de cumplimiento normativo. La dependencia de la tecnología y la falta de un ambiente de protección sólido son problemas comunes.

Los principales puntos de vulnerabilidad incluyen la falta de concienciación, software desactualizado, contraseñas débiles, acceso no autorizado, correo electrónico malicioso, dispositivos no seguros, falta de actualizaciones, escasa inversión en ciberseguridad, suministradores y terceros, falta de plan de respuesta, malware y ransomware, sistemas internos sin protección, conexiones inseguras, exposición en la nube y falta de monitorización. Abordar estos puntos requiere una estrategia de ciberseguridad integral.

La ausencia de ciberseguridad puede perjudicar a las empresas de múltiples maneras, incluyendo brechas de seguridad, pérdida de confianza, daño a la marca, pérdida de ventaja competitiva, interrupciones operativas, incumplimiento normativo, reparación de daños a largo plazo, disrupción de la cadena de suministro y requisitos de inversión emergentes.

Los datos de vital importancia, como información financiera, datos de clientes y propiedad intelectual, deben ser protegidos debido a su valor estratégico. La falta de protección de estos datos puede tener graves consecuencias, incluyendo la pérdida de confianza y la pérdida de ventaja competitiva.

La ciberseguridad ofrece ventajas fundamentales, como la protección de activos, la confianza del cliente, el cumplimiento normativo, ventaja competitiva, continuidad operativa, gestión de riesgos, detección y respuesta rápida, mejora de la cultura de seguridad, reducción de costos y protección de la reputación. Estas ventajas pueden utilizarse para abordar debilidades mediante la inversión en tecnologías de ciberseguridad, formación del personal, desarrollo de políticas de seguridad, evaluación continua y mejora.

En resumen, la ciberseguridad es esencial para las empresas contemporáneas. Su ausencia puede tener consecuencias devastadoras, mientras que su implementación adecuada no solo protege a las empresas de amenazas cibernéticas, sino que también brinda ventajas estratégicas y fortalece la confianza del cliente. Proteger los datos de vital importancia y utilizar las ventajas de la ciberseguridad son imperativos para asegurar un futuro sólido en el entorno empresarial actual.

8.0 Discusión

8.1 Aspectos relevantes

A lo largo de la investigación se encontraron importantes aportes y aspectos relevantes que ayudaron al desarrollo de la pregunta de investigación, asimismo, se presenta información de interés tanto para el ámbito académico como para el ámbito práctico de las instituciones educativas aportando nuevos conocimientos y perspectivas a estas. La investigación se centró en desarrollar los siguientes objetivos específicos: a) Comprender los nuevos riesgos empresariales que surgen a partir de la digitalización y nuevas IA, b) Determinar la importancia de la ciberseguridad para las empresas contemporáneas, c) Especificar los riesgos internos y externos que se generan en torno a los ataques cibernéticos en las empresas contemporáneas.

Partiendo de estos objetivos, los principales hallazgos encontrados en la investigación para el primer objetivo específico “Comprender los nuevos riesgos empresariales que surgen a partir de la digitalización y nuevas IA” se entiende que la digitalización empresarial y la integración de nuevas tecnologías de inteligencia artificial (IA) están remodelando el panorama de los negocios a nivel mundial. La transformación de procesos y operaciones a través de tecnologías digitales es esencial para la competitividad y eficiencia de las empresas. Sin embargo, esta revolución también trae consigo riesgos específicos, desde

amenazas cibernéticas hasta desafíos en la privacidad de datos. La adaptación y resiliencia son clave; las estrategias para mitigar estos riesgos, como inversiones en ciberseguridad y formación del personal

La innovación responsable se vuelve fundamental en un contexto donde la ética y el impacto social de las tecnologías emergentes deben ser cuidadosamente considerados. Los modelos de negocio existentes y la necesidad de mantener la competitividad requieren una comprensión profunda de estos cambios. La formación y concientización del personal son elementos cruciales en la gestión de riesgos digitales, ya que las amenazas a menudo involucran aspectos del tema social.

La presencia constante de dispositivos inteligentes, el almacenamiento de información en la nube y la automatización de procesos han facilitado la vida cotidiana, pero también han creado oportunidades para ciberdelincuentes. En este contexto, la ciberseguridad se destaca como defensa crucial, protegiendo la información virtual en un mundo donde los datos confidenciales, la reputación y la confianza son moneda de cambio en la economía digital.
Para el segundo objetivo específico "Determinar la importancia de la ciberseguridad para las empresas contemporáneas" teniendo en cuenta la ciberseguridad se presenta como una piedra angular en el mundo empresarial contemporáneo, caracterizado por una creciente digitalización. Su importancia radica en la necesidad de resguardar activos críticos, datos sensibles y la reputación de las empresas frente al constante aumento de amenazas cibernéticas. Con la conectividad y el intercambio de información en línea, las empresas se encuentran expuestas a riesgos como ataques de malware, violaciones de datos y ciberataques avanzados, que podrían resultar en pérdidas financieras y desconfianza con los clientes. La ciberseguridad va más allá de la defensa ante amenazas conocidas; implica una mentalidad proactiva, la implementación de medidas preventivas y la educación de los empleados en prácticas seguras.
Además, se resalta que las vulnerabilidades informáticas pueden originarse por diversos factores, como la falta de medidas de seguridad, actualizaciones de software insuficientes y carencias en la formación sobre seguridad digital y controles de acceso. La respuesta a incidentes y la protección de infraestructuras críticas son aspectos clave, con la necesidad de analizar escenarios y políticas para mejorar el rendimiento del sistema.
Para el tercer objetivo específico "Especificar los riesgos internos y externos que se generan en torno a los ataques cibernéticos en las empresas contemporáneas" las empresas se enfrentan a una creciente amenaza de ataques cibernéticos, originados tanto desde el interior como desde el exterior de la organización. Los riesgos internos pueden surgir de factores como la falta de conciencia y formación en seguridad entre los empleados, el descuido en la implementación de políticas de seguridad interna, y la mala gestión de accesos y privilegios. Por otro lado, los riesgos externos provienen de agentes externos malintencionados, como hackers y estados-nación. Estos actores pueden explotar vulnerabilidades en sistemas, realizar ataques de phishing dirigidos y comprometer la seguridad a través de malware avanzado. La especificación detallada de estos riesgos es esencial para desarrollar estrategias efectivas de ciberseguridad.

El desarrollo constante de ciberataques y piratería informática representa un problema

significativo, con adversarios que emplean métodos cada vez más sofisticados. Los ataques pueden causar daños financieros, pérdida de datos críticos y violaciones de privacidad, afectando la reputación y la confianza de las empresas. La ciberseguridad se presenta como un escudo esencial en la era digital, protegiendo ambiciones, secretos comerciales y la confianza del cliente.

Implementar la ciberseguridad efectiva enfrenta desafíos complejos, desde la falta de conocimiento hasta la evolución constante de amenazas y la escasez de talento en ciberseguridad. La resistencia al cambio, la integración de nuevas tecnologías y la comunicación efectiva entre equipos de TI y la alta dirección son consideraciones clave.

Revisión de la literatura

El autor Nova (2016) evalúa la estrategia nacional en el ciberespacio de Colombia, considerando sus impactos en áreas clave como la gestión del conocimiento, investigación, desarrollo e innovación. Además, compara estas estrategias con modelos de defensa establecidos junto con países aliados, destacando la colaboración con naciones como Inglaterra, Israel y Estados Unidos. Ademas Nova señala la evolución de los modelos de seguridad cibernética, lo que implica nuevas funcionalidades y capacidades frente a arquitecturas de seguridad informática y conceptos emergentes en relaciones internacionales como el "ciberpoder".

Mitnick (2018) aborda de manera clara y directa la importancia de la privacidad en un mundo cada vez más digitalizado. Sus recomendaciones van más allá de las medidas técnicas y se centran en la conciencia, la educación y el empoderamiento individual para proteger la información personal en línea y fuera de ella. Mitnick presenta la privacidad como un poder que todos necesitamos y merecemos en la era moderna. Sugiere que las técnicas de élite, cuando se utilizan adecuadamente, pueden maximizar la privacidad y ayudar a las personas a mantenerse invisibles en un mundo digital.

Recomendaciones

Se puede seguir investigando sobre la era de la transformación digital y la inteligencia artificial, las empresas se enfrentan a riesgos empresariales emergentes que demandan respuestas estratégicas y proactivas. Para abordar estos desafíos, se proponen recomendaciones integrales.

Asimismo, la adaptación y resiliencia se destacan como imperativos en un entorno donde la rápida transformación digital exige estrategias flexibles para ajustarse a riesgos en constante evolución. La innovación responsable se presenta como un principio clave, instando a las empresas a considerar no solo la eficiencia, sino también la ética y el impacto social de las nuevas tecnologías. La participación activa de todo el personal en la gestión de riesgos digitales, respaldada por formación continua, se postula como esencial. La inversión en ciberseguridad se presenta como crítica, con medidas proactivas y tecnologías especializadas para proteger activos digitales. La colaboración externa, la gestión del cambio, la comunicación efectiva y la evaluación continua complementan estas recomendaciones, abordando aspectos clave para fortalecer la seguridad cibernética y la resiliencia empresarial en un entorno digital dinámico. Su implementación contribuirá a

mantener una postura segura frente a los riesgos cibernéticos en constante evolución y protegerá los activos digitales de la empresa.

Conclusiones

- La digitalización y la adopción de nuevas tecnologías, incluida la inteligencia artificial, han transformado la forma en que las empresas operan y se relacionan en un mundo interconectado. Sin embargo, este avance también ha dado lugar a una serie de desafíos significativos en términos de ciberseguridad. La ampliación de la superficie de ataque, las amenazas en constante evolución y la creciente importancia de los datos como activos críticos son aspectos clave que las empresas deben abordar para proteger su integridad y reputación en la economía digital.

- La ciberseguridad se ha convertido en un elemento indispensable y estratégico para las empresas contemporáneas. Los riesgos empresariales actuales, desde la expansión de la superficie de ataque hasta la necesidad de cumplir con regulaciones estrictas, destacan la urgencia de tomar medidas proactivas en la gestión de la seguridad cibernética. Además, la falta de conciencia y formación, así como los riesgos asociados con terceros y la cadena de suministro, subrayan la necesidad de una cultura de seguridad sólida y una evaluación constante de las amenazas emergentes.

- En la era digitalizada actual, donde la información es una moneda de cambio vital, la ciberseguridad no solo es una preocupación técnica, sino un componente esencial de la estrategia empresarial. Las empresas deben reconocer la dinámica y evolución constante de las amenazas cibernéticas, adoptar soluciones de seguridad avanzadas y fomentar una cultura de seguridad entre sus empleados. La integración acelerada de nuevas tecnologías en el entorno empresarial ofrece oportunidades de crecimiento, pero su éxito depende de abordar de manera proactiva los desafíos de seguridad y mantenerse al tanto de las tendencias y tácticas cambiantes en el panorama cibernético.

- La digitalización de las empresas trae consigo desafíos en materia de ciberseguridad. Para tener éxito, las empresas deben mejorar la protección de datos, el cumplimiento normativo y la formación de los empleados. La ciberseguridad ya no es sólo una cuestión técnica, sino una parte integral de la estrategia empresarial que requiere atención constante. Integrar sólidas medidas de seguridad en la transformación digital es fundamental para proteger los activos y las operaciones en un mundo digital en constante cambio.
- La creciente adopción de la inteligencia artificial (IA) presenta desafíos de ciberseguridad. La falta de comprensión y capacitación en ciberseguridad deja a las empresas vulnerables a amenazas invisibles. La inteligencia artificial y las TIC

están cambiando la forma en que compiten las empresas, pero también están exponiendo sus debilidades. La seguridad es un requisito básico para la supervivencia en el mundo empresarial digital y competitivo. En la era de la inteligencia artificial y la tecnología avanzada, son necesarias inversiones en formación y soluciones de ciberseguridad adecuadas para proteger los activos y la reputación.

- En la era digital actual, la ciberseguridad ha alcanzado un papel estratégico y central en empresas con una gran superficie de ataque y riesgos cambiantes. La gestión proactiva de la ciberseguridad se vuelve crítica en un entorno donde la información es un activo clave. Además, la falta de concientización, capacitación y riesgos de terceros y de la cadena de suministro requieren una sólida cultura de seguridad y una evaluación continua de las amenazas. La adopción de nuevas tecnologías en las empresas ofrece oportunidades de crecimiento, pero su éxito depende de responder activamente a los desafíos de seguridad de la información y mantenerse al día con las tendencias en constante evolución del ciberespacio.

9.0 REFERENCIAS

Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones - ProQuest. (s. f.). Recuperado 26 de febrero de 2023, de https://www.proquest.com/openview/a8a7f26365baadfda3accf15818ab729/1?pq-origsite=gscholar&cbl=1006393

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys*, *54*(8), 1-35. https://doi.org/10.1145/3469886

Díaz, C. R. F. (2018). La amenaza de las nuevas tecnologías en los negocios: El ciberespionaje empresarial. *Revista de Derecho de la UNED (RDUNED)*, *23*, Art. 23. https://doi.org/10.5944/rduned.23.2018.24001

Echeverría Samanes, B., & Martínez Clares, P. (2018). Revolución 4.0, Competencias, Educación y Orientación. *Revista Digital de Investigación en Docencia Universitaria*, *12*(2), 4-34. https://doi.org/10.19083/ridu.2018.831

Jensen, M. L., Wright, R. T., Durcikova, A., & Karumbaiah, S. (2022). Improving Phishing Reporting Using Security Gamification. *Journal of Management Information Systems*, *39*(3), 793-823. https://doi.org/10.1080/07421222.2022.2096551

La ciberseguridad en la era de hipercompetitividad: ¿puede la UE afrontar l...: Discovery Service para Universidad Pontificia Bolivariana. (s. f.). Recuperado 26 de febrero de 2023, de https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=9&sid=20717784-4db9-4a0b-8c5c-331d6c0fc185%40redis

La ciberseguridad tiene mucho más que ver con psicología que con tecnología. (2021). *Capital Humano*, *369*, 23-32.

Niño, F. Y. A. (2023). Ransomware, una amenaza latente en Latinoamérica. *InterSedes*, *24*(49), Art. 49. https://doi.org/10.15517/isucr.v24i49.50765

Rea-Guaman, M., Calvo-Manzano, J. A., & Feliu, T. S. (2018). Prototipo para Gestionar la Ciberseguridad en Pequeñas Empresas: A Prototype to Manage Cybersecurity in Small Companies. *CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings*, 1-6.

Rodrigo Cando-Segovia, M., & Medina-Chicaiza, P. (2021). Prevención En Ciberseguridad: Enfocada a Los Procesos De Infraestructura Tecnológica: CYBERSECURITY PREVENTION: FOCUSED ON TECHNOLOGICAL INFRASTRUCTURE PROCESSES. *3C TIC*, *10*(1), 17-40. https://doi.org/10.17993/3ctic.2021.101.17-41

Serrahima, J. (2009). *La amenaza digital: Conozca los riesgos informáticos que pueden arruinar su negocio*. Profit Editorial.*Volumen-31-2016-libre.pdf*. (s. f.). Recuperado 27 de febrero de 2023, de https://d1wqtxts1xzle7.cloudfront.net/62103447/Volumen-31-2016-libre.pdf?1581746693=&response-content-disposition=inline%3B+filename%3DLOS_DESAFIOS_QUE_ENFRENTA_LA_EDUCACION_A.pdf&Expires=1677522446&Signature=dUDj~MBgXFf7-xmFNm7-PU0gXzKq60YDK~s24l8F00BHNrvb7CPf0MTZZj9FQvi72MDwL-pLP6jGRQB4pPRFp2ZxDdv4NPVN72mNkN00KngyZuKZ0QuQ6YJqLk1jkx9KKCr9lVDh3ueRn-NH01Jgle044jlMATJGHm9o-jnpwZUCSH4hg1e18sKpbtGPAmSrMn4NOuXrC5-yFJvkzgQrRPs9k80sGMFsRKGxKrIC2vkWWqtEyVVZYDe1fKqcRlRXIc7WJa8MbuPtqiUcNEcyMCwXHuazTu1ywy2TkyA7AoXbQLTNG7RGmCA9s5qy1zS8PSM5QL1LukXfCQXbUZWUDw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA#page=61

Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones - ProQuest. (s. f.). Recuperado 26 de febrero de 2023, de https://www.proquest.com/openview/a8a7f26365baadfda3accf15818ab729/1?pq-origsite=gscholar&cbl=1006393

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys*, *54*(8), 1-35. https://doi.org/10.1145/3469886

Díaz, C. R. F. (2018). La amenaza de las nuevas tecnologías en los negocios: El ciberespionaje empresarial. *Revista de Derecho de la UNED (RDUNED)*, *23*, Art. 23. https://doi.org/10.5944/rduned.23.2018.24001

Echeverría Samanes, B., & Martínez Clares, P. (2018). Revolución 4.0, Competencias, Educación y Orientación. *Revista Digital de Investigación en Docencia Universitaria*, *12*(2), 4-34. https://doi.org/10.19083/ridu.2018.831

Jensen, M. L., Wright, R. T., Durcikova, A., & Karumbaiah, S. (2022). Improving Phishing Reporting Using Security Gamification. *Journal of Management Information Systems*, *39*(3), 793-823. https://doi.org/10.1080/07421222.2022.2096551

La ciberseguridad en la era de hipercompetitividad: ¿puede la UE afrontar l...: Discovery Service para Universidad Pontificia Bolivariana. (s. f.). Recuperado 26 de febrero de 2023, de https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=9&sid=20717784-4db9-4a0b-8c5c-331d6c0fc185%40redis

La ciberseguridad tiene mucho más que ver con psicología que con tecnología. (2021). *Capital Humano*, *369*, 23-32.

Niño, F. Y. A. (2023). Ransomware, una amenaza latente en Latinoamérica. *InterSedes*, *24*(49), Art. 49. https://doi.org/10.15517/isucr.v24i49.50765

Rea-Guaman, M., Calvo-Manzano, J. A., & Feliu, T. S. (2018). Prototipo para Gestionar la Ciberseguridad en Pequeñas Empresas: A Prototype to Manage Cybersecurity in Small Companies. *CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação)*

Proceedings, 1-6.
Rodrigo Cando-Segovia, M., & Medina-Chicaiza, P. (2021). Prevención En Ciberseguridad: Enfocada a Los Procesos De Infraestructura Tecnológica: CYBERSECURITY PREVENTION: FOCUSED ON TECHNOLOGICAL INFRASTRUCTURE PROCESSES. *3C TIC*, *10*(1), 17-40. https://doi.org/10.17993/3ctic.2021.101.17-41