La Ciberseguridad en las Pymes

César David Díaz Jiménez
Edgar Ariza Rodríguez
Maycol Yesid Ruiz Moncada

Escuela de Administración de Negocios
Especialización de Gerencia en Tecnología
Wilken Giussepe Rodríguez

Bogotá D.C., 23 de mayo de 2023

Contenido

1. Introducción

La ciberseguridad es un componente clave para la transformación digital de las empresas y debe estar alineado con la estrategia del negocio para que se ajuste a las necesidades de protección de la información. Debe ser adoptada por cualquier empresa u organización sin importar su tamaño teniendo en cuenta que desde el inicio de la pandemia los ciberataques han aumentado de manera exponencial y diversas empresas han sido blanco de estos. Empresas del sector bancario y salud han sido algunas de las más afectadas por los atacantes lo que las ha llevado a robustecer su infraestructura e implementar controles y políticas adecuadas para mitigar los riesgos de los ciberataques. La ciberseguridad debe ser una estrategia que se extienda desde empleados hasta los mismos clientes creando una cultura de concientización ya que permitirá que se conozcan las amenazas y se garantice el cumplimiento de las normas que se establezcan en pro de la protección de la información. Las pymes deben entender los riesgos existentes debido a que, a pesar de que operan en mercados locales, las amenazas son globales y esto las convierte en vulnerables también (Moro, 2022).

1.1. Planteamiento del problema

La falta de interés por parte de los directivos para proteger sus empresas puede deberse a varios factores, incluyendo la falta de conciencia, asignación recursos, tiempo y experiencia en ciberseguridad, así como a la cultura empresarial. Para abordar este problema, los directivos deben educarse sobre la importancia de la ciberseguridad y asignar recursos adecuados para implementar medidas de seguridad de la información efectivas. Además, deben establecer una cultura empresarial que priorice la ciberseguridad como una parte integral de la gestión empresarial, pues se podría pensar que con la implementación de una tecnología correcta se pensaría que las pymes estarían asegurando la integridad, confidencialidad y disponibilidad de la información, pero la realidad es que esto no es así, pues una de las principales causas de que los ciberataques sean éxitos se deben al factor humano y este último en el que menos se invierte o capacita. (Aldeco, 2020,p.31).

Se podría pensar que las grandes empresas no se ven afectas por los ciberataques por contar con robustos y experimentados equipos de profesionales de TI para implementar las soluciones necesarias en ciberseguridad y combinar equipos de alta gama y personal excelentemente calificado que se encarga de establecer las estrategias y políticas de seguridad de la información ante las amenazas que se presentan en el mundo digital, pero no es así, un claro ejemplo de ello es el artículo publicado por el diario la república el 17 de febrero del año 2023, en el que afirma que 1- “Colombia fue el cuarto país más ciber atacado en Latinoamérica en el 2022, y entidades como EPM, EPS Sanitas, INVIMA, Viva Air, Claro Colombia, Carvajal, Universidad Javeriana y la fiscalía general de la Nación fueron algunas de las entidades

más afectadas.” (Molano, 2023).

De acuerdo con un informe de INTERPOL, a partir de la pandemia de COVID-19 se presentó un aumento de los ciberataques hacia las empresas. Esta situación debe ser considerada de alta relevancia en las pymes para lograr la mitigación de los riesgos asociados a la seguridad de la información. Los directivos de las empresas deben tomar conciencia frente a la importancia que tiene la ciberseguridad dado que este tipo de proyectos no hacen parte únicamente del área de las TIC, sino que se deben enfocar como parte de la planeación estratégica de las empresas. (INTERPOL, 2020)

1.2. Objetivos de investigación

1.2.1. General:

- Identificar el nivel de uso de las herramientas de ciberseguridad en las pymes ubicadas en el barrio Toberín de la ciudad de Bogotá, Colombia.

1.2.2. Específicos:

- Determinar si las pymes destinan un porcentaje del presupuesto detecnología para invertir en el área de ciberseguridad.
- Reconocer las actividades que realizan las empresas para fomentar el uso de herramientas tecnológicas y políticas de seguridad que se implementan dentro de las pymes del barrio Toberín en la ciudad de Bogotá, Colombia.

1.3. Preguntas de investigación

- ¿Qué políticas y procesos están adoptando las pequeñas y medianas empresas en el área de ciberseguridad y cuál es el nivel de uso de las herramientas tecnológicas para afrontar los desafíos que se presentan en esta materia para los mercados actuales?

- ¿Cuánto es el presupuesto establecido por las pymes para que el área de TI proteja su infraestructura e información de los ciberataques?

- ¿Qué actividades realiza la empresa en sus procesos internos para que se reconozcan y adopten las buenas prácticas de ciberseguridad?

1.4. Justificación

Esta investigación se hace necesaria porque a medida que la tecnología avanza, las empresas deben prepararse para competir en un entorno digital que implica, entre otros, importantes desafíos en temas de ciberseguridad. Es fundamental que las empresas comprendan la importancia de establecer procesos para salvaguardar la información y protegerse de ataques que interrumpan o impidan su operación (Álvarez, 2023).

Gracias a la información recolectada también será posible publicar un informe que puedaservir como alerta para que los empresarios tomen las medidas requeridas en la seguridad de la información además de que se obtendrá información relevante de estas empresas para realizar asesoramiento y consultorías en seguridad de la información, luego, verificar si en estas empresasexiste un mercado donde se puedan ofrecer consultorías en ciberseguridad, capacitaciones, soluciones de tecnología u otros.

De igual manera, es importante realizar esta investigación porque en muchas empresas esprobable que exista desconocimiento acerca de los riesgos a los que están expuestas cuando utilizan tecnologías de la información.

Algunas publicaciones que dan cuenta de la importancia de que las empresas enfoquen esfuerzos en la implementación de ciberseguridad:

> Los ciberdelincuentes están creando nuevos ataques e intensificando su ejecución a un ritmo alarmante, aprovechándose del miedo y la incertidumbre provocados por la inestabilidad de la situación socioeconómica generada por la COVID-19. (INTERPOL, 2020)

Según declaraciones de Don Mackenna, vicepresidente sénior de ingeniería, administración de productos y protección de correo electrónico de Barracuda, afirma que: "Las pequeñas empresas a menudo tienen menos recursos y carecen de experiencia en seguridad, lo que las hace más vulnerables a los ataques de phishing selectivo, y los ciberdelincuentes se están aprovechando" (Hageman, 2022)

Es fundamental tener en cuenta que las amenazas cibernéticas afectan tanto a las grandes como a las pequeñas empresas. Un informe de la firma de seguridad informática Hiscox reveló que, en 2020, el 28% de las pequeñas empresas sufrieron al menos un ciberataque, y el costo promedio de recuperación fue de más de $200,000 dólares (Hiscox, 2021).

De acuerdo con Kaspersky, las pequeñas empresas son especialmente vulnerables a los ciberataques debido a su limitada capacidad tecnológica para hace frente a los ciberataques y la escasa asignación de recursos para invertir en tecnología de seguridad y en la capacitación de empleados (Kaspersky, 2022).

Por lo tanto, es importante que las pequeñas empresas tomen medidas para protegerse de los ciberataques, como la implementación de soluciones de seguridad de la información, la formación del personal en cuestiones de ciberseguridad y la sensibilización y formación al usuario final de manera regular. Al tomar estas medidas, las pequeñas empresas empiezan a mitigar el riesgo para evitar sufrir un ciberataque y evitar los altos costos asociados con la recuperación de un ataque exitoso. (El ransomware: qué es, cómo se lo evita, cómo se elimina, 2022)

Los beneficios de realizar esta investigación son:

- Conocer las políticas con las que actualmente cuentan las pymes

para gestionar los riegos en ciberseguridad y seguridad de la información y evaluar si son las más apropiadas o por el contrario, se puedan fortalecer de acuerdo con el negocio de cada una.

- Identificar los métodos que utilizan las empresas para concientizar a sus colaboradores respecto a la seguridad de la información.
- Obtener cifras de los costos entregados al área de TI para invertir en ciberseguridad; con esto se determinará si está al alcance del presupuesto de la organización.
- Lograr un análisis en el cual nos permita asesorar a las pequeñas y medianas empresas para implementar elementos de ciberseguridad en su infraestructura a un costo asequible.

1.5. Viabilidad

El equipo a cargo de esta investigación se encuentra conformado por profesionales del sector de las TICS con experiencia en la administración de infraestructura tecnológica, servicios de tecnología y conocimientos de gestión de seguridad de la información en empresas pequeñasy medianas. El tiempo con el que cuenta el equipo es escaso por lo tanto será necesario tomar una muestra pequeña de empresas donde se efectuará la investigación. Los recursos financieros serán mínimos y aportados por el equipo de estudio. El alcance de la investigación es lograr conocer e identificar las políticas de seguridad informática que tienen implementadas y por supuesto la cultura organizacional de la compañía respecto a la confidencialidad de la información.

2. Marco teórico

2.1. Sistema de información

2.1.1. Definición

Para hablar de ciberseguridad y las implicaciones que tiene su implementación en las empresas, es importante conocer algunos conceptos que ayudan a dar más claridad a todo el tema de seguridad en los sistemas de información. Podemos comenzar definiendo al sistema de información como “un conjunto ordenado de mecanismos que tienen como fin la administración de datos y de información, de manera que puedan ser recuperados y procesados fácil y rápidamente” (Equipo editorial, 2021). De acuerdo con lo anterior surge la necesidad de que estos sistemas de información estén protegidos de manera que la información que almacenan se mantenga fuera del alcance de personas u otros sistemas no autorizados.

2.1.2. Vulnerabilidades

Una vulnerabilidad informática define una debilidad en el software o hardware de un sistema tecnológico conformado por infraestructura TI. Son productos de errores o fallos del diseño de los fabricantes y también de la tecnología en la cual fueron diseñadas las aplicaciones. La manera de que los ciber atacantes aprovechen las vulnerabilidades es mediante ‘exploit’, los cuales causan un efecto como instalar malware o algún tipo de intrusión en los sistemas informáticos. “Incluso si existe una determinada vulnerabilidad, no existe ningún peligro inmediato hasta que alguien averigua cómo crear un exploit para ella. Sin embargo, una vez que se descubre la vulnerabilidad, puede estar seguro de que alguien intentará desarrollar un exploit.” (Belcic, 2020).

2.1.3. Estrategias de protección

La implementación de un sistema de gestión de la seguridad informática es fundamental para cualquier organización que desee proteger sus sistemas informáticos y datos de las ciber amenazas. En primer lugar, ayuda a proteger los datos y sistemas confidenciales del acceso no autorizado y los ataques maliciosos, lo que reduce el riesgo de filtraciones de datos y pérdidas financieras. En segundo lugar, ayuda a garantizar el cumplimiento de los requisitos reglamentarios y los estándares de la industria, lo que puede evitar sanciones legales y financieras. En tercer lugar, mejora la reputación de la organización y la confianza del cliente al demostrar el compromiso de proteger sus datos. Finalmente, mejora la eficiencia operativa general al reducir el tiempo de inactividad y los costos asociados con los incidentes de seguridad.

Otro aspecto importante que se debe contemplar al elaborar un plan de desarrollo e implantación de un sistema de gestión de la seguridad informática es la vinculación de directivos y colaboradores de la organización, ya que son estos los que día a día estás haciendo uso de los dispositivos tecnológicos para gestionar el principal activo de la organización: la información. Es fundamental fomentar el desarrollo de una cultura de seguridad en la empresa formando y concientizar a todas la personas que hacen parte de estas (colaboradores Directivos), teniendo siempre presente las políticas, normativas y procedimientos de seguridad establecidas; supervisando que se cumplen las buenas prácticas en seguridad definidas; y realizando acciones de sensibilización en seguridad de manera continua. (¿Cuáles son los motivos por los que implementar un Sistema de Gestión de Seguridad de la Información?, 2020)

Otra estrategia para mitigar riesgos son los DRP. Un DRP es un plan de recuperación ante desastres (del inglés *Disaster Recovery Plan*), en el cual tiene

cobertura sobre la información, el software y el hardware tecnológico de una compañía y su propósito es dar la continuidad del negocio ante causas como desastres naturales, errores humanos o ataques maliciosos informáticos. Las organizaciones no están exentas a una interrupción en su negocio y un plan de recuperación es la solución alternativa inmediata para otorgar el más mínimo servicio. En datos para las empresas se puede estipular que “el 30% de los daños causados a infraestructuras, es causado por desastres, el 70% de las empresas en Latinoamérica no tienen un plan de continuidad de Negocio, y ante cualquier eventualidad, solamente el 18% de la información es la que pueden recuperar sin un Plan de Continuidad de Negocio” según la compañía mexicana TEAM. (Lefort, 2019).

De acuerdo con Cibernos (2023) las empresas pueden implementar diversas estrategias para proteger sus sistemas informáticos, entre ellas está la identificación de los activos de información y hacer un inventario de ellos para conocer cuál debe ser protegida, luego de esto hacer un diagnóstico y evaluar los riesgos a los que está expuesta esta información. Conociendo esto se deben implementar medidas de seguridad para la protección de esos activos. Una de esas medidas puede ser estableciendo copias de seguridad periódicamente con el fin de tener un recurso de recuperación en caso de que suceda una afectación.

Por otro lado existen otras estrategias igualmente efectivas que ayudan a incrementar la seguridad de la información en las empresas, por ejemplo, la capacitación de los empleados, mantener el software actualizado, implementar software antivirus, cifrar la información de alta importancia, limitar el accesos a datos de alta confidencialidad, proteger la red wifi, establecer directivas estrictas de contraseñas, administradores de contraseñas, utilizar un firewall, utilizar VPN y tener en cuenta los

accesos de los terceros ajenos a la organización (Kaspersky, 2023).

2.2. Ciberseguridad

2.2.1. Definición

La ciberseguridad protege los sistemas informáticos asociados a la tecnología de ataques cibernéticos; que por lo general estos ataques tienen el fin de secuestrar información para posteriormente divulgarla y en el caso de las empresas interrumpir la continuidad del negocio.

Cuando hablamos de seguridad de la información, definimos el conjunto de reglas preventivas y reactivas en las compañías que permiten resguardar la información basándose en sus principios básicos de integridad, confidencialidad y disponibilidad. Este concepto no debe confundirse con seguridad informática, ya que este se encarga de solamente seguridad en sistemas informáticos; mientras que la información puede existir en diferentes medios. Tal como lo establece el sistema de gestión de seguridad de la información el riesgo cero no existe, ninguna organización puede garantizar el nivel de protección absoluto. (Komlev, 2022).

Tal como lo menciona AWS en su sitio web *"*un programa de ciberseguridad de éxito implica la formación de los empleados sobre las prácticas recomendadas de seguridad y la utilización automatizada de tecnologías de defensa cibernética para la infraestructura de TI existente.*"* (¿Qué es la ciberseguridad?, 2021)

2.2.2. Importancia

La importancia de la seguridad informática corporativa no solo radica en preservar los pilares principales de la información (Confidencialidad, Disponibilidad, Integridad) o los que hace mención COBIT, se debe contemplar un plan de trabajo enfocado en evitar

todo tipo de ataques, ya sean externos o internos, físicos o electrónicos con un objetivo claro, evitar consecuencias para todas las áreas de la organización. (Institute, 2007)

2.2.3. Tendencias

En 2023 la ciberseguridad sigue siendo un factor fundamental a considerar en la planeación estratégica de las empresas, por lo que estas deben convivir en un ecosistema digital que les exige permanecer operando en todo momento. Las tendencias de ciberseguridad para este año se enfocan en la nube y dispositivos de internet de las cosas. La amenaza que se ha hecho más popular en los últimos meses es el ramsonware, el cual ha evolucionado y se ha convertido en el ciberataque más sofisticado creado por los ciberdelincuentes además porque ha venido en aumento en los últimos meses (Sánchez, 2023).

La pandemia del año 2020 llevó a que, en las empresas, la modalidad el teletrabajo aumentara significativamente. Esta modalidad de trabajo abre las puertas de la productividad, el progreso y el crecimiento empresarial, pero al mismo tiempo implica el establecimiento de muchos riesgos asociados a la seguridad de la información. Por esto, las empresas deben tener en cuenta algunas pautas de seguridad que eviten dolores de cabeza al momento de ejecutar el trabajo remoto. Entre estas pautas está establecer buenas prácticas dentro de los empleados para que no utilicen herramientas no permitidas que pongan en riesgo la información de la empresa, uso de VPN y controlar los accesos que tiene cada empleado a la red de la empresa según el rol que desempeña (Dell, 2021).

En relación con lo anterior, se hace claridad acerca de que la responsabilidad frente a la ciberseguridad en las empresas debe ser compartida. De acuerdo con Parra

(2022), *“en el Espacio de Ciberseguridad Intel 2022, el Vicepresidente de Network Edge de la compañía Intel, Brad Haczynski, indicó que la ciberseguridad es una responsabilidad compartida.”.* Por lo que destaca que, dado que la ciberseguridad es un desafío global, se requiere que proveedores, organizaciones, empleados y demás actores cooperen con el fin de mitigar los riesgos de la seguridad de la información para lograr mejores resultados.

2.3. Ciberataque

2.3.1. Definición

Los componentes de software de los sistemas de información pueden poseer riesgos de seguridad, entre otros factores, por los ciberataques. “Un ciberataque es un conjunto de acciones ofensivas contra sistemas de información. Estos pueden ser bases de datos, redes informáticas, etc. El objetivo es dañar, alterar o destruir organizaciones o personas” (Bello, 2021). Estos pueden ocurrir principalmente por la motivación del atacante para obtener dinero, de manera que puede robar la información y solicitar dinero a cambio de que la misma no sea difundida públicamente.

2.3.2. Tipos de ciberataques

En la actualidad existen diferentes tipos de ciberataques entre los cuales se encuentran: el phishing, virus troyanos, el ransomware, etc. Este último es uno de los más empleados por los ciberdelincuentes, ya que, según (Seguin & Latto, 2022) es un tipo de malware que cifra los archivos o en algunos casos todo el sistema para luego solicitar pago de un rescate a cambio de entregar la herramienta de desencriptación. Este tipo de ataque se aprovecha de las vulnerabilidades del sistema informático para ingresar

al sistema de archivos y encriptar la información de tal manera que quede inutilizable por el usuario.

Por otro lado, el phishing es otra modalidad de ciberataque, es un tipo de fraude que emplea ingeniería social para obtener datos valiosos de sus víctimas. Se realiza principalmente por medio de correos electrónicos, aunque también es posible por medio de mensajes de texto o llamadas telefónicas. El atacante se hace pasar por una entidad o persona reconocida y su objetivo es engañar a la víctima para acceder a su información de credenciales de inicio de sesión o números de tarjetas de crédito (Belsic, 2020).

2.3.3. Tipos de amenazas

Existen diferentes amenazas que pueden causar afectación en las empresas, entre ellos la ignorancia de los usuarios en este tema, pues ellos en muchos casos no están conscientes de los riesgos que conlleva el uso de dispositivos, visitas a sitios web de dudosa reputación o la realización de descargas de software no autorizado o verificado ya que esto ocasiona que los archivos descargados vengan acompañados de malware que al ser instalado en el equipo puede causar daños al mismo y a los demás que se encuentren en la misma red (Thompson, 2014).

Malware y bots son dos tipos de amenazas que también pueden afectar la seguridad de la información. El malware es un trozo de software que contiene código malicioso y está diseñado para irrumpir en un computador de usuario final o un servidor con el objetivo de filtrar información privada, obtener acceso no autorizado a un sistema, privar el acceso a la información a los diferentes usuarios o sistemas propietarios de la misma. Por medio de este, los piratas informáticos toman el poder de los dispositivos y pueden robar la información. (DocuSign, 2022).

2.4. Datos de ciberataques

2.4.1. En Colombia

Durante el 2022 en Colombia varias empresas de diferentes industrias fueron blanco de ciberataques. (Vargas, 2023) hace referencia al informe de Lumu Technologies en el cual se afirma que los ciberataques a las empresas colombianas aumentaron en un 133%. Según su reportaje, entre enero y octubre de 2022, en el país se reportaron 54121 denuncias por ciberataques de acuerdo con las cifras del Centro Cibernético de la Policía Nacional. Adicional a esto, también se ha evidenciado que en los últimos meses las empresas que han sido blancos de los ataques de una manera más constante son las del sector de la salud, como es el caso de Sanitas cuyos sistemas fueron vulnerados en noviembre del 2022.

Hablando de las cifras de ciberseguridad, en Colombia durante el 2022 hubo más de 20.000 millones de intentos de ciberataques lo que representa un aumento del 80% el cual es muy importante si se realiza una comparación con los resultados del año 2021. Este crecimiento se debe principalmente al crecimiento en el uso de dispositivos conectados a Internet y uso de redes sociales a nivel mundial. Importantes y reconocidas empresas en Colombia como Arturo Calle y Olímpica reportaron haber sido víctimas de los ciberdelincuentes (Semana, 2023).

2.4.2. En Latinoamérica

A nivel Latinoamérica, en el 2022 el 48% de las empresas de esta región sufrió algún tipo de incidente relacionado con la seguridad de la información. El malware fue el principal tipo de amenaza reportada por las empresas de América Latina en 2022, en segundo lugar, quedó el phishing. Un 13% de las empresas sufrió por accesos no

autorizados a sus sistemas y el 5% manifestó haber sido víctima de filtración de información confidencial. Esto eleva la preocupación de las empresas debido a que el robo de información puede causarles problemas graves de reputación y fácilmente dejarlos fuera de operación al exponer información confidencial (Harán, 2022).

2.5. Pymes

2.5.1. Definición

Este proyecto está enfocado en investigar el estado de implementación de ciberseguridad en las pymes. El concepto de pymes es acrónimo de pequeñas y medianas empresas, y son aquellas compañías que su cantidad de empleados suele ser inferior a 200 colaboradores e ingresos brutos de hasta 30.000 smmlv representando el 99.5 % del parque empresarial nacional (Murillo y Restrepo, 2016). Dado este contexto, el ministerio de comercio, industria y turismo lo designo como “empresa con características distintivas, tienen dimensiones con ciertos límites ocupacionales y financieros prefijados por los Estados o Regiones. Son agentes con lógicas, culturas, intereses y espíritu emprendedor específico.” (PYME, 2021).

2.5.2. Generalidades

Las pymes deben prepararse para afrontar los desafíos y retos de un mundo cambiante, cada vez más digitalizado y tecnológico, en el que la información se ha convertido en uno de los activos más valiosos y se deben adoptar medidas y control enfocados en garantizar la confidencialidad, disponibilidad e integridad de la información de organizaciones y de quienes hacen parte de estas. Para abordar estos desafíos, las

Pymes deben priorizar la seguridad de la información y establecer políticas y procedimientos formales para su implementación. También deben dedicar recursos suficientes para implementar y mantener controles efectivos que les permitirá ofrecer tranquilidad y generar confianza en la gestión de protección y tratamiento de datos, de clientes proveedores empleados, entre otros. (OEA, 2018).

Muchas pymes suelen caer en la equivocación de creer que por el volumen de su negocio no generan interés para los ciber atacantes y por ello deciden restar importancia a la implementación de seguridad de los datos, lo que es un grave error ya que para los atacantes no importa cuál sea el tamaño de la empresa, cualquiera puede ser atacada (ElevenPaths, 2019).

2.6. marco COBIT

2.6.1. definición

El marco de trabajo COBIT (Control Objectives for Information and Related Technology) establece un conjunto de objetivos y buenas prácticas para garantizar la calidad y seguridad de la información. Este marco de trabajo hace énfasis en que la información debe poseer las siguientes características o propiedades “efectividad, eficiencia, confidencialidad, integridad, disponibilidad, apego a los estándares y confiabilidad”. (Institute, 2007).

Para preservar las características que señala en marco de trabajo COBIT; se debe contemplar planes de trabajado enfocados en prevenir no solo los ataques externos, sino que también se debe contemplar los ataques internos, físico o de cualquier otra índole. Además, en caso de que llegara a suceder cualquier daño a la información, ya sea

alteración o robo, también se debe contar con planes para la recuperación de esa información en su totalidad. (Urbina, 2016)

2.6.2. Propiedades del marco COBIT

Efectividad

Hace referencia a la manera en que se proporciona la información, que esta sea oportuna, correcta, consistente y utilizable.

Eficiencia

Es la generación de la información haciendo uso óptimo de los recursos con los que cuenta la empresa.

Integridad

Hace referencia a que la información que se genera está sea precisa y, así como con su validez de acuerdo con los valores y expectativas del negocio.

Disponibilidad

La información debe estar disponible siempre que sea requerida para atender las necesidades del negocio.

Cumplimiento

Este criterio ace referencia a las obligaciones que deben cumplir las organizaciones a nivel contractual y leyes en el marco de desarrollo del negocio.

Confiabilidad

Hace referencia a la integridad de la información y que esta no haya sido alterada y que de alguna manera los procesos o la actividad de la empresa se vean afectados.

La confidencialidad hace referencia que, no toda la información corporativa debe estar expuesta sin una respectiva clasificación, lo que es de dominio público, confidencial

o no clasificada.

3. Método

3.1. Enfoque de investigación

La investigación que se llevará a cabo tendrá un enfoque cuantitativo.

3.2. Alcance

La metodología que se utilizará para el proyecto de investigación se basa en un enfoque cuantitativo que implica la recolección de datos a través de encuestas estructuradas, y que al final nos permitan realizar el análisis de información obtenida. Estas encuestas serán aplicadas a una muestra representativa de las PYMES ubicadas en el barrio Toberín de la ciudad de Bogotá, Colombia. Para garantizar la representatividad de los resultados, se utilizarán técnicas estadísticas para determinar el tamaño de la muestra.

El objetivo principal de esta investigación es obtener información sobre el nivel de uso de diferentes herramientas de ciberseguridad en las PYMES del barrio Toberín y el nivel del presupuesto destinado al área de TI para invertir en planes de ciberseguridad. Para lograr esto, se buscará obtener información sobre las políticas de seguridad implementadas por estas empresas para proteger sus activos de ciberseguridad, tales como políticas de contraseñas, políticas de acceso a la red y políticas de seguridad de la información, entre otras.

En resumen, el alcance de esta investigación es utilizar una metodología de investigación descriptiva que permita obtener un panorama completo del nivel de uso de herramientas de ciberseguridad en las PYMES del barrio Toberín, identificando si se utilizan de manera adecuada, actualizada y eficiente para proteger los activos de

ciberseguridad. Esto con el fin de identificar áreas críticas y proponer estrategias para mejorar la seguridad informática de estas empresas.

Limitaciones:

El estudio se limitará al barrio Toberín de la ciudad de Bogotá, Colombia, y no incluirá otras zonas geográficas. Además, se enfocará exclusivamente en el nivel de uso de herramientas tecnológicas y políticas de seguridad en pymes, excluyendo otros aspectos de la ciberseguridad como la seguridad física.

Recursos disponibles:

El estudio contará con recursos limitados, incluyendo acceso a las pymes del barrio Toberín para la recolección de datos, personal de investigación capacitado en ciberseguridad, herramientas y software para la recopilación y análisis de datos, y tiempo y presupuesto para llevar a cabo el estudio.

3.3. Hipótesis

"Hay una relación directamente proporcional entre la inversión en ciberseguridad de las pymes y su capacidad para proteger la información ante los ciberataques".

“La relación es inversamente proporcional entre la Ciberseguridad y la capacidad de proteger la información, lo que permite que aumenten las vulnerabilidades informáticas.”

“De forma alternativa, las empresas realizan una inversión en ciberseguridad en donde los efectos serán nulos sobre la capacidad para proteger sus datos ante los ciberataques.”

3.4. Diseño

En esta investigación implementaremos un diseño cuantitativo no experimental transversal causal de acuerdo a las hipótesis planteadas. Con la realización de recolección de los datos y el análisis de los mismos se podrá establecer si existe una relación entre el nivel de inversión que realizan las pymes y su capacidad para protegerse en los aspectos de ciberseguridad.

3.5. Población

La población seleccionada para esta investigación serán las pymes ubicadas en el barrio Toberín de la ciudad de Bogotá pertenecientes a diversas industrias y que ofrecen variedad de productos o servicios.

3.6. Muestra

De acuerdo con la población especificada, la muestra corresponde a 50 pymes las cuales fueron seleccionadas de manera aleatoria tomadas de diferentes segmentos de negocio. Esta muestra fue seleccionada a partir de la idea de identificar el nivel de inversión en ciberseguridad de las empresas sin tener en cuenta cual sea el sector o industria al que pertenezcan.

3.7. nstrumento de recolección de datos

Variable	Definición operacional	¿Cómo lo vas a medir?	Preguntas
1. Inversión en ciberseguridad			
1.1. Gestión presupuestal para el área de tecnología para Ciberseguridad	La eficiencia y efectividad de la gestión presupuestal en relación con la implementación de medidas de ciberseguridad.	Cumplimiento del presupuesto y costo por incidente de seguridad Variación presupuestaria Retorno de la inversión (ROI) Nivel de satisfacción del cliente interno	1. ¿Cuál es el nivel de inversión de recursos financieros para la implementación de medidas de ciberseguridad? 2. ¿Existen mecanismos de seguimiento y control para garantizar la adecuada gestión presupuestal en ciberseguridad? 3. ¿Cuál es el nivel de satisfacción del cliente interno(usuarios) en cuanto a la implementación de herramientas de ciberseguridad en la empresa?
1.2. Activos (Herramientas de software)	Las herramientas y soluciones de software utilizadas para proteger los sistemas y datos de la empresa.	Lista de herramientas utilizadas o categorías predefinidas. por ejemplo: • Cortafuegos. • Sistemas de detección de intrusiones. • Antivirus.	1. ¿Qué herramientas de software se utilizan actualmente para la protección de los sistemas y datos de la empresa? 2. ¿Existe un proceso de evaluación para implementar herramientas de ciberseguridad? 3. ¿Se realiza un monitoreo constante de las herramientas de ciberseguridad para asegurar su correcto funcionamiento?
1.3. Formación y capacitación del recurso Humano	El nivel de conocimientos y habilidades del personal de la empresa en temas de ciberseguridad	Escala de evaluación de 1 a 5, en donde 1 es muy bajo y 5 es excelente. • Participación en programas de capacitación. • Evaluaciones de conocimientos. • Nivel de cumplimiento de políticas y procedimientos	1. ¿Se proporciona capacitación específica en ciberseguridad para el personal de la empresa? 2. ¿Con cuáles de los conceptos dados a continuación están familiarizados los trabajadores de su empresa? 3. De acuerdo al listado a continuación ¿Cuáles de estas buenas prácticas son implementadas por el personal en su empresa?

2. Protección de la información			
2.1. Nivel y frecuencia de ciberataques	El grado de exposición de la empresa a ciberataques y la frecuencia con la que ocurren.	Estadísticas de incidentes de seguridad. • Número de intentos de ciberataque por mes. • Tipo de ataques más comunes	1. ¿En cuantas ocasiones en su empresa han experimentado ciberataques en los últimos 12 meses? 2. ¿La empresa cuenta con un DRP? (Plan de recuperación ante desastres) 3. ¿Cuál sería el nivel de impacto de un ciberataque en la operación de la empresa?
2.2. Vulnerabilidades sobre la información	Las debilidades o fallos en los sistemas y procesos que pueden ser explotados por atacantes para comprometer la seguridad de la información	Lista de vulnerabilidades identificadas o categorías predefinidas. • Gestión de parches. • Pentest • Evaluación de contraseñas	1. Del listado de vulnerabilidades a continuación, ¿Cuáles han sido identificadas en la empresa? 2. ¿Con qué frecuencia se realizan auditorías de seguridad de manera periódica para detectar nuevas vulnerabilidades? 3. ¿Cuenta la empresa con certificación ISO 27001? 4. ¿Con qué frecuencia se realiza cambio de contraseñas en los diferentes sistemas de información de la empresa?
2.3. Gestión de accesos sobre la información	Los controles y procedimientos establecidos para gestionar los permisos de acceso a los sistemas y datos de la empresa.	Monitoreo de eventos de seguridad. Auditorías de accesos	1. De las estrategias de control de acceso a continuación, ¿cuáles son implementados en la empresa? 2. ¿ Los permisos de acceso a la los sistemas de información se asignan de acuerdo a?

3.7.1. Preguntas y opciones de respuesta

¿Cuál es el nivel de inversión de recursos financieros para la implementación de medidas de ciberseguridad?
Responder del 1 al 5, donde 5 es Muy Eficiente y 1 es Deficiente

¿Existen mecanismos de seguimiento y control para garantizar la adecuada gestión presupuestal en ciberseguridad?
Responder si o no

¿Cuál es el nivel de satisfacción del cliente interno(usuarios) en cuanto a la implementación de herramientas de ciberseguridad en la empresa?
Responder del 1 al 5, donde 5 es Muy Satisfecho y 1 es Muy insatisfecho

¿Qué herramientas de software se utilizan actualmente para la protección de los sistemas y datos de la empresa?
Responder seleccionando una o varias opciones:

- Cortafuegos.
- Sistemas de detección de intrusiones.
- Antivirus.
- Otros(cuáles)

¿Existe un proceso de evaluación para implementar herramientas de ciberseguridad?
Responder si o no

¿Se realiza un monitoreo constante de las herramientas de ciberseguridad para asegurar su correcto funcionamiento?
Responder si o no

¿Se proporciona capacitación específica en ciberseguridad para el personal de la empresa?
Responder si o no

¿Con cuáles de los conceptos dados a continuación están familiarizados los trabajadores de su empresa?

- Virus informático
- Ciberataque
- Phishing
- Vulnerabilidad

De acuerdo al listado a continuación ¿Cuáles de estas buenas prácticas son implementadas por el personal en su empresa?

- Control en la navegación en Internet
- Control en las descargas de Internet
- Manejo responsable de dispositivos USB

- Cambio de contraseñas periódicamente

¿En cuantas ocasiones en su empresa han experimentado ciberataques en los últimos 12 meses?
Responder con un número

¿La empresa cuenta con un DRP? (Plan de recuperación ante desastres)
Responder si o no

¿Cuál sería el nivel de impacto de un ciberataque en la operación de la empresa?
Responder del 1 al 5, donde 5 es Muy grave y 1 es Leve

Del listado de vulnerabilidades a continuación, ¿Cuáles han sido identificadas en la empresa?

- Accesos otorgados a terceros
- Brechas de seguridad física
- Contraseñas débiles o compartidas
- Sistemas desactualizados
- Gestión y asignación de permisos
- Puertos abiertos públicos
- Otros, ¿cuáles?

¿Con qué frecuencia se realizan auditorías de seguridad de manera periódica para detectar nuevas vulnerabilidades?

- Una vez al año
- Dos veces al año
- Tres o más veces al año
- Nunca

¿Cuenta la empresa con certificación ISO 27001?
Responder si o no
¿Con qué frecuencia se realiza cambio de contraseñas en los diferentes sistemas de información de la empresa?

- Una vez al año
- Dos veces al año
- Tres o más veces al año

De las estrategias de control de acceso a continuación, ¿cuáles son implementados en la empresa?

- Perfilación de usuario
- Asignación de roles
- Software externo
- Aplicaciones permitidas

¿Los permisos de acceso a la los sistemas de información se asignan de acuerdo a?

- Cargo del usuario
- Área del usuario
- Antigüedad del usuario
- Preferencias de los directivos
- No se realiza

3.8. Análisis de datos

Para llevar a cabo el análisis de datos, emplearemos técnicas de estadística descriptiva, teniendo en consideración el tipo de preguntas formuladas. El análisis descriptivo nos permitirá calcular tanto la media como la desviación estándar de las respuestas, lo cual nos brindará una visión general del nivel de inversión en ciberseguridad, así como de la variabilidad de las respuestas obtenidas.

4. Referencias

¿Por qué es importante analizar los riesgos en ISO 27001? (29 de Octubre de 2020). Obtenido de PMG SSI: https://www.pmg-ssi.com/2020/10/por-que-es-importante-analizar-los-riesgos-en-iso-27001/

¿Qué es la ciberseguridad? (2021). Obtenido de AWS AMAZON: https://aws.amazon.com/es/what-is/cybersecurity/

(22 de Octubre de 2020). Obtenido de ¿Cuáles son los motivos por los que implementar un Sistema de Gestión de Seguridad de la Información?: https://www.pmg-ssi.com/2020/10/cuales-son-los-motivos-por-los-que-implementar-un-sistema-de-gestion-de-seguridad-de-la-informacion/

Aldeco, R. (2020). *Introducción a la Ciberseguridad y sus aplicaciones en México.* México: Academia Mexicana de Computación.

Álvarez, C. (13 de Enero de 2023). *Colombia registró un crecimiento de ataques informáticos en el último año* . Obtenido de Voz de America: https://www.vozdeamerica.com/a/colombia-registro-crecimiento-ataques-informaticos-ultimo-ano-/6916577.html#:~:text=Colombia%20registr%C3%B3%20en%202022%20m%C3%A1s,computadoras%2C%20tablets%20y%20tel%C3%A9fonos%20celulares.

Belcic, I. (22 de Octubre de 2020). *¿Qué es un exploit?* Obtenido de AVG: https://www.avg.com/es/signal/computer-security-exploits

Bello, E. (29 de Noviembre de 2021). *iebschool*. Obtenido de iebschool: https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia

Belsic, I. (5 de Febrero de 2020). *avast*. Obtenido de avast: https://www.avast.com/es-es/c-phishing

Bustinza, S. (23 de Octubre de 2022). *Ciberguerra*. Obtenido de Prezi: https://prezi.com/p/qvgh_rbjbzst/ciberguerra/

Cibernos. (01 de enero de 2023). *Grupo Cibernos*. Obtenido de Grupo Cibernos: https://www.grupocibernos.com/blog/prevenir-ciberataque-empresa

Día de la Seguridad Informática: conoce la importancia de proteger a tu empresa. (30 de Noviembre de 2022). Obtenido de UPAX: https://upax.com.mx/dia-de-la-seguridad-informatica-conoce-la-importancia-de-proteger-a-tu-empresa/

DocuSign. (27 de Junio de 2022). *DocuSign*. Obtenido de DocuSign: https://www.docusign.mx/blog/amenazas-la-ciberseguridad#:~:text=La%20transformaci%C3%B3n%20digital%2C%20los%20modelos,ciberseguridad%20en%20los%20%C3%BAltimos%20a%C3%B1os

El ransomware: qué es, cómo se lo evita, cómo se elimina. (2022). Obtenido de KASPERSKY: https://latam.kaspersky.com/resource-center/threats/ransomware

El ransomware: qué es, cómo se lo evita, cómo se elimina. (2022). Obtenido de KASPERSKY: https://latam.kaspersky.com/resource-center/threats/ransomware

ElevenPaths. (26 de Diciembre de 2019). *Telefonica Tech*. Obtenido de Telefonica Tech: https://empresas.blogthinkbig.com/importancia-ciberseguridad-pymes/

Equipo editorial, E. (5 de Agosto de 2021). *Concepto.de*. Obtenido de Concepto.de: https://concepto.de/sistema-de-informacion/

Hageman, M. (12 de Marzo de 2022). *Ataques de spear-phishing en aumento, con riesgo para las pequeñas empresas*. Obtenido de Security Brief: https://securitybrief.com.au/story/spear-phishing-attacks-on-the-rise-with-risk-to-small-businesses

Harán, M. (4 de Agosto de 2022). *welivesecurity*. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2022/08/04/empresas-america-latina-incidentes-seguridad/

Hiscox. (2021). *Informe de Ciberpreparación de Hiscox.* Madrid: Hiscox.

Institute, I. G. (2007). *Cobit 4.1.* Rolling Meadows.

INTERPOL, S. G. (04 de Agosto de 2020). *CIBERDELINCUENCIA: EFECTOS DE LA COVID-19.* Lyon. Obtenido de interpol.int: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

IT Governance institute. (2007). Rolling Meadows.

Kaspersky. (1 de Junio de 2022). *Kaspersky*. Obtenido de Kaspersky: https://latam.kaspersky.com/resource-center/preemptive-safety/small-business-cyber-security

Komlev, A. (7 de Abril de 2022). *Seguridad de la información para empresas: de lo simple a lo complejo.* Obtenido de Linkedin: https://www.linkedin.com/pulse/seguridad-de-la-informaci%C3%B3n-para-empresas-lo-simple-complejo-komlev?trk=public_profile_article_view

La breve historia de la ciberseguridad. (Diciembre de 2019). Obtenido de SOFISTIC: https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/

La importancia de la Seguridad de la Información. (10 de Julio de 2020). Obtenido de IBERO: https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/

Lefort, A. (2 de Octubre de 2019). *La importancia de un DRP (Disaster Recovery Plan).* Obtenido de teamnet: https://www.teamnet.com.mx/blog/drp-disaster-recovery-plan

Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. (1 de Febrero de 2018). Obtenido de PMG SSI: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

Molano, D. (23 de 02 de 2023). *https://www.larepublica.co*. Obtenido de https://www.larepublica.co/analisis/diego-molano-aponte-3548807/ciberseguridad-empresas-bajo-ataque-3548714

Moro, C. (7 de 04 de 2022). *eleconomista.* Obtenido de eleconomista.: https://www.eleconomista.es/empresas-finanzas/noticias/11703079/04/22/La-ciberseguridad-es-un-pilar-para-la-transformacion-digital-de-las-empresas.html

OEA, O. d. (2018). OPORTUNIDADES Y DESAFÍOS PARA LAS PYMES EN EL CONTEXTO DE UNA MAYOR ADOPCIÓN DE LAS TICs. *White paper series*.

Parra, R. (1 de Septiembre de 2022). *dpl news*. Obtenido de dpl news: https://dplnews.com/la-ciberseguridad-es-una-responsabilidad-compartida-intel/#:~:text=La%20ciberseguridad%20es%20un%20desaf%C3%ADo,y%20de%20software%2C%20para%20salvaguardarla

PYME. (7 de Noviembre de 2021). Obtenido de mincit Kids: https://www.mincit.gov.co/kids/haciendo-tesoros-desarrollo-empresarial/pyme#:~:text=Es%20una%20empresa%20con%20caracter%C3%ADsticas,intereses%20y%20esp%C3%ADritu%20emprendedor%20espec%C3%ADfico.

Sanchez, G. (27 de Marzo de 2023). *Inforges*. Obtenido de Inforges: https://inforges.es/blog/6-tendencias-de-ciberseguridad-en-2023/

Seguin, P., & Latto, N. (29 de Septiembre de 2022). *avast*. Obtenido de avast: https://www.avast.com/es-es/c-what-is-ransomware

Semana. (27 de 2 de 2023). *Semana*. Obtenido de Semana: https://www.semana.com/tecnologia/articulo/atentos-en-2022-hubo-alarmante-cifra-de-intentos-de-ciberataques-en-colombia/202314/

Technologies, D. (30 de Octubre de 2021). *Dell*. Obtenido de Dell: https://www.dell.com/es-es/blog/claves-de-seguridad-en-el-teletrabajo-del-dispositivo-a-las-aplicaciones/

Tenga en cuenta las estafas más comunes en la red para evitar ser víctima de ciberdelincuentes. (21 de Noviembre de 2022). Obtenido de EL TIEMPO: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/whatsapp-con-mensajes-falsos-delincuentes-buscan-robar-datos-719225#:~:text=De%20acuerdo%20con%20la%20empresa,%2C%20compa%C3%B1%C3%ADas%20de%20energ%C3%ADa%20etc.)

Thompson, F. (31 de Julio de 2014). *CIO Mexico*. Obtenido de CIO Mexico: https://cio.com.mx/las-7-amenazas-en-ciberseguridad-que-pueden-afectar-su-vida-2/

Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19. (4 de Agosto de 2020). Obtenido de INTERPOL: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

Urbina, G. B. (2016). *Introduccion a la seguridad Informatica.* Mexico: GRUPO EDITORIAL PATRIA.

Vargas, N. (25 de Enero de 2023). *larepublica*. Obtenido de larepublica: https://www.larepublica.co/empresas/las-empresas-que-han-sido-blanco-de-ciberataques-en-colombia-en-el-ultimo-ano-3529667