UNIVERSIDAD EAN

ESPECIALIZACIÓN EN GERENCIA DE PROYECTOS

SEMINARIO DE INVESTIGACION - ESPECIALIZACION

ESTRATEGIAS DE CIBERSEGURIDAD EN ORGANIZACIONES EN COLOMBIA

ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS, CONCLUSIONES Y

SUSTENTACIÓN FINAL

ELABORADO POR:

ALEXANDER MOSQUERA BERNAL
CHRYSTIAN CAMILO FONTECHA BERNAL
JULIANA ROCIO ROMERO GOMEZ
IAMEL ANTONIO SANTOS SANABRIA
ZULMA CONSTANZA PITA MORENO

DOCENTE:

ANTONIO RODRIGUEZ PEÑA

Bogotá, D.C., 28 de noviembre de 2022

TABLA DE CONTENIDO

Listado de tablas

Listado de Imágenes

Listado de gráficas

Anexos de la investigación

Anexo 1: Encuesta Ciberseguridad en formato PDF

Anexo 2 Herramienta de visualización de estado en formato PDF

1. RESUMEN

Ante las nuevas formas de trabajo como el home office o trabajo remoto, las organizaciones se ven más expuestas a sufrir ataques cibernéticos y ante este escenario las empresas en Colombia requieren aplicar estrategias que mitiguen este riesgo para que se tenga una protección adecuada de los activos así como de la información misma.

A partir del problema expuesto, se tiene como objetivo identificar y caracterizar las estrategias de ciberseguridad que están implementando las organizaciones en Colombia, es decir, conocer las estrategias y en qué medida se aplican, así como saber que otras herramientas no se implementan pero que deberían ser usadas.

Lo anterior pretender ser hallado respondiendo a la pregunta ¿Qué estrategias de ciberseguridad están siendo implementadas en las organizaciones en Colombia?

La metodología de la investigación es de tipo cuantitativa, exploratoria, transaccional y correlacional, apoyada en el uso de una encuesta cuyas respuestas se valoran con una escala Likert y sus respuestas serán validadas con la metodología Alpha Cronbach.

Con relación a los datos encontrados y a la investigación realizada, podemos describir que a partir de las quince (15) preguntas formuladas dentro de la encuesta y enfocadas a varios sectores económicos colombianos, pudimos concluir que en las organizaciones, el planear o asignar un presupuesto destinado

a ciberseguridad y estar abiertas a confrontar estos retos digitales solo se evidencia en un 34.5% de la población encuestada, así mismo, tan solo el 36.2% de las empresas, cuenta con un oficial o profesional encargado de la seguridad informativa, por otro lado, tan solo el 39.7% de las empresas considera que tener una política de respaldo de información es importante y fundamental. Basados en lo anterior, el 53.4% de las organizaciones cuenta con software especializado y respaldan sus activos informáticos en nubes digitales y/o otros dispositivos físicos, lo que nos lleva a identificar que el 62.1% de la muestra es consciente de informar de a sus superiores cuando existe riesgos en la seguridad informática de sus dispositivos, por las posibles consecuencias que puede generar la perdida de información crítica para la organización.

A partir de los datos y análisis realizados se puede concluir que existe una baja aplicabilidad de estrategias de ciberseguridad en las empresas colombianas y aunque las organizaciones se preocupan por el tema no se toman las acciones adecuadas para contrarrestar el riesgo por lo que se recomienda aplicar normas especializadas como la ISO 27001: 2018.

Palabras claves: Seguridad de la información, ciberseguridad, ISO 27001, ciberataques, modelo de Seguridad, confidencialidad

.

2. PROBLEMA DE INVESTIGACIÓN

2.1 Descripción Del Problema

El constante cambio de la forma de trabajo del recurso humano en la organizaciones ha cambiado, como lo es home office o de manera hibrida, en el que la información está en constante exposición, el riesgo es inminente por el cómo o el dónde se realiza la manipulación de la información, debido a que no se tienen las consideraciones de seguridad para la manipulación en los mismos, las organizaciones en Colombia evidencian un gran desconocimiento de políticas de control de la seguridad en la información.

ESET (2020) dice en el reporte de seguridad:

> Las buenas prácticas en los estándares de protección de ciberseguridad, se requiere socializarlos en el Recurso Humano de las organizaciones en Colombia, ya que les permita robustecer sus estructuras de seguridad para el manejo y protección de la información en entornos digitales que se desarrollan.

La seguridad en Latinoamérica el 60% de las empresas observan una gran preocupación, ya que el acceso a la información se realiza de manera fraudulenta a sus datos, el 55% de las empresas les inquieta en gran medida que su información sea hurtada y el 53% observa una gran intimidación a la contaminación con técnicas de códigos maliciosos en los dispositivos para los sistemas de información.

Actualmente las organizaciones tienen una gran volatilidad en el manejo de la información, en la que se genera una gran brecha del uso adecuado y responsable de la misma, es por eso que se hace imperioso establecer los mecanismos y herramientas que fortalezcan el recurso humano con las políticas, estándares y mejores prácticas del mercado, logrando en la organización mitigar las amenazas que se encuentran en el día a día por los ciberdelincuentes, y desarrollar procesos robustos para el sistema de seguridad de la información.

Pregunta de investigación:

¿Qué estrategias de ciberseguridad están siendo implementadas en las organizaciones en Colombia?

Mintic que es la entidad en Colombia que lidera por medio de este ministerio el modelo de seguridad y privacidad de la información, fundamentado en el conjunto estándares la norma *International Standard Organization* (ISO) 27000, entrega una herramienta con el objetivo de mitigar el nivel de riesgo que están expuestas la organizaciones en Colombia, por las continuas amenazas y riesgos de los ciberdelincuentes, en el que el modelo de gestión de riesgos de seguridad digital del Ministerio de defensa de Colombia, desarrollado por el comando de conjunto cibernético del grupo de ciberseguridad y defensa, permite a las organizaciones en Colombia, tener la guía de referencia del modelo de Gestión de Riesgos de Seguridad Digital (MGSD) el conocimiento necesario de los estándares de la seguridad de la información.

La OEA (2021) dice en su manual de riesgos informáticos: “Se debe analizar con la gerencia, los riesgos de ciberseguridad y la preparación que se debe tener en cuenta las amenazas cibernéticas”, una investigación en la seguridad en la información, abordando diversos aspectos en el análisis de riesgos, sistemas de gestión de seguridad y estándares de calidad, permiten en las organizaciones en Colombia, identificar su estado actual para la mitigación ante los posibles riesgos y amenazas, fortaleciendo sus modelos de seguridad con políticas de seguridad informática y estándares de calidad.

3. OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS

3.1 Objetivo General

Identificar y caracterizar las estrategias de ciberseguridad que están implementando las organizaciones en Colombia.

3.2 Objetivo Específicos

- Realizar una revisión de literatura de riesgos y estrategias de ciberseguridad en organizaciones del mundo.
- Realizar una revisión de literatura de los estándares y reglamentaciones de ciberseguridad en el mundo.
- Diseñar una herramienta que permita visualizar información, del estado actual en las organizaciones con respecto a las variables más destacadas en seguridad de la información.
- Analizar los resultados obtenidos, para realizar recomendaciones y mejores prácticas para enfrentar los riesgos de ciberseguridad en organizaciones en Colombia.

4. JUSTIFICACION

El desarrollo de la investigación es de vital conveniencia y de relevancia social para las organizaciones en Colombia, porque entrega un valor teórico en el conocimiento de los estándares de Seguridad de la información , promueve una metodología investigativa constante buscando mitigar cualquier nuevo riesgo que se presente para la seguridad de la información, y contribuyendo en la relevancia social el conocimiento técnico, que les permita fortalecer sus plataformas digitales y aportar al cumplimiento del ODS 16: Paz, justicia e instituciones sólidas, fortaleciendo sus plataformas digitales, mitigando la posibilidad de un ciberataque a cualquier organización (ONU, 2015).

CONPES 3854 (2016) establece la política nacional de seguridad digital con el objetivo de “fortalecer las capacidades de los interesados para identificar, gestionar, tratar y mitigar los riesgos de seguridad en sus actividades dentro del entorno digital, con el fin de contribuir al crecimiento de la economía digital nacional”**.** Con el aumento de la densidad digital, se advierte un mayor flujo de datos personales a través de dispositivos, relojes inteligentes, aplicaciones móviles, entre otras plataformas, en un entorno donde el ciber riesgo se puede materializar en cualquier conexión o acoplamiento de iniciativas digitales disponibles.

Cano (2020) afirma:

Los ataques cibernéticos en Colombia han venido tomando fuerza en los últimos 3 años, estimulados por la situación de la pandemia y las medidas

para controlarla, específicamente por la cuarentena y el confinamiento, que dieron paso al aumento del crecimiento del comercio electrónico, las ventas por internet y redes sociales y las transacciones digitales, teniendo así ventas billonarias en 2022.

5. MARCO TEORICO

La seguridad de la información se desarrolla en la mitigación de los riesgos presentes en los activos de toda organización, actualmente existen estándares mundiales establecidos que son la guía de las buenas prácticas de la industria, siendo la base para la confidencialidad e integridad de la información, las referencias de estándares internacionales en el ámbito de la ciberseguridad se pueden enunciar las del conjunto de la *ISO / IEC – 27000.*

Tabla 1. Norma ISO 27000

ISO / IEC – 27000	
NORMA	**DESCRIPCION**
ISO 27001	Es la norma certificable contiene (39 objetivos, 133 Controles, 11 Dominios), hace referencia en la identificación de riesgos de manera continua en el tiempo
ISO 27002	que hace referencia a buenas prácticas para la gestión de la seguridad, enuncia los objetivos de control y gestión que deberían tener las organizaciones
ISO 27003	que contiene las directrices para la implementación SGSI (Sistema de Gestion de seguridad de información)
ISO 27004	Métricas para la gestión de la seguridad de la información
ISO 27005	la gestión de riesgos
ISO 27006	los requisitos para los que emiten la certificación, todos estos estándares de desarrollan en el ámbito de las Personas, los procesos y la tecnología.

Fuente: Elaboración propia

5.1 Antecedentes.

CONSGOM (2022) Ciberseguridad, primer riesgo para las empresas: Un estudio de Mercer Marsh Beneficios (MMB) revela las preocupaciones de las organizaciones, que se resumen de la siguiente manera:

La ciberseguridad, la privacidad de datos, y la naturaleza cambiante del trabajo encabezan los riesgos que enfrentan las personas con las organizaciones en Colombia. Así lo señala el nuevo reporte de Mercer Marsh Beneficios (MMB), Riesgos de Personas 2022, informe que encuestó a más de 2500 profesionales de riesgos y recursos humanos en 25 países a nivel mundial e incluye datos de más de 490 encuestados de Latinoamérica. Según el análisis, el 99% de las empresas consideran invertir en la gestión de los riesgos que tienen que ver con ciberseguridad y privacidad de datos.

> Con los crecientes casos de ciberataques en Colombia y el mundo, las empresas han visto la importancia de contar con los recursos adecuados para gestionar estos riesgos. El 78% de las empresas encuestadas dijeron que cuentan con las personas adecuadas para gestionar este riesgo. (CONSGOM 2022).

Por otro lado, las culturas que no están alineadas con los valores corporativos, los comportamientos no deseados o un entorno tóxico son el segundo riesgo más importante para los líderes de recursos humanos. En ese sentido, el 51% de las empresas considera invertir en la gestión de la cultura organizacional en los próximos dos años. Otra de las conclusiones es que "Los trabajos de hoy y del futuro requerirán habilidades y conocimientos específicos. Lo

que solía funcionar debe redefinirse para reaccionar a la demanda cambiante del mercado" (CONSGOM 2022).

En esa línea, el 60% de las empresas encuestadas en Colombia planean invertir en estrategias para crear equipos flexibles e innovadores, señala. Igualmente, el informe revela la creciente inquietud en materia de responsabilidad ambiental y social dentro de las organizaciones. Es así como el 59% de C-Suit (el grupo más importante e influyente de individuos en una empresa) y el 70% de los empleados respondieron como fundamental gestionar los riesgos asociados a esta categoría. Además, el 14% de las compañías del país considera que no cuenta con las personas necesarias para enfrentar los desafíos que trae la gestión de la responsabilidad social y ambiental como el cambio climático y la falta de propósito empresarial deseable.

CESGIR (2022) La ciberseguridad, de costo a inversión, indica que el crecimiento y la madurez de la industria Fintech ha sido de beneficio para la economía en nuestro país. La relación que los usuarios de la banca tienen con el manejo de su dinero, así como la forma de hacer negocios, fue sin duda un gran diferenciador para los pequeños comercios durante la pandemia. Sin embargo, su auge ha puesto a los usuarios y la banca en general en la mira de la ciberdelincuencia.

De acuerdo con el reporte de Amenazas móviles en 2021 de Kaspersky, el número de ataques con troyanos bancarios ha mantenido su ritmo en los últimos meses. En 2021 se produjeron 2,36 millones de ataques a nivel mundial, 600 mil menos que en 2020. Así mismo, se detectaron más de 95.000 nuevas versiones,

muchas de ellas con capacidades mejoradas. Por ejemplo, el troyano bancario Fakecalls es capaz de interrumpir las llamadas cuando los usuarios intentan ponerse en contacto con el banco, sustituyendo las grabaciones de audio por respuestas preparadas del operador. De este modo, logra engañarlos haciéndoles creer que están hablando con un empleado del banco o con el habitual contestador automático y terminan compartiendo involuntariamente información sensible con los atacantes. No cabe duda de que las aplicaciones bancarias y de pago por móvil están cada vez más extendidas en todo el mundo; en el caso de Colombia, según datos de Colombia Fintech, el 76% de la población digital usa soluciones financieras, por lo que se espera que para este año el promedio general de crecimiento en este sector sea de 12,5%.

En este sentido, de acuerdo con el informe Fintech Market Forecast de Velmie, el sector de pagos transfronterizos y billeteras digitales tendrán un crecimiento del 17,2% y 15,5%, respectivamente, mientras que para la banca móvil será de 10,4% y los pagos por comercio electrónico 7,7%. Esto no solo representa beneficios para la economía, sino que también genera más posibilidades de que los ciberdelincuentes ataquen a los usuarios de estas soluciones de forma más activa. Es por esto por lo que recomendamos a los usuarios descargar aplicaciones sólo de tiendas oficiales como Apple Store, Google Play o Amazon Appstore.

También es importante comprobar los permisos que otorgamos, así como utilizar una solución de seguridad confiable que bloqueé las apps maliciosas, troyanos y adware. A los representantes de los servicios financieros, les

sugerimos limitar el número de intentos para realizar una transacción y educar a los clientes sobre los posibles trucos que pueden utilizar los defraudadores, así como realizar auditorías de seguridad y pruebas de penetración anualmente con el fin de detectar problemas de seguridad en la red de la empresa. Los ciberdelincuentes emplean nuevas técnicas para burlar las tecnologías antifraude, lo que implica que hay que tener un cambio de mentalidad y dejar de ver a la ciberseguridad como un gasto, para verla como una oportunidad de construir capacidades de resiliencia.

De acuerdo con STIAMA (2022) la Dian exige que se cumpla con la ISO27001, lo cual permite garantizar la seguridad de la información.

Teniendo en cuenta que para acceder a la plataforma Radian de la Dirección de Impuestos y Aduanas Nacionales (Dian) se pueden utilizar alternativas directas, como la de desarrollar un ‘software’ propio, o indirectas, a través de un proveedor tecnológico, con sistemas de negociación como lo ofrecen algunas compañías o con el ‘software’ gratuito de la Dian, esta entidad hace recomendaciones de gran utilidad para las organizaciones. En esa línea, si el usuario del Radian va a ingresar de forma indirecta, ya sea con un proveedor tecnológico, un sistema de negociación y/o factor, el organismo indica que solo se debe buscar la empresa y seleccionarla. Por el contrario, si va a gestionar de forma directa la circulación de las facturas electrónicas, este debe contar con un ‘software’ propio activo para realizar todo el proceso de registro y habilitación en ese sistema. El ‘software’, reiteran, puede ser desarrollado directamente y/o adquirido. Y para saber si el ‘software’ seleccionado es confiable y avalado para el

proceso, los portavoces de la Dian explican que todos los participantes que se registran de forma directa en el Radian, ya sea como facturadores electrónicos, proveedores tecnológicos, sistemas de negociación y/o factores, deben cumplir con una serie de requisitos que se encuentran establecidos en el Decreto 1154 de 2020 y, posteriormente, ser avalados por esa entidad, lo que garantiza que los usuarios que deseen registrarse de forma indirecta puedan elegir una empresa confiable para registrar, consultar y ver la trazabilidad de sus facturas electrónicas. Al respecto, Alexandra Durán, Socia de Asesoría Tributaria en EY, anota que, para participar en el ecosistema de facturación electrónica, la Dian exige que se cumpla con la ISO27001, lo cual permite garantizar la seguridad de la información.

Por otra parte, sostiene que el éxito del proceso se conocerá una vez se puedan generar y transmitir los documentos electrónicos ante la Dian y participar de forma satisfactoria en el Radian, mediante el registro de la factura electrónica y los demás eventos asociados a la misma. A su vez, la Dian recomienda que los usuarios que deseen ingresar tengan definido cómo van a registrarse.

Chambers (2022) en su informe: Exploring the Standards Cybersecurity Practitioners Need to Comply with Multinational Cybersecurity Requirements, señala que:

La ciberseguridad ha aparecido en muchos artículos en los últimos años, especialmente en lo que respecta al cumplimiento. En la sociedad actual, la ciberseguridad se ha convertido en una faceta de la vida cotidiana con tecnologías avanzadas, como la inteligencia artificial y muchas otras tecnologías, que siguen integrándose en la vida de las personas. Ha sido difícil ofrecer una iniciativa de

cumplimiento para estas tecnologías más nuevas, ya que la tecnología suele preceder a los aspectos de cumplimiento y seguridad. Algunas personas y organizaciones consideran que el cumplimiento es «marcar la casilla», y se ha discutido que algunas iniciativas de cumplimiento contrarrestan la esencia de la seguridad. Hoy en día hay cientos de programas de cumplimiento de ciberseguridad en el mundo; sin embargo, hay dos que se destacan en los Estados Unidos y el Reino Unido. El cumplimiento y la seguridad comienzan a combinarse con las actualizaciones recientes de las publicaciones especiales de la serie 800 del Instituto Nacional de Estándares y Tecnología y las actualizaciones recientes de la Organización Internacional de Estandarización de los documentos de la serie 27000. El cumplimiento es ahora más importante que nunca gracias a la combinación de cumplimiento y seguridad. El propósito de este estudio de método mixto tuvo como objetivo explorar los requisitos de cumplimiento que los profesionales de la ciberseguridad deben implementar para cumplir con los requisitos de ciberseguridad multinacionales. Este estudio confirmó que todas las organizaciones deberían tener una base de referencia de ciberseguridad global que sea rentable de implementar a nivel mundial con un plan eficiente y en constante evolución para proteger la cadena de suministro global. Este estudio también reveló la necesidad de una estandarización tecnológica global

5.2 Bases teóricas

Existen diferentes conceptos de delito informático, por lo que a continuación se relacionan las definiciones más relevantes asociadas con los delitos cibernéticos.

Ramírez y Castro (2018) afirma lo siguiente: “el delito cibernético es cualquier acto ilegal que se produce a través de medios informáticos o intentos de manipular o destruir computadoras, redes de Internet o medios electrónicos".

También Besares (2015) afirma de manera similar que: “el delito informático Es un acto ilegal y criminal típico que afecta la seguridad informática y la privacidad humana a través del procesamiento fraudulento de datos, que es diferente de otros casos de delitos informáticos o electrónicos”.

Por otro lado, Téllez (2012) dice: "actitudes ilegales que usan la cibernética como herramienta o propósito, o actos típicos, ilegales y criminales que usan la cibernética como instrumento o propósito".

De igual manera que Villavicencio (2014) dice:

> Se entiende por ciberdelincuencia una conducta encaminada a evadir los sistemas de equipos de seguridad, es decir, inmiscuirse en un sistema informático, de correo electrónico o de datos a través de un código de acceso; comportamiento típico que solo se puede lograr a través de la tecnología.

Los delitos cibernéticos se encuentran en un contexto, de acuerdo con las siguientes definiciones:

Ojeda (2010) opina:

A los sistemas informáticos le han ocurrido algo similar a lo observado en la historia. La sociedad se ha interesado y condicionado a los avances tecnológicos e informáticos, debido a su eficaz desarrollo y a la enorme influencia que ha alcanzado en muchas de las actividades diarias de las personas y las organizaciones.

De manera similar, Álvarez y Pérez (2004) describen:

Los denominados “delincuentes cibernéticos” viajan por el mundo virtual realizando incursiones fraudulentas cada vez más frecuentes y variadas, como el acceso sin autorización a sistemas de información, piratería informática, fraude 27 financiero, sabotaje informático, entre otros. Así mismo, sustentan que, para enfrentarlos, varios países han desarrollado y dispuesto un sistema judicial especializado que permite procesarlos y castigarlos. A ese grupo de países se unió Colombia en el año 2009.

Respecto a las Tendencias se destacan las siguientes:

CCIT (2020) referencia que:

En Colombia los delitos cibernéticos han experimentado un crecimiento durante los últimos años casi de forma paralela al uso de las nuevas tecnologías y las pérdidas generadas por los ciberataques, sitúan a dicha problemática como una de las principales economías ilegales en el País.

También Acuña y Villa (2018) afirman que:

El impacto que sufren las empresas colombianas luego de un ciberataque trasciende el coste económico por pérdidas de sus activos financieros y

conlleva de manera colateral afectaciones sobre productividad e incluso conlleva a implicaciones de carácter legal por fuga de información privilegiada y data sensible.

Finalizando, CCIT (2020) evidencia en los registros de denuncia:

que a través de los canales de atención a empresas y ciudadanos dispuestos por la Policía Nacional fueron registrados 28.827 casos durante el 2019, del total de los casos registrados, 15.948 fueron denunciados como infracciones a la ley 1273 de 2009 por parte de las víctimas, esta cifra corresponde al 57% del total de casos informados. Respecto al 2018 las denuncias disminuyeron en un 5.8 % tras una variación negativa de 983 casos.

En cuanto a los conceptos de Ciberseguridad y su relación con el delito informático, se tiene lo siguiente:

ITU (2011), establece que:

Ciberseguridad, como realidad complementaria de la ciberdefensa, materializa el concepto de defensa nacional digital, en un conjunto de variables claves, acertadamente definidas por la ITU -International Telecommunication Union-, en las cuales son necesarias el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad de una nación, en el contexto de una realidad digital y de información instantánea.

De igual manera, Kostopoulos (2012) describe que la ciberseguridad debe salvaguardar los siguientes principios:

Confidencialidad: Todos los datos transmitidos o almacenados son privados, solo pueden ser vistos por las personas autorizadas. Integridad: Todos los datos transmitidos o almacenados deben estar libre de error. Disponibilidad: Todos los datos transmitidos o almacenados de disponibles para los autorizados. ben estar No Repudio: Todos los datos transmitidos o almacenados son de indiscutible autenticidad, especialmente cuando están soportados por certificados digitales, firmas digitales u otros identificadores explícitos.

Por otro lado, Jimeno Muñoz (2017) afirma que:

El riesgo cibernético puede definirse como aquel asociado al uso de tecnologías de información, en términos que cualquier sistema tecnológico que se encuentre conectado a otro puede verse afectado por estos riesgos emergentes, pudiendo afectar tanto intereses públicos como privados.

De otro lado, se encuentran diferentes maneras de evaluar el riesgo, resaltando:

La ISO (1996) define riesgo tecnológico como:

La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole perdidas o daños, identificando los elementos que se deben comprender integralmente, estos elementos son: probabilidad, amenazas, vulnerabilidades, activos e impactos.

También Rodríguez (2014) afirma de manera similar que:

Verificar las vulnerabilidades de los activos más críticos de las empresas, clasificando el riesgo de la vulnerabilidad de estos activos, y recomendando las medidas de control adecuadas de acuerdo con la norma estándar ISO 27001, la empresa pueda minimizar sus riesgos y desarrollar planes de contingencia para los riesgos que enfrenta.

De igual manera Excellence (2022) dice que: “La gestión de cualquier incidente o actividad ilegal o maliciosa que comprometa la disponibilidad, confiabilidad, integridad y confidencialidad de los datos, genera planes de mitigación enfocados a los riesgos en cada activo de la organización”.

5.3 Conceptos Claves

Los conceptos claves de ciberseguridad en los que se desarrolla la investigación se enuncian a continuación:

Tabla 2. Conceptos del desarrollo de investigación

Concepto	Definición
Ciberdelincuencia.	Acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático. (Ministerio de Defensa de Colombia).
Delito cibernético	Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia).
Ciberespacio.	Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
CSIRT.	Computer Security Incident Response Team (Equipo de respuesta a incidentes de seguridad cibernética). (http:// www.first.org).

Concepto	Definición
Entorno digital.	Ambiente, tanto físico como virtual, sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).
Evaluación del riesgo.	Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables. (NTC ISO 31000:2011).
Evento de seguridad de la información	Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles. (ISO/IEC 27035:2016).
Gestión de riesgos de seguridad digital.	Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. (CONPES 3854, pág. 24).
Incidente digital.	Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).
Incidente de seguridad de la información.	Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones. (ISO/IEC 27035:2016).
Infraestructura crítica cibernética nacional.	Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (CONPES 3854, pág. 29).

Concepto	Definición
ISO.	Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización, cuyo objetivo es establecer, promocionar y gestionar estándares. (http://www.iso.org).
Seguridad de la información.	Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. (ISO/IEC 27001:2016).
Seguridad digital.	Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854, pág. 29).
Vulnerabilidad.	Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).
Ataques bancarios.	Estos buscan no solo lucrarse sino además obtener datos personales, por lo que generalmente se usan ataques de malware y afectan la infraestructura tecnológica de las entidades bancarias.
Estafas electrónicas.	Son supuestos servicios que se anuncian a través de sitios web, en redes sociales, o por correo electrónico pero que no se prestan finalmente cuando ya han obtenido dinero.
Forjacking.	Son eventos donde se utiliza código dañino para introducirlo en páginas web con el fin de obtener información de manera ilegal y en donde, por lo general, se afecta la cadena de abastecimiento de las entidades y en consecuencia a los proveedores.
Malware.	Es una modalidad donde se usan programas maliciosos, con el fin de robar datos y obtener dinero o lucrarse se alguna manera, agregado a esto también suelen dañarse los dispositivos que sufrieron dicho ataque.
Phishing.	Método utilizado a través de correos electrónicos o sitios web falsos, que engañan a las víctimas pudiendo así conseguir información confidencial como lo son las contraseñas.
Ransomware.	Los intrusos o ciberdelincuentes consiguen la información para luego solicitar un rescate.
Smishing.	Este tipo de delito se configura cuando el delincuente informático, por medio de aplicaciones de mensajería instantánea le solicita a la víctima hacer una llamada o

Concepto	Definición
	ingresar a una página web y así lograr conseguir información confidencial.
Troyano.	Software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero al momento de ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

Fuente: Elaboración propia

6. MARCO INSTITUCIONAL

6.1 Marco Legal

Las políticas relacionadas con Ciberseguridad y la Seguridad Informática en Colombia, están bajo el liderazgo del Ministerio de las TIC, que a su vez se apoya en la academia para estudiar y analizar las verticales de Cibercrimen y Ciberguerra.

MINTIC (2011) estableció y estructuro:

Las políticas y estrategias relacionadas con la seguridad de la información, la cultura cibernética, la gestión de las amenazas para la infraestructura crítica del país, lo que finalmente se traduce en la gestión del riesgo en el CONPES 3701 del 14 de julio de 2011, en donde se dejaron establecidos los lineamientos para Colombia en relación con la ciberdefensa y ciberseguridad.

De igual manera DNP (2011) establece en su contexto:

Colombia es pionero en temas de defensa cibernética en la región, pues se planearon acciones concretas que incluyen normativas sectoriales y nacionales, incluyendo medidas para controlar el derecho al buen nombre y a la intimidad, así como controles al comercio electrónico, a la regulación del espectro y en general a ciberdelitos**.**

Tabla 3. Normatividad en Colombia de ciberseguridad

NORMA	Descripción
Ley 527	Acceso y uso de mensajes de datos, comercio electrónico y firmas digitales, y se determinan entes certificadores (Congreso de la República de Colombia, 1999).
Ley 594	Seguridad de archivos (Congreso de la República de Colombia, 2000a).
Ley 599	Violación ilícita de comunicaciones, derechos de autor y algunos delitos informáticos en el Código Penal (Congreso de la República de Colombia, 2000b).
Ley 679	Prevención y ataque contra la explotación, la pornografía y el turismo sexual con menores (Congreso de la República de Colombia, 2001).
Ley 962	Reducción de trámites y procedimientos administrativos de entidades públicas o privadas con funciones públicas o de servicios públicos (Congreso de la República de Colombia, 2005).
Ley 1266	Habeas data y manejo de información de bases de datos personales (Congreso de la República de Colombia, 2008).
Ley 1273	Modificación del Código Penal para acoger la protección de la información y la preservación integral de los sistemas que usan TIC (Congreso de la República de Colombia, 2009a).
Ley 1341	Principios y conceptos sobre la sociedad de la información y la organización de las TIC y creación de la Agencia Nacional del Espectro (Congreso de la República de Colombia, 2009b).
Ley 1437	Pruebas electrónicas para tipificar los delitos en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo (Congreso de la República de Colombia, 2011a).
Ley 1480	Protección al consumidor por medios electrónicos y seguridad en transacciones electrónicas en el Estatuto del Consumidor (Congreso de la República de Colombia, 2011b).
Decreto-Ley 019	Reducción de trámites en el estado a través de medios electrónicos y establecimiento de criterios de seguridad (Presidencia de la República de Colombia, 2012a).
Decreto 2693	Estrategia de gobierno electrónico (Presidencia de la República de Colombia, 2012b).
Decreto 2364	Posibilidad de la firma electrónica (Presidencia de la República de Colombia, 2012c).
Decreto 2609	Posibilidad del expediente electrónico en el esquema de gestión documental estatal (Presidencia de la República de Colombia, 2012d).
Ley 1581	Regula la protección de datos personales de los individuos (Congreso, 2012).
Ley Estatutaria 1621	Normatividad para las labores de Inteligencia y contrainteligencia y criterios de seguridad para este rol (Congreso de la República de Colombia, 2013).
Decreto 1377	Reglamenta la protección de datos personales de los individuos (Presidencia de la República de Colombia, 2013a).
Decreto 1510	Contratación y compra pública por medios electrónicos (Presidencia de la República de Colombia, 2013b).
Ley 1712	Criterio de transparencia en el acceso a la información pública (Congreso de la República de Colombia, 2014).

NORMA	Descripción
Decreto 333	Determina las entidades de certificación digital (Presidencia de la República de Colombia, 2014).
Ley 1978	Modernización del sector de las tecnologías de la información y las comunicaciones (Congreso de la República de Colombia, 2019).
Decreto 620	Lineamientos generales en el uso y operación de los servicios ciudadanos digitales (Presidencia de la República de Colombia, 2020).
Conpes 3975	Política Nacional para la transformación digital e inteligencia artificial (DNP, 2019).

Fuente: Elaboración propia

7. METODOLOGÍA

Con la investigación se busca la validación de las estrategias que manejan las pymes en Colombia, y como realizan la mitigación de riesgos para cuando se compromete la información por medio de ataques cibernéticos.

7.1 PRIMER NIVEL

7.1.1 Diseño De Investigación

La presente investigación es de tipo cuantitativa, exploratoria, transaccional y correlacional.

- Cuantitativa. El estudio se desarrolla en mediciones numéricas.
- No Exploratoria. No se manipularán las variables, sólo se validará su comportamiento.
- Transaccional. La recolección de datos se realizará en el mismo tiempo y no se evaluará su evolución.
- Correlacional. Se generalizan los resultados y obtendrán las relaciones entre las diferentes variables del estudio.

7.1.2 Hipótesis

Basado en la pregunta de investigación **¿Qué estrategias de ciberseguridad están siendo implementadas en las organizaciones en Colombia?**, se plantea la siguiente hipótesis:

Si se aplican estrategias de ciberseguridad de las Pymes en Colombia, se mejorará en la mitigación de riesgos para ataques cibernéticos.

7.1.3 Población y Muestra

La población de muestra son las empresas clasificadas como pymes (20 a 250 trabajadores), se seleccionó una muestra representativa de los sectores y la industria clasificadas a nivel nacional, por las características de activos tecnológicos, conformación y estructura organizacional.

En la definición del tamaño de la muestra se tomó como referencia la información del directorio de empresas, que utilizan en gran medida los servicios virtuales, de los cuales se pudo establecer a la fecha de su consulta (8 de octubre de 2022), que en Colombia se tenían registradas un total de 926.879 empresas divididas en 21 sectores económicos.

Tabla 4. Clasificación Pymes

CIIU	Sector	Empresas (Unidades)
G	Comercio al por mayor y al por menor reparación de vehículos automotores y motocicletas	180705
M	Actividades profesionales científicas y técnicas	125853
F	Construcción	97911
S	Otras actividades de servicios	95658
C	Industrias manufactureras	90.405
L	Actividades inmobiliarias	50.003
N	Actividades de servicios administrativos y de apoyo	48.868
J	Información y comunicaciones	43.581
H	Transporte y almacenamiento	33.557
A	Agricultura ganadería caza silvicultura y pesca	33.167

CIIU	Sector	Empresas (Unidades)
Q	Actividades de atención de la salud humana y de asistencia social	28.28
I	Alojamiento y servicios de comida	23.866
K	Actividades financieras y de seguros	22.401
P	Educación	16.767
R	Actividades artísticas de entretenimiento y recreación	13.383
E	Distribución de agua evacuación y tratamiento de aguas residuales gestión de desechos y actividades de saneamiento ambiental	9.858
B	Explotación de minas y canteras	7.66
D	Suministro de electricidad gas vapor y aire acondicionado	2.605
O	Administración pública y defensa planes de seguridad social de afiliación obligatoria	2.045
T	Actividades de los hogares individuales en calidad de empleadores actividades no diferenciadas de los hogares individuales como productores de bienes y servicios para uso propio	197
U	Actividades de organizaciones y entidades extraterritoriales	109
	TOTAL	926.879

Fuente: Informa Colombia (2022).

7.2 SEGUNDO NIVEL

7.2.1 Técnicas

Las variables que se contemplan en la tabla No. 5, desarrollan una serie de preguntas seleccionadas con el fin de enfocar las encuestas, obtener resultados y determinar si las pequeñas y medianas empresas conocen y tienen implementado

el concepto de ciberseguridad como estrategia dentro su funcionamiento y operación. (Ver Anexo 1: Encuesta Ciberseguridad).

Tabla 5. Determinación de las preguntas para el instrumento

Variable	Preguntas asociadas para cada variable
Determinar si se aplican las políticas existentes de ciberseguridad en la legislación colombiana.	1. ¿Su empresa aplica las leyes y/o políticas colombianas que rigen y condenan los riesgos informáticos?
Nivel de importancia de la Ciberseguridad en Colombia: Evidenciar la importancia y la prioridad de implementar estas estrategias dentro de la empresa.	2. ¿En su organización tiene identificado todos los activos informáticos?
	3. ¿Su empresa tiene un plan de formación del personal en temas de seguridad digital?
Herramientas Tecnológicas: Establecer si las pymes disponen de herramientas que les ayude a proteger sus activos tecnológicos.	4. ¿Su empresa tiene dispositivos de control de software, para la seguridad de la información en los computadores de la empresa?
	5. ¿Su empresa tiene oficial de seguridad de la información?
	6. ¿Existe una política de seguridad de la información?
Identificación de Activos y análisis de riesgo:	7. ¿Existe una política de cambio de password de ingreso a los sistemas de información?
Consultar si se gestiona al riesgo tecnológico es un punto esencial en la empresa para lograr sus objetivos empresariales.	8. ¿Si recibe un correo de un mail desconocido, para que ingrese a un sitio web, ingresa?
	9. ¿Existe en la empresa una política de ingreso a redes sociales y consulta de mail externos?
Cultura organizacional, capacitación y entrenamiento:	10. ¿Si se encuentra fuera de la organización y requiere consultar una información corporativa, se conecta a una red wifi de libre uso?

Variable	Preguntas asociadas para cada variable
Establecer si la seguridad informática forma parte de la cultura organizacional de la empresa.	11. ¿La organización cuenta con una política de pruebas de vulnerabilidades en sus sistemas de información?
Estructura organizacional	12. ¿En presupuesto organizacional, hay un rubro para la adquisición de tecnología, en la protección de la información?
	13. ¿se realizan auditorías internas, para el cumplimiento de la política de la seguridad en la información?
Planes de Contingencia: Comprobar si las pymes están dispuestas a responder frente a una amenaza que cause vulnerabilidades tecnológicas en la empresa	¿Si usted identifica un riesgo de seguridad en su computador, informaría a su superior de la empresa de este acontecimiento?
	15. ¿Su organización cuenta con una política de respaldo de la información?

Fuente: elaboración propia

7.2.2 Instrumento de Medición

Para la presente investigación se han considerado los siguientes instrumentos de medición según lo expuesto por Hernández, Fernández y Baptista (2010):

- Encuesta digital aplicadas en las organizaciones de los sectores indicados (Ver Anexo 1: Encuesta Ciberseguridad).
- Escala de Likert.

7.2.3 Escala de calificación de las preguntas asociadas a las variables

Para la calificación de las preguntas se determinó una escala cuantitativa, donde el encuestado tiene cinco (5) opciones basadas en la escala de Likert, que utiliza una escala para cuestionar al encuestada sobre su nivel de acuerdo o

desacuerdo frente a una pregunta formulada. Para las variables se asignaron los siguientes valores:

Tabla 6. Escala de valores para calificar las variables.

Nunca	**1**
Casi nunca	2
Ocasionalmente	3
Frecuentemente	4
Siempre	5

Fuente: Bisquerra & Pérez, (2015)

7.2.4 Determinación del tamaño de la muestra

Para nuestra investigación, se determinó el tamaño de la muestra tomando una población aproximada de 926.879 empresas clasificadas por sectores económicos, utilizando la fórmula de muestro aleatorio simple de acuerdo con la siguiente formula:

Donde se establece:

Tabla 7. Fórmula de muestreo aleatorio simple

N	Es el tamaño de la población	*N = 926.879*
Z	Nivel de confianza del 95%;	Z = 1.95
p	Es la proporción esperada	*p* = 0.5
q =1-p	Es el complemento de la proporción esperada	q = 0.5
d	Margen de error	*d = 10%*

Fuente: Cortés et al. (2020)

Imagen 1. Fórmula de muestreo aleatorio simple

$$n = \frac{N * Z_{\alpha}^{2} p * q}{d^{2} * (N-1) + Z_{\alpha}^{2} * p * q}$$

Fuente: Cortés et al. (2020)

Aplicando la fórmula anterior y haciendo los correspondientes cálculos aritméticos, se obtiene el siguiente resultado:

n = tamaño de la muestra = Mínimo 35 unidades

De lo anterior, se aplicará el tamaño de la muestra a profesionales y tecnólogos a las empresas seleccionadas a nivel nacional, que actualmente cuentan con una amplia experiencia en el tema y se desempeñan en los sectores económicos escogidos por el grupo de trabajo.

7.2.5 Metodología Alpha Cronbach

Rodríguez-Rodríguez & Reguant-Álvarez (2020) afirman que: “la calificación de las variables se determina una escala cuantitativa donde se asignan los siguientes valores utilizando la metodología Alfa Cronbach”, Es el método de cálculo del coeficiente de confiabilidad, donde se toma valores entre 0 y 1. Cuanto más se aproxime al número 1, mayor será la fiabilidad del instrumento utilizado.

A continuación, se mostrará el desarrollo de la fórmula:

Imagen 2. Fórmula de cálculo metodología alfa Cronbach y su escala de medición

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum Vi}{Vt}\right]$$

Dónde:

$\alpha = Alfa\ de\ Crombach$

$K = Número\ de\ Items$

$V_i = Varianza\ de\ cada\ Item$

$V_t = Varianza\ del\ total$

ESCALA DE ALFA CRONBACH (α)

0-0,2	MUY BAJA
0,21-0,4	BAJA
0,41-0,6	MODERADO
0,61-0,8	BUENA
0,81-1	ALTA

Fuente: Rodríguez-Rodríguez & Reguant-Álvarez (2020)

Para la utilización de la metodología alfa Cronbach, se utilizará un tamaño de la muestra de mínimo de 35 encuestas para determinar un coeficiente de confiabilidad apropiado para conseguir los objetivos de la investigación, donde a cada individuo se le asignaran quince (15) preguntas, como se muestra en la tabla No. 8.

7.2.6 Construcción del instrumento de recolección de datos

La metodología utilizada se hará mediante encuestas digitales utilizando los formularios de Google, con las preguntas seleccionadas y formuladas por el grupo de trabajo, con un enfoque cuantitativo y exploratorio, como se muestra a continuación:

Para complementar la información anterior se adjunta el link de la encuesta en el formulario de Google:

https://docs.google.com/forms/d/1n56lXkqOPtzeCXjUYWdhdbHubgs9YkFl4wlLzwEFWkI/prefill

8. REPORTE DE RESULTADOS Y DISCUSION

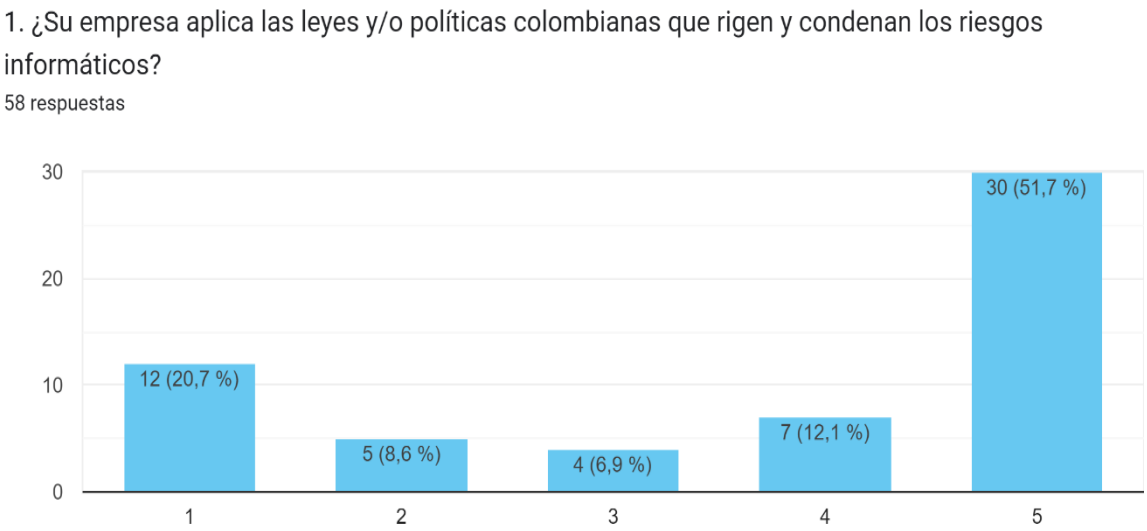
8.1 Análisis de Datos Cuantitativos

A continuación, se presentará el análisis de los resultados de las encuestas empleadas como instrumento de recolección de datos, con el fin de cumplir el objetivo principal de la investigación. Las encuestas fueron aplicadas a cincuenta y ocho (58) personas con diferentes cargos en empresas colombianas y diferentes sectores económicos propuestos dentro de la investigación, llegando con esta metodología a más personas en menos tiempo. Con los datos resultantes de los formularios de Google, se obtuvieron una base de datos de 870 registros que se pudieron medir y verificar utilizando la herramienta de Excel. Con la información obtenida, se procedió a organizar y filtrar los datos para interpretar y descubrir los patrones y tendencias en las preguntas formuladas a los encuestados. De esta recolección de datos cuantitativos, se aplicará el siguiente análisis:

1. Gráficas con porcentajes alcanzados por preguntas.
2. Tabla de frecuencias en la escala Likert por cada una de las preguntas.
3. Análisis de los sectores económicos encuestados.
4. Análisis de correlación de las variables utilizados.
5. Análisis de datos general del instrumento.

8.1.1 Grafica con porcentajes alcanzados por preguntas

Para el cálculo de los porcentajes, se presenta el siguiente análisis representados en graficas de barras, para este proceso se partió de las 15 preguntas formuladas en las encuestas, de acuerdo con la siguiente escala de



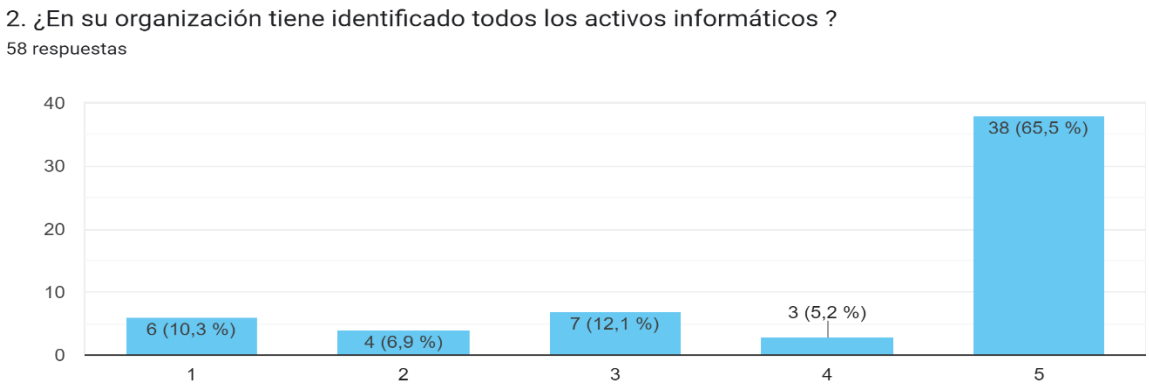
Likert: 1. Nunca, 2. Casi nunca, 3. Ocasionalmente, 4. Frecuentemente, y 5. Siempre, obteniendo los siguientes resultados.

Gráfica 1. Resultados pregunta 1

Fuente: elaboración propia

Para esta pregunta se obtuvo un 51,7%, donde las empresas aplicarían las leyes y/o políticas colombianas que rigen y condenan los riesgos informáticos en caso de un ataque de ciberseguridad, para una muestra de 58 encuestados.

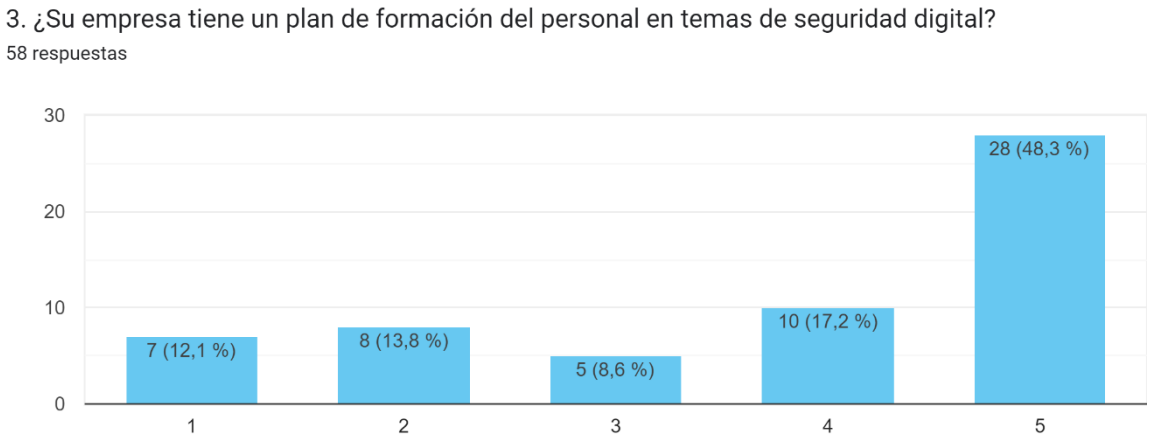
Gráfica 2. Resultados pregunta 2



Fuente: elaboración propia

Según la muestra poblacional, en un 65.5% las empresas tienen identificados sus activos informativos, pues forman parte en su mayoría del funcionamiento propia de las empresas.

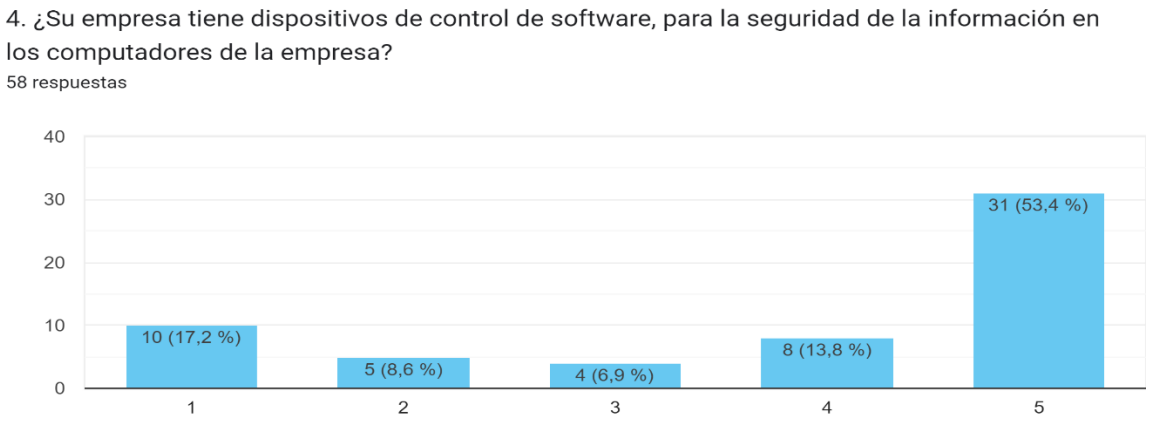
Gráfica 3. Resultados pregunta 3



Fuente: elaboración propia

En este caso, la mayoría el personal encuestado pertenece a empresas tecnologías y nos arroga un resultado de 48.3% de la muestra.

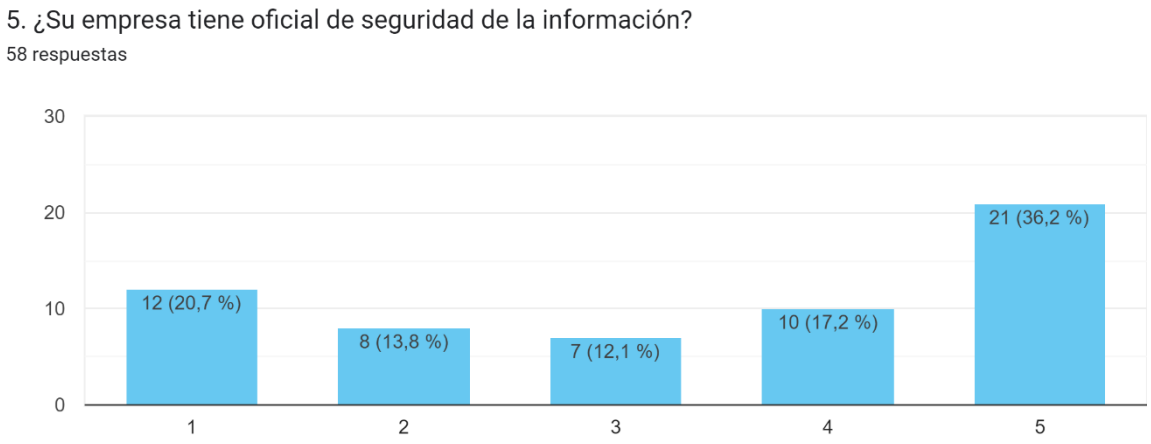
Gráfica 4. Resultados pregunta 4



Fuente: elaboración propia

Esta pregunta de mucha importancia para el tema de nuestra investigación encontró en la muestra, que alrededor del 53.4% cuenta con dispositivos de control de software para protección de la información sensible en la operación de la empresa.

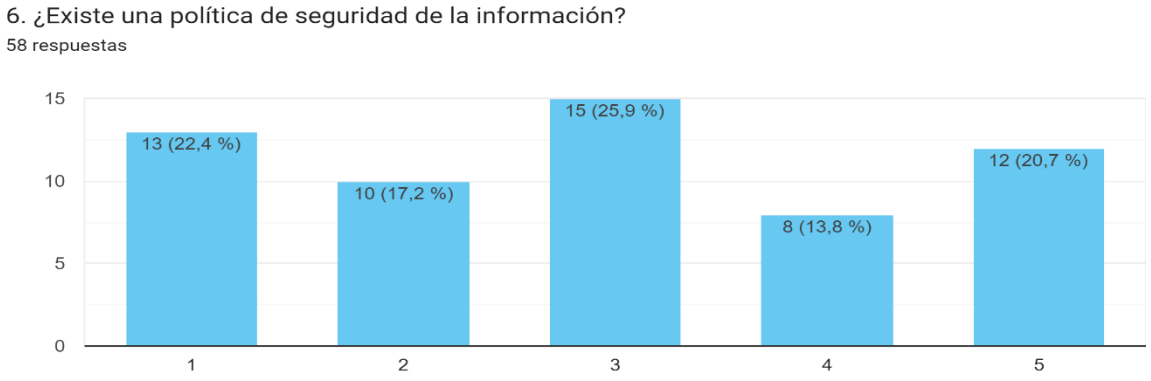
Gráfica 5. Resultados pregunta 5



Fuente: elaboración propia

Tan solo el 36.2% del personal de las empresas encuestadas tiene un oficial o personal encargado de la seguridad de la información.

Gráfica 6. Resultados pregunta 6

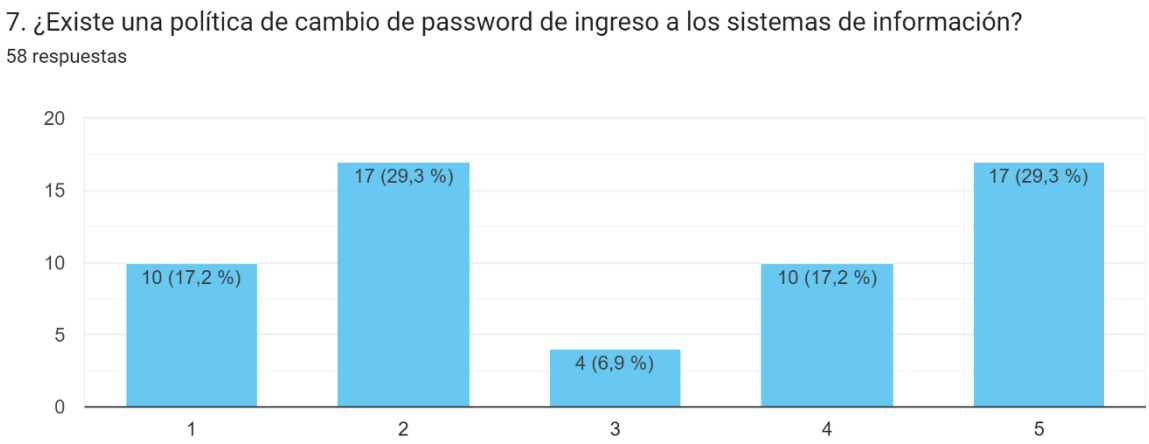


Fuente: elaboración propia

De acuerdo con la investigación, podemos concluir que se obtiene gran rango de respuestas muy variado, sobresaliendo la respuesta “ocasionalmente”

donde las políticas de seguridad de la información son aplicables solo en un 25.9%.

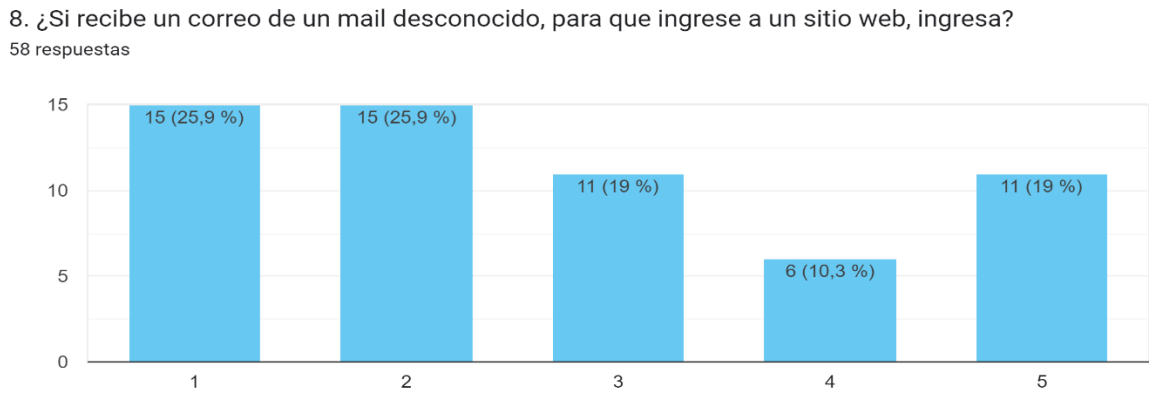
Gráfica 7. Resultados pregunta 7



Fuente: elaboración propia

Según la muestra, vemos claramente que el sector de la tecnología en un 29.3% tiene políticas de cambio de password en sus dispositivos, mientras el otro 29.3% casi nunca tiene esta política, representándose en empresas de sectores dedicados a manufacturación y servicios de consultoría.

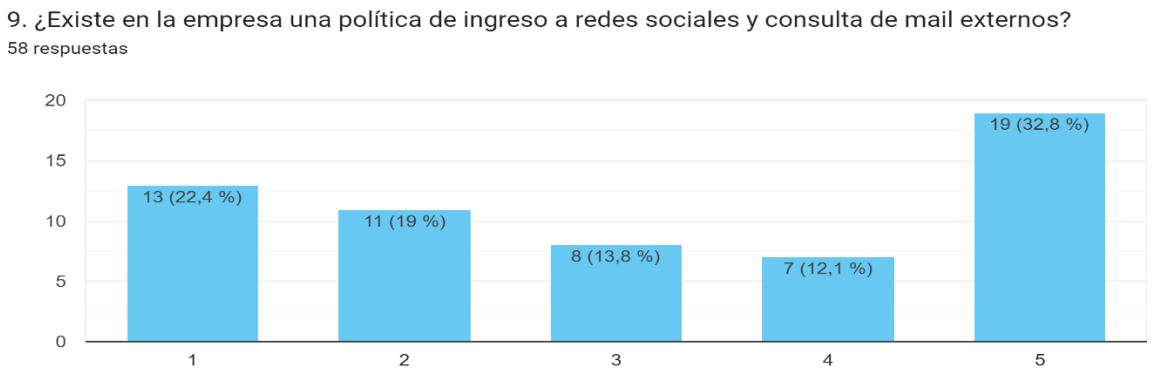
Gráfica 8. Resultados pregunta 8



Fuente: elaboración propia

Esta pregunta, en su mayoría fue contestada con respuestas “nunca y casi nunca” representadas en un 25.9%, lo que infiere que muchas de las empresas conoces los riesgos de recibir este tipo de información en sus dispositivos empresariales.

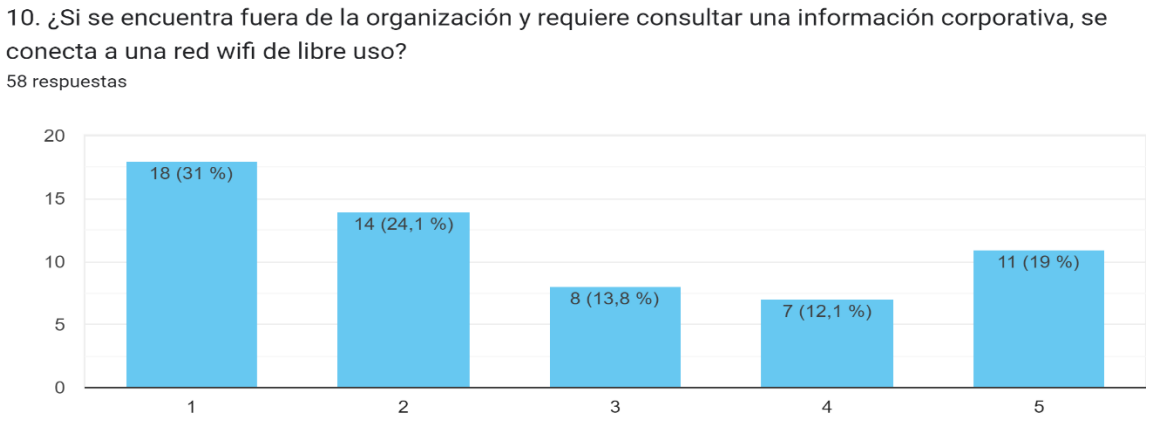
Gráfica 9. Resultados pregunta 9



Fuente: elaboración propia

Como vemos, la pregunta tiene la finalidad de demostrar que muchas empresas consideran que las redes sociales y consulta de mails externos dispersan el trabajo de los empleados, por eso el valor obtenido fue de 32.8%.

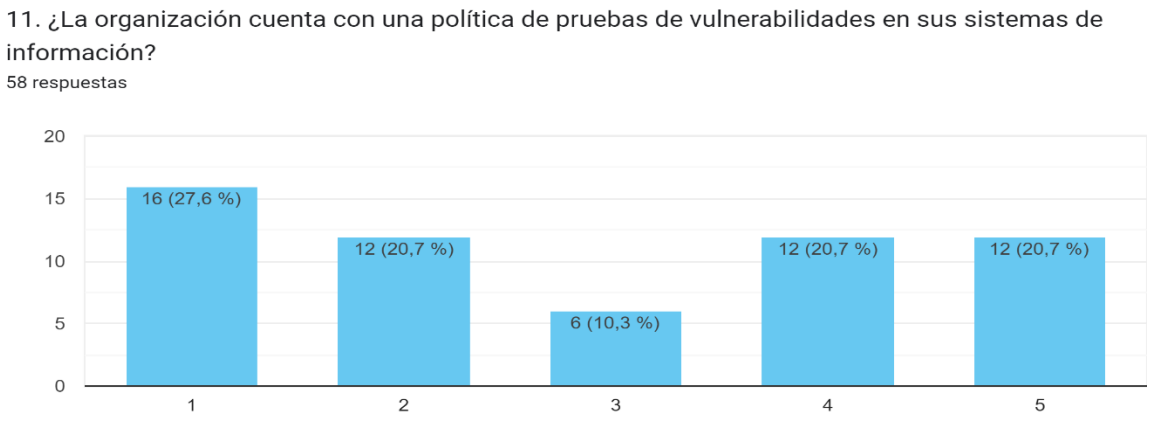
Gráfica 10. Resultados pregunta 10



Fuente: elaboración propia

En un 31% del personal encuestado, considera que esta práctica nunca puede ocasionar riesgos de perdida de información sensible de la empresa.

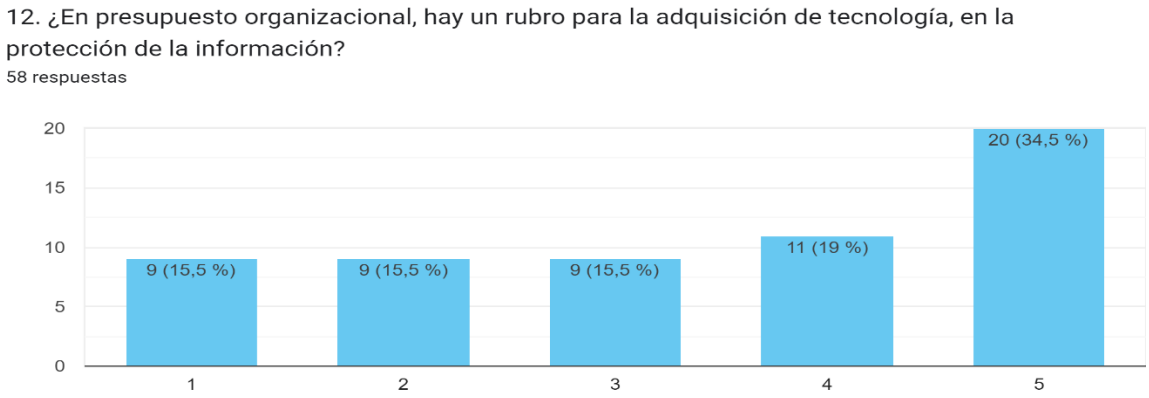
Gráfica 11. Resultados pregunta 11



Fuente: elaboración propia

Se obtuvo un porcentaje de 27.6%, pues en la actualidad las empresas desconocen o nunca tienen políticas empresariales para combatir este tipo de vulnerabilidades en sus sistemas en el caso de que se presenten.

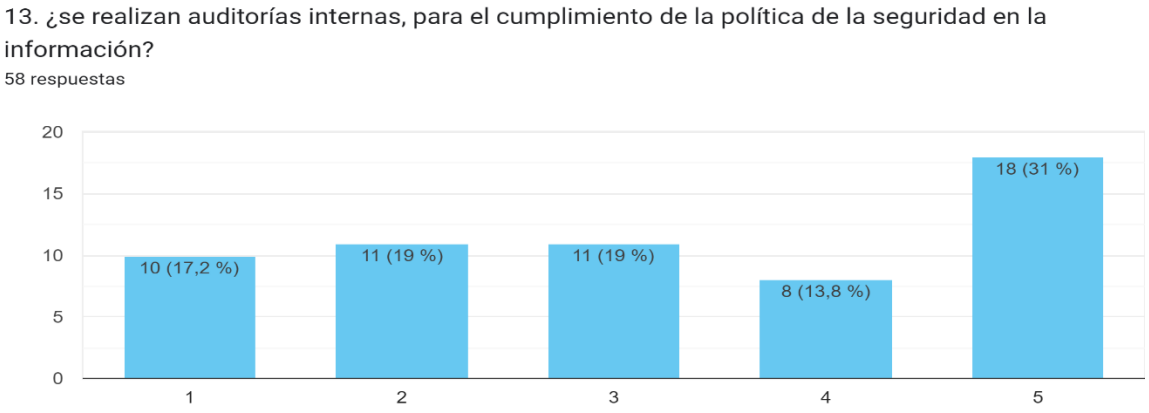
Gráfica 12. Resultados pregunta 12



Fuente: elaboración propia

De acuerdo con la muestra analizada, vemos que la mayoría de las empresas tecnológicas cuenta siempre con un presupuesto para protección de la información, pues consideran que su mayor activo.

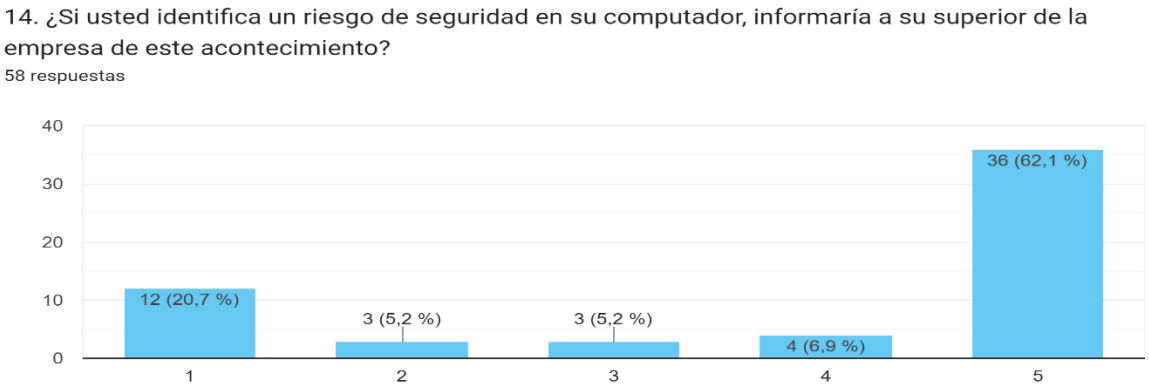
Gráfica 13.Resultados pregunta 13



Fuente: elaboración propia

Si en la anterior pregunta era importante, la existencia de auditorías internas para asegurar la información en las empresas de tecnología se ve reflejada en un 31%, pero en los demás sectores económicos encuestados resulta bastante similar los datos obtenidos.

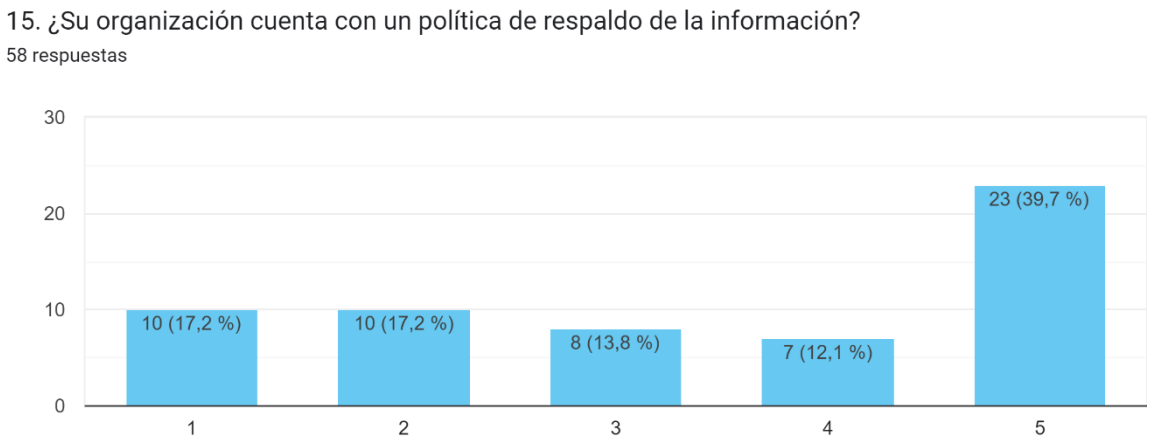
Gráfica 14. Resultados pregunta 14



Fuente: elaboración propia

En la mayoría de los casos encuestados en un 62.1%, el personal de diferentes sectores económicos considera que siempre se debe informar los riesgos de seguridad en los dispositivos empresariales, debido a que estos ataques sino se controlan pueden llegar a causar más perdidas de información importante para la empresa.

Gráfica 15. Resultados pregunta 15



Fuente: elaboración propia

Vemos que la pregunta fue relevante para muchos del personal encuestado, pues en un 39.7% si hay políticas de respaldo de la información sensible de la empresa.

8.1.2 Frecuencias en la escala Likert por cada una de las preguntas.

De la siguiente tabla agrupa y filtrada en Excel se obtiene lo siguiente:

Imagen 3. Frecuencia de respuestas por escala

		PREGUNTADAS FORMULADAS																
Escala Likert		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	MAX	MIN
Nunca	Cuantas veces 1	12	6	7	10	12	13	10	15	13	18	16	9	10	12	10	18	6
Casi nunca	Cuantas veces 2	5	4	8	5	8	10	17	15	11	14	12	9	11	3	10	17	3
Ocasionalmente	Cuantas veces 3	4	7	5	4	7	15	4	11	8	8	6	9	11	3	8	15	3
Frecuentemente	Cuantas veces 4	7	3	10	8	10	8	10	6	7	7	12	11	8	4	7	12	3
Siempre	Cuantas veces 5	30	38	28	31	21	12	17	11	19	11	12	20	18	36	23	38	11
TOTAL RESPUESTAS		58	58	58	58	58	58	58	58	58	58	58	58	58	58	58		

Fuente: elaboración propia

En resumen:

Tabla 8. Preguntas con escalas máximas y mínimas

	PREGUNTA	
Escala Likert	**MAX**	**MIN**
Nunca	Pregunta 10	Pregunta 2
Casi nunca	Pregunta 7	Pregunta 14
Ocasionalmente	Pregunta 15	Pregunta 14
Frecuentemente	Pregunta 12	Pregunta 3
Siempre	Pregunta 2	Pregunta 11

Fuente: elaboración propia

La pregunta 10: ¿Si se encuentra fuera de la organización y requiere consultar una información corporativa, se conecta a una red wifi de libre uso? fue la más contestada como NUNCA.

La pregunta 2: ¿En su organización tiene identificado todos los activos informáticos? fue la menos contestada como NUNCA.

La pregunta 2: ¿En su organización tiene identificado todos los activos informáticos? fue la más contestada como SIEMPRE.

La pregunta 11: ¿La organización cuenta con una política de pruebas de vulnerabilidades en sus sistemas de información? fue la menos contestada como SIEMPRE.

8.1.3 Análisis de los sectores económicos encuestados.

Para este ítem, se tiene la siguiente representación gráfica de acuerdo a los datos obtenidos:

Imagen 4. Sectores participantes del estudio

Fuente: elaboración propia

De lo anterior, tenemos que los tres primeros sectores con mayor participación en la investigación son información y comunicaciones (44,8%), otras actividades de servicios (19%) y los sectores de transporte y almacenamiento y actividades inmobiliarias (6.9%).

8.1.4 Análisis de correlación de las variables utilizados.

A continuación, se realizará el análisis variable por variable de su índice de correlación, apoyado de la siguiente imagen:

Imagen 5. Correlación entre las variables

1. ¿Su empresa aplica las leyes y/o políticas colombianas que rigen y condenan los riesgos informáticos?	2. ¿En su organización tiene identificado todos los activos informáticos ?	3. ¿Su empresa tiene un plan de formación del personal en temas de seguridad digital?	4. ¿Su empresa tiene dispositivos de control de software, para la seguridad de la información en los computadores de la empresa?	5. ¿Su empresa tiene oficial de seguridad de la información?	6. ¿Existe una política de seguridad de la información?	7. ¿Existe una política de cambio de password de ingreso a los sistemas de información?	8. ¿Si recibe un correo de un mail desconocido, para que ingrese a un sitio web, ingresa?	9. ¿Existe en la empresa una política de ingreso a redes sociales y consulta de mail externos?	10. ¿Si se encuentra fuera de la organización y requiere consultar una información corporativa, se conecta a una red wifi de libre uso?	11. ¿La organización cuenta con una política de pruebas de vulnerabilidades en sus sistemas de información?	12. ¿En presupuesto organizacional, hay un rubro para la adquisición de tecnología, en la protección de la información?	13. ¿se realizan auditorías internas, para el cumplimiento de la política de la seguridad en la información?	14. ¿Si usted identifica un riesgo de seguridad en su computador, informaría a su superior de la empresa de este acontecimiento ?	15. ¿Su organización cuenta con un política de respaldo de la información?
1	0,763097087	0,648586483	0,670365479	0,751070885	0,544824207	0,599057668	0,279527527	0,378610001	0,301822498	0,637697387	0,602682224	0,592290658	0,683707134	0,461190933
	1	0,721461964	0,66715336	0,626940654	0,502384354	0,575890654	0,293920234	0,491373983	0,458373876	0,576663643	0,690048303	0,609871241	0,772289262	0,489894098
		1	0,773008412	0,755021373	0,41308705	0,593113759	0,309872331	0,349249688	0,20420361	0,447866512	0,56479622	0,578890487	0,562471206	0,451047753
			1	0,795845701	0,449255278	0,547348341	0,353709675	0,402782906	0,289787081	0,427657323	0,622985938	0,473769883	0,701550862	0,589843186
				1	0,503712266	0,63213081	0,266015099	0,230847386	0,097307614	0,538066318	0,630780145	0,520857693	0,599975484	0,459909215
					1	0,441490717	0,444432887	0,295176665	0,35286716	0,590774119	0,399385379	0,381906428	0,413908306	0,292899749
						1	0,158025142	0,251282922	0,14826439	0,505224603	0,508295552	0,552547724	0,578280028	0,43233291
							1	0,510685351	0,520345938	0,209488049	0,349857085	0,240432957	0,366183596	0,283567788
								1	0,649223959	0,36552809	0,382446345	0,339177155	0,511137963	0,469407483
									1	0,333818784	0,318580041	0,215216393	0,397333954	0,270021565
										1	0,669516346	0,660288314	0,581300369	0,518124978
											1	0,728874461	0,700384293	0,703964379
												1	0,59133608	0,589040674
													1	0,636926091
														1

Fuente: elaboración propia

La Variable 1 (leyes) tiene una alta correlación con la Variable 2 (Identificación de activos); La V1 también tiene alta correlación con la V5 (Oficial de seguridad de la información). De lo anterior, se puede decir que las variables asociadas a “normalización” o “regulación” tienen una correlación. De otro lado, esta variable no se correlaciona con la Variable 8 (Emails) ni la Variable 10 (Redes Wifi).

La Variable 2 (Identificación de activos) tiene una alta correlación con la Variable 14 (Informar riesgos), lo que se podría traducir como que las personas son conscientes de los activos y su importancia por eso se informan los inconvenientes, también podría asociarse a lo tangible de los activos; la Variable 2 también se correlaciona con la Variable 3 (Formación), de lo cual también se puede decir que se le da la importancia a la concientización en el tema. Sin embargo, la Variable 2 no se correlaciona la Variable 8 (Emails) ni la Variable 10 (Redes Wifi).

La Variable 3 (Formación) se correlaciona altamente con la Variable 4 (Dispositivos de control) y con la Variable 5 (Oficial de Seguridad de la Información), lo que a su vez indica la importancia que se le da a la cultura de seguridad de la información. Sin embargo, la Variable 3 tampoco se correlaciona la Variable 8 (Emails) ni la Variable 10 (Redes Wifi).

La Variable 4 (Dispositivos de control) se correlaciona en gran medida con la Variable 5 (Oficial de Seguridad de la Información), lo que es coherente con lo mencionado en el punto anterior. Mientras que esta variable no se correlaciona con la Variable 10 (Redes Wifi).

La Variable 5 (Oficial de Seguridad de la Información), se correlaciona medianamente con la Variable 7 (Política de cambio de password), pero no se correlaciona con Variable 10 (Redes Wifi) siendo estas dos variables las que menos se correlacionan de todas las consideradas en el análisis, que también podría reflejar que a pesar que haya una persona responsable de liderar las estrategias en seguridad de la información, las personas de una organización se siguen conectando a redes Wifi sin validar la seguridad de la misma.

La Variable 6 (Política de seguridad de la información) tiene una correlación media con la Variable 11 (Política de pruebas de vulnerabilidad) y el menor nivel de correlación con la Variable 9 (Acceso a redes sociales) ni con la V15 (Política de respaldos).

La Variable 7 (Política de cambio de password) no tiene correlaciones significativas, sin embargo, es claro que no se correlaciona con la Variable 8 (Emails) ni la Variable 10 (Redes Wifi).

A su vez, la Variable 8 (Emails), tampoco cuenta con correlaciones relevantes, y no se correlaciona con la Variable 11 (Política de pruebas de vulnerabilidad) ni con la Variable 13 (Auditorías internas en seguridad de la información). De esta variable se podría decir que, en general, no cuenta con correlaciones.

La Variable 9 (Acceso a redes sociales) se correlaciona medianamente con la Variable 10 (Redes Wifi), lo que tiene sentido dado que el acceso a redes sociales normalmente está condicionado por el uso de internet. Además, esta

variable no se correlaciona con las Variables 11, 12 y 13, relacionadas con política de pruebas de vulnerabilidad, presupuesto y auditorías internas, respectivamente.

Por su parte la Variable 10 (Redes Wifi) no se correlaciona con ninguna otra variable y con la que menos se relaciona es con la Variable 13 (Auditorías internas en seguridad de la información).

Del lado de las Variables 11, 12 y 13, y como se mencionó en un punto anterior se correlacionan entre sí. Adicionalmente, la Variable 12 (Presupuesto) también se correlaciona con las Variables 14 (Informar riesgos) y 15 (Política de respaldo), de lo que se puede inferir que la materialización de los riesgos y la pérdida de información se asocia al dinero.

Y finalmente, las variables 14 y 15 se correlacionan medianamente entre sí.

A modo de conclusión se podría decir, que las variables 8 (Emails) y 10 (Redes Wifi) no se correlacionan, y que además son las variables de menor implementación como estrategias en ciberseguridad y que a su vez, dicha falta de aplicación podría conducir a ataques usando técnicas de forkjacking, malware, randsomware o smishing.

8.1.5 Análisis de datos general del instrumento.

A partir de las respuestas obtenidas de los entrevistados, en las 58 empresas de diferentes sectores económicos en Colombia y con el énfasis de determinar cuáles fueron barreras organizacionales más comunes encontradas al momento de implementar el concepto de estrategias ciberseguridad, se determinar que en el 100% de las empresas, el personal no presenta resistencia al cambio, el

65.5% ha identificado todos los activos informáticos sensibles para la operación de la organización y conoce las leyes y/o políticas colombianas que rigen y condenan los riesgos informáticos, lo que nos con lleva a que en la mayoría de las empresas de tecnología busquen nuevas oportunidades y retos para contrarrestar estos sucesos; así como el hecho que las empresas solo tengan implementado planes de auditoria internas en tan solo el 31% para combatir estos ataques de seguridad enfatizado solo en el sector de la tecnología, al igual se detectó que en el 34.5% de las organizaciones asignarán o incrementarán el presupuesto como estrategia de ciberseguridad en los próximos años.

En términos numéricos también se puede encuentran los siguientes resultados promedios por variable:

Imagen 6. Resultados promedio de cada variable

A	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
No.	1. ¿Su empresa aplica las leyes y/o políticas colombianas que rigen y condenan los riesgos informáticos?	2. ¿En su organización tiene identificado todos los activos informáticos ?	3. ¿Su empresa tiene un plan de formación del personal en temas de seguridad digital?	4. ¿Su empresa tiene dispositivos de control de software, para la seguridad de la información en los computadores de la empresa?	5. ¿Su empresa tiene oficial de seguridad de la información?	6. ¿Existe una política de seguridad de la información?	7. ¿Existe una política de cambio de password de ingreso a los sistemas de información?	8. ¿Si recibe un correo de un mail desconocido, para que ingrese a un sitio web, ingresa?	9. ¿Existe en la empresa una política de ingreso a redes sociales y consulta de mail externos?	10. ¿Si se encuentra fuera de la organización y requiere consultar una información corporativa, se conecta a una red wifi de libre uso?	11. ¿La organización cuenta con una política de pruebas de vulnerabilidad es en sus sistemas de información?	12. ¿En presupuesto organizacional, hay un rubro para la adquisición de tecnología, en la protección de la información?	13. ¿se realizan auditorías internas, para el cumplimiento de la política de la seguridad en la información?	14. ¿Si usted identifica un riesgo de seguridad en su computador, informaría a su superior de la empresa de este acontecimiento ?	15. ¿Su organización cuenta con un política de respaldo de la información?
PROMEDIO	3,66	4,09	3,76	3,78	3,34	2,93	3,12	2,71	3,14	2,64	2,86	3,41	3,22	3,84	3,40

Fuente: elaboración propia

La imagen anterior representa de forma numérica y visual el resultado promedio de aplicación de cada una de las variables analizadas. Cuando el valor se acerca más a 5, quiere decir que la variable tiene un mejor comportamiento lo que a su vez se relaciona con el color verde; cuando el valor se acerca a 1, se indica que la variable tiene una baja aplicación y se asocia al color rojo; mientras que los valores que se acercan a 3, se refieren a que la variable tiene una implementación media y se identifican con el color amarillo.

De las variables con mejor desempeño, se evidencia que la Variable 2, tiene el mayor promedio, es decir, sería la variable con mayor aplicación dentro de las empresas colombianas, para enfrentar los ataques cibernéticos.

La segunda variable con mejor comportamiento es la 3, que hace referencia a la formación y conocimiento en ciberseguridad.

Por su parte la variable con peor desempeño es la 10, la cual nos indica que las personas poco se preocupan por el uso de redes seguras fuera de la organización.

La siguiente con peor comportamiento es la 8, referente a emails con contenido malicioso. Mientras que las variables 5, 7, 9, 12, 13 y 15 (asociadas con diferentes políticas organizacionales de seguridad informática) tienen resultados medios, es decir, se aplican ocasionalmente como estrategias para mitigar los riesgos en ciberseguridad.

De acuerdo con la información recolectada el promedio de implementación de las estrategias para gestionar la ciberseguridad en las organizaciones colombianas es de 3,33.

Lo anterior indica que hay una aplicación media de dichas estrategias, que también refleja el interés de las compañías en proteger su información, sin embargo, faltan acciones para la concientización y uso de los controles que garanticen la protección de los sistemas, datos, información y en general el conocimiento de las organizaciones.

8.2 Validez y Confiabilidad

A partir de la metodología Alpha Cronbach aplicada, se obtiene los siguientes resultados:

Imagen 7. Confiabilidad

METODOLOGIA ALPHA CRONBACH

		PREGUNTAS											
No.	A que sector pertenece la organización:	5. ¿Su empresa tiene oficial de seguridad de la información?	6. ¿Existe una política de seguridad de la información?	7. ¿Existe una política de cambio de password de ingreso a los sistemas de información?	8. ¿Si recibe un correo de un mail desconocido, para que ingrese a un sitio web, ingresa?	9. ¿Existe en la empresa una política de ingreso a redes sociales y consulta de mail externos?	10. ¿Si se encuentra fuera de la organización y requiere consultar una información corporativa, se conecta a una red wifi de libre uso?	11. ¿La organización cuenta con una política de pruebas de vulnerabilidades en sus sistemas de información?	12. ¿En presupuesto organizacional, hay un rubro para la adquisición de tecnología, en la protección de la información?	13. ¿se realizan auditorías internas, para el cumplimiento de la política de la seguridad en la información?	14. ¿Si usted identifica un riesgo de seguridad en su computador, informaría a su superior de la empresa de este acontecimiento?	15. ¿Su organización cuenta con un política de respaldo de la información?	SUMA
43	Servicios públicos	4	3	2	2	4	3	3	4	4	5	5	56
44	Tecnología	5	5	5	1	1	1	4	5	5	5	5	62
45	Tecnología	5	5	5	5	5	5	4	5	5	5	5	74
46	Telecomunicaciones	5	5	4	5	5	2	5	4	4	5	5	69
47	Vigilancia	3	3	1	2	3	3	5	4	5	4	4	56
48	Retail	5	3	5	5	5	5	3	5	5	5	5	71
49	Tecnología	4	3	5	2	2	3	4	5	4	3	2	53
50	Área jurídica	5	3	2	4	3	4	4	5	4	5	2	61
51	Servicio al Cliente	5	3	4	2	2	2	1	3	3	5	1	49
52	Transporte	4	2	5	2	5	2	3	3	1	5	5	52
53	Servicios profesionales	3	3	2	4	4	4	2	4	1	5	5	52
54	Servicios profesionales	5	1	5	2	1	2	5	5	5	5	5	61
55	Sector hidrocarburos	5	5	5	2	2	2	5	5	5	5	1	62
56	Educación	4	2	2	1	5	2	4	5	5	5	5	58
57	Educación	5	4	5	3	4	2	1	1	2	5	1	53
58	Gestión documental	5	5	5	1	5	1	5	5	5	5	5	67
	DESVIACIONES	2,068627451	2,028520499	2,377896613	2,10695187	2,19607843	2,382352941	2,274509804	1,779857398	1,983065954	0,788770053	2,325311943	

Fuente: elaboración propia

Resultados obtenidos:

Tabla 9. Resultados de validez y confiabilidad

ALFA =	0,958374059	ALTA
K PREGUNTAS=	15	
VI=	29,30310956	
VT=	277,708409	

Fuente: elaboración propia

Donde concluimos que la confiabilidad y validez del instrumento utilizado fue del 95% (ALTA). Lo que nos indica que la escala seleccionada tiene las preguntas muy correlacionadas entre sí. Lo que podemos inferir, que cuanto más próximo esté el alfa de Cronbach este cercano a 1, más consistentes fueron las preguntas de la investigación entre sí.

9. CONCLUSIONES

Para muchas empresas colombianas, el planear o asignar un presupuesto destinado a ciberseguridad y estar abiertas a confrontar estos retos digitales solo se evidencia en un 34.5%, debido a que sus políticas en ataques de ciberseguridad, herramientas tecnológicas avanzadas y planes de contingencia a futuro no están implementadas como requisito de funcionamiento dentro de las organizaciones.

De acuerdo con los resultados obtenidos de la investigación, las pymes colombianas deben dar importancia a asegurar todos los activos asociados a estos riesgos informáticos y crear la cultura de protección entorno a las nuevas tecnologías informáticas para lograr sus objetivos empresariales.

Así mismo, tan solo el 36.2% de las organizaciones encuestadas, cuenta con un oficial o profesional encargado de la seguridad informativa, hecho que nos hace concluir que el concepto de ciberseguridad está muy relacionado con el grado de implementación tecnológica en la empresa junto con la cantidad de dispositivos tecnológicos y su estructura organizacional destinada solamente a su funcionamiento.

Por otro lado, tan solo el 39.7% de las empresas considera que tener una política de respaldo de información es importante y fundamental, pues tienen identificados sus activos críticos, amenazas y vulnerabilidad. De esto podemos relacionar que el 53.4% de las empresas que cuenta con dispositivos de control de software en sus computadores también respaldan sus activos informáticos, lo que

nos hace concluir que estos procesos identifican una estratégica en ciberseguridad que pueden implementar dentro de las organizaciones.

También se identificó que 62.1% de los encuestados, informaría a su superior si existe riesgos en la seguridad informática en sus dispositivos, pues para ellos son conscientes de las posibles consecuencias que podría causar a la empresa, por tal motivo alinear este suceso como impacto dentro de la organización, las consecuencias generadas por la pérdida de la información crítica junto con la optimización de las decisiones a tomar forman parte de una estrategia en ciberseguridad en las pymes colombianas.

Cabe mencionar, que una de las estrategias en ciberseguridad encontradas, se ve reflejada en tener herramientas tecnológicas que permitan asegurar y proteger la información de las empresas, adicionando un plan de contingencia ante un evento de ciberseguridad, donde se identifican los activos digitales críticos.

También, una estrategia de ciberseguridad encontrada es contar con una personal capacitado en estos eventos que aplicará todos los protocolos necesarios para que la información comprometida pueda recuperarse para bien de la compañía.

Por consiguiente, el asignar o incrementar el presupuesto de ciberseguridad anualmente, refuerza las estrategias en riesgos informáticos en caso de enfrentar nuevos retos y desafíos cuando en las empresas se tiene cambios sustanciales en su organización.

Otra de las estrategias en ciberseguridad que las empresas deberían implementar, es que a pesar de que existen metodologías para contrarrestar las amenazas informáticas, muchas de las organizaciones encuestadas no realizan una identificación, valoración y el análisis de los diferentes componentes que puedan causar la materialización de estas amenazas informáticas dentro de sus organizaciones. En este orden de ideas, es importante destacar que las estrategias de ciberseguridad van acompañadas de normas y cultura organizacional que permita conocer a sus empleados las amenazas, riesgos y la forma de enfrentar estas situaciones.

10. REFERENCIAS

Arboleda Vélez, G. (2014). Proyectos - Identificación, Formulación, evaluación y gerencia. Bogotá: Alfaomega.

Amaya, Amaya, A. J., & Camacho Laiton, R. (2013). *Ciberseguridad y ciberdefensa en Colombia* (Bachelor's thesis, Universidad Piloto de Colombia).

A Inoguchi Rojas, EL Macha Moreno - 2017 - repositorio.usil.edu.pe. Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016

Banco Interamericano de Desarrollo. (2020). Reporte de Ciberseguridad 2020: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe. Disponible en: https://observatoriociberseguridad.org/#/final-report

Bernal, C. A. (2006). Metodología de la investigación. Pearson educación.

Bisquerra Alzina, R., & Pérez Escoda, N. (2015). Pueden las escalas Likert aumentar en sensibilidad? REIRE. Revista d'Innovació i Recerca en Educació, 2015, vol. 8, num. 2, p. 129-147.

Buchtik - Uruguay: Gráfica Mosca, 2012. La Gestión de Riesgos en proyectos

Cano, J. J. (2020). Retos de seguridad/ciberseguridad en el 2030. Sistemas, No. 154, pp. 68-79

CCTI. (2021). *Tendencias del CIBERCRIMEN 2021-2022*. Obtenido de https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

CCCE. (2021). *INFORME DEL COMERCIO ELECTRÓNICO EN EL SEGUNDO TRIMESTRE DE 2021.* Obtenido de https://www.ccce.org.co/gestion_gremial/informe-del-comercio-electronico-en-el-segundo-trimestre-de-2021/

CCCE. (2020). *Nueva Normalidad, Los Delitos Informáticos*. Obtenido de https://www.ccce.org.co/noticias/con-la-nueva-normalidad-los-delitos-informaticos-

se-multiplicaron-en-el-pais-pero-pueden-contrarrestarse-con-inversiones-en-seguridad-digital/

CCCE. (2020). *¿Adivina Quién? ¿Las Mil Caras De Una Identidad Fraudulenta?* Obtenido de https://www.ccce.org.co/noticias/adivina-quien-las-mil-caras-de-una-identidad-fraudulenta/

Castillo Parra, X. Y. (2018). Normatividad de ciberseguridad en el sector financiero colombiano. Tomado de http://repository.unipiloto.edu.co/handle/20.500.12277/8625

CYBERSECURITYVENTURES. (2021). *Global Cybersecurity Spending to Exceed $1.75 Trillion From 2021-2025*. Obtenido de https://cybersecurityventures.com/cybersecurity-spending-2021-2025/

CONPES 3995. (01 de Julio de 2020). *POLÍTICA NACIONAL DE SEGURIDAD DIGITAL.* Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

CONPES 3854. (11 de abril de 2016). *POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL*. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854_Adenda1.pdf

CONSGOM. (2022). Ciberseguridad, primer riesgo para las empresas: Un estudio de mercer marsh beneficios (MMB) revela las preocupaciones de las organizaciones. Portafolio, Retrieved from https://login.bdbiblioteca.universidadean.edu.co/login?url=https://www.proquest.com/trade-journals/ciberseguridad-primer-riesgo-para-las-empresas/docview/2714292075/se-2.

Cortés, M. E. C., Villar, N. M., León, M. I., & Iglesias, M. C. (2020). Algunas consideraciones para el cálculo del tamaño muestral en investigaciones de las Ciencias Médicas. MediSur, 18(5), 937-942.

Chambers, M. D. (2022). Exploring the standards cybersecurity practitioners need to comply with multinational cybersecurity requirements (Order No. 29324922). Available from ProQuest Dissertations & Theses A&I. (2700794098). Retrieved

from https://login.bdbiblioteca.universidadean.edu.co/login?url=https://www.proquest.com/dissertations-theses/exploring-standards-cybersecurity-practitioners/docview/2700794098/se-2.

Elijah, L. (2020). *Ciberseguridad*: *Guía completa para principiantes aprende todo de la ciberseguridad de la A a la Z.*

Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova*, *18*(30), 357-377.

Departamento Nacional de Planeación. Colombia. (2011). Documento Conpes 3701: Lineamientos de Política para Ciberseguridad y Ciberdefensa.

Gómez Rengifo, J. N. La ciberseguridad en el Estado colombiano. Tomado de https://repository.unimilitar.edu.co/handle/10654/39827

Franco Suárez, K. A., & Zambrano Hernández, L. F. Análisis documental para la creación de un equipo de respuestas a incidentes informáticos orientado a pequeñas y medianas empresas del sector económico colombiano. Tomado de https://repository.unad.edu.co/handle/10596/42683

Gonzalez Solarte, N. A. (2020) Casos de estudio de cibercrimen en Colombia. Tomado de https://repository.unad.edu.co

(Giraldo, R., (2007). Estadísticas de la microempresa en Colombia: análisis comparativo 1990-2005). Corporación para el Desarrollo de las Microempresas, Bogotá. Niño, 2015).

IDC. (2021). *El surgimiento de la detección y respuesta gestionadas (MDR)*. Obtenido de http://www.idccolombia.com.co/el-surgimiento-de-la-deteccion-y-respuesta-gestionadas-mdr/

Informa Colombia S.A. (2022). Directorio de empresas de Colombia. Obtenido de https://directorio-empresas.einforma.co/

ISACA. (2019). *Obtener los fundamentos de la ciberseguridad correcta.* Obtenido de https://www.isaca.org/es-es/resources/isaca-journal/issues/2018/volume-4/getting-the-basics-of-cybersecurity-right

Isotools. (2012). *Conociendo la ISO 27032 para ciberseguridad.* Obtenido de https://www.isotools.org/2022/05/06/conociendo-la-iso-27032-para-ciberseguridad/

Janke, F., & Packova, M. (2013). Impact of ICT investments on performance of companies in transition economies: Evidence from Czech Republic, Hungary and Slovakia. Quality Innovation Prosperity, 17(2), 9-21.

Llinares, F. M. (2021). Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. IDP: revista d'Internet, dret i política, (32).

MinTIC. (2020). *Modelo de Seguridad*. Obtenido de https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

Modelación y simulación: Modelos de análisis de Datos. Ángel Santana (2018). www.https://estadistica-dma.ulpgc.es/)

Naghi Namakforoosh, M. (2005). *Metodología de la Investigación (Segunda ed.). (G. NORIEGA, Ed.) México: LIMUSA S.A.*

NCSI. (2022). *National Cyber Security Index.* Obtenido de https://ncsi.ega.ee/ncsi-index/

Nikki, G. (2017). *Ciberseguridad para la i-generación: Usos y riesgos de las redes sociales y sus aplicaciones. (Narcea Ed).*

OEA. (2021). *Programa de Ciberseguridad.* Obtenido de https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

ONU. (2015). *Objetivos de desarrollo sostenible*. Obtenido de https://www.un.org/sustainabledevelopment/es/peace-justice/

Ortiz Osorio, M. Importancia de las buenas prácticas en ciberseguridad en el trabajo remoto de entidades públicas de Colombia en época de pandemia. Tomado de https://repository.unad.edu.co/handle/10596/44501

Ospina Díaz, M. R., & Sanabria Rangel, P. E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad*, *62*(2), 199-217.

Pardo Echegaray, J. (2021). Delitos cibernéticos y confidencialidad en las redes sociales, Ica - 2020.

Peralta Cuadrado, M y Roa Ibarra, E. (2021-01-24.). El impacto del delito cibernético en las operaciones de comercio electrónico en Colombia. Facultad de Ciencias Económicas, Jurídicas y Administrativas.

Pérez, F. A. G. (2017). Impacto del cibercrimen: bajo la realidad aumentada. La corrupción en la contratación administrativa: el caso de Costa Rica 8, 67.

Pérez Pérez, Y. (2017). *Importancia de la ciberseguridad en Colombia* (Bachelor's thesis, Universidad Piloto de Colombia). Tomado de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2676/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

PMI. (2017). Guía para los Fundamentos de la Dirección de Proyectos (Guía del PMBOK) 6ª edición (Septima ed.). Pennsylvania: PMI. Recuperado el 31 de Enero de 2020

Portafolio. (2022). *A concientizarse de invertir en ciberseguridad*. Obtenido de https://www.proquest.com/docview/2702881494/70A8019AA6E7493BPQ/1?accountid=34925

Portafolio. (2022). *La demanda de servicios de ciberseguridad creció 40%*. Obtenido de https://www.proquest.com/docview/2626853387/70A8019AA6E7493BPQ/5?accountid=34925

Portafolio. (2022). *El país se ha convertido en foco de interés para los ciberdelincuentes* Obtenido de https://www.proquest.com/docview/2632717890/70A8019AA6E7493BPQ/12?accountid=34925

Ramírez Montealegre, B. J. (2016). Medición de madurez de ciberseguridad en pymes colombianas. *Departamento de Ingeniería de Sistemas e Industrial*. Repositorio.unal.edu.co.

https://repositorio.unal.edu.co/handle/unal/57956

Rodríguez-Rodríguez, J., & Reguant-Álvarez, M. (2020). Calcular la fiabilidad de un cuestionario o escala mediante el SPSS: el coeficiente alfa de Cronbach. REIRE Revista d'Innovació i Recerca en Educació, 13(2), 1-13.

Saavedra, B., & Parraguez, L. (2018). La ciberseguridad: análisis político y estratégico I. *Rev. Fuerzas Armadas*, *91*(243), 44-51.

Santoleri, P. (2015). Diversidad e intensidad de uso de tecnologías de información y comunicación e innovación de productos: evidencia a partir de microdatos chilenos. Economía de la Innovación y Nuevas Tecnologías, 24 (6), 550-568.

Salkind, N. J. (1999). Métodos de investigación. Pearson Educación.

Sampieri, R., & Collado, C. (2014). Metodología de la Investigación. Las rutas cuantitativa, cualitativa y mixta. MacGraw-Hill Education.

Serna Patiño, A. M. (2018). *Análisis de la capacidad de ciberseguridad para la dimensión tecnológica en Colombia: una mirada sistémica desde la organización* (Master's thesis, Escuela de Ingenierías). Tomado de https://repository.upb.edu.co/handle/20.500.11912/4152

SonicWall. (2021). Informe de Amenazas Cibernéticas 2021 de SonicWall. Tomado de https://www.sonicwall.com/es-mx/resources/white-papers/executive-summary-2021-sonicwall-cyber-threat-report-spanish-latam/

Ticona Bustinza, O. R. (2022). Modelo de seguridad de la información basado en la normativa ISO/IEC 27001: 2013 para mitigar los riesgos de los activos de la información en la entidad privada Severox Perú SAC, Arequipa, 2021.