**INFORMAR ESTRATEGIAS DE CIBERSEGURIDAD IMPLEMENTADAS EN LA INDUSTRIA 4.0 APLICADA EN PYMES.**

**RICARDO ESTEBAN AGREDA PASAJE**

**CÓDIGO: I010116**

**INSTITUCIÓN UNIVERSITARIA CESMAG**

**FACULTAD DE INGENIERÍA**

**PROGRAMA DE INGENIERÍA DE SISTEMAS**

**PASTO, NARIÑO.**

**2019**

**INFORMAR ESTRATEGIAS DE CIBERSEGURIDAD IMPLEMENTADAS EN LA INDUSTRIA 4.0 APLICADA EN PYMES.**

**RICARDO ESTEBAN AGREDA PASAJE**

**CÓDIGO: I010116**

**TRABAJO PROYECTO DE INVESTIGACIÓN**

**PROFESOR**

**SANDRA VALLEJO CHAMORRO**

**MAGISTER EN INGENIERÍA**

**INSTITUCIÓN UNIVERSITARIA CESMAG**

**FACULTAD DE INGENIERÍA**

**PROGRAMA DE INGENIERÍA DE SISTEMAS**

**ALTERNATIVA TRABAJO DE INVESTIGACIÓN**

**PASTO, NARIÑO.**

**2019**

**CONTENIDO**

[INTRODUCCIÓN 5](#_Toc9534623)

[1. PROBLEMA DE INVESTIGACIÓN 7](#_Toc9534624)

[1.1 OBJETO O TEMA DE INVESTIGACIÓN 7](#_Toc9534625)

[1.2 ÁREA DE INVESTIGACIÓN 7](#_Toc9534626)

[1.3 LÍNEA DE INVESTIGACIÓN 7](#_Toc9534627)

[1.4 PLANTEAMIENTO DEL PROBLEMA 7](#_Toc9534628)

[1.5 FORMULACIÓN DEL PROBLEMA 8](#_Toc9534629)

[1.6 OBJETIVOS 8](#_Toc9534630)

[1.6.1 OBJETIVO GENERAL 8](#_Toc9534631)

[1.6.2 OBJETIVOS ESPECÍFICOS 9](#_Toc9534632)

[1.7 JUSTIFICACIÓN 9](#_Toc9534633)

[1.8 VIABILIDAD 10](#_Toc9534634)

[1.8.1 VIABILIDAD OPERATIVA 10](#_Toc9534635)

[1.8.2 VIABILIDAD TÉCNICA 10](#_Toc9534636)

[1.8.3 VIABILIDAD ECONÓMICA 10](#_Toc9534637)

[1.9 DELIMITACIÓN 10](#_Toc9534638)

[1.9.1 Espacio 10](#_Toc9534639)

[1.9.2 Tiempo 11](#_Toc9534640)

[1.9.3 Contenido 11](#_Toc9534641)

[1.9.4 Alcance 11](#_Toc9534642)

[1.10 ANTECEDENTES INICIALES 11](#_Toc9534643)

[1.10.1 ANTECEDENTES INTERNACIONALES 11](#_Toc9534644)

[1.10.2 ANTECEDENTES NACIONALES 15](#_Toc9534645)

[1.10.3 ANTECEDENTES LOCALES 18](#_Toc9534646)

[1.11 METODOLOGÍA BÁSICA 18](#_Toc9534647)

[Tipo de investigación 18](#_Toc9534648)

[Cuantitativa 19](#_Toc9534649)

[Aplicada: 19](#_Toc9534650)

[Descriptiva: 19](#_Toc9534651)

[Explicativa: 19](#_Toc9534652)

[Diseño metodológico: 19](#_Toc9534653)

[1.12 TALENTO HUMANO 20](#_Toc9534654)

[1.13. RECURSOS FÍSICOS 20](#_Toc9534655)

[1.14. PRESUPUESTO 20](#_Toc9534656)

[1.15. FINANCIACIÓN 20](#_Toc9534657)

[1.16 CRONOGRAMA DE ACTIVIDADES (DE LA EJECUCIÓN DEL PROYECTO) 20](#_Toc9534658)

[BIBLIOGRAFÍA 20](#_Toc9534659)

# **INTRODUCCIÓN**

A través de la historia se han presentado transformaciones radicales, las cuales han impactado la productividad de las industrias. Estas transformaciones son denominadas revoluciones industriales. La cuarta revolución industrial, conocida como la concentración de tecnologías digitales, físicas y biológicas que consiste en la digitalización de los procesos productivos en las fábricas mediante sensores y sistemas de información para transformar los procesos productivos y hacerlos más eficientes (INTELIGENCIA, 2016),esto permite a las organizaciones en los diferentes sectores económicos utilizar de forma más eficiente los recursos, potencializando los efectos de la toma de decisiones respecto a los sistemas de producción. Esta revolución industrial presenta oportunidades, pero también desafíos para las empresas. Como ocurre con todos los avances de la industria, los beneficios solo son capitalizados por quienes son capaces de innovar y adaptarse. Las PYMES por su tamaño son más flexibles y esto les permite adaptarse a los cambios, más fácilmente que las grandes empresas, siempre y cuando los conozcan y decidan aprovecharlos. El consumidor en la actualidad está empoderado y con información clara acerca de los bienes o servicios que adquiere, la demanda es más personalizada y se basa en la experiencia, actualmente las pymes tienen gran importancia pues su aporte económico en el país es de gran valor “ según cifras del Ministerio de Comercio, Industria y Turismo, las micro, pequeñas y medianas empresas, MiPymes, representan el 99.9% de los establecimientos productivos, contribuyen con el 80% del empleo en el país y aportan el 40% del Producto Interno Bruto nacional.” (EMPLEO, 2018) sin embargo las pymes se encuentran amenazadas frecuentemente por ataques cibernéticos , el campo empresarial desconoce  el tema de ciberseguridad y estrategias para poner frente a dichas vulnerabilidades, pues “las pequeñas y medianas empresas las que más concienciación y formación necesitan debido a que, en muchas ocasiones, no tienen ni los recursos necesarios ni un interés especial en invertir en este ámbito. Pero las estadísticas lo dejan patente, y tal y como ha recordado María Teresa Gómez, directora general de Ametic, el 50% de los ataques se dirigen a este grupo empresarial porque cuentan con sistemas abiertos y suponen una puerta de acceso muy fácil para los malos” (computerworld, 2018). Es  el caso de la ciudad de pasto donde es mínimo por no decir nula la importancia al tema, teniendo en cuenta esto es necesario abordar la ciberseguridad la cual pesa mucho en estas pequeñas y medianas empresas ya que estas, sufren un sinfín de riesgos, y esto es causado por la falta de un buen conocimiento de este tema así mismo la implementación de una seguridad informática de calidad, ya que no solo  ponen en riesgo la información que administran la Pymes sino que además causa muchos daños económicos, por eso es preciso informar y concientizar sobre la implementación de estrategia de ciberseguridad en la industria 4.0 a los empresarios para que estén preparados ante cualquier ataque cibernético.

# **1. PROBLEMA DE INVESTIGACIÓN**

# **1.1 OBJETO O TEMA DE INVESTIGACIÓN**

Ciberseguridad Empresarial.

# **1.2 ÁREA DE INVESTIGACIÓN**

Sistema de gestión de seguridad de la información. En la cual el área de estudio donde tiene mayor aplicación es: empresarial, industria 4.0.

# **1.3 LÍNEA DE INVESTIGACIÓN**

Seguridad de la información.

# **1.4 PLANTEAMIENTO DEL PROBLEMA**

Actualmente  las pymes se encuentran en alta conectividad informática ya que el progreso tecnológico ha dado paso a la revolución digital, esto ha representado para la industria 4.0 múltiples vulnerabilidades y riesgos digitales , por lo que la ciberseguridad se ha convertido en un factor de gran importancia ,así  las pymes deben considerar la necesidad de un sistema de control puesto que las ciberamenazas no solo afectan a la industria 4.0 sino también implica riesgos para la pequeña y mediana empresa que han generado la afectación de muchos de sus procesos industriales. En Colombia las pymes desconocen la ciberseguridad, “El informe anual de Symantec 2017 específica que Colombia sufrió el 0.36% de todas las amenazas que se reportaron en Latinoamérica en ese año a través de Spam y Bots. Asimismo la Encuesta Anual de Seguridad de la Información reveló que, en Colombia el 78% de las empresas invierte menos de un US$1 millón anual para evitar ataques informáticos.” (Colombia.com, 2018), esto indica que en Colombia la ciberseguridad no ha sido considerada por la mayoría de empresas generando la necesidad de concientizar al campo empresarial en la importancia de inversión en ciberseguridad aplicada en la industria 4.0 para que las pymes logren mantenerse en el mercado y no logren verse afectadas por ciertos ataques informáticos. Según la más reciente Encuesta Global de Seguridad de la Información desarrollada por la firma de consultoría EY “42% de las empresas colombianas encuestadas no tiene un centro de operaciones de ciberseguridad, o un grupo de trabajo especializado en monitoreo, ataques o amenazas. Sin embargo, se dio a conocer que 56% de las empresas evaluadas planea realizar cambios en las estrategias por el aumento de las ciberamenazas.” (Bolaños, 2018), es así como las pymes están siendo promovidas a una transición industrial 4.0 , ya que los riesgos tecnológicos significan un trato de gran relevancia, que al ser  manejados con estrategias que promuevan la ciberseguridad garantizan a la empresa su continuidad y su calidad de innovación futura. La ciudad de pasto según la cámara de comercio cuenta con 3.668 empresas lo que indica que está en pleno desarrollo, sin embargo, en los últimos años ninguna entidad universitaria del departamento de Nariño se ha enfocado en investigar este tema de gran interés, que aún se encuentra en un nivel poco conocido frente a la comunidad empresarial. Por esto se puede evidenciar que en el presente año solamente se ha realizado un congreso sobre ciberseguridad en las entidades universitarias y en Nariño no se han realizado estudios pertinentes que indiquen cómo está nuestra ciudad en cuanto a ciberseguridad empresarial, es por esto que se genera la idea de implementar un proyecto enfocado en la  ciberseguridad de las pymes en la ciudad de pasto e informar la necesidad de conocer y tener como principio empresarial estrategias que garanticen la seguridad digital aprovechadas por la industria 4.0

# **1.5 FORMULACIÓN DEL PROBLEMA**

La alta competencia en el mercado empresarial ha implicado su alta relación con la tecnología Datos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic) revelan que las Pymes incrementaron en un 60% su adopción de tecnologías en el 2017.Sin embargo, según el estudio *Cyber Risk for Small and Medium- Sized Enterprises*, el 93% de las Pymes a nivel mundial han sido víctimas de incidentes cibernéticos (Bolaños, 2018). Sin embargo, la ciberseguridad aún no es considerada como un tema primordial de inversión empresarial, no obstante, es una condición que las pymes vean la ciberseguridad no solo como un paso a futuros proyectos industriales 4.0 sino como una obligación de la futura industria relacionada de esta forma ¿Cómo las pymes pueden implementar estrategias de ciberseguridad promovidas en la industria 4.0?

# **1.6 OBJETIVOS**

A continuación, se describe el objetivo general y los objetivos específicos.

## **1.6.1 OBJETIVO GENERAL**

Informar estrategias de ciberseguridad implementadas en la industria 4.0 aplicada en pymes.

## **1.6.2 OBJETIVOS ESPECÍFICOS**

* Informar y analizar la utilización de herramientas informáticas de la industria 4.0 por parte de pymes
* Exponer los riesgos cibernéticos que afronta la industria 4.0
* Proponer estrategias de ciberseguridad aplicadas en la cuarta revolución industrial
* Analizar la transición de las pymes a la industria 4.0 y sus efectos

# **1.7 JUSTIFICACIÓN**

La presente investigación se enfoca en la socialización de estrategias en ciberseguridad de la industria 4.0 aplicada en pymes, que  busca  facultar las pymes  en seguridad digital, ya que actualmente se enfrentan a cibercriminales , pues  “ en el 2017 los delitos informáticos tuvieron incremento del 28,3%” , respecto al año anterior, y afectaron a 446 empresas del país” (Portafolio, 2019)sensibilizar al empresario sobre las vulnerabilidades digitales , dar a conocer estrategias que logre enfrentarlas  y promover una mayor inversión en ciberseguridad permitirá a la empresa mantener competencia en el mercado por su confidencialidad y evitar ataques a sus sistemas informáticos , dado que “  el 61% de los pequeños negocios ha experimentado un ciberataque y un 52% ha sufrido ataques de ransomware” (Empresa, 2019). Esta investigación se orienta al campo empresarial de la ciudad de Pasto que en los últimos años “2017- 2018 tuvieron un aumento de 1651 pymes en la ciudad “ (Pasto, Cámara de Comercio de Pasto, 2017)

Así pues, el  proyecto asegura una visualización de concientización  en seguridad digital que les permita considerar estrategias y acceso a métodos de organización e inversión en ciberseguridad  , además de sostener una economía estable que responda al incremento del “ PIB nacional que en el año 2016, en el Departamento de Nariño fue del 0.8%” (Pasto, Cámara de Comercio de Pasto, 2017), asumiendo  el contexto socioeconómico en el que se busca que las pymes desarrollen su actividad afrontando los retos de la inseguridad que puede afectar a sus sistemas empresariales, Pero también la globalización, que provoca una mayor competencia del mercado, está obligando a las pymes a una transformación digital por lo que es útil que estas pequeñas y medianas empresas se eduquen en ciberseguridad.

Esta iniciativa, que tiene como objetivo concienciar sobre los ataques informáticos resaltan “que el coste medio de un incidente es de 67.000 dólares para estas empresas y que no todas logran recuperarse y volver a la normalidad tras estos sucesos” (computerworld, 2018), además  “ El 43% de las empresas colombianas no están preparadas contra los ciberataques, durante el año anterior, Colombia sufrió pérdidas de alrededor de $1 billón debido a los ciberataques” (Dinero, 2016)., por eso la importancia en que las pymes indaguen en el tema de ciberseguridad industrial 4.0. Actualmente “las pymes nariñenses se han integrado a la página web y correo corporativo gratis por un año, de acuerdo con datos del MinTIC, el 64 % de los colombianos ya usa Internet y el país cuenta con 28,4 millones de conexiones a Internet de Banda Ancha. En este sentido, Nariño le apuesta a la era digital de sus emprendedores,  con el fin de fomentar la imagen corporativa en la web de estas pymes” (Ramírez, 2019), sin embargo Por el poco conocimiento que se tiene en cuanto a la ciberseguridad en la industria 4.0 las pymes de la ciudad de Pasto tienen la necesidad  de conocer lo riesgos a los que se enfrentan y los métodos de cómo contrarrestar los ataques cibernéticos al acceder a dichos programas informáticos .

En el entorno empresarial no existe un software capaz de abarcar todos los entornos de vulnerabilidad digital pues “Cada empresa es distinta y, por ello, tiene una mayor o menor exposición a las distintas amenazas externas e internas, por lo que tanto el análisis inicial de situación como la posterior definición y priorización de proyectos relacionados deben estar personalizados”. (Exive, 2019) no obstante este proyecto tiene como finalidad saber qué incidentes han sufrido las pymes de la ciudad de Pasto  y cómo nos afecta para poner a disposición un software informático con el cual se ayude a tomar conciencia y la exigencia que conlleva la cuarta revolución industrial sobre implementar la ciberseguridad, del mismo modo  apunta a investigaciones futuras que se dirijan al análisis de inversión de pymes en Nariño en ciberseguridad industrial 4.0, ya que es necesario estudiar cómo evolucionan los riesgos digitales y los índices de inversión en seguridad digital.

# **1.8 VIABILIDAD**

## **1.8.1 VIABILIDAD OPERATIVA**

## **1.8.2 VIABILIDAD TÉCNICA**

El proyecto hará uso de recursos tecnológicos, aparatos informáticos, materiales de encuesta.

## **1.8.3 VIABILIDAD ECONÓMICA**

# **1.9 DELIMITACIÓN**

## **1.9.1 Espacio**

Este proyecto se desarrollará en la ciudad de Pasto – Colombia.

## **1.9.2 Tiempo**

Este proyecto de investigación se enfoca en informar al sector empresarial lo importante y necesario que es la aplicación de la ciberseguridad en cuarta revolución industrial.

## **1.9.3 Contenido**

Análisis, socialización e información de las vulnerabilidades digitales a las que están expuestas las pymes; y la importancia de adoptar estrategias de ciberseguridad correspondientes a la industria 4.0

## **1.9.4 Alcance**

Fomentar la utilización de estrategias de ciberseguridad de la industria 4.0 en pymes de la ciudad de pasto, e incitar al conocimiento de seguridad digital

# **1.10 ANTECEDENTES INICIALES**

## **1.10.1 ANTECEDENTES INTERNACIONALES**

**Título** LA CIBERSEGURIDAD DE LA INDUSTRIA 4.0: UN MEDIO PARA LA CONTINUIDAD DEL NEGOCIO.

**Autor:** Ana Ayerbe.

**Año** 2018

**URL:**<https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/ANA%20I%20AYERBE.pdf>

**Resumen:** Industria 4.0 o de la Internet Industrial estamos hablando de digitalización, de conectar máquinas, sistemas, empresas, de recoger cantidades ingentes de datos que permitan tomar decisiones de la forma más precisa y en el menor tiempo, con el objetivo final de incrementar la productividad. el volumen de negocio y en consecuencia los resultados de la empresa, además de múltiples beneficios la digitalización y la conectividad aumentan la superficie de exposición de las empresas a ciberataques y las consecuencias de un ciberataque, perpetrado por cibercriminales, pueden ir desde el secuestro de datos para pedir un rescate, el robo de IPR, la parada de máquinas o el malfuncionamiento de las mismas, la modificación de setpoints   que haga que el producto fabricado no salga con la calidad prevista o la manipulación de datos que puede hacer tomar decisiones equivocadas al basarse en datos manipulados. Todo ello puede impactar tanto en los resultados económicos de la empresa, como en un deterioro del medio ambiente, daños de distinta consideración a personas o en una mala imagen de la empresa”. (Ayerbe, 2018)

**Aporte:** En relación con este proyecto se logra consolidar como la ciberseguridad está sin duda conectada en un entorno industrial, así pues, la obligación industrial es mantener un enfoque, gestión y control en programas de ciberseguridad que minimicen impactos de ciberataques en el campo empresarial.

**Título**: INNOVACIÓN EN CIBERSEGURIDAD. ESTRATEGIA Y TENDENCIAS.

**Autor**: JUAN GONZÁLEZ MARTÍNEZ.

**Año:** 2018

**URL:** <https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/JUAN%20GONZ%C3%81LEZ%20MART%C3%8DNEZ.pdf>

La adopción masiva de tecnologías de la información y telecomunicaciones está transformando nuestra sociedad y todos los sectores de nuestra economía. Está cambiando como nos relacionamos como sociedad, como interactuamos con las Administraciones Públicas y como las empresas desarrollan y entregan sus productos. Si bien son indudables los beneficios derivados de esta transformación digital también han aumentado los riesgos asociados a la adopción de nuevas tecnologías, principalmente los generados por amenazas a la seguridad de la información o ciberamenazas. Estas amenazas ponen en riesgo no solo el crecimiento y la sostenibilidad de nuestra economía, sino también nuestro modo de vida. (Martínez, 2018)

**Aporte:** En relación con este proyecto permite apoyar el objetivo de las vulnerabilidades industriales 4.0 y como la ciberseguridad es una opción esencial para mantener control de la empresa y asegurar un equilibrio y convicción de las oportunidades que se presentan en el mercado industrial minimizando efectos de delitos informáticos a través de estrategias de ciberseguridad.

**Título:** ESPAÑA Y LA CIBERSEGURIDAD: HORA DE REMANGARSE.

**Autor:** LUIS FERNÁNDEZ DELGADO.

**Año:** 2018

**URL:** <https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/LUIS%20FERN%C3%81NDEZ%20DELGADO.pdf>

**Resumen:** La ciberseguridad se ha imbricado en el ADN de la sociedad, siendo cómplice de su destino, para lo bueno y lo malo, y en lo que concierne a nuestro país, cabe preguntarse en estas primeras bocanadas del nuevo siglo qué papel están en disposición de jugar los diversos actores públicos y privados en este ámbito, y qué cabe esperar de las fuerzas contrarias que, valiéndose de una dimensión perennemente inestable, legalmente desestructurada y ilegal en muchos frentes, como es el entramado de Internet, se sirven de él para exprimir y saquear el fértil valle del ciberespacio. La ciberseguridad se ha convertido en un elemento común, se está viviendo una intensa proliferación de la oferta que ha causado la aparición de numerosos proveedores de servicio, los cuales se han sumado a esta tendencia, detectándola como la más provechosa y, en parte, como el único camino para seguir evolucionando en un mercado que cada día se ha de enfrentar a nuevos retos. (Delgado, 2018)

**Aporte:** con respecto a este proyecto favorece la idea del interés que requiere la ciberseguridad en el mundo empresarial tanto para mantener su convicción como su competencia en el mercado y como la ciberseguridad es ahora un servicio específico.

**Título:** Cybersecurity awareness and market valuations.

**Autor:** Henk Berkman, Jonathan Jona, Gladys Lee, Naomi Soderstrom.

**Año:** 18 de mayo del 2018

**URL:** <https://www.sciencedirect.com/science/article/pii/S0278425418302370>

**Resumen:** Comprender la conciencia de la seguridad cibernética a nivel de la empresa es importante porque las empresas están experimentando un número creciente de ciberataques (Deloitte, 2017; PwC, 2016). La evidencia anecdótica sugiere que los costos de estos ataques pueden ser significativos. En 2013, Target Corporation experimentó una violación de datos que afectó a aproximadamente 40 millones de clientes con un costo estimado de al menos $ 162 millones (Prince, 2015). Tras el anuncio de Yahoo! de un ataque cibernético en 2014, Verizon Communications, que se encontraba en ese momento buscando comprar Yahoo, bajó el precio de su oferta en $ 350 millones (Athavaley, 2017). Más recientemente, Equifax experimentó una brecha, en los datos financieros personales de unos 143 millones de consumidores estadounidenses fueron robados. La compañía se enfrenta a más de 240 demandas colectivas y ya ha incurrido en gastos de $ 87.5 millones (Cowley, 2017). Además de comprometer los datos financieros personales, los ataques cibernéticos se han dirigido a información altamente sensible y propiedad intelectual (Pentland, 2011). La ciberdelincuencia ha sido estimada en costos La economía global aproxima los $ 450 mil millones (Hiscox, 2017). (Henk Berkman, 2018)

**Aporte:** así pues, en relación con este proyecto permite visualizar la importancia de la concientización en ciberseguridad como un trabajo de gran relevancia empresarial frente a la inseguridad digital que puede influir en el comportamiento de la empresa y su producción.

**Título:** Cybersecurity for Industry 4.0 in the current literature.

**Autor:** Marianna Lezzi, Mariangela Lazoi y Angelo Corallo.

**Año:** 1 de diciembre del 2018

**URL:** <https://www.sciencedirect.com/science/article/pii/S0166361518303658>

**Resumen:** Dentro de los contextos de la Industria 4.0, la ciberseguridad juega un papel importante en la prevención de la pérdida de competitividad de las empresas. De hecho, el equipo industrial es hoy vulnerable a una serie de Ciberataques, que pueden afectar a todo el modelo de negocio. Según los Informes anuales de ciberseguridad de Cisco 2018 [2], el 31% de organizaciones han experimentado ataques cibernéticos en Operational Tecnología (OT); mientras que el 38% espera que los ataques extiendan la tecnología de la información a la tecnología operativa. La seguridad cibernética es percibida como una prioridad por el 75% de los expertos, sólo El 16% dice que su empresa está bien preparada para enfrentar los retos de la ciberseguridad. Esto se debe principalmente a la falta de normas precisas a las que pueden referirse las empresas, así como la falta de gestión empresarial y las habilidades técnicas necesarias para implementarlas. (Marianna Lezzi, 2018)

**Aporte:** En relación con mi proyecto este articulo me permite fundamentarme en una revisión de la literatura y partir de ella comprender de una forma más amplia la ciberseguridad en el mundo de la industria 4.0 así como reafirmar en datos las vulnerabilidades del sistema y su influencia en la confidencialidad empresarial, para dar a entender la importancia de la búsqueda de estrategias para implementar contramedidas a la amenaza informática.

## **1.10.2 ANTECEDENTES NACIONALES**

**Título:** EY calcula que 42% de empresas colombianas no cuenta con centro de ciberseguridad.

**Autor:** Laura Fernanda Bolaños.

**Año:** 9 de enero de 2018

**URL:**<https://www.larepublica.co/empresas/estudio-de-ey-calcula-que-42-de-empresas-colombianas-no-cuentan-con-centro-de-ciberseguridad-2586868>

**Resumen:** En la más reciente Encuesta Global de Seguridad de la Información desarrollada por la firma de consultoría EY, en la que se evaluó sobre las debilidades y fortalezas de la ciberseguridad, más de 1.200 ejecutivos de grandes empresas dieron su opinión respecto a los ataques cibernéticos.

Según los resultados arrojados, 42% de las empresas colombianas encuestadas no tiene un centro de operaciones de ciberseguridad, o un grupo de trabajo especializado en monitoreo, ataques o amenazas. Sin embargo, se dio a conocer que 56% de las empresas evaluadas planea realizar cambios en las estrategias por el aumento de las ciberamenazas.

Este aumento, según la firma, se debe principalmente al uso de dispositivos de Internet de las Cosas (IoT) que crean nuevas vulnerabilidades. Y es que en el país 78% de las entidades invierten menos de US$1 millón anuales en estrategias que sirven como muro de contención para diferentes tipos de ataques. (Bolaños, 2018)

.[**Aporte:** Con esto se concluye que más empresas deben prestar más atención en cuanto se refiere a la seguridad y para ello es necesario invertir en un centro de operaciones de ciberseguridad el cual esté preparado ante cualquier amenaza](https://www.larepublica.co/empresas/estudio-de-ey-calcula-que-42-de-empresas-colombianas-no-cuentan-con-centro-de-ciberseguridad-2586868). En relación la nota periodística con el proyecto se ve que es necesario que las empresas realicen la implementación de un grupo especializado en ciberseguridad con el fin de mantener las empresas libres de estos ataques cibernéticos que pueden ser una amenaza para su infraestructura.

**Título:** CIBERSEGURIDAD EN LA ERA DE LA REVOLUCIÓN FINTECH.

**Autor:** Cámara de Comercio de Bogotá.

**Año:** 9 enero de 2019

**Url:** <https://bibliotecadigital.ccb.org.co/handle/11520/22727>

**Resumen:** La aparición de las fintech, empresas innovadoras del sector de servicios financieros que se caracterizan por su fuerte componente tecnológico, está introduciendo profundos cambios en el sector financiero, debido a la utilización cada vez más frecuente de dispositivos móviles, la Internet y las redes sociales, los cuales se alejan cada vez más de los tradicionales procesos bancarios. Conozca cuáles son los riesgos de seguridad más comunes, casos famosos de ciberfraudes, tendencias en ciberseguridad y lo que trae el futuro para el sector. (Bogotá, 2019)

**Aporte:** El artículo citado anteriormente corrobora con los objetivos de la investigación ya que se propone contrarrestar estos ataques de ciberdelincuentes, con la aplicación de la ciberseguridad en cuanto al ámbito empresarial y a las vulnerabilidades a las que se expone.

**Título:** Impacto del Riesgo Cibernético en el Bienestar del Segmento Mipyme.

**Autor:** Sara Villa Mesa.

**Año:** 2018

**URL:** <https://repository.eafit.edu.co/bitstream/handle/10784/12890/Sara_VillaMesa_2018.pdf?sequence=2&isAllowed=y>

**Resumen:** Teniendo en cuenta el panorama del riesgo cibernético en las empresas colombianas, se hace necesario revisar la oferta de seguros vigente enfocada en el segmento. Actualmente en Colombia, solo tres compañías de seguros, cuentan con ofertas para el riesgo cibernético, Chubb, SBS y Seguros SURA Colombia.

Estas ofertas son de seguros de responsabilidad civil por daños a terceros, donde se ofrecen coberturas por fallas en el tratamiento de datos personales, protección a la reputación, gastos de defensa, pérdidas de activos digitales, interrupción del negocio y en algunos casos extorsión cibernética.

Estas soluciones de aseguramiento, son aún incipientes cuando se habla de daños propios, pues como bien su nombre lo indica, su principal objetivo es cubrir la responsabilidad civil por daños a terceros, por lo tanto, los daños propios de la empresa pasan a un segundo plano y en ninguna de las soluciones de seguros actuales se tiene un cubrimiento de incremento de la seguridad de la información o de contratación de personas para reconstruir la información.

Se concluye entonces a partir del desarrollo de la metodología que el seguro de riesgo cibernético, si aporta a la protección de las utilidades de las Mipymes. Sin embargo, es importante tener en cuenta que la financiación de riesgos para el caso de las Mipymes es aún un desafío para el mercado asegurador colombiano, pues si bien son un segmento poderoso económicamente, sus inversiones en la actualidad están enfocadas en crecer, mejorando su negocio físicamente, comprando maquinaria y capacitando su personal. La inversión en aseguramiento aun es poca y en su mayoría se realiza por obligación, debido al cumplimiento de un deber, un contrato o asociado a un crédito bancario. (Mesa, 2018)

**Aporte:** En el trabajo de grado citado anteriormente se manejan aspectos en los cuales se ayuda en la protección de responsabilidad por uso y Tratamiento de Información gracias a la implementación de los seguros cibernéticos y beneficios que nos ofrecen al contar con este servicio.

**Título:** ANÁLISIS DE LA CAPACIDAD DE CIBERSEGURIDAD PARA LA DIMENSIÓN TECNOLÓGICA EN COLOMBIA: UNA MIRADA SISTÉMICA DESDE LA ORGANIZACIÓN

**Autor:** Alexis Mauricio Serna Patiño.

**Año:** 2018

**URL:** <https://repository.upb.edu.co/bitstream/handle/20.500.11912/4152/AN%C3%81LISIS%20DE%20LA%20CAPACIDAD%20DE%20CIBERSEGURIDAD%20PARA.pdf?sequence=1&isAllowed=y>

**Resumen:** Colombia como país, ha realizado esfuerzos evidentes, como por ejemplo la generación del Conpes 3701 dándole vida al CERT colombiano cuyo objetivo no dista de la definición principal enunciada por Cardazzone y Carlini, el cual se enmarca en proteger la seguridad y la economía nacional propendiendo por la continuidad de las operaciones en caso de un incidente de seguridad; y el Conpes 3854, definiendo la política de ciberseguridad para Colombia (Ministerio de Interior y Justicia et al., 2011; Ministerio de Interior y Justicia para enfrentar los desafíos emergentes de la ciberseguridad, y en ese sentido, el Gobierno colombiano ha desarrollado avances importantes alineados con el Banco Interamericano de Desarrollo (BID) y Organización de Estados Americanos (OEA) (2016) en materia de políticas, marcos legales y tecnología respecto a la ciberseguridad. (Patiño, 2018)

**Aporte:** En relación con mi proyecto logra indicar que Colombia a tratado la ciberseguridad sin embargo la seguridad digital es aún el reto de la gestión tecnológica.

## **1.10.3 ANTECEDENTES LOCALES**

En el departamento de Nariño Colombia, encontrar antecedentes ante un tema de gran interés resulta bastante complejo puesto que no se han implementado como tal proyectos de investigación enfocados en este tema sin embargo se  ha tratado de dar a conocer este campo mediante el primer congreso realizado el 25 de abril del presente año promovido por la Institución Universitario Cesmag, Universidad Mariana, Autónoma de Nariño (UNAR), las únicas universidades que hasta el momento se han enfocado en la ciberseguridad y que como se logró visualizar hubo una gran participación para la comunidad estudiantil y comunidad en general lo que indica que se deben realizar  una mayor perspectiva y relevancia a la implementación de la ciberseguridad y sus vulnerabilidades en nuestro departamento. (Mariana, 2019)

Cabe resaltar que según la noticia publicada 29 de octubre de 2018 — Agencia de Noticias UN-Colombia se “raja” en ciberseguridad pues El profesor Jorge Ortiz, del Departamento de Ingeniería de Sistemas e Industrial de la U.N. y organizador de esta primera jornada, comentó que “aunque hemos trabajado en procesos que mitiguen esas situaciones, en Colombia no hay estudios completamente serios que den cuenta del estado de la seguridad cibernética del país”.  Señaló que entre los retos está el de concientizar a las personas de la importancia de la seguridad de la información, pues en la vida cotidiana todavía no son conscientes del manejo de las claves en redes sociales o en el correo electrónico. Así que mi proyecto busca dar empezar a dar un visión y consideración a los riesgos empresariales y esencial presencia de sistemas de ciberseguridad. (Colombia, 2018)

# **1.11 METODOLOGÍA BÁSICA**

## **Tipo de investigación**

Se desarrollará mediante investigación cuantitativa, aplicada, descriptiva y explicativa.

## **Cuantitativa**

se realizará la socialización de las estrategias de ciberseguridad de la industria 4.0 en las pymes, del cual se espera la participación de un gran número de empresarios relacionado con la totalidad de pymes de la ciudad de Pasto, además de determinar la cantidad de empresas a ser encuestadas basada en los principios estadísticos.

## **Aplicada:**

se utiliza conocimientos adquiridos en el programa académico y estudios de revistas indexadas con el fin de identificar la problemática y respuestas para buscar su solución.

## **Descriptiva:**

Describe la situación actual de las vulnerabilidades a las que se exponen las pymes y las estrategias aplicadas en la industria 4.0

## **Explicativa:**

Identificar algunos problemas o causas a los que pueden estar sometidas las pymes y proponer estrategias de la industria 4.0 para afrontar los riesgos informáticos

## **Diseño metodológico:**

Socializar estrategias de ciberseguridad de la industria 4.0  en pymes de la ciudad de Pasto utilizando además la técnica de muestra no probabilística que permita realizar una encuesta previa a la capacitación  basándose en la participación a la socialización por parte de las pymes, encuesta que permita conocer la situación actual de la problemática en la ciudad y su nivel de conocimiento en el tema, Para dicha encuesta se tendrá en cuenta la variable empresarial con categorías de gerente o propietario de la empresa .

Finalmente proponer soluciones y dar a conocer estrategias que les permitan a las pymes afrontar situaciones de riesgo cibernético.

# **1.12 TALENTO HUMANO**

# **1.13. RECURSOS FÍSICOS**

# **1.14. PRESUPUESTO**

# **1.15. FINANCIACIÓN**

# **1.16 CRONOGRAMA DE ACTIVIDADES (DE LA EJECUCIÓN DEL PROYECTO)**

# **BIBLIOGRAFÍA**

Ayerbe, A. (2018). *Ministerio de Industria, Comercio y Turismo*. Obtenido de :https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/ANA%20I%20AYERBE.pdf

Bogotá, C. d. (09 de 01 de 2019). *Centro de Información Empresarial (CIEB)*. Obtenido de https://bibliotecadigital.ccb.org.co/handle/11520/22727

Bolaños, L. F. (18 de 01 de 2018). *larepublica*. Obtenido de https://www.larepublica.co/empresas/estudio-de-ey-calcula-que-42-de-empresas-colombianas-no-cuentan-con-centro-de-ciberseguridad-2586868

Colombia, U. N. (29 de 10 de 2018). *Universidad Nacional de Colombia*. Obtenido de https://agenciadenoticias.unal.edu.co/detalle/article/colombia-se-raja-en-ciberseguridad.html

Colombia.com. (18 de 07 de 2018). *Colombia.com*. Obtenido de https://www.colombia.com/tecnologia/emprendimiento/asi-le-apuestan-las-pymes-en-colombia-a-la-seguridad-digital-198833

computerworld. (08 de 10 de 2018). *computerworld*. Obtenido de https://cso.computerworld.es/alertas/los-riesgos-de-ciberseguridad-de-las-pymes-en-el-punto-de-mira

Delgado, L. F. (2018). *Ministerio de Industria, Comercio y Turismo*. Obtenido de https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/LUIS%20FERN%C3%81NDEZ%20DELGADO.pdf

Dinero. (06 de 08 de 2016). *Dinero*. Obtenido de https://www.dinero.com/pais/articulo/colombia-tuvo-perdidas-de-1-billon-por-ciberataques/224404

EMPLEO, E. (09 de 02 de 2018). *EL EMPLEO*. Obtenido de https://www.elempleo.com/co/noticias/investigacion-laboral/pymes-la-base-del-mercado-laboral-5510

Empresa, T. P. (5 de 02 de 2019). *Tecnologia Para Tu Empresa*. Obtenido de https://tecnologiaparatuempresa.ituser.es/seguridad/2019/02/ciberseguridad-para-pymes-mismos-desafios-menos-presupuesto

Exive. (2019). *Exive*. Obtenido de https://www.exevi.com/soluciones/elaboracion-de-planes-de-ciberseguridad-y-privacidad/

Henk Berkman, J. J. (18 de 05 de 2018). *ScienceDirect*. Obtenido de https://www.sciencedirect.com/science/article/pii/S0278425418302370

INTELIGENCIA, P. D. (2016). *PAPELES DE INTELIGENCIA*. Obtenido de https://papelesdeinteligencia.com/que-es-industria-4-0/

Mariana, U. (25 de 04 de 2019). Obtenido de http://isistemas.umariana.edu.co/cic/

Marianna Lezzi, M. L. (1 de 12 de 2018). *ScienceDirect*. Obtenido de https://www.sciencedirect.com/science/article/pii/S0166361518303658

Martínez, J. G. (2018). *Ministerio de Industria, Comercio y Turismo*. Obtenido de https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/JUAN%20GONZ%C3%81LEZ%20MART%C3%8DNEZ.pdf

Mesa, S. V. (2018). *Universidad EAFIT*. Obtenido de https://repository.eafit.edu.co/bitstream/handle/10784/12890/Sara\_VillaMesa\_2018.pdf?sequence=2&isAllowed=y

Pasto, C. d. (2017). *Cámara de Comercio de Pasto*. Obtenido de http://www.ccpasto.org.co/wp-content/uploads/2018/02/Informe-de-Coyuntura-2017.pdf

Pasto, C. d. (2017). *Cámara de Comercio de Pasto*. Obtenido de http://www.ccpasto.org.co/wp-content/uploads/2018/04/CENSO-EMPRESARIAL-2017.docx

Patiño, A. M. (2018). *Repositorio Universidad Pontifica Bolivariana*. Obtenido de https://repository.upb.edu.co/bitstream/handle/20.500.11912/4152/AN%C3%81LISIS%20DE%20LA%20CAPACIDAD%20DE%20CIBERSEGURIDAD%20PARA.pdf?sequence=1&isAllowed=y

Portafolio. (29 de 01 de 2019). *Portafolio*. Obtenido de https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

Ramírez, Y. (14 de 03 de 2019). *Cámara de Comercio de Pasto*. Obtenido de http://www.ccpasto.org.co/?p=8778