TELETRABAJO EN COLOMBIA: ANÁLISIS DEL ESTADO DE LA CIBERSEGURIDAD EN PEQUEÑAS Y MEDIANAS EMPRESAS

Ingeniero de Sistemas
RHONALD DE JESÚS LLANOS PALACIOS
Estudiante

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
PROGRAMA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD SANTA MARTA
ZONA CARIBE
2022

TELETRABAJO EN COLOMBIA: ANÁLISIS DEL ESTADO DE LA CIBERSEGURIDAD EN PEQUEÑAS Y MEDIANAS EMPRESAS

Ingeniero de Sistemas
RHONALD DE JESÚS LLANOS PALACIOS
Estudiante

Monografía para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Mg. Ing. Yolima Esther Mercado Palencia
Asesora de grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD SANTA MARTA
ZONA CARIBE
2022

NOTA DE ACEPTACIÓN
MONOGRAFÍA

Firma del Presidente de Jurado
Sustentación

Firma del Jurado Sustentación

Firma del Jurado Sustentación

Santa Marta., 21 de junio de 2023 Monografía.

DEDICATORIA

La formación de posgrado no es fácil primero que todo doy gracias a Dios por ser la guía y fortaleza en segundo lugar a mis padres y hermanos por ser testigos día a día en el crecimiento personal y profesional y tercero al equipo académico de la escuela ECBTI en el país en la Especialización en Seguridad Informática.

AGRADECIMIENTOS

Todos los líderes que hacen parte el proyecto educativo a nivel nacional llamado Universidad Nacional Abierta y a Distancia – UNAD, que trabajan día a día ofertando educación de calidad. El equipo de la Gerencia de Plataformas e Infraestructura Tecnológica – GPIT y la Escuela de Ciencias Básicas Tecnología e Ingeniería – ECBTI en el programa posgradual en la Especialización en Seguridad Informática los tutores que motivaron a seguir adelante y aportar el aprendizaje significativo a la sociedad.

TABLA DE CONTENIDO

pág.

1. DEFINICIÓN DEL PROBLEMA 13

1.1 ANTECEDENTES DEL PROBLEMA 13

1.2 FORMULACIÓN DEL PROBLEMA 14

2. JUSTIFICACIÓN 15

3. OBJETIVOS 16

3.1 OBJETIVOS GENERAL 16

3.2 OBJETIVOS ESPECÍFICOS 16

4. MARCO REFERENCIAL 17

4.1 MARCO conceptual 17

4.2 MARCO TEÓRICO 20

4.3 MARCO HISTÓRICO 21

4.4 ANTECEDENTES O ESTADO ACTUAL 22

4.5 EL MARCO LEGAL 23

5. ESTABLECER LOS FACTORES DE RIESGOS DE CIBERSEGURIDAD PRESENTADOS EN EL TELETRABAJO ACTUALMENTE EN COLOMBIA QUE PERMITAN IDENTIFICAR VECTORES DE AMENAZAS PERSISTENTES. 26

6. REVISAR LA NORMATIVIDAD, LEGISLACIÓN Y DOCUMENTOS DE BUENAS PRÁCTICAS QUE POSIBILITAN Y GARANTIZAN EN TÉRMINOS DE CIBERSEGURIDAD EL TELETRABAJO EN COLOMBIA. 36

7. PRESENTAR UN INFORME DEL ESTADO ACTUAL DE LA CIBERSEGURIDAD, VENTAJAS Y DESVENTAJAS DE LOS DIFERENTES RECURSOS PROPUESTOS POR LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO Y OTROS ENTES DE CONTROL CON RELACIÓN A LA APLICACIÓN DE BUENAS PRÁCTICAS EN EL TELETRABAJO PARA PYMES. 49

8. CONCLUSIONES 61

9. RECOMENDACIONES 63

10. BIBLIOGRAFÍA 64

LISTA DE FIGURAS Y GRÁFICOS

Pág.

Figura 1. Dispositivos electrónicos……25

Figura 2. Amenaza de software…..……27

Figura 3. Usuarios finales …… 28

Figura 4. Modalidad de delitos informáticos……31

Figura 5. Falta de capacitación…… 32

Figura 6. Ciberseguridad en Colombia 2019 – 2020…….……47

Figura 7. Ciberseguridad en Colombia 2021……49

Figura 8. Buenas prácticas de ciberseguridad……56

Gráfico 1. Delitos Informáticos año 2019……..52

Gráfico 2. Delitos Informáticos año 2020……..52

Gráfico 3**.** Delitos Informáticos año 2021……..53

GLOSARIO

ACTIVO: Se denomina activo a los elementos informáticos que tienen las organizaciones de acuerdo con (ISO/IEC 27000) son elementos clasificados en la informática cómo equipos, soporte y la participación de los usuarios.

AMENAZAS: Son la serie de anomalías que pueden ocurrir y pueden ocasionar afectaciones en las organizaciones (ISO/IEC 27000).

AUDITORÍA: Es el trabajo bajo la norma (ISO/IEC 27000) permite la realización del proceso de análisis y detección de hallazgos que puedan afectar a las organizaciones y donde se aplican medidas de corrección para evitar sucesos posteriores.

ARQUITECTURA DE SEGURIDAD: Es el análisis y diseño de protocolos de seguridad en la minimización de los riesgos que puedan ocasionar las amenazas detectadas teniendo en cuenta las necesidades de las organizaciones.

AUTENTICACIÓN: Mecanismo de seguridad en el acceso de personas autorizadas en las organizaciones y restringir el ingreso de personas no autorizadas o externas a los sistemas.

BLACKLISTING: Es un listado que las agencias de seguridad informática emiten para la protección de los ataques de los ciberdelincuentes.

CIBERDELITO: Es el actuar de los ciberdelincuentes con altos conocimientos en programación con el objetivo de ocasionar daños a los sistemas de información en las organizaciones.

CIBERSEGURIDAD: Se determina como el ejercicio de la protección de los equipos tecnológicos frente a los ciberataques que día a día tratan de atacar a los sistemas de información y con ello los datos.

DATO: Se determina en el mundo informático como la información procesada como el ingreso, transformación y resultado de los datos que se determina como información.

EXPLOITS O PROGRAMAS INTRUSOS: Son programas que presentan potencial riesgo que son fachada para atacar la información de las organizaciones y usuarios finales.

FILTRACIÓN DE DATOS: Es la mala gestión de la información que no es debidamente clasificada y esto ocasiona fuga de datos para terceras personas para ciberdelincuentes.

INGENIERÍA SOCIAL: Son las diferentes estrategias o trampas para que los usuarios incautos o falta de conocimiento de seguridad informática puedan ser víctimas de los ciberdelincuentes.

RIESGO: Se clasifican en tres tecnológico, usuarios y ambientales en donde no se gestiona políticas contra los riesgos la información está a merced de los ciberdelincuentes.

RESUMEN

La ciberseguridad es prioridad para el desarrollo del teletrabajo en Colombia en las pymes representan muchos sectores emergentes realizan esta modalidad de trabajo en donde presentan productos y/o servicios que ofrecen mediante el uso de las TIC. La modalidad de trabajo se encuentra regulado por leyes, decretos y convenios de ciberseguridad. El mayor peligro de las pymes en Colombia es la falta de conocimiento frente los ataques de los ciberdelincuentes que planean día a día con la intención de afectar los sistemas en donde pueden dejar a las pymes sin operación. Bajo esta perspectiva es el propósito de la monografía en el análisis de la ciberseguridad en las pequeñas y medianas empresas en Colombia donde es necesario la participación del sector de la seguridad informática no solamente en la protección de los equipos tecnológicos sino en informar a los usuarios la importancia de la ciberseguridad en donde se demuestra mediante boletines de seguridad sobre los ataques cibernéticos y como las pymes deben estar atentos para que no sean afectados mediante las diferentes estrategias que estos crean.

Palabras claves: Ciberseguridad, Ciberdelitos, Normas, Pymes, Teletrabajo, TIC.

ABSTRACT

Cybersecurity is a priority for the development of telework in Colombia in SMEs they represent many emerging sectors. They carry out this type of work where they present products and / or services that they offer through the use of ICT. The work modality is regulated by laws, decrees and cybersecurity agreements. The greatest danger for SMEs in Colombia is the lack of knowledge in the face of attacks by cybercriminals who plan daily with intention in affecting the systems where they can leave SMEs without operation. Under this perspective, the purpose of the monograph on the analysis of cybersecurity for SMEs in Colombia where the participation of the information security sector is necessary not the protection of technological equipment also in informing users about of the importance of cybersecurity where it is demonstrated through security bulletins on cyberattacks and how SMEs must be vigilant so that they are not affected by the different strategies that they create.

Keywords: Cybersecurity, cybercrime, standards, pymes, telework, TIC.

INTRODUCCIÓN

El teletrabajo es reconocido como trabajo por fuera del entorno laboral mediante las tecnologías de la información y comunicaciones, pero esto puede llegar a generar problemas en materia de ciberseguridad teniendo en cuenta que los teletrabajadores no tienen conocimientos básicos en el tema que se basa en la recolección de información acerca de los problemas en materia de ciberseguridad que afecta el teletrabajo teniendo en cuenta la falta de conocimientos en materia de seguridad informática por parte de los teletrabajadores por fuera de las oficinas en las pymes.

La característica principal de la problemática es la falta de conocimiento de los ciberdelitos debido al desconocimiento en materia de ciberseguridad en las pymes diariamente esto ocasiona un alto riesgo de ataques informáticos.

La investigación tiene el interés de conocer como las pymes se enfrentan como han avanzado en materia de la ciberseguridad mediante normatividad, legislación, documentos de buenas prácticas y el análisis actual que garanticen en términos de ciberseguridad el teletrabajo en Colombia.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Los ciberdelitos que afectan al sector de las pequeñas y medianas empresas en el país tienden a generar dudas en materia de ciberseguridad de acuerdo con el informe de Tendencias Cibercrimen Colombia 2019 – 2020"[1] CCIT Cámara Colombiana de Informática y Telecomunicaciones, donde los teletrabajadores establecen conexiones no seguras para trabajar siendo víctimas de los ciberdelincuentes que conlleva que se afecte la imagen y el prestigio de las pymes.

Los problemas basados por la falta de conocimientos en ciberseguridad de los teletrabajadores en las pymes, esto permiten a los ciberdelincuentes realizar diferentes ataques informáticos mediante estrategias de engaños y filtración en la conectividad no segura desde la casa, el trabajo remoto en las pymes puede ocasionar problemas en la gestión comercial sino se tiene medidas mínimas de protección contra los delincuentes informáticos.

Según CCIT "En Colombia con los ciberdelitos que afectan la gestión empresarial como el robo, la suplantación, la ingeniería social, entre otros de acuerdo con el Informe Tendencias del Cibercrimen primer trimestre 2020"[2]. Los ciberdelitos generan riesgos a las pymes durante la realización de la gestión comercial debido a las estrategias de los ciberdelincuentes.

En la actualidad los ciberdelitos pueden afectar el teletrabajo se deben a dos factores en las pequeñas y medianas empresas:

[1] CCIT, Tendencias del Cibercrimen en Colombia; 2019 – 2020; https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/#:~:text=Actualmente%2C%20el%2045.5%25%20de%20las,sido%20denunciados%20ante%20la%20fiscal%C3%ADa.

[2] CCIT, Tendencias del Cibercrimen en Colombia; primer trimestre del 2020; https://www.ccit.org.co/estudios/el-tictac-presenta-el-informe-de-tendencias-del-cibercrimen-en-colombia-primer-trimestre-de-2020/#:~:text=En%20el%20primer%20trimestre%20de,el%20mismo%20periodo%20de%202019.

El primer factor es el humano por la falta de la cultura de capacitación de la ciberseguridad de los teletrabajadores al no tener conocimiento pueden ser víctimas de ciberdelincuentes.

Segundo es la son los riesgos de la infraestructura tecnológica no son las adecuadas teniendo en cuenta que realizan grandes inversiones en tecnología.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuál es el estado de la ciberseguridad en las pymes que ejercen el teletrabajo en Colombia?

2 JUSTIFICACIÓN

La monografía busca impactar acerca de la ciberseguridad en el teletrabajo en las pymes donde se determina la importancia en estar informados acerca de los ciberdelitos que son blanco de los ciberdelincuentes.

El teletrabajo está regulado por el Ministerio de Trabajo y por el Ministerio de Tecnología Información y Comunicaciones mediante la Ley 1221 de 2008. que mejoren las relaciones laborales de los teletrabajadores en las pequeñas y medianas empresas aportando progreso al país. El teletrabajo se realiza fuera de la oficina sin el mínimo de los protocolos en materia de ciberseguridad esto se convierte en alto riesgo en suplantación o robo de identidad, entre otros. A diario se ejerce el teletrabajo y para ello es necesario que los usuarios tengan conocimientos en materia de ciberseguridad en las pequeñas y medianas empresas.

La ciberseguridad está relacionada en las estrategias y políticas de acuerdo con organizaciones internacionales en materia de políticas de protección frente a los ciberdelincuentes en donde se genera la confianza necesaria para el desarrollo del teletrabajo en las pequeñas y medianas empresas.

La preocupación de las pequeñas y medianas empresas son las estrategias que generan los delincuentes informáticos con el objetivo de atacar a las pymes y vulnerar la gestión comercial como el robo y alteración de la información. El apoyo de expertos en seguridad informática es posible minimizar los ciberataques que sufren a diario.

Busca aportar el conocimiento necesario mediante el estado de la ciberseguridad en las pequeñas y medianas empresas en Colombia para el fortalecimiento del teletrabajo como alternativa de desarrollo económico.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar el estado de la ciberseguridad que presenta el teletrabajo en el desarrollo de las actividades diarias en las pequeñas y medianas empresas.

3.2 OBJETIVOS ESPECÍFICOS

- Establecer los factores de riesgos de ciberseguridad presentados en el teletrabajo actualmente en Colombia que permitan identificar vectores de amenazas persistentes.

- Revisar la normatividad, legislación y documentos de buenas prácticas que posibilitan y garantizan en términos de ciberseguridad el teletrabajo en Colombia.

- Presentar un informe del estado actual de la ciberseguridad, ventajas y desventajas de los diferentes recursos propuestos por la superintendencia de industria y comercio y otros entes de control con relación a la aplicación de buenas prácticas en el teletrabajo para pymes.

4 MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL

4.1.1 Teletrabajo, “El teletrabajo se entiende como una modalidad a distancia[3].” “MinTic realiza el acompañamiento en la asesoría de la implementación del teletrabajo en el país[4].” Las pymes se normalizan bajo las normas, leyes, decretos, acuerdos para el desarrollo de esta modalidad de trabajo logrando la reglamentación de esta fuente de empleo en Colombia.

4.1.2. Pymes: “Las pymes son pequeñas y medianas empresas, esto es, las empresas que cuentan con no más de 250 trabajadores en total y una facturación moderada. Son empresas de facturación, con un número limitado de trabajadores y que no disponen de los grandes recursos de las empresas de mayor tamaño.” [5]. Las pymes por ser pequeñas y medianas no son grandes empresas, pero aporta a la economía y el capital humano necesario para el desarrollo del sector.

4.1.3 Según Red Brands: “Los emprendimientos de la micro, pequeña y mediana empresa en Colombia, han sido, como en cualquier lugar del mundo, fuente de ingresos para innumerables familias. Ante esto se estima que el 80% de los nuevos empleos son generados por las ideas de emprendimiento. Y no solo eso, según los expertos el 96,4% de los establecimientos empresariales está representado por este grupo.”[6] El emprendimiento genera fuentes de empleo mediante las pymes junto al uso de las TICS como el complemento ideal para la gestión comercial.

4.1.4. Según Hernández, (2020) “La transformación digital en las pymes es necesario para la competitividad, para dar la iniciativa es necesario establecer

[3] MinTIC: Teletrabajo, Definición, https://teletrabajo.gov.co/622/w3-article-8228.html
[4] MinTIC: Conozca cómo puede implementar el teletrabajo con el acompañamiento del MinTIC; https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126002:Conozca-como-puede-implementar-el-teletrabajo-con-el-acompanamiento-del-MinTIC
[5] Pymes: Características pymes tecnológicas; https://www.logicbus.com.mx/caracteristicas-pymes-tecnologicas.php
[6] La importancia de las Pymes en la economía colombiana; https://www.red-brands.com/importancia-pymes-economia/

conexiones de calidad, dispositivos tecnológicos, soluciones digitales adaptados a requerimientos específicos y herramientas que potencien las oportunidades de negocios". La integración tecnológica aporta a las pymes la cadena de valor en la relación con los clientes disminuyendo los riesgos que se presentan en el sector del comercio electrónico en relación a las compras vía web.

4.1.5. Ciberdelito: Según UDI-TIPS "Es un término genérico que hace referencia a la actividad delictiva, llevada a cabo mediante equipos informáticos o a través de Internet. El ciberdelito puede hacer uso de diferentes métodos y herramientas, como el phishing, los virus, spyware, Ransomware o la ingeniería social, normalmente con el objetivo de robar información personal o de realizar actividades fraudulentas"[7]. Teniendo en cuenta la forma como el delincuente informático se aprovecha de los usuarios que no poseen conocimientos de ciberseguridad en la era digital y el avance de la tecnología los teletrabajadores pueden caer fácilmente ante el ataque del ciberdelincuente mediante diferentes formas de ataques.

4.1.6. Constitución del ciberdelito: Según UDI-TIPS "Se constituye en una amenaza, riesgo y vulnerabilidad, ya que los usuarios están conectados a la internet mediante dispositivos portátiles, teléfonos inteligentes, tabletas, entre otros". El ciberdelito es un delito informático que ocasiona pérdidas de información, ataques, robo o secuestro de información esto conlleva a que los cibercriminales se lucran con esto se basa por se generan espacios en donde los delincuentes informáticos pueden aprovechar.

4.1.7. Tipos de delitos informáticos: Según ALDAMA Informática Legal "La tecnología avanza a pasos agigantados al igual los ciberdelitos. Se relacionan cinco tipos de delitos informáticos como: Sitios falsos, Suplantación de Identidad, Hackeo

[7] Escuela Nacional de Ciencias Biológicas Unidad de Informática. ¿Qué es el ciberdelito? [documento en línea]. Recuperado de: https://www.encb.ipn.mx/assets/files/encb/docs/alumnos/udi/udiTips/udiTip-22.pdf

Ilegal, Extorsión y Acoso."[8] Teniendo en cuenta los delitos informáticos recurrentes los ciberdelincuentes logran de todas formas atacar y robar los datos en las pymes bajo el teletrabajo en Colombia.

- **Consecuencias económicas:** puede verse afectar las inversiones en el sector de las pymes de manera fiscal el movimiento financiero afectando la actividad económica en la cual dependen familiares de los teletrabajadores.

- **Otras consecuencias:** los ataques cibernéticos afectan notablemente la gestión comercial como la fuga de información ocasionados por terceras personas con el objetivo de robar, manipular y alterar la información afectado el prestigio de las pymes.

4.1.8. Ciberseguridad: Según Kaspersky "La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos"[9]. Bajo este concepto participa en la generación de creación de políticas y estrategias que tiene como objetivo de minimizar los ataques y que los teletrabajadores en las pequeñas y medianas empresas tengan el conocimiento. Mediante la asociación de entidades y organizaciones internacionales en defensa y han logrado fortalecer en la judicialización de los ciberdelincuentes y generar confianza en las pymes en el desarrollo de las actividades económicas.

[8] Aldama informática legal: cinco delitos informáticos más comunes de lo que crees [en línea]. 2017, Ene 24. Recuperado de: https://informatica-legal.es/delitos-informaticos-comunes-internet-ciberdelito/

[9] Kaspersky: ¿Qué es la ciberseguridad?, [en línea] 2023. Recuperado de: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

4.2 MARCO TEÓRICO

El teletrabajo en Colombia toma fuerza teniendo en cuenta que esta modalidad de trabajo gracias a las normativas y decretos en donde es posible la generación de empleo en el país. Las pequeñas y medianas empresas - pymes son organizaciones que se basan en la prestación de bienes y/o servicios a los clientes. La ciberseguridad es el arte de proteger los equipos tecnológicos ante los ciberdelitos mediante tratados nacionales e internacionales un ejemplo de ello es el convenio sobre la ciberdelincuencia de Budapest[10] que busca la prioridad, recursos que permita el actuar de las leyes penales a través de la cooperación internacional con las agencias de ciberseguridad.

Según la Asociación Colombiana de Ingenieros de Sistemas – ACIS[11] informa a las empresas que se dedican a la Seguridad Informática mediante las políticas contra los ciberdelincuentes que buscan la protección ante los ataques informáticos mediante la estrategia de Ethical Hacking donde identifican las fallas de seguridad y establecer las estrategias de seguridad para minimizar los riesgos, vulnerabilidades y amenazas que enfrentan las pymes.

Es necesario el análisis de la ciberseguridad en Colombia, como están las pymes con los ciberataques afrontan a diario, en la cual necesitan el apoyo de los expertos en minimizar los ataques generando tranquilidad y confianza.

[10] Consul de Europa, Serie de Tratados Europeos No. 185, Convenio sobre la ciberdelincuencia; Budapest, 2001, noviembre 23, [en línea], Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
[11] Asociación Colombiana de Ingenieros de Sistemas, ACIS; Listado de Empresas en Seguridad Informática [en línea], 2022. Recuperado de; https://acis.org.co/portal/content/lista-de-empresas-de-seguridad-inform%C3%A1tica-en-colombia

4.3 MARCO HISTÓRICO

“Las cifras de ciberseguridad en Colombia prenden las alarmas al cierre del año 2020”[12] Según Adriana Ceballos, esto se debió al replanteamiento y los diferentes modelos de empleo. El teletrabajo es una modalidad de empleo regulado por la legislación colombiana y diferentes tratados mediante el uso de las TIC. Bajo esta opción se crean los diferentes canales de comunicación virtual sin la debida consulta de expertos en ciberseguridad en la cual se incrementó los ciberdelitos mediante tipos de estrategias engañosas donde los ciberdelincuentes atacan los usuarios.

Según Adriana Ceballos, directora de desarrollo de programas del Tanque de Análisis y Creatividad de las Tic (TicTac) “la ciberseguridad es el área que mayor atención deberá tener en el 2021, pues un gran número de colaboradores seguirán operando desde sus hogares”[13] además agregó que “el nuevo documento construido por el programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE), llamado ciberseguridad en entornos cotidianos, en el que participó Claro, es precisamente, el análisis de diferentes contextos como, trabajo remoto, ciberseguridad en dispositivos móviles, ciberataques a correos electrónicos, entre otros.” Es importante la opinión de la experta citada las pequeñas y medianas empresas en Colombia basados en el teletrabajo donde busca el fortalecimiento en materia de ciberseguridad.

[12] Portafolio, Cifras de ciberseguridad en Colombia prenden las alarmas al cierre de 2020 [artículo en línea], diciembre, 10 de 2020. Recuperado de: https://www.portafolio.co/tendencias/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020-547412

[13] Arias, D. Enter.co, Ciberseguridad: uno de los retos que dejo el 2020; [artículo en línea], enero 28, 2021. Recuperado de; https://www.enter.co/guias/lleva-tu-negocio-a-internet/ciberseguridad-uno-de-los-retos-que-dejo-el-2020/

4.4 ANTECEDENTES O ESTADO ACTUAL

Teniendo en cuenta que en el país “El 60% de las pequeñas y medianas empresas en Colombia no pueden sostener sus negocios luego de sufrir ataques informáticos, el agravante de esta realidad es que las pymes no poseen de sistemas robustos de ciberseguridad, lo que las hace el blanco preferido de los ciberdelincuentes que a diario las atacan[14]”. Las pymes no tienen la capacidad para la adquisición de servicios de protección de los datos en los equipos en la cual desarrollan la gestión comercial y este es un punto que no tienen en cuenta se puede invertir en equipos para el trabajo remoto, pero no invierten en la consultoría de expertos en Seguridad Informática.

En materia de ciberseguridad según “Comparitech, un portal web dedicado en ciberseguridad Colombia ocupa el puesto 40, entre 76 países analizados en el 2020”. “Argelia es el país menos ciberseguro del mundo esto debido a falta de legislación en materia de ciberseguridad y el país liderado es Dinamarca con un mejor puntaje esto debido a las políticas de ciberseguridad implementadas y las cifras de ciberataques son bajas”[15]. En Colombia es necesario mejorar el indicador de ciberseguridad mediante el aumento de soporte que necesitan las pymes en políticas de protección frente a los ciberdelincuentes que no vean afectadas las operaciones comerciales trabajando de manera remota desde casa.

“Unos 28.827 incidentes informáticos se registraron en Colombia durante el 2019, las más afectadas fueron las pymes, según datos de la Cámara Colombiana de Informática y Telecomunicaciones (CCIT)[16]”. Esto se debió a los nuevos canales de comunicación y comercial sin la debida protección frente a los ciberdelincuentes

[14] Py+ Equipo Editorial Py+, Bloquee a los ladrones, active la ciberseguridad en su pyme; [información en linea], recuperado de; https://www.pymas.com.co/ideas-para-crecer/ayuda-legal/ciberseguridad-pymes-colombia
[15] Vanguardia ¿Cómo va Colombia en materia de ciberseguridad?, [reporte en línea], abril 19, 2021, recuperado de; https://www.vanguardia.com/tecnologia/como-va-colombia-en-materia-de-ciberseguridad-MD3656079
[16] TicTac, Cámara Colombiana de Informática y Telecomunicaciones, CCIT, Tendencias del Cibercrimen en Colombia 2019-2020, [en línea], octubre 2019, recuperado de; https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

mediante la ingeniería social en la cual los ciberdelincuentes generan estrategias para engañar a los usuarios y este sector es uno de los más afectados.

De acuerdo con CCIT: “El fraude BEC, los ataques de Ransomware, las oleadas de Malware, las ciberextorsiones entre otras amenazas vienen afectando la cadena productiva de las empresas, y por ello es importante conocer las tipologías y modalidades que utiliza el Cibercrimen en Colombia”. Las amenazas que enfrentan las pymes es el diario vivir este sector que surge como fuente de empleo necesita el apoyo de expertos en ciberseguridad para minimizar los ciberataques en donde no se vean afectados.

Ransomware es el mayor riesgo que presentan las pymes los delincuentes informáticos mediante engaños secuestran la información del computador del teletrabajador a cambio de pagar por la devolución. Denegación de Servicios DDOS: El más conocido que imposibilita el funcionamiento de portales web donde las pymes ofrecen productos y/o servicios que ofrecen en los sitios web los empleados y usuarios pueden verse afectados porque la denegación del servicio puede ocasionar pérdidas económicas y el prestigio de las pymes.

4.5 EL MARCO LEGAL

Es importante tener en cuenta los recursos legales en la actividad económica de las pymes además los documentos, leyes y acuerdos en la ciberseguridad en la cual este sector puede contar con el apoyo de expertos en seguridad informática.

El documento Conpes 3701[17] aporta en contrarrestar el incremento de los ciberataques que pueden afectar la seguridad informática al país en todas las

[17] Consejo Nacional de Política Económica y Social, República de Colombia, Departamento Nacional de Planeación, Lineamientos de Política para Ciberseguridad y Ciberdefensa. Documento CONPES 3701, [documento en línea], recuperado de; https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

organizaciones públicas y/o privadas para las pymes es necesario generar la confianza que necesitan para el desarrollo de las actividades de comercio.

El comercio electrónico en los últimos años se ha incrementado gracias a la ley 527 de 1999[18] Según la ley "la cual reglamentó este tipo de escenarios mediante las TIC's en donde se establecen, además, las organizaciones que permiten generar la certificación por el Organismo Nacional de Acreditación en Colombia – ONAC." Esta ley permite la regulación del comercio electrónico, la firma digital, la entidad certificadora y el intercambio electrónico de datos para las pymes es importante la citada ley en donde deja las bases en la actividad económica.

La protección de los datos es primordial la ley estatutaria 1266 de 2008[19] Según la ley "reglamenta la administración de la información en las bases de datos almacenadas desde el punto de vista financiero, crediticio, comercial, de servicios, entre otros". Para las pymes es importante esta ley porque aporta la fortaleza en la administración de los datos en las pequeñas y medianas empresas en la respectiva ciberseguridad frente a los ataques de los delincuentes cibernéticos.

El Congreso de la República de Colombia mediante la ley 1273 de 2009[20] Según la ley la cual "permite fortalecer la seguridad informática en el país en donde pueden sancionar económicamente y cárcel a los ciberdelincuentes que incurren en delitos informáticos". En las pymes gracias a esta ley permite fortalecer los sistemas de información donde se basan en la tecnología de la información y las comunicaciones TIC's teniendo en cuenta los tres pilares de la seguridad informática la confidencialidad, integridad y la disponibilidad.

[18] Red Jurista, Ley 527 de 1999, [documento en línea], agosto 21 de 1999, Diario Oficial, recuperado de; https://www.redjurista.com/Documents/ley_527_de_1999_congreso_de_la_republica.aspx#/
[19] Red Jurista, Ley estatutaria 1266 de 2008, [documento en línea], diciembre 31 de 2008, Diario Oficial, recuperado de; https://www.redjurista.com/Documents/ley_1266_de_2008_congreso_de_la_republica.aspx#/
[20] Daccach T., J. Empresa Digital, Ley de Delitos Informáticos en Colombia, Ley 1273 de 2009, [documento en línea], 2023, recuperado de; https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/#:~:text=La%20Ley%201273%20de%202009,legales%20mensuales%20vigentes%5B1%5D

La protección de los datos es primordial en las pymes gracias a la Ley 1581 de 2021[21] Según la ley “permite la protección de los datos personales que busca en preservar la información de los usuarios a terceras personas para evitar demandas penales a las pymes y la Superintendencia de Industria y Comercio SIC es la entidad que vigila a las pymes que se cumpla estrictamente de acuerdo con las normas y los tratados internacionales”. La Superintendencia de Industria y Comercio – SIC es la entidad delegada por el gobierno y el congreso de la república de Colombia en proteger a los usuarios en materia de protección de los datos que se cumpla estrictamente los datos no pueden ser compartidos ni vendidos a terceros.

[21] Superintendencia de Industria y Comercio – SIC, Ley 1581 de 2021, [en línea],2021, recuperado de; https://www.sic.gov.co/preguntas-frecuentes-pdp

5 ESTABLECER LOS FACTORES DE RIESGOS DE CIBERSEGURIDAD PRESENTADOS EN EL TELETRABAJO ACTUALMENTE EN COLOMBIA QUE PERMITAN IDENTIFICAR VECTORES DE AMENAZAS PERSISTENTES.

La preocupación que afrontan las pymes en Colombia son los riesgos que viven a diario en la gestión comercial con los ciberataques al trabajar por fuera del entorno laboral mediante la conectividad desde los hogares. Los equipos desactualizados a nivel de hardware, software y el poco conocimiento en materia de ciberseguridad. Los ciberdelincuentes mediante la ingeniería social y otras estrategias tienen como objetivo de engañar a los teletrabajadores que no tienen conocimientos en materia de seguridad informática ocasionando el daño a los sistemas, la alteración, robo de información, entre otros. La falta de atención a las políticas en ciberseguridad lleva consigo la pérdida de información en las pymes y pone en amenaza la información de los clientes. Actualmente existen tres factores de riesgo a nivel tecnológico, humano y ambientales:

5.1 A nivel de Tecnológico

El uso de equipos tecnológicos desactualizados en los drivers de computadores de escritorio, portátiles y los equipos de comunicaciones desde los hogares por desconocimiento de los teletrabajadores puede ocasionar una entrada trasera a los ciberdelincuentes en donde pueden atacar la infraestructura tecnológica en las pymes de manera remota y así manipular la información confidencial de los clientes en las pymes afectando la gestión comercial. La figura 1 los dispositivos electrónicos como herramientas de trabajo y hace parte de la vida cotidiana de los teletrabajadores como los computadores de escritorio, portátiles, Smartphone, entre otros son los elementos en la cual los teletrabajadores realizan la gestión comercial en las pymes en Colombia.

Figura 1. Dispositivos Electrónicos

Fuente: ACTUALIDAD. ¿Cómo nos afecta la tecnología en la vida cotidiana? [imagen] Disponible en: https://medium.com/@jorge.nicho/actualidad-c%C3%B3mo-nos-afecta-la-tecnolog%C3%ADa-en-la-vida-cotidiana-ba410b91d753

5.1.2 A nivel Software. Los sistemas operativos requieren de actualizaciones periódicas, en la cual los teletrabajadores no atienden los requerimientos y esto ocasiona que los dispositivos no estén actualizados a nivel de software, como tampoco en el antivirus pueden verse afectados por los ciberdelincuentes y en no prestar atención en las recomendaciones de seguridad a nivel de software ocasionan las siguientes consecuencias:

- Virus informáticos son programas realizados por programadores entusiastas con el fin de conocer, pero llegan afectar el funcionamiento del computador mediante aplicaciones maliciosas desde la web, el correo electrónico y mensajes en cadena.

- Uso de sistemas no autorizados en los equipos que ingresan alterando la información. Los ciberdelincuentes pueden ingresar a la infraestructura tecnológica afectando los datos y las comunicaciones.

- Robo de información el uso de la ingeniería social buscando engañar a los usuarios. Esto lo realizan mediante falsas páginas web, correos electrónicos con falsos enlaces, entre otros.

- Fraudes digitales como estafas o el uso de enlaces enviados por correo electrónico. Los usuarios al no tener cuidado sobre la información de dudosa procedencia pueden acceder robando la de mayor importancia.

- Suplantación de identidad los ciberdelincuentes lo utilizan para suplantar los datos de los teletrabajadores afectando la información. Esto se realiza cuando los sistemas no tienen aplicaciones que permitan alertar a las pymes sobre los delincuentes informáticos en tiempo real.

- Denegación de Servicios (DoS) como su nombre lo indica es la negación de los servicios en las aplicaciones web. Los delincuentes informáticos realizan este tipo de ataque mediante el uso de la dirección IP pública (la IP es la identificación física de un sitio web) al crear un comando realizando múltiples peticiones al servidor web se forma un cuello de botella y esto ocasiona la suspensión de los servicios web.

- Alteración de la información los ciberdelincuentes pueden acceder, dañar, alterar o modificar la información. Son ocasionados por exempleados de las pymes que facilitan los ingresos a un tercero para adulterar, secuestrar la información de los usuarios.

5.1.3 Las principales amenazas a nivel de software. El software de dudosa procedencia sea libre o licenciado tiene como objetivo de evadir la seguridad del sistema operativo y esto puede llegar afectar la gestión comercial teniendo en cuenta los riesgos que las organizaciones deben enfrentar. Las agencias de ciberseguridad mediante boletines informativos los riesgos que llevan a las pymes el uso de aplicaciones dudosas. Figura 2 las amenazas de software las pymes continúan instalando aplicaciones gratuitas o demos sin tener en cuenta las amenazas que ocurren a continuación:

Figura 2. Amenazas de Software.

Fuente: ARROBA SYSTEM. ¿Qué son las amenazas informáticas y cómo protegerte de ellas?, [imagen]. Disponible en; https://arrobasystem.com/blogs/blog/que-son-las-amenazas-informaticas-y-como-protegerte-de-ellas

- **Spyware** (Programas espías) es un código malicioso que tiene como objetivo revisar y recoger toda la información de los usuarios de los equipos por ejemplo es las instalaciones o archivos de dudosa procedencia pueden espiar las actividades que realicen los teletrabajadores.

- **Troyanos, virus y gusanos** son códigos maliciosos que atacan con el objetivo de ingresar a los computadores de manera remota que tiene como fin negar servicios y afectar las actividades cotidianas de las pequeñas y medianas empresas. Los virus llegan a infectar los computadores mediante el uso de memorias usb o el uso del correo electrónico pueden llegar en afectar la información de la gestión comercial de las pymes.

- **Phishing:** Los ciberdelincuentes mediante el uso de la ingeniería social engañando a los usuarios con el fin de obtener las credenciales de los usuarios donde no tienen conocimiento de esta clase de virus. Esta modalidad de riesgo en la web para las pymes es que obtienen la información de segundo plano de los usen este caso los teletrabajadores.

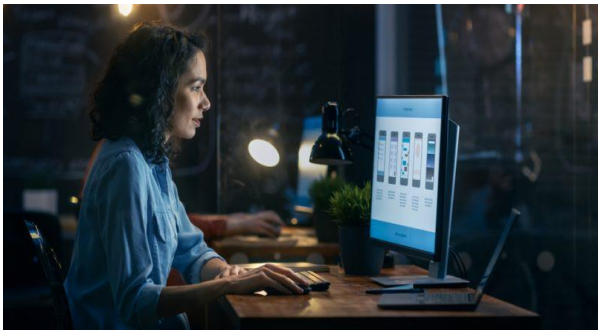
- **Spam:** Es el recibo de mensajes no autorizados mediante el correo electrónico con publicidad. Estos mensajes instantáneos de publicidad

pueden llegar a contener información de manera fraudulenta en busca de captar datos de los usuarios.

- **Ransomware:** Es una clase de malware representa un alto riesgo para los usuarios y los equipos tecnológicos que usan para el teletrabajo. Ransomware significa rescate extorsivo que buscan los ciberdelincuentes con el fin de afectar a las organizaciones. Ejemplo de ataque es por medio de correos con archivos adjuntos como Word, Excel, PowerPoint, PDF, entre otros en donde puede estar oculto el código malicioso.

5.1.5 A nivel de Humanos. Los usuarios sin el conocimiento de la ciberseguridad en las pequeñas y medianas empresas corren un riesgo de ser víctimas por el desconocimiento de la normatividad, leyes y/o decretos en materia de ciberseguridad, donde son blanco fácil de los ciberdelincuentes por medio de la ingeniería social. Figura 3 Usuarios finales la falta de capacitación en materia de la ciberseguridad por parte de las directivas puede llevar hasta el cierre de las pymes por ataques en las cuales no se pueden recuperar en materia de información de la gestión comercial.

Figura 3. Usuarios Finales.



Fuente: CONCEPTO, Usuario. [imagen]. Disponible en: https://concepto.de/usuario/

5.1.5 Los teletrabajadores en las pymes pueden verse afectados. Los teletrabajadores es el equipo indiscutible en las pymes donde aportan conocimiento desde las diferentes disciplinas en el sector comercial, son dinámicos y generan estrategias de mercado frente a la competencia. Utilizan aplicaciones que desde las pequeñas y medianas empresas para el registro de la gestión diaria. En el trabajo remoto pueden verse afectados por la suplantación, filtración, robo de información por delincuentes informáticos que buscan afectar los equipos que utilizan los trabajadores.

5.1.6 Desconocimiento de políticas de ciberseguridad. La falta de conocimiento en las políticas en materia de ciberseguridad puede ocasionar graves problemas a nivel jurídico como el prestigio en la imagen. Cuando son víctimas de ataques cibernéticos en las pymes tienden a estar en estadísticas en los informes de las agencias de seguridad informática a nivel internacional. Las pymes tienen la obligación de buscar el apoyo del equipo de TI Tecnología de la Información en que les informen acerca de las últimas novedades en materia de ciberdelitos.

5.1.7 Falta de conocimiento de los tipos de ciberdelitos. A diario las autoridades expertas en ciberseguridad informan los diversos tipos de ciberdelitos que existen y pueden afectar la gestión comercial de las pymes. Figura 4 Modalidad de delitos informáticos los ciberdelitos comunes son:

- Robo de información el uso de la ingeniería social buscando engañar a los usuarios. El ejemplo típico es las historias que inventan los ciberdelincuentes para llamar la atención mediante información y hasta pedir donaciones en efectivo para llevar a fundaciones ficticias.

- Suplantación de Identidad los ciberdelincuentes lo utilizan para suplantar los datos de los teletrabajadores afectando la información. Ejemplo los delincuentes informáticos logran obtener los datos para realizar compran a nombre de las victimas a pesar de que las entidades financieras llamen a los usuarios reales.

- Explotación Infantil bandas de delincuentes cibernéticos utilizan la información de los hijos de los teletrabajadores con fines extorsivos. Los niños pueden ingresar a páginas web de videojuegos en línea sean gratuitas o por suscripción pueden ingresar al equipo y copiar la información del equipo.

- Software Falsificado instalación de software de dudosa procedencia instalado en segundo plano. Esto ocasiona un alto riesgo para las pymes porque a menudo pueden dejar defectos en la seguridad de los equipos deja la puerta trasera para los ataques cibernéticos.

- Uso de computadores públicos: Los usuarios pueden cometer el error de consultar la información financiera desde un computador de uso público ejemplo los cibercafés no son seguros de usar por el alto tráfico de usuarios que asisten al establecimiento donde terceras personas instalan keylogger que es un software malicioso que capta y guarda los datos guardados para ocasionar diferentes delitos como la extorsión.

- Fraudes por redes sociales falsos grupos con fines de obtener información personal. Ejemplo el servicio de atención al cliente mediante medios electrónicos como las redes sociales es riesgoso porque falsos asesores pueden obtener los datos personales.

- Carding es la estrategia de los ciberdelincuentes con el objetivo de obtener los datos de las tarjetas de crédito a la hora de la realización de transferencias online. Ejemplo copian y falsifican los datos de los usuarios de manera fraudulenta por los delincuentes informáticos para la realización de pequeñas compras diarias sin dejar sospechas.

- Suplantación de correo corporativo los ciberdelincuentes por medio de la ingeniería social con el fin de los teletrabajadores caigan en la trampa. Ejemplo la creación del medio electrónico falsificado donde los usuarios envían los correos y es una trampa establecida por los delincuentes informáticos para obtener información.

Figura 4. Modalidad de Delitos Informáticos.

Fuente: UNAD. Nueva modalidad de delitos informáticos en Colombia. [imagen], Disponible en: https://noticias.unad.edu.co/index.php/unad-noticias/todas/93-gidt/2333-nueva-modalidad-de-delitos-informaticos-en colombia#:~:text=Dentro%20de%20las%20modalidades%20con,trav%C3%A9s%20de%20correos%20electr%C3%B3nicos)%20y

5.1.8 Falta de conocimiento y formación. Los teletrabajadores en Colombia no tienen conocimiento ni mucho menos en la formación en materia de ciberseguridad.

Figura 5 Falta de capacitación las pymes presentan un riesgo por el desconocimiento en el personal que apoya la gestión comercial.

Figura 5. Falta de Capacitación.

Fuente: PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ, Curso de Capacitación en Ciberseguridad y Hacking Ético con Software Open Source. [imagen]. Disponible en: https://cetam.pucp.edu.pe/curso/curso-capacitacion-ciberseguridad-hacking-etico/

5.1.9 A nivel Ambiental. Los fenómenos ambientales como:

- Tormentas eléctricas (Instalaciones sin pararrayos). Los hogares de los teletrabajadores no tengan sistemas contra tormentas eléctricas a excepción los que vivan en edificaciones de más de cuatro pisos.

- Terremotos. (Instalaciones en alto riesgo). Las instalaciones de las pymes que no sean sismo resistente a los terremotos y réplicas de acuerdo a los materiales que fueran construidas.

- Inundaciones. (Falta de sistemas de drenaje de aguas lluvias). Las oficinas de las pymes donde los teletrabajadores están ubicados en zonas de inundaciones o calles canal de lluvias.

- Incendio. (Cortocircuitos o intencionados y falta de equipos contraincendios). Las oficinas de las pymes de los teletrabajadores sean propensas a incendios

de acuerdo a las instalaciones eléctricas no cuenten con sistemas de extinción del fuego.

- Saboteo intencional (Destrucción de las instalaciones personal interno o externo). Exempleados inconformes o despedidos pueden afectar los sistemas que cuentan las pymes como sistemas de cómputo, telecomunicaciones y eléctricos.

6 REVISAR LA NORMATIVIDAD, LEGISLACIÓN Y DOCUMENTOS DE BUENAS PRÁCTICAS QUE POSIBILITAN Y GARANTIZAN EN TÉRMINOS DE CIBERSEGURIDAD EL TELETRABAJO EN COLOMBIA.

El desarrollo del teletrabajo en Colombia se basa en la revisión de los artículos, leyes, decretos, acuerdos internaciones, convenios que aportan los expertos en ciberseguridad mediante las buenas prácticas para el desarrollo de las pymes en el país y contrarrestar a los delincuentes informáticos.

6.1.1 Teletrabajo. El teletrabajo[22] en Colombia está definido por la Ley 1221 de 2008 como "forma de organización laboral mediante el uso de las tecnologías de la información y las comunicaciones – TIC mediante el desempeño de las actividades asignadas remuneradas o mediante la orden de prestación de servicios en donde no se requiere la presencia física del teletrabajador." Esta ley permite a los teletrabajadores el concepto que actores participan y el medio tecnológico para la realización de trabajo remoto.

6.1.2 Regulación del teletrabajo en Colombia. En la actualidad el teletrabajo en Colombia se encuentra regulado por la Ley 1221 del 2008 y el decreto 884 del 2012.

- **Ley 1221 de 2008**

Se reconoce el teletrabajo en Colombia como una modalidad de empleo en el país en donde se fomenta la política pública para la población vulnerable, en donde se genera la red nacional de fomento en donde se socializa y donde se establecen garantías.

- **Decreto 884 de 2012**

[22] Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, ¿Qué es el teletrabajo?, [en línea], marzo 12 de 2020, recuperado de; https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/126148:Todo-lo-que-se-debe-saber-sobre-el-teletrabajo#:~:text=En%20Colombia%2C%20el%20teletrabajo%20se,para%20el%20contacto%20entre%20el

Establece las condiciones laborales que rigen el teletrabajo, la dependencia y las relaciones de los empleadores y teletrabajadores, así como las responsabilidades en las organizaciones públicas y privadas, las administradoras de riesgos laborales – ARL y la red de fomento para el trabajo.

A continuación, leyes, decretos y acuerdos de cooperación

6.2.1 Leyes

6.2.2 El comercio electrónico Ley 527 de 1999. Mediante la ley se reglamenta el acceso y el uso de la información para el fomento del comercio electrónico y el uso de las firmas digitales, entre otros. Esta ley fomenta la regulación de la actividad económica mediante el uso de las TIC que se realiza a través de internet.

6.2.3 Código Penal Colombiano Ley 599 de 2000. Se trata de "violación ilícita de comunicaciones" es un delito que determina acerca de "Acceso abusivo a un sistema informático" de acuerdo con el Artículo 195 "El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa". Es un delito que es castigado penalmente el que altere, manipule o destruya información mediante el ingreso de manera fraudulenta.

6.2.4 Habeas Data Ley 1266 de 2008. Se establece el uso del habeas data y la regulación de la información en los sistemas de información como los datos personales de los usuarios a nivel financiero, comercial, servicios, entre otros.

6.2.5 Delitos Informáticos Ley 1273 de 2009. La ley de los delitos informáticos está presente en el Código Penal Colombiano denominado "de la protección de la información y de los datos". En la ley mencionado se determinan los diferentes delitos informáticos como el ingreso a sistemas no autorizado, copiar información,

suplantar usuarios, entre otros. Cada delito está penalizado y sancionado económicamente.

6.2.6 Protección de Datos Personales Ley 1581 de 2012. La protección de los datos está bajo la supervisión de la Superintendencia de Industria y Comercio es la entidad asignada que vigila y sanciona a las empresas que afecten los datos personales de los usuarios.

6.3.1 Decretos

6.3.2 Gobierno en Línea Decreto 2693 de 2012. El Estado bajo el manual de Gobierno en Línea, permite la autogestión en los lineamientos que deben establecer las organizaciones públicas y privadas que se fundamentan en las funciones administrativas bajo la implementación en Colombia.

6.3.3 Protección de Datos Personales Decreto reglamentario 1377 de 2013. Este decreto autoriza al administrador de la información en el tratamiento de los datos personales, bajo las políticas de responsabilidad y encargados por ser los titulares de la información.

6.4.1 Acuerdos

6.4.2 Acuerdo CONPES 3701 de 2011[23]. En el acuerdo se establecen las políticas de ciberseguridad y ciberdefensa que permite generar estrategias por el incremento de las amenazas que afecta de manera directa al país. El problema central se basa en la capacidad actual del Estado para enfrentar los ciberataques. Gracias a este acuerdo se permiten establecer las causas y efectos la cual generan estrategias

[23] Concejo Nacional de Política Económica y Social, Documento Conpes 3701, Lineamientos de Política para ciberseguridad y ciberdefensa. [documento en línea], julio 14 de 2011, recuperado de; https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

para la disminución de las amenazas cibernéticas. El uso de las tecnologías de información y las comunicaciones es el camino del avance de la economía como las pymes, pero es necesario minimizar los ciberdelitos mediante el apoyo de Estado.

Este acuerdo permite la creación de la comisión intersectorial ColCERT el grupo de respuesta a emergencias cibernéticas de Colombia. es el equipo coordinador a nivel nacional en los aspectos de seguridad informática gracias a esta asociación participan dos unidades de ciberdefensa: Comando Conjunto Cibernético equipo encargado de la Defensa del país en el ciberespacio y el Centro Cibernético Policial equipo encargado de la Seguridad ciudadana en el ciberespacio mediante vigilancia 24 horas al día los 7 días de la semana.

ColCERT es la estrategia de seguridad nacional donde participan los organismos judiciales, el Ministerio de Defensa Nacional es el coordinador de emergencias mediante con los organismos del Estado, la academia y el sector privado.

En el sector de las pymes buscan mecanismos de protección frente a los ciberdelincuentes gracias al este acuerdo no están desprotegidos y cuentan con el Ministerio de Defensa Nacional teniendo en cuenta las políticas nacionales e internacionales de la ciberseguridad.

6.4.3 Marco de Ciberseguridad del NIST[24]. NIST significa Instituto Nacional de Estándares y Tecnología. Este marco nace en el departamento de comercio de los Estados Unidos. El NIST ayuda a los negocios como deben comprender mejor los riesgos en ciberseguridad en las pequeñas empresas, administrar y reducir sus riesgos, y proteger sus redes y datos. Este marco es voluntario en el marco de la

[24] Comisión federal de comercio, Marco de ciberseguridad del NIST, [en línea], recuperado de; https://www.ftc.gov/es/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework-es.pdf

ciberseguridad la cual tiene como objetivo de reducir los riesgos, y proteger las redes y datos parte de cinco puntos importantes que son:

1. **Identificación.**

Las pymes deben realizar un listado tecnológico de equipos y el software la cual realizan la gestión comercial computadores portátiles, smartphones, tabletas, entre otros.

Las funciones y responsabilidades de los teletrabajadores, proveedores y el personal autorizado a la información delicada.

Proteger y minimizar frente a los ciberataques limitando los daños.

2. **Protección.**

Controlar el acceso a la red de la pyme.

Programas para protección de los datos.

Realización de copias de seguridad programadas.

Implementación de la ISO 270001.

Capacitar sobre ciberseguridad al todo el personal.

3. **Detección.**

Monitoreo de los computadores para el control de personal no autorizado el uso de medios de almacenamiento USB y software.

Revisión de la red corporativa de la pyme.

Investigar mediante auditorías la usabilidad de la red.

4. Respuesta.

Informar a los empleados y cliente de la pyme.

No suspender las operaciones comerciales.

Informar a las autoridades de ciberseguridad y ciberdefensa.

Investigar y resistir a los ciberataques.

Informar por actas los ciberataques y el uso de la política de la protección de los datos.

Alistarse frente a los eventos de la naturaleza que pueden poner en riesgo los datos.

5. Recuperación.

Después del ciberataque:

Reparar la infraestructura tecnológica, la red y los equipos de cómputo afectados.

Informar al equipo de teletrabajadores y los clientes mediante boletines de seguridad y respuesta.

6.4.4 CompTIA y NICE:[25] Estableciendo las normas para lograr prácticas cibernéticas seguras. NICE Iniciativa nacional de Educación en Seguridad Cibernética. Se basa en el Instituto Nacional de Estándares y Tecnología NIST es una alianza del gobierno de los Estados Unidos, las universidades y el sector privado quienes se enfocan a la educación y seguridad cibernética y en el desarrollo personal. Las certificaciones como CompTIA A+, Network+, Security+, CySA+ y CASP en donde se establecen las mejores prácticas de ciberseguridad mediante las directivas como FISMA y DoD 8570/8140.

En la gestión del teletrabajo en Colombia las pymes en el área de soporte técnico las siguientes fases con las respectivas especialidades:

Investigar

Las áreas de la especialidad que son responsables de detectar y analizar eventos cibernéticos y/o delitos de sistemas de TI, redes y evidencia digital. La investigación que deben hacer el equipo de soporte técnico de las pymes es basada en la informática forense y la investigación cibernética.

Supervisar y Gobernar

Proporciona, liderazgo gestión, dirección o desarrollo y defensa para que la organización pueda realizar el trabajo de seguridad cibernética de manera efectiva. Es necesario tener en cuenta la gestión y adquisición de programas y/o proyecto, planificación estrategia y política, gestión de la ciberseguridad y también la capacitación, educación y conciencia.

[25] CompTIA y NICE: Estableciendo el estándar para prácticas cibernéticas seguras, [en línea], recuperado de; https://www.comptia.org/content/tools/comptia-and-the-national-initiative-for-cybersecurity-education

Proteger y defender

Áreas de especialidad responsables de la identificación, análisis y mitigación de amenazas a los sistemas o redes de TI internas. El área de soporte técnico de las pymes debe tener en cuenta el análisis de defensa informática, soporte de infraestructura de ciberdefensa, respuesta al incidente y la evaluación y gestión de las vulnerabilidades.

Operar y mantener

Áreas de especialidad responsables de brindar el soporte, la administración y el mantenimiento necesario para garantizar un rendimiento y seguridad efectivos y eficientes del sistema TI. El área de soporte técnico de las pymes tiene la responsabilidad de tener operativo y mantener la infraestructura tecnológica frente a los ciberdelitos. Debe tener en cuenta la atención al cliente y soporte técnico, administración de datos, servicios de red, conocimientos administrativos, administración del sistema y análisis de seguridad de sistemas.

Provisión segura

Áreas de especialidad relacionadas con la conceptualización, el diseño y la construcción de sistemas de TI seguros, con responsabilidad sobre algún aspecto del desarrollo de los sistemas. El área de soporte técnico de las pymes debe tener las siguientes especialidades: La gestión de riesgos, desarrollo de software, la arquitectura de sistemas, desarrollo de sistemas, planificación de requisitos de sistemas, I+D en tecnología y prueba y evaluación.

Analizar

Áreas de especialidad responsables de la revisión y evaluación altamente especializadas de la información de seguridad cibernética entrante para determinar su utilidad para la inteligencia. Esta área de soporte técnico de las pymes es importante que se deben cumplir con las siguientes especialidades: Análisis de todas las fuentes, análisis de explotación y análisis de amenazas.

Recoger y operar

Áreas de especialidad responsables de operaciones especializadas de denegación y engaño y recopilación de información de ciberseguridad que pueden usarse para desarrollar inteligencia. El equipo de soporte técnico de las pymes debe investigar casos de ciberataques mediante: la planificación operativa cibernética, operaciones de cobranza y operaciones cibernéticas.

6.4.5 Acuerdo internacional de Budapest frente a los ciberdelincuentes. Este acuerdo permite a Colombia en intervenir en las políticas de ciberseguridad. La nación debe asumir por principio de autoridad mediante del derecho penal en la cual se puede sancionar y/o castigar penalmente los delitos informáticos cometidos para la prevención.

En la actualidad Colombia se basa en varias organizaciones que trabajan de manera conjunta contra el delito informático las organizaciones contra los ciberdelitos permiten la realización de investigaciones en el reporte y solución de vulnerabilidades que permiten generar confianza que permitan una acción penal en el reporte de fallas en los sistemas informáticos.

6.4.6 Entidades del Estado de vigilancia y control en ciberseguridad en Colombia en las pymes en Colombia

- **Superintendencia de Industria y Comercio en Ciberseguridad**

La Superintendencia de Industria y Comercio en la entidad del estado encargado de vigilar y cumplir con las políticas en protección de los datos y sanciona a las pymes que no cumplan con la ciberseguridad a nivel económico. La entidad emite guías o folletos en materia de protección en ciberseguridad y apoya a las agencias de seguridad.

- **Policía Nacional Ministerio de Defensa**

La Policía Nacional de Colombia del Ministerio de Defensa tiene un equipo de Respuesta a Incidentes de Seguridad Informática CSIRT – PONAL es la unidad dedicada a seguimiento y control a los ciberdelitos de acuerdo con las leyes, decretos y acuerdos nacional e internacional en materia de ciberseguridad.

- **El teletrabajo MinTIC, Mintrabajo y Colombia Digital**

El punto débil de los ciberataques, son los empleados. Los ataques están a un clic, pero es necesario que los teletrabajadores en las pymes deben tener en cuenta las siguientes recomendaciones:

- Conexión a una VPN (Virtual Private Network) red privada virtual directa con las pymes en donde pueden realizar el teletrabajo con toda seguridad.
- Usar claves fuertes, complejas, difícil de descifrar por los ciberdelincuentes.
- No aceptar correos electrónicos de dudosa procedencia.
- No ingresar a ningún enlace dudoso.

Entes de control de buenas prácticas en las pymes en Colombia.

- La Superintendencia de Industria y Comercio.
- Cámara Colombiana del Comercio Electrónico.
- MinTIC.

6.4.7 ISO 27001[26]: Seguridad de la Información

La Organización Internacional de Estandarización (ISO), mediante la ISO 27001 permite la preservación de la información en este caso las pymes. Los requisitos de la Norma ISO 27001 del Sistema de Gestión de la Seguridad de la Información (SGSI) permite preservar la:

Confidencialidad – Integridad – Disponibilidad de la información.

La implementación de la norma ISO 27001 en las pymes mediante siete pasos:

1. **Identificar los activos de la información.** El activo de las pymes elementos de valor como la información, equipos tecnológicos, bienes físicos e intelectual.

2. **Identificar las vulnerabilidades.** Las debilidades que puedan sufrir las pymes sea a nivel físico los equipos tecnológicos y/o aplicaciones que estén usando en la gestión comercial.

3. **Identificar las amenazas.** Verificar aquellas que puedan afectar la operación comercial de las pymes oficinas como naturales o provocados con el fin de ocasionar robo de información.

[26] Normas ISO, ISO 27001 Seguridad de la Información [en línea], recuperado de; https://www.normas-iso.com/iso-27001/

4. **Identificar los requisitos legales.** El cumplimento en la protección de los datos de los clientes, teletrabajadores y socios.

5. **Identificar los riesgos.** Establecer el activo que presente las pymes y se analiza la probabilidad de las amenazas o las vulnerabilidades pueda ocasionar daño parcial o total.

6. **Cálculo del riesgo.** Se realiza el proceso de control de la probabilidad que ocurra la amenaza. Donde el (Riesgo = impacto x probabilidad de la amenaza).

7. **Plan de tratamiento del riesgo.** En este punto se realiza la implementación de acuerdo con las fases mencionadas se selecciona los controles que permitan:

    - Asumir el riesgo.
    - Reducir el riesgo.
    - Eliminar el riesgo.
    - Transferir el riesgo.

6.4.8 ¿Qué es el MSPI?[27] Gobierno Digital – MINTIC

El Modelo de Seguridad y Privacidad de la Información – MSPI, se basa en la implementación de lineamientos en las entidades públicas teniendo en cuenta referencia estándares internacionales que permite la (Planeación, Implementación, Evaluación, Mejora Continua) permitiendo implementar la Política de Gobierno Digital.

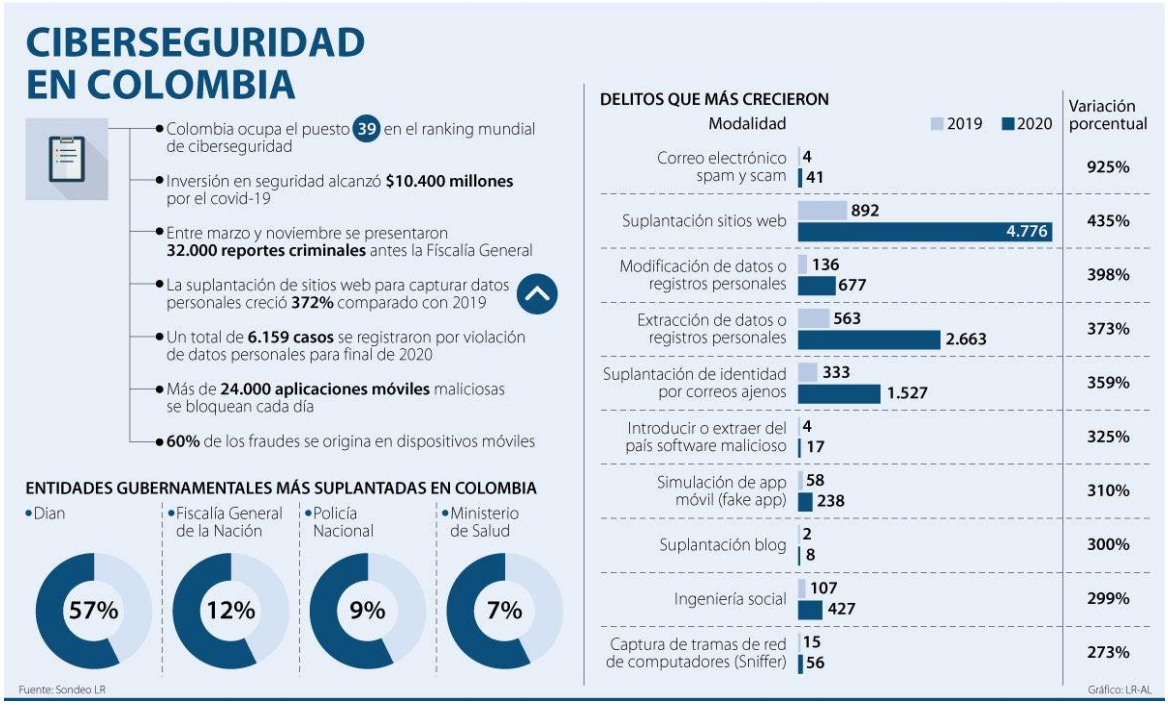
[27] Gobierno Digital, ¿Qué es el MSPI?, [en línea], recuperado de; https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

En las pymes tienen el respaldo de MSPI permite a través del Gobierno Digital proteger la información en los procesos, trámites, servicios, sistemas de información, infraestructura y, en general todos los activos de información teniendo en cuenta la confidencialidad – integridad – disponibilidad y la privacidad de los datos. El sector de las pymes necesita este modelo de seguridad que busca disminuir los ciberataques junto al equipo de soporte técnico y los teletrabajadores de manera conjunta.

7 PRESENTAR UN INFORME DEL ESTADO ACTUAL DE LA CIBERSEGURIDAD, VENTAJAS Y DESVENTAJAS DE LOS DIFERENTES RECURSOS PROPUESTOS POR LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO Y OTROS ENTES DE CONTROL CON RELACIÓN A LA APLICACIÓN DE BUENAS PRÁCTICAS EN EL TELETRABAJO PARA PYMES.

7.1.1 Informe del estado actual de la ciberseguridad. Los delitos que se reportan ante las autoridades frente a los ciberdelitos es la suplantación de sitios web y el robo de los datos los delincuentes informáticos realizan diferentes ataques mediante la ingeniería social. Figura 6 Ciberseguridad en Colombia 2019 – 2020 a través del presente informe se da a conocer la actualidad de la ciberseguridad en las pymes en el país mediante la siguiente figura se muestra el estado en Colombia.

Figura 6. Ciberseguridad en Colombia 2019 - 2020



Fuente: ASUNTOS LEGALES, Ciberdelitos subieron 37% durante el primer trimestre de 2020, en los peores meses de la crisis, 2021 [imagen] Disponible en: https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480

7.1.2 La ciberseguridad en Colombia en estadísticas

- Colombia está ocupa el puesto 39 en el ranking mundial de ciberseguridad.
- La inversión en seguridad alcanzó $10.400 millones de pesos en la pandemia del Covid-19.
- Entre marzo y noviembre de 2020 se presentaron 32.000 reportes de delitos informáticos ante la Fiscalía General de la Nación.
- Se presentaron suplantación de sitios web para capturar datos personales creció 372% comparando con el 2019.
- Se registraron 6.159 casos se registraron por la violación de los datos personales para final de 2020.
- Más de 24.000 aplicaciones móviles maliciosas se bloquean cada día.
- El 60% de los fraudes electrónicos se origina en dispositivos móviles.

7.1.3 Delitos que más crecieron en Colombia. El ciberdelito en Colombia presenta mayor crecimiento en hurtos informáticos desde el año 2019 – 2021 teniendo en cuenta al debido crecimiento del comercio electrónico el cual creció en un 59.4% en todas las transacciones y un 35% durante el año 2021 en ventas de 37 billones de pesos al finalizar el año anterior según datos de la Cámara de Comercio Electrónico de Colombia CCCE.

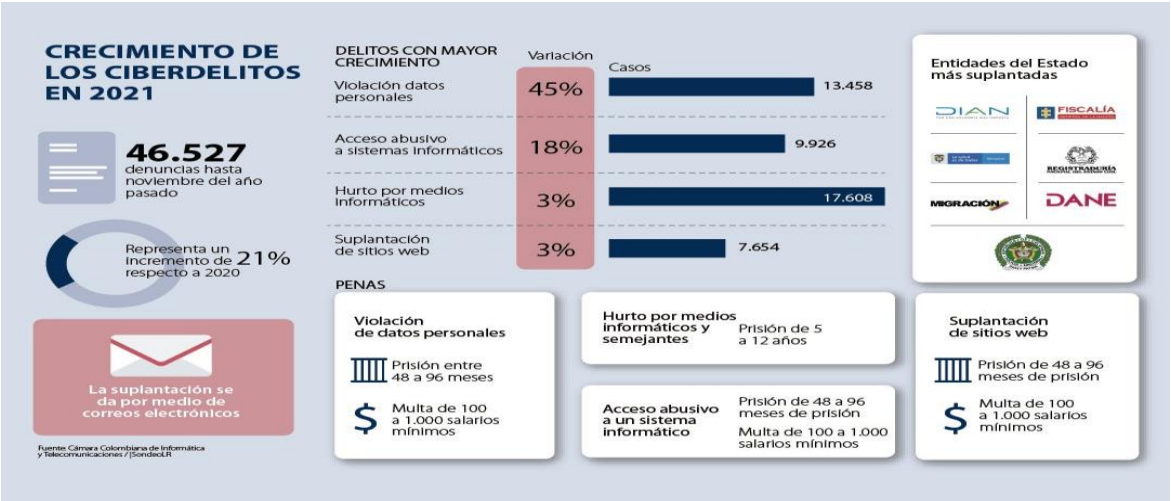
7.1.4 Modalidades. El cibercrimen no descansa cada día afectan a todos los usuarios y esto genera desconfianza del uso de los canales electrónicos en la realización de cualquier gestión a través de la internet. En la actualidad se conocen métodos para afectar la información que almacenen los usuarios. A continuación, delitos denunciados:

- Correo electrónico spam y scam en el 2019 4 casos – 2020 41 casos 925%
- Suplantación sitios web en el 2019 892 casos – 2020 4776 casos 435%

- Modificación de datos o registros personales en el 2019 136 casos – 2020 677 casos 398%
- Extracción de datos o registros personales en el 2019 563 casos – 2020 2663 casos 373%
- Suplantación de identidad por correos ajenos en el 2019 333 casos – 2020 1527 casos 359%
- Introducir o extraer del país software malicioso en el 2019 4 casos – 2020 17 casos 325%
- Simulación de app móvil (fake app) en el 2019 58 casos – 2020 238 casos 310%
- Suplantación blog en el 2019 2 casos – 2020 8 casos 300%
- Ingeniería social en el 2019 107 casos – 2020 427 casos 299%
- Captura de tramas de red de computadores (Sniffer) en el 2019 15 casos – 2020 56 casos 273%

Los ciberdelitos no dan tregua en la Figura 7 Ciberseguridad en Colombia 2021 aumentaron en comparación con los años 2019 y 2020.

Figura 7. Ciberseguridad en Colombia 2021



Fuente: ASUNTOS LEGALES, Conozca las sanciones por los ciberdelitos que más crecieron durante el año pasado. 2022, [imagen], Disponible en: https://www.asuntoslegales.com.co/consumidor/conozca-las-sanciones-por-los-ciberdelitos-que-mas-crecieron-durante-el-ano-pasado-3291291

7.1.4 Entidades gubernamentales más suplantadas en Colombia 2021

- Dian – Dirección de Impuestos y Aduanas Nacionales.
- Fiscalía General de la Nación.
- Ministerio de Salud.
- Registraduría Nacional del Estado Civil.
- Migración Colombia.
- DANE – Departamento Administrativo Nacional de Estadísticas.
- Policía Nacional de Colombia.

7.1.5 Delitos con mayor crecimiento en el 2021. La suplantación de correo electrónico es la vía donde los ciberdelincuentes usan para ocasionar la mayor afectación posible:

- Violación datos personales variación 45% 13458
- Acceso abusivo a sistemas informáticos variación 18% 9926
- Hurto por medios informáticos variación 3% 17608
- Suplantación de sitios web variación 3% 7654

7.1.6 Penas. De acuerdo con la ley 1273 de 2009 estos son las condenas y multas pecuniarias:

- Violación de datos personales prisión de 48 a 96 meses de prisión y la multa de 100 hasta 1000 salarios mínimos.
- Hurto por medios informáticos y semejantes prisión de 5 a 12 años.
- Acceso abusivo a un sistema informático prisión de 48 a 96 meses de prisión y multa de 100 a 1000 salarios mínimos.
- Suplantación de sitios web prisión de 48 a 96 meses de prisión y multa de 100 a 1000 salarios mínimos.

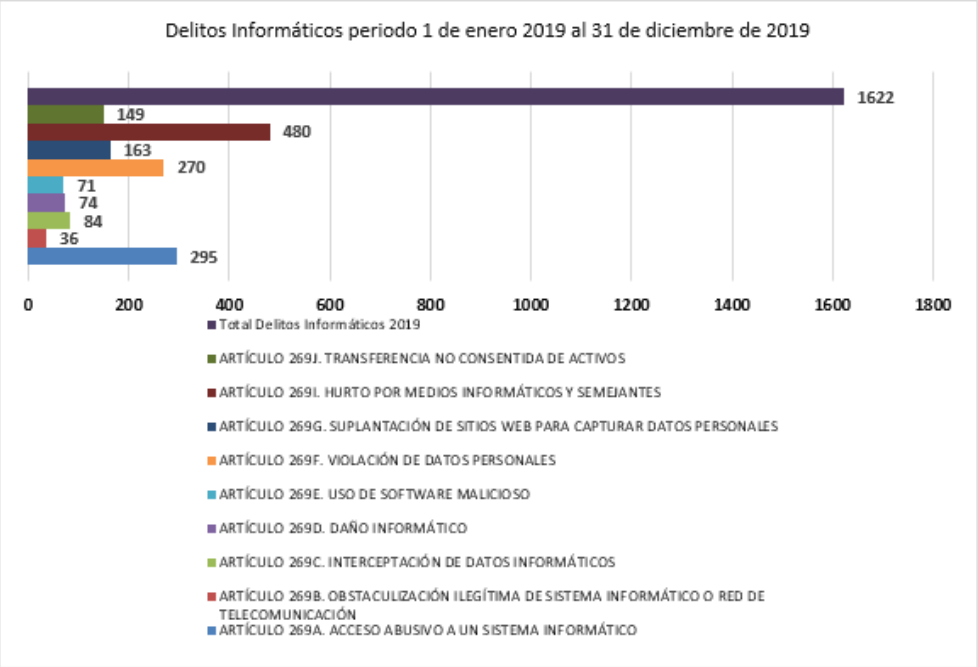
7.1.5 Pymes, vulnerabilidades a ciberataques. Según cifras conocidas por BDO Colombia[28], de acuerdo con el Departamento de Delitos Informáticos de la Policía Nacional de Colombia, el año pasado se recibieron 7.118 denuncias.

"El 43% de las empresas en Colombia no están preparadas para responder y desafortunadamente son las pymes las más vulnerables, ya sea en materia de capacidad instalada o recursos económicos, afirmó Keith Farlinger, CEO para América de BDO internacional. Todas las empresas serán atacadas tarde o temprano, por lo que es necesario involucrar a los funcionarios en una política empresarial que sopese los efectos de los riesgos cibernéticos". De acuerdo con esta afirmación es necesario que las pymes se deben fortalecer en materia de ciberseguridad en tres factores importantes inversión tecnológica, capital humano y protección contra los ciberdelincuentes.

7.1.7 Reportes de delitos informáticos de la Policía Nacional DIJIN. Gráficos 1, 2 y 3 la unidad contra el ciberdelito recibió en las vigencias 2019, 2020 y 2021 los delitos informáticos denunciados por las personas o empresas en los 32 departamentos.

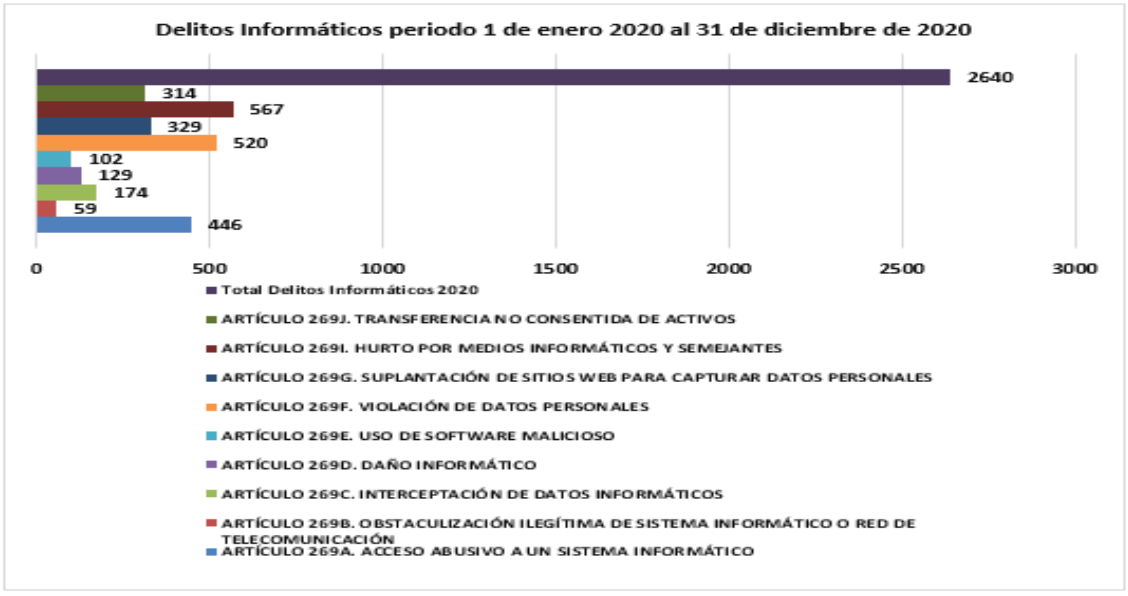
[28] Revista LatinPyme, Pymes, vulnerables a ciberataques [en línea], recuperado de; https://www.latinpymes.com/pymes-vulnerables-a-ciberataques/

Gráfico 1. Delitos Informáticos año 2019



Fuente: Elaboración Propia, con base en, Disponible en; https://www.policia.gov.co/grupo-informacion-criminalidad/estadistica-delictiva

Gráfico 2. Delitos Informáticos año 2020



Fuente: Elaboración Propia, con base en, Disponible en; https://www.policia.gov.co/grupo-informacion-criminalidad/estadistica-delictiva

Gráfico 3. Delitos Informáticos año 2021

Fuente: Elaboración Propia, con base en, Disponible en; https://www.policia.gov.co/grupo-informacion-criminalidad/estadistica-delictiva

7.1.6 Ventajas y Desventajas de SIC y OIT. En el ejercicio del teletrabajo mediante las pymes en Colombia es reconocer los avances en materia de leyes, la tecnología y la importancia de este sector en el desarrollo de la economía.

Superintendencia de Industria y Comercio – SIC[29]

Ventajas

La superintendencia de industria y comercio es la entidad encargada de proteger a los usuarios mediante la ley 1581 del 2012 protección de datos la cual tiene la directriz de sancionar las pymes en el manejo de la información.

- Promueve el empleo formal como estabilidad laboral en alianza mediante las tic's con las pymes.
- Requisitos básicos como persona disciplinada, conocimiento básico en sistemas, capacidad para el trabajo a distancia, entre otros.
- Priorización como padres o madres cabeza de hogar, madres lactantes, personas que habitan en zonas periféricas, personas en condición de discapacidad y/o problemas de salud.

Desventajas

El teletrabajador que no cumpla con la ley de protección de datos puede ser multado y destituido.

- El teletrabajador está obligado a entregar la información sensible a la pyme cuando termine el periodo de trabajo.
- No puede divulgar ni vender la información una vez no tenga continuidad laboral.

[29] Superintendencia de Industria y Comercio – SIC, Procedimiento teletrabajo, [en línea], recuperado de;: https://sigi.sic.gov.co/SIGI/files/mod_documentos/documentos/GT02-P08/versiones//TELETRAB11O_V3_copia_controlada.pdf

- Entregar el equipo asignado en la cual trabajó para la pyme.

Organización Internacional del Trabajo[30]

Ventajas

- El teletrabajo es voluntario para la persona y para la empresa para la cual trabajo en donde puede formar parte de la descripción inicial del puesto de trabajo o puede incorporarse de forma voluntaria más tarde.
- La decisión de incorporar un empleado a la modalidad de teletrabajo debe ser producto debe ser consensuada entre la empresa (eventualmente la gerencia del sector) y la persona.
- Mantenimiento de los derechos y obligaciones de las partes, especificando puesto de trabajo, funciones, dependencia jerárquica, remuneración, derecho de acceso a la formación, capacitación y oportunidades de desarrollo profesional en igualdad de condiciones y posibilidades que las personas que trabajan en forma presencial.

Desventajas

- Se recomienda que las empresas paguen a los teletrabajadores un importe que compense los gastos derivados de la implementación del teletrabajo en su domicilio.
- Afectación de un espacio en el domicilio del teletrabajador.
- Probables cambios en el entorno familiar del teletrabajador.
- Probable mayor consumo de energía eléctrica.

[30] Organización Internacional del Trabajo, Manual de buenas prácticas en teletrabajo, [documento en línea], primera edición 2011, recuperado de; https://ilo.org/wcmsp5/groups/public/---americas/---ro-lima/---ilo-buenos_aires/documents/publication/wcms_bai_pub_143.pdf

- Potenciales riesgos de siniestro a causa del equipamiento que la empresa entrega al teletrabajador.

7.1.7 Buenas prácticas que posibilitan garantizan en términos de ciberseguridad el teletrabajo en Colombia. Figura 8 Buenas prácticas de ciberseguridad cada día se recomienda tener precauciones en el uso de los dispositivos electrónicos de los teletrabajadores ejercen en las pymes. Cualquier equipo digital que esté conectado por fuera del entorno laboral genera precauciones, deben ser conscientes y responsables en los riesgos que se pueden presentar cuando esté conectados a red no confiables. Alertas de ciberseguridad como phishing, ransomware, robo de datos, virus, ataques en la infraestructura, entre otros.

Figura 8. Buenas prácticas de Ciberseguridad

Fuente: PIRANIRISK, 5 buenas prácticas de ciberseguridad que debes conocer. [imagen]. Disponible en: https://www.piranirisk.com/es/blog/5-buenas-practicas-de-ciberseguridad-que-debe-conocer

A continuación, se comparte las buenas prácticas de ciberseguridad:

- **Antivirus**. Es obligatorio la instalación y actualización de las bases de datos del mismo para contrarrestar los riesgos que están expuestos los equipos para la gestión comercial de las pymes.

- **Software actualizado.** Es necesario la actualización del software de los equipos para disminuir las vulnerabilidades de ser atacados. Existe un grupo de personas que se dedican a la programación y actualización de las aplicaciones.
- **Copias de seguridad.** Las copias de seguridad son necesarias para evitar pérdidas de datos. El equipo de soporte técnico programa con los empleados fechas para la respectiva copia de seguridad ejemplo actualización del sistema operativo o migración de datos.

- **Firewall empresarial.** Es necesario que los equipos que utilicen los teletrabajadores deben tener instalado aplicación de firewall que detecta en tiempo real cualquier amenaza o ataque.

- **Conexiones seguras.** No se recomienda a los teletrabajadores que se conecten en redes WiFi públicas como en los aeropuertos, restaurantes o parques no garantiza el mínimo de seguridad. Se debe tener el cuidado especial en conexiones remotas desde la casa.

- **Cifrado de datos.** La protección de la información es responsabilidad de todos. Es importante consultar con el equipo de soporte técnico la aplicación ideal para el cifrado de la información confidencial.

- **Contraseñas sólidas.** No se recomienda usar la misma contraseña para diferentes cuentas. Los teletrabajadores deben crear contraseñas fuertes con combinación de letras minúsculas, mayúsculas, números y caracteres especiales y es obligatorio cambiarlas y no guardarlas en los equipos.

- **URLs seguras.** Se recomienda a los teletrabajadores usar direcciones web en la barra del navegador de preferencia y evitar ingresar a enlaces de dudosa procedencia sea por el correo electrónico o por redes sociales para evitar fraudes o infecciones de virus informáticos.

- **Descargas de confianza.** Se recomienda las descargas de programas o archivos en sitios web de alta confianza. Se debe evitar descargar aplicaciones en sitios web de dudosa procedencia, como sitios de aplicaciones gratuitas que pueden llegar a afectar los equipos.

- **Capacitación a todo el personal.** Es necesario que los teletrabajadores reciban toda la información de ciberseguridad mediante boletines emitidos por el área de Tecnología de la Información con el objetivo de mitigar los delitos en la web.

- **Auditorías del buen uso de los equipos tecnológicos.** Es necesario la realización de al menos dos (2) veces al año la realización de la auditoría para la detección y protección de posibles amenazas que puedan ocasionar ataques informáticos.

8 CONCLUSIONES

Se estableció los factores de riesgos de ciberseguridad en las pymes mediante el teletrabajo en Colombia causantes de los ciberataques por medio de la ingeniería social y otras estrategias que los teletrabajadores no tienen el conocimiento necesario en materia de la protección ocasionando fuga de información.

Los equipos tecnológicos que tienen las pymes por el desconocimiento a nivel de hardware y software al trabajar remotamente pueden ocasionar la entrada de ciberdelincuentes en donde pueden llegar a manipular hasta destruir la información afectando la gestión comercial.

Se revisó la normatividad, legislación y documentos de buenas prácticas que permiten el apoyo fundamental de las pymes en materia de ciberseguridad en Colombia bajo la modalidad del teletrabajo. Generando la confianza desde lo legislativo en la generación de empleo, trabajo en línea y la implementación de políticas de ciberseguridad mediante el apoyo del Estado.

La norma ISO 27001 la seguridad de la información estableció los tres pilares del SGSI confidencialidad – integridad – disponibilidad en donde las pymes deben identificar los activos, las vulnerabilidades, las amenazas, requisitos legales, riesgos, cálculo del riesgo y el plan de tratamiento del riesgo.

El estado actual de la ciberseguridad Colombia es preocupante ocupa el puesto 39, se invirtieron 10.400 millones de pesos durante la pandemia del Covid-19. Los ciberdelitos que recibieron la Fiscalía General de la Nacional y la Policía Nacional de Colombia.

Los ciberdelitos reportados fueron la suplantación de datos personales, correos maliciosos, uso de aplicaciones móviles de dudosa procedencia, ingeniería social (engaños). El 43% de las pymes no están preparadas para responder los ciberataques es necesario que se realicen mayores inversiones no solamente en el capital humano y equipos tecnológicos se necesita compromiso en la ciberseguridad.

9 RECOMENDACIONES

El teletrabajo en Colombia bajo el análisis de la ciberseguridad presenta las siguientes recomendaciones:

Los equipos tecnológicos deben estar configurados a nivel de hardware y de software de acuerdo con los criterios de expertos en seguridad informática para minimizar los ciberataques en donde las pymes no se pueden recuperar después de ataques cibernéticos. El equipo humano de las pymes debe ser conscientes que deben estar capacitados en temas de ciberseguridad no solamente en la inversión de computadores además la capacitación a los teletrabajadores en temas de ciberseguridad.

Es importante que los teletrabajadores revisen periódicamente las normas, leyes, decretos, entre otros en la cual se basan el teletrabajo bajo el enfoque de la ciberseguridad en las pymes, donde se presentan información que les permiten reforzar las acciones al momento de realizar el teletrabajo.

El panorama de la ciberseguridad es complejo por los diferentes ataques cibernéticos que sufren a diario las pymes y es necesario aunar esfuerzos para bajar los indicadores de ataques. La superintendencia de industria y comercio – SIC y la Organización Internacional del Trabajo – OIT protege y permite un trabajo digno con sus ventajas y desventajas en donde se focalizan a las personas con disciplina, compromiso con las pymes que aportan al progreso del país.

10 BIBLIOGRAFÍA

Ciberdelitos subieron 37% durante el primer trimestre de 2020, en los peores meses de la crisis. Asunto: Legales. {En línea}. {Consultado el 27 de mayo de 2021}. Disponible en: https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480

CompTIA y NICE: Estableciendo las normas para lograr prácticas cibernéticas seguras. CompTIA. {En línea}. {Consultado el: 14 de junio de 2021}. Disponible en: https://certification.comptia.org/es/por-qu%C3%A9-certificarse/gobierno/comptia-y-la-iniciativa-nacional-de-educaci%C3%B3n-en-ciberseguridad-(nice)

Confederación de Empresarios de Andalucía (CEA), Guía Práctica de Protección de Datos para PYMES, Fomento de la Cultura Emprendedora y del Autoempleo 2017, Consejería de Economía, Hacienda y Administración Pública. Junta de Andalucía. Julio 2018, P. 176.

Confederación Canaria de Empresarios. Pasos prácticos para la implementación de un sistema de gestión en privacidad de la información. Basado en la norma ISO/IEC 27701, Gobierno de Canarias, diciembre de 2019. P. 62.

CORTÉS, Rodríguez. Estado Actual de la Política Pública de Ciberseguridad y ciberdefensa en Colombia. {En línea}, Universidad Santo Thomas. Especialización. Publicado en 2015 {Recuperado el 27 de mayo de 2021}. Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/14032/2015rodrigocortes.pdf?sequence=1&isAllowed=y

El Convenio de Budapest en contexto: la seguridad digital como parte de la política criminal. {En línea}, {Consultado el 14 de junio de 2021}. Disponible en: https://www.derechosdigitales.org/12410/el-personal-administrativo-de-una-universidad-colombiana-descubrio-un-dia-que-todas-las-notas-de-sus-alumnos-habian-sido-cambiadas-a-5-la-maxima-posible-todas-la-notas-de-todos-los-programas-el-his/

El marco de ciberseguridad del NIST. FTC. {En línea}. {Fecha de consulta 14 cd junio de 2021}. Disponible en: https://www.ftc.gov/es/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework-es.pdf

Guía de Ciberseguridad para Pymes, Deloitte. Makros Cyber Security Expert. {En línea}. {Fecha de consulta: Noviembre de 2019}. Disponible en https://www2.deloitte.com/content/dam/Deloitte/cl/Documents/risk/CyberMonth2019/guia-ciberseguridad-para-pymes-2019.pdf

HERNANDEZ, Camilo. Estrategias para la transformación digital en mipymes. INCP (2020). {En línea}. {fecha de consulta: 18 de octubre de 2020}. Disponible en: https://www.incp.org.co/estrategias-para-la-transformacion-digital-en-mipymes/

IBM, Sithis. Ciberseguridad y pymes: Nuevo Escenario. P. 8.

INCIBE, Instituto Nacional de Ciberseguridad, Cómo gestionar una fuga de información. Una guía de aproximación para el empresario. Gobierno de España. Ministerio de Industria, Energía y Turismo P. 22.

Informe Tendencias Cibercrimen Colombia 2019 – 2020, CCIT. {En línea}. {Fecha de consulta 14 de junio de 2021}, Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Informe Tendencias Abril 2020, CCIT. {En línea}. {Fecha de consulta 14 de junio de 2021}, Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-abril-2020-final.pdf

La importancia de las Pymes en la economía colombiana. Red Brands (2019). {E línea}. {fecha de consulta: 18 de octubre de 2020}. Disponible en: https://www.red-brands.com/importancia-pymes-economia/

Ley estatutaria 1266 de 2008. RedJurista. {En línea}. {Consultado el 25 de mayo de 2021}. Disponible en: https://www.redjurista.com/Documents/ley_1266_de_2008_congreso_de_la_republica.aspx#/

Ley 1581 de 2012. Función Pública. {En línea}. {Consultado el 25 de mayo de 2021}. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Legislación Informática de Colombia. Informática jurídica. {En línea}. {fecha de consulta: 18 de octubre de 2020}. Disponible en: http://www.informatica-juridica.com/legislacion/colombia/

LEÓN, Carlos Andrés. Estrategias para la clasificación de la información y la prevención fuga de información, Especialización en Seguridad Informática, Universidad Piloto de Colombia, P. 7.

Marco Jurídico teletrabajo en Colombia. Teletrabajo. {En línea}. {fecha de consulta: 18 de octubre de 2020}. Disponible en: https://www.teletrabajo.gov.co/622/w3-article-8098.html

MINDefensa. Ciberseguridad. {En línea}. {Consultado el 27 de mayo de 2021}. Disponible en: https://www.policia.gov.co/ciberseguridad

MINTIC, Vive digital, Policial. Seguridad y privacidad de la información. Guía para la implementación dad de la Información en una MIPYME. Guía Técnica, versión 1.2 6 de noviembre de 2016, Actualización CCP – MINTIC, P. 31.

ORTEGA, Luisa Fernanda. Teletrabajo: Una opción para la mejora de los beneficios de las organizaciones y de los empleados. Universidad Santo Tomás, Facultad de Administración de Empresas, Bogotá, D.C. 2017, P. 50.

PÉREZ, Oscar Eduardo. El habeas data en Colombia: su desarrollo y conectividad con los derechos fundamentales. Universidad Católica de Colombia. {En línea} {Fecha de consulta: 15 de diciembre de 2020}. Disponible en https://repository.ucatolica.edu.co/bitstream/10983/14745/1/HABEAS%20DATA%20CON%20%20LICENCIA.pdf

Privacy International. Las claves para Mejorar la Protección de Datos, August 2018, P. 111.

¿Qué son las Pymes? Gestion.org. {En línea}. {fecha de consulta: 18 de octubre de 2020}. Disponible en: https://www.gestion.org/que-son-las-pymes/

¿Qué es el teletrabajo? Teletrabajo. {En línea}. {Fecha de consulta: 18 de octubre de 2020}. Disponible en: https://www.teletrabajo.gov.co/622/w3-propertyvalue-8010.html

¿Qué es la ciberseguridad? Saber más ser más {En línea}. {fecha de consulta 29 de mayo de 2021}. Disponible en: https://www.sabermassermas.com/que-es-la-ciberseguridad/

RATTI, Gabriela. Desarrollo de una guía de controles de ciberseguridad para la protección integral de la PYME. Trabajo Final Máster, Instituto Nacional de Ciberseguridad de España (INCIBE), diciembre 2017, 97 P.

RIASCOS, Sandra Cristina, CASTRO, Adriana Aguilera, ÁVILA, Gloria Patricia. Seguridad de los sistemas de información en las Pymes de Santiago de Cali (Colombia). Junio del 2014, P. 12.

Superintendencia de Industria y Comercio – SIC. Delegatura para la Protección de Datos Personales. Noviembre 22 de 2019, P. 42.

Tendencias Cibercrimen Colombia 2019 – 2020. CCIT. {En línea}. {Consultado el 27 de mayo de 2021}. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Todo lo que se debe saber sobre el teletrabajo. MinTIC 2020. {En línea}. {Fecha de consulta: 18 de octubre de 2020} Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126148:Todo-lo-que-se-debe-saber-sobre-el-teletrabajo

TELEFÓNICA, Fundación, Ciberseguridad, la protección de la información en un mundo digital. P. 145.

TORRES, Miguel Ángel. DLP: Prevención de fuga de información (Data loss prevention). Especialización en Seguridad Informática, Universidad Piloto de Colombia. Artículo, P. 6.

VILLANUEVA, Miguel. Adaptación de una pyme al RGPD, Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC), Universidad Oberta de Catalunya, 2018, P. 54.

ZUÑA, Edgar René, ARCE, Ángel Alberto, ROMERO, Wilson Javier, SOLEDISPA, César Jorge. Análisis de la seguridad de la información en las pymes de la ciudad de Milagro. Universidad Agraria del Ecuador. Guayaquil. Ecuador, julio 2019, 6 P.