GESTIÓN DE LA CIBERSEGURIDAD EN EL TELETRABAJO PARA PYMES EN COLOMBIA

ANDRÉS FELIPE SÁNCHEZ CASTILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CHIQUINQUIRÁ (BOYACÁ)
2023

GESTIÓN DE LA CIBERSEGURIDAD EN EL TELETRABAJO PARA PYMES EN COLOMBIA

ANDRÉS FELIPE SÁNCHEZ CASTILLO

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Nombre
EDUARD ANTONIO MANTILLA TORRES
Ingeniero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CHIQUINQUIRÁ (BOYACÁ)
2023

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Este proyecto lo dedico en primer lugar a Dios y a mi familia y a todas personas que me apoyaron y depositaron su confianza para conseguir cada meta propuesta a lo largo y arduo camino

AGRADECIMIENTOS

Agradezco el apoyo de mi familia, mis amigos y así mismo el apoyo y colaboración presta por los profesionales académicos de la Universidad Nacional Abierta y a Distancia UNAD en cada uno los semestres cursados durante el desarrollo de este posgrado.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURA

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

Amenaza: Evento determinado que este destinado a afectar la información contenida en un sistema o una red.

Ataque Informático También es denominado ciberataque, es la denominación que se le da a la instrucción abusiva a un sistema, mediante la violación de los sistemas de seguridad.

Ciberseguridad: Hace referencia a las buenas practica y lineamientos guías, es decir, normas y métodos, que tiene como principal objetivo la prevención, detección y protección de los sistemas de una empresa u organización.

Confidencialidad: Hace referencia a la privacidad de la información de una empresa u organización.

Disponibilidad: Hace referencia a la capacidad de una empresa de tener acceso y transformar su información en el momento que sea necesario

Integridad: Hace regencia a la información que posee una empresa, sin que esta sea alterada o manipulada de forma maliciosa.

Pharming modalidad de fraude en donde un ordenador o dispositivos es infectado por un malware malicioso (virus, troyanos etc.), el cual se puede adquirir por medio de ingresar a páginas web no seguras o descargar archivos multimedia (imágenes, audio o video).

PYMES: micro, pequeña y mediana empresa.

Red Privada Virtual - VPN: Término usado cuando se habla de un tipo de red de computadora la cual emplea conexiones seguras, esto con el fin de tener acceso a las conexiones LAN (publicas).

Riesgo Informático Es la posibilidad latente de un ataque.

Vishing: modelo de estafa que se emplea por medio de un teléfono, con fin obtener información sensible o confidencial de una persona, una vez que esta está en manos de los ciberdelincuentes es empleada para suplantar y adquirir servicios o productos con los datos de la víctima.

Vulnerabilidad Es todo punto frágil que se pueda encontrar en un sistema o red, que da una entrada a ciberdelincuentes para realizar ciberataques.

RESUMEN

Dentro del contenido de esta monografía se presentará la gestión de la ciberseguridad como una las piezas fundamentales a la hora de aplicar la modalidad del Teletrabajo en cualquier organización, esto teniendo en cuenta los conceptos básicos e identificación de riesgos, amenazas y vulnerabilidades, que de acuerdo con el planteamiento del problema, será analizado mostrando las diversas alternativas para desempeñar la modalidad de teletrabajo tomando las precauciones necesarias y de esta manera salvaguardar la información como activo.

Como objetivo de la presente monografía se encuentra la construcción de una guía de recomendaciones de ciberseguridad que será el resultado de esta que, mediante el análisis de conceptos, el estudio de la legislación y metodologías planteadas para el teletrabajo logrará dar una pauta a las PYMES, para la construcción de políticas de seguridad de la información y la toma de mejores decisiones en cuanto a la implementación de la modalidad de teletrabajo en sus organizaciones.

Lo anterior con el fin de tener una mejor adaptabilidad en la prevención y/o mitigación de estos. Así mismo protegiendo los principales activos y mejora de la calidad de prestación del servicio de las Pymes. Este proceso será llevado a cabo de manera estructurada, permitiendo al que el lector genere un juicio de valor sobre la importancia de la ciberseguridad

Palabras claves: Amenazas, Ciberseguridad, Normatividad, Riesgos y Teletrabajo

ABSTRACT

Within the content of this monograph, cybersecurity management will be presented as one of the fundamental pieces when applying the Teleworking modality in any organization, taking into account the basic concepts and identification of risks, threats and vulnerabilities, which according to With the statement of the problem, it will be analyzed showing the various alternatives to carry out the teleworking modality taking the necessary precautions and in this way safeguarding the information as an asset.

The objective of this monograph is the construction of a guide to cybersecurity recommendations that will be the result of this that, through the analysis of concepts, the study of the legislation and methodologies proposed for teleworking, will be able to give a guideline to SMEs, for the construction of information security policies and making better decisions regarding the implementation of the teleworking modality in their organizations.

The foregoing in order to have a better adaptability in the prevention and/or mitigation of these. Likewise, protecting the main assets and improving the quality of service provision of SMEs. This process will be carried out in a structured manner, allowing the reader to generate a value judgment on the importance of cybersecurity.

Keywords: Threats, Cybersecurity, Regulations, Risks and Teleworking

INTRODUCCIÓN

Una sociedad siempre está en constante cambio, y con el desarrollo que ha tenido los medios de telecomunicación, el mundo se ha integrado en una verdadera globalización, permitiendo tener una interacción en tiempo real desde dos puntos diferentes del mundo; Este desarrollo abrió las puertas a la implementación de nuevas modalidades de trabajo, permitiendo que las empresas con diferentes necesidades se ajustaran a nuevos entornos, incrementando su productividad y permitiendo que sus empelados contaran con nuevas ventajas con respeto a la modalidad de trabajo tradicional.

En el año 2020 el mundo se enfrenta a una nueva variante del coronavirus que se denominó covid-19, esta variante gracias a sus características se convirtió en una pandemia que ha afectado a millones de personas a nivel mundial, obligando a los países a decretar confinamientos por periodos de tiempo determinados según como se presentara los niveles de contagio; a raíz de todo esta problemática muchas empresas se vieron en la necesidad de buscar una forma en la cual no se vieran obligadas a suspender sus actividades, es en este momento cuando muchas empresas comenzaron a implementar el teletrabajo (siempre y cuando este permitiera que el trabajar desarrollara sus actividades), y con esto también llegaron una serie de preguntas e inquietudes sobre las ventajas y dificultades que esta modalidad de trabajo trae consigo.

Teniendo en cuenta lo anterior a continuación se presenta un documento tipo monografía, en el cual se presentará una descripción sobre el teletrabajo y como la ciberseguridad juega un papel importante en este, identificando y analizando las vulnerabilidades que se encuentren, las cuales serán clasificadas y posteriormente presentadas por medio de una guía de recomendaciones, con el fin de proteger los principales activos y servicios de las Pymes (pequeñas y medianas empresas).

Este proceso será efectuado de forma estructurada cumpliendo con los objetivos que se plantearon inicialmente, permitiendo que el lector genere su propio juicio de valor sobre la importancia de la ciberseguridad.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En el año 2020, como consecuencia de la Pandemia del COVID-19, el mundo sufrió un cambio drástico en su forma de vida, afectando el desarrollo tradicional de diferentes actividades, tales como el estudio y el trabajo.

Como consecuencia de la Pandemia del COVID-19, conllevó a una revolución forzada en materia de Tecnologías de la Información en Colombia, en la cual se adoptaron medidas para garantizar el continuo y normal desarrollo de las actividades laborales, implementado una modalidad de poco empleada por las empresas como es el TELETRABAJO; y con esto también llegaron nuevos riesgos y amenazas en CIBERSERGURIDAD, debido a que las empresas u organizaciones ven la ciberseguridad como un elemento accesorio y opcional, esto se puede evidenciar en la frase del criptógrafo Bruce Schneier “Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología”[1]

Un ejemplo claro de esto, es que, en Colombia la mayoría de las empresas no proporcionan a sus empleados equipos que cuenten con las debidas especificaciones en cuanto ciberseguridad, obligándolos que para desarrollar sus actividades laborales, se vean abocados utilizar diferentes dispositivos de uso personal, como lo son ordenadores, tabletas, smartphone, entre otros y así mismo haciendo uso una red doméstica en lugar de una VPN, lo cual conlleva a ser más vulnerables a ciberataques y afectando la integridad, confiabilidad y accesibilidad de la información de la empresa y de su propia familia.

En el ámbito Colombiano, las pymes se ven duramente afectadas por las diferentes amenazas y problemas de ciberseguridad, de acuerdo a un estudio realizado tomando como base del año 2017 al 2020 denominado “Estudio de Tendencias del Cibercrimen en Colombia” que fue liderado por el programa Seguridad Aplicada al Fortalecimiento Empresarial (SAFE) del Tanque de Análisis y creatividad de las TIC (TicTac), se dio a conocer más de un 150% de incremento en problemas de hurto por medios informáticos, robo de información, entre otros delitos informáticos, en donde las principales ciudades afectadas fueron Bogotá, Cali y Medellín. [2]

[1] JUÁREZ, César. Las 80 mejores frases sobre la Tecnología [en línea]. Psicología y Mente. [Consultado: 10 de marzo de 2021]. Disponible en: https://psicologiaymente.com/reflexiones/frases-tecnologia#:~:text=Si%20piensas%20que%20la%20tecnolog%C3%ADa,(Bruce%20Schneier)

[2] ANALITIK Valora. Actividad maliciosa en internet aumentó en un 150 % en Colombia durante aislamiento [en línea]. valoraanalitik.com. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.valoraanalitik.com/2021/02/27/actividad-maliciosa-en-internet-aumento-un-150-durante-el-aislamiento/

Así mismo, la Policía Nacional en su área de delitos informáticos, da estadísticas en el año 2020 de un 45%[3] de los ataques informáticos fueron destinados o tuvieron como objetivo Pymes. Estas estadísticas demuestran que la seguridad en trabajo en red y almacenamiento en la nube es bastante importante y es todo un reto para las Pymes, teniendo en cuenta que, al ser empresas no tan grandes en su estructura organizacional, sufren también de problemas operativos y financieros limitados que les impiden muchas veces adquirir planes o tratamientos con empresas de seguridad de la información.

1.2 FORMULACIÓN DEL PROBLEMA

Las nuevas modalidades de trabajo remoto imponen nuevos retos y los ideales de ciberseguridad cobran mayor relevancia para las empresas, las cuales buscan una protección eficiente y eficaz, considerando que el nivel de exposición a riesgos contemplados al tener nuevos puntos de interconexión, desde los cuales se tiene acceso a la creación, modificación y eliminación de la información de la empresa, y sumando el incremento de los ciberataques ya sean conocidos o desconocidos.

Teniendo en cuenta lo anterior, se puede plantear la siguiente cuestión: ¿CÓMO GESTIONAR LA CIBERSEGURIDAD EN EL TELETRABAJO EN LAS PYMES DE COLOMBIA?

[3] ANALITIK Valora. Actividad maliciosa en internet aumentó en un 150 % en Colombia durante aislamiento [en línea]. valoraanalitik.com. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.valoraanalitik.com/2021/02/27/actividad-maliciosa-en-internet-aumento-un-150-durante-el-aislamiento/

2 JUSTIFICACIÓN

"LA SEGURIDAD NO ES UN PRODUCTO, ES UN PROCESO"[4] (criptógrafo Bruce Schneier), esto quiere decir que, la ciberseguridad no solamente es la implementación de una aplicación, guías y/o recomendaciones y que por el hecho de contar con ellas automáticamente los problemas que se tengan van hacer solucionados, por el contrario al emplear estas medias estamos dando el primer paso para crear un entorno digital seguro que se construye identificado los riesgos y amenazas y gestionando las medidas más eficientes según las necesidades, las cuales serán continuamente monitorizadas y sujetas a modificaciones.

Con el paso del tiempo las Tecnologías de la Información – TI, se fueron convirtiendo en unas de las herramientas cada vez más indispensables para el diario vivir, dando lugar a nuevas modalidades de trabajo como es el TELETRABAJO, pero así mismo con ellas también llegaron diversos tipos de riesgos y amenazas en cuanto a la ciberseguridad, como por ejemplo los estándares de seguridad exigidos en el equipo personal utilizado, que conlleva a tener conexiones poco seguras que pueden dejar filtrar virus e incluso abrir la puerta a los delincuentes informáticos a través de cualquier tipo de ataque ya sea de fuerza bruta, entre otros existentes.[5] Las amenazas y riesgos fueron evolucionando de manera exponencial y perjudicando a un sin número de usuarios y PYMES; en respuesta a estos y para mitigarlos, se fueron creando guías de recomendaciones de ciberseguridad que tomaban como base la forma del impacto del ciberataque con el fin de estructurar medias enfocadas a prevenir futuros ataques.

Teniendo en cuenta lo anterior, desarrollara una guía base para el mejoramiento de la Ciberseguridad en la modalidad del Teletrabajo, en la cual se explorará las principales amenazas que se presentan; esto debido que durante el último año por las restricciones establecidas con motivo del COVID - 19, esta modalidad se incrementó sustancialmente trayendo consigo un sin número de desafíos que obligó a las empresas a adoptar un entorno seguro y confiable para el normal desarrollo de las actividades laborales.

Este documento tiene como objetivo crear conciencia sobre los riesgos y amenazas en cuanto a la ciberseguridad en el TELETRABAJO y su vez brindar recomendaciones en caminadas a mejorar la interacción segura entre el usuario y su entorno digital.

---

[4] Bruce Schneier. [en línea]. wikipedia.org [Consultado: 10 de marzo de 2021]. Disponible en: https://es.wikipedia.org/wiki/Bruce_Schneier#:~:text=A%20Schneier%20se%20deben%20frases,personas%2C%20procesos%20y%20tecnolog%C3%ADa%22

[5] Martínez Cortes, John Fredy Seguridad de la Información en pequeñas y medianas empresas (pymes) [en línea] Universidad Piloto de Colombia [Consultado: 15 de febrero de 2023] disponible en http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2860/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

Al crear conciencia sobre la problemática de ciberseguridad y encaminar a las empresas Pymes a las buenas prácticas de seguridad de la información en sus procesos y transacciones, se quiere crear una experiencia de alto valor o valor agregado para las mismas, generando así experiencias exitosas que se puedan replicar en más de una empresa al reducir el impacto que genera la perdida de información y el hurto por medios informáticos de recursos financieros, entre otros problemas informáticos de la actualidad.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

- ✓ Analizar la normatividad legal y técnica para mejorar la ciberseguridad de actividades desarrolladas bajo la modalidad de Teletrabajo para PYMES en Colombia

3.2 OBJETIVOS ESPECÍFICOS

- ✓ Examinar los diferentes marcos legales y técnico vigente entre el Teletrabajo y Trabajo Remoto para su adopción en pymes colombianas.

- ✓ Evaluar los riesgos y amenazas que afectan a la Ciberseguridad en la modalidad del Teletrabajo en las Pymes Colombianas mediante la aplicación de la metodología MAGERIT para el Análisis y Gestión de Riesgos de los Sistemas de Información.

- ✓ Diseñar una guía base para el mejoramiento de la Ciberseguridad en la modalidad del Teletrabajo en organizaciones Colombianas que permita a las Pyme mejorando los niveles de seguridad en el desarrollo de sus actividades.

4 MARCO REFERENCIAL

Con la transformación digital de las empresas tanto privadas como públicas y la aparición de las nuevas modalidades de trabajo, para este caso en específico el teletrabajo, se hacen presentes también las amenazas y riesgos ya conocidos en el medio tecnológico. La materialización de los riesgos y amenazas cada vez es mayor, teniendo en cuenta el entorno de interconexión de las personas y las empresas y se hace necesario cambiar el pensamiento o la falsa creencia que los ataques cibernéticos solo les ocurren a las grandes empresas, por lo que en la actualidad las pequeñas y medianas empresas así mismo sufren este flagelo.

Por lo anterior, se realiza un análisis de las diferentes fuentes de información encontradas con el fin de entender los problemas de ciberseguridad enfocados específicamente al teletrabajo en Colombia y su contexto, en donde de acuerdo a las estadísticas y estudios realizados,[6] se encuentra en proceso de regulación total por parte de las empresas a nivel jurídico y en la implementación de políticas y estrategias que permitan la protección de la información manejada, ofreciendo de esta manera mayor confiabilidad e ir creciendo en este tipo de modalidad de trabajo.[7]

Por consiguiente, se crea una guía base para el mejoramiento de la Ciberseguridad en la modalidad del Teletrabajo PARA PYMES EN COLOMBIA, que abarque los temas y conceptos de interés frente a la problemática y sea una estrategia que sirva para la creación de políticas de ciberseguridad.

4.1 MARCO CONCEPTUAL

4.1.1 Sistema de Gestión de Seguridad de la Información - SGSI.

Consiste en una herramienta de gestión que permite conocer, gestionar y minimizar los riesgos que se puedan presentar en una empresa u organización, mediante la conformación de guías, destinadas a la protección de los activos de información fundamentales, teniendo como base tres criterios primordiales como es la integridad, confidencialidad y disponibilidad.[8]

[6] Tovar Salazar, Alvaro Isidro Elaboración De Una Guía De Seguridad Informática Para La Implementación Del Teletrabajo [en linea] Universidad Nacional Abierta Y A Distancia – Unad [Consultado 05 de junio de 2023] disponible en https://repository.unad.edu.co/bitstream/handle/10596/51472/aitovars.pdf?sequence=1&isAllowed=y

[7] Gonzalez David, Pulido Saul La ciberseguridad política clave dentro de las organizaciones [en linea] Universidad Santo Tomás Tunja [Consultado 15 de febrero de 2023] disponible en https://repository.usta.edu.co/bitstream/handle/11634/37635/2021davidgonzalezsaulpulido.pdf?sequence=1&isAllowed=y

[8] iso27000.es. SGSI. ¿Qué es un SGSI?- Integridad. [en línea]. iso27000.es. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.iso27000.es/sgsi.html

4.1.2 Ciberseguridad

Con la evolución digital, comenzó a surgir nuevos términos que como es el de ciberseguridad, el cual hace referencia a las buenas practica y lineamientos, que al ser aplicados se convertirán en la primera línea de defensa para hacer frente a los ciberdelincuentes, todo está contenido en guías, normas y métodos, que tiene como principal objetivo la prevención, detección y protección de los sistemas de una empresa u organización.

4.1.3 Confidencialidad de la información

Hace referencia a la privacidad de la información de una empresa u organización, esta información es la que se genera o produce por medio del ejercicio de una función o actividad, que es de dominio confidencial y solo es conocida por el personal debidamente autorizado.[9]

4.1.4 Integridad de la información

Hace regencia a la información que posee una empresa, organización o cualquier usuario, la cual puede estar almacenada o ser transmitida por un canal de comunicación, pero sin que esta sea alterada o manipulada de forma maliciosa.[10]

4.1.5 Disponibilidad de la información

Hace referencia a la capacidad de una empresa, organización o un usuario de tener acceso y transformar su información en el momento que sea necesario, sin que esta se vea afectada por pérdida o corrupción.[11]

4.1.6 Red Privada Virtual - VPN

Término usado cuando se habla de un tipo de red de computadora la cual emplea conexiones seguras, esto con el fin de tener acceso a las conexiones LAN (publicas). Su principal característica está centrada en el permitir a cualquier dispositivo el poder recibir o transmitir información en redes compartidas o públicas como si se tratara de una red privada con todos los beneficios que esta tiene.[12]

---

[9] pmg-ssi.com Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad [en linea]. 1 febrero, 2018 [Consultado: 20 de septiembre de 2022]. Disponible en https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

[10] pmg-ssi.com Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad [en linea]. 1 febrero, 2018 [Consultado: 20 de septiembre de 2022]. Disponible en https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

[11] pmg-ssi.com Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad [en linea]. 1 febrero, 2018 [Consultado: 20 de septiembre de 2022]. Disponible en https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

[12] latam.kaspersky.com ¿Qué es una VPN y cómo funciona? [en linea]. [Consultado: 20 de septiembre de 2022]. Disponible en https://latam.kaspersky.com/resource-center/definitions/what-is-a-vpn

4.1.7 Vulnerabilidad

Es todo punto frágil que se pueda encontrar en un sistema o red, que da una entrada a ciberdelincuentes para realizar ciberataques.[13]

4.1.8 Amenaza

Hace referencia a un evento determinado que este destinado a afectar la información contenida en un sistema o una red, cuando la amenaza se materializa se convierte en un ataque, dependiendo del tipo de amenaza serán los riesgos. [14]

4.1.9 Ataque Informático

También es denominado ciberataque, es la denominación que se le da a la instrucción abusiva a un sistema, mediante la violación de los sistemas de seguridad, con el fin de extraer, modificar o eliminar información, dependiendo del tipo de ciberataque se determinara las acciones a seguir. [15]

4.1.10 Riesgo Informático

Es la posibilidad latente de un ataque, estos son determinados dependiendo de las actividades que son realizadas por las empresas, organizaciones o los usuarios. [16]

4.1.11 Teletrabajo

Se conceptualiza como una modalidad de trabajo que se realiza a distancia, es decir, fuera de las instalaciones de las organizaciones lo que permite que el trabajador no tenga contacto con el jefe inmediato o compañeros de oficina, sin dejar de tener un vínculo laboral.[17]

---

[13] RODRÍGUEZ ARROYO Hugo Alfonso Importancia De Controlar Todas Las Amenazas Detectadas A Través De Magerit V.3 E Iso/Iec 27002 Según Análisis De Ataques Informáticos En Latinoamérica [en línea]. Monografía. universidad nacional abierta y a distancia unad escuela de ciencias básicas, tecnología e ingeniería especialización en seguridad informática barranquilla 2019. [Consultado: 10 de marzo de 2021]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/31879/harodriguezar.pdf?sequence=1&isAllowed=y

[14] RODRÍGUEZ ARROYO Hugo Alfonso Importancia De Controlar Todas Las Amenazas Detectadas A Través De Magerit V.3 E Iso/Iec 27002 Según Análisis De Ataques Informáticos En Latinoamérica [en línea]. Monografía. universidad nacional abierta y a distancia unad escuela de ciencias básicas, tecnología e ingeniería especialización en seguridad informática barranquilla 2019. [Consultado: 10 de marzo de 2021]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/31879/harodriguezar.pdf?sequence=1&isAllowed=y

[15] RODRÍGUEZ ARROYO Hugo Alfonso Importancia De Controlar Todas Las Amenazas Detectadas A Través De Magerit V.3 E Iso/Iec 27002 Según Análisis De Ataques Informáticos En Latinoamérica [en línea]. Monografía. universidad nacional abierta y a distancia unad escuela de ciencias básicas, tecnología e ingeniería especialización en seguridad informática barranquilla 2019. [Consultado: 10 de marzo de 2021]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/31879/harodriguezar.pdf?sequence=1&isAllowed=y

[16] RODRÍGUEZ ARROYO Hugo Alfonso Importancia De Controlar Todas Las Amenazas Detectadas A Través De Magerit V.3 E Iso/Iec 27002 Según Análisis De Ataques Informáticos En Latinoamérica [en línea]. Monografía. universidad nacional abierta y a distancia unad escuela de ciencias básicas, tecnología e ingeniería especialización en seguridad informática barranquilla 2019. [Consultado: 10 de marzo de 2021]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/31879/harodriguezar.pdf?sequence=1&isAllowed=y

[17] COLOMBIA. Ministerio de Tecnologías de la Información y las comunicaciones. Definición [en línea]. Santa Fe de Bogotá, D.C. [Consultado: 04 de diciembre de 2022]. Disponible en: https://teletrabajo.gov.co/622/w3-article-8228.html

4.2 MARCO TEÓRICO

Dentro de la gestión de la ciberseguridad en la modalidad del Teletrabajo en Colombia, en este caso contextualizado para las PYMES (pequeñas y medianas empresas), se hace necesario tener claro los diferentes conceptos que permitan desarrollar la Temática de una manera clara y concisa.

Es importante resaltar que en Colombia la gestión de Ciberseguridad específicamente para el Teletrabajo lleva muy poco tiempo y en el marco de la emergencia sanitaria del COVID-19, ha tomado relevancia y más visible a nivel nacional, teniendo en cuenta que de acuerdo a las normas y precauciones tomadas por el Gobierno Nacional, ha optado por autorizar la modalidad del Teletrabajo con el fin de no afectar el desarrollo económico de las diferentes empresas, siendo esto un motivo de preocupación al momento de salvaguardar la información.

A continuación, se abordarán los diferentes temas que permitirán el desarrollo de los objetivos planteados para este trabajo.

4.2.1 Vulnerabilidad, riesgos y amenazas.

Dentro del desarrollo organizacional de las PYMES, deben tener conocimiento acerca de las Vulnerabilidad, Riesgos y Amenazas, que se puedan materializar en el proceso de la manipulación de la información, en este caso de manera digital en cuanto al teletrabajo se refiere; debido a que al manipular la información en una comunicación punto a punto como por ejemplo el envío y recibo de datos o a través de un chat de una herramienta ofimática conectada a una VPN, se debe garantizar que la información se mantenga integra, disponible y confiable cumpliendo así con los principios de la seguridad informática, es decir, las PYMES en sus procesos diarios deben tener precaución con los diversos ataques informáticos o amenazas de otro tipo que se puedan presentar afectando los recursos tecnológicos y económicos y más con el uso de la internet, en donde los datos pueden estar expuestos sino se realizan la debida protección.

Teniendo en cuenta lo anterior, se considera que las vulnerabilidades son debilidades que exponen la información a posibles ataques cibernéticos que si se llegan a materializar afectan la integridad, confidencialidad y disponibilidad de la misma, lo que supone un riesgo para la organización, en varios ámbitos operacionales y financieros, como se menciona en el artículo “Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia”[18]

[18] Sanchez Paola A., García Jose R, Triana Antony y Perez Leydy, Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia [en línea]. www.scielo.cl Información tecnológica versión On-line ISSN 0718-0764 Inf. tecnol. vol.32 no.5 La Serena oct. 2021 http://dx.doi.org/10.4067/S0718-07642021000500121 [Consultado: 15 de febrero de 2023]. Disponible en: https://www.scielo.cl/scielo.php?pid=S0718-07642021000500121&script=sci_arttext

Dentro de las medidas preventivas que pueden tomar en cuenta las PYMES para disminuir o mitigar las vulnerabilidades y amenazas a las que están expuestas, se pueden considerar las siguientes:

1. Capacitación a los usuarios de manera continua, esto hará una gran diferencia en cada proceso llevado a diario y en el manejo de la información
2. Medidas correctivas en caso de presentarse siniestros, estas medidas implican una investigación y seguimiento de actividades mitigadoras del riesgo
3. Medidas de detección que implican la búsqueda o rastreo de las posibles evidencias de un ataque informático y la activación de controles ya sean preventivos o correctivos

Las medidas anteriormente mencionadas son bastante útiles, sin dejar de lado la gestión de las amenazas, que, de acuerdo a un estudio practicado en el Reino Unido, específicamente en Escocia en donde se buscaba obtener resultados frente a la percepción de PYME frente a la ciberamenazas y las prácticas de gestión de la seguridad, los resultados arrojaron que el 32% eran negocios individuales, el 63% tenía 30 o menos empleados y el 5% tenía hasta 100 empleados. [19]

Este tipo de estudios permiten concluir que las PYMES no están en la capacidad aún de aplicar las suficientes medidas para mitigar ataques cibernéticos de cualquier tipo y que aún falta profundizar en el trema e implementar estrategias, que permitan alcanzar los objetivos propuestos frente a esta temática

4.2.2 Sistema de Gestión de Seguridad de la Información – SGSI

De acuerdo a la norma ISO/IEC 27001, se define como:

“Es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio”[20]

De esta manera a nivel organizacional este concepto debe estar en marcado en la dependencia o dirección tecnológica de la información de las PYMES, toda vez que allí se definen las normas, guías, procedimiento y políticas de seguridad de la información que son tomados para salvaguardar los activos que incluyen datos sensibles gestionados por las empresas. De allí también se toman las políticas utilizadas para gestionar todo lo correspondientes a la ciberseguridad.

[19] Renaud Karen, Cómo luchan las pequeñas empresas con los consejos de seguridad, [en línea] sciencedirect.com [Consultado: 15 de febrero de 2023] Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S1361372316300628?via%3Dihub

[20] iso27000.es. SGSI. ¿Qué es un SGSI?. [en línea]. iso27000.es. [Consultado: 06 de marzo de 2021]. Disponible en: https://www.iso27000.es/sgsi.html

En este orden de ideas, las empresas deben implementar políticas y deseñar un esquema para el monitorio, mitigación y prevención de los riesgos de los activos de información a través del Sistema de Gestión de Seguridad de la Información – SGS.

Observando la situación actual de las PYMES en Colombia en relación con la seguridad informática, no prestan mucha relevancia a este tema a diferencia de las grandes compañías y cometen errores como los siguientes:

- No valorar la infraestructura de una red
- La seguridad se limita solo al hardware software
- Se considera seguridad solo tener activo un antivirus
- No se le da la importancia necesaria a los mecanismos jurídicos o know how que les permitan tener una defensa frente a eventualidades de delitos informáticos materializados
- No contemplar el plan de continuidad del negocio y las políticas de seguridad informática
- No se contempla la inversión en tecnología adecuada

Se han realizado estudios por parte de la compañía de seguridad Kaspersky denominado “Informe Especial ¿Quién le espía? Ninguna empresa está a salvo del ciberespionaje” señala en su conclusión que ninguna empresa se encuentra exenta de sufrir ataques cibernéticos o de ciberespionaje, en donde las PYMES tienen el mayor riesgo por su falta de concientización y de recursos para implementar en sus operaciones e infraestructura física. [21]

4.2.3 Ciberseguridad.

Este es un concepto que durante los últimos tiempos cada vez toma relevancia para muchas personas, empresas u organizaciones, esto es debido a la globalización digital mostro como se podía llegar a un sin número de personas sin la necesidad de realizar grandes desplazamientos y mostrando al mundo lo que pueden ofrecer en el caso de las empresa u organización, y para el caso de las personas mostrando cuáles son sus gustos o preferencias, esto llevo a que personas con un conocimiento avanzado diseñaran métodos por medio de los cales se pudieran apoderar de la información de las personas con fines maliciosos; teniendo en cuenta esto diversos expertos y compañías a nivel mundial se dieron a la tarea de crear protocolos encaminados a la protección de computadoras, dispositivos móviles o redes, a este conjunto de medidas se le conoce como ciberseguridad.

La ciberseguridad es una de las áreas de la informática que se actualiza contantemente, esto se debe a que los delitos informáticos hacen exentamente lo

[21] Martínez Cortes, John Fredy Seguridad de la Información en pequeñas y medianas empresas (pymes) [en linea] Universidad Piloto de Colombia [Consultado: 15 de febrero de 2023] disponible en http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2860/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

mismo y se ha convertido en una carrera por preservar la seguridad e integridad de la información, es por este motivo que muchas empresas u organizaciones han estado invirtiendo grandes cantidades de dinero en la capacitación de su personal, lo cual está creando una conciencia de la importancia de la ciberseguridad en las personas.

Mencionando el estudio realizado en Colombia por parte de la Universidad de Córdoba realizado sobre la temática de delitos informáticos y su impacto en el comercio electrónico, muestra en gran porcentaje el riesgo de las PYMES en ser afectadas considerablemente en el desarrollo de sus operaciones o transacciones llevadas a cabo por medios electrónicos o digitales.

Se habla en gran medida en este estudio de la posibilidad de aumentar la educación en seguridad informática como un tema fundamental, teniendo en cuenta que, con la expansión del comercio, de las nuevas tecnologías y avances es necesario un buen desarrollo, fortalecimiento y crecimiento tanto en conocimiento como en la parte organizacional que permita mitigar las amenazas y ataques en las empresas colombianas.[22]

4.2.4 Teletrabajo

Lo que para muchos hace años era un sueño o fantasías, gracias a los grandes cambios que ha traído la globalización digital, hoy en día se está viendo como gradualmente se han generado nuevas alternativas laborales apoyadas en las nuevas tecnologías como es el caso del teletrabajo, que mediante la implementación de una o varias herramientas de telecomunicaciones permite que una o varias personas puedan desempeñar su trabajo fuera de las instalaciones o las oficinas de la empresa para la cual labora, este concepto ha planteado una nueva forma de ver el mundo laboral, conocido como la revolución digital.

Teniendo en cuenta lo anterior, se puede observar que esta alternativa o modalidad de trabajo que implementa la creación de espacios flexibles que brindan una oportunidad para un sin número de personas, las cuales pueden realizar sus actividades laborarles desde sus hogares, que ya sea por al tipo de discapacidad o condiciones familiares que les impiden realizar desplazamiento a sus lugares de trabajo, esto acompañado por otra serie de beneficios para la empresa como el a disminución de costos en servicios, creación de ambientes laborales dinámicos que les perite tener diversas perspectivas, facilidad de contratar personal altamente calificado; pero a si mismo también presenta desventajas como es la implementación del trabajo individual sobro el grupal, la inversión requerida para

[22] Gonzalez David, Pulido Saul La ciberseguridad política clave dentro de las organizaciones [en linea] Universidad Santo Tomás Tunja [Consultado 15 de febrero de 2023] disponible en https://repository.usta.edu.co/bitstream/handle/11634/37635/2021davidgonzalezsaulpulido.pdf?sequence=1&isAllowed=y

dotar de todos los elementos necesarios a los empleados y el cambio en las condiciones contractuales existentes.

La principal característica del teletrabajo radica en el cambio de mentalidad, tanto a nivel de empleados como de las organizaciones o empresas, esto se debe a que con la implementación de esta forma laboral se deben replantear las estrategias, estructura corporativa, así mismo como la visión a futuro ya que este modelo permite contar con empleados en diferentes puntos de la tierra, rompiendo con la barrera de lugar expandiendo el alcance de los servicios prestados. [23]

4.2.4.1 Modalidades.

Como en toda nueva modalidad laboral que surge, se debe tener en cuenta con una serie de característica que permitan el óptimo desarrollo de las actividades laborales, para este caso en concreto se relaciona con el punto o lugar que se empleara para el teletrabajo, esto influye debido a que dependiendo del lugar se puede identificar si se cuenta con una recepción de señal adecuada, que tan saturada se encuentra las autopistas de información, capacidad del ordenador o dispositivo, tipo de servicio de internet (en esta parte se toma en cuenta si este es simétrico, banda ancha etc.).

De acuerdo con Ortiz F. (1996) menciona los diferentes lugares desde los cuales se puede teletrabajar:

- **El domicilio del trabajador:** como su nombre lo dice es el domicilio del trabajador, el cual se adapta para cumplir sus funciones laborales, una de sus principales desventajas es el aislamiento del trabajador generando niveles de estrés altos, por otro, lado representa una oportunidad para el compartir con la familia.
- **Las oficinas satélites**: esta es una modalidad que se ha implementado por pymes, esto se debe a la gran facilidad de organizar lugares de trabajo en ubicaciones determinadas, las cuales son seleccionadas dependiendo del mercado que estas representan para el potencial de crecimiento de la empresa, una de sus mayor dificultada está relacionada con el modelo de dirección y comunicación con respecto a la oficina principal.
- **Los telecentros:** es una modalidad en la cual una o más empresas comparten recursos informáticos, estos deben contar con una serie de normas de seguridad en cuanto al manejo de información.
- **Telecottages**: esta es una modalidad creada con la intención de llegar a

[23] GONZÁLEZ ZULUAGA, Andrea, FLORÉZ LONDOÑO Kelly Danitza y PELÁEZ RAMÍREZ Viviana Vera Gestión Del Cambio Y El Teletrabajo [en línea]. Trabajo De Grado Para Optar El Titulo De Especialistas En Gestión Del Talento Humano Y La Productividad. Universidad de Medellín facultad de ciencias-económico administrativas especialización de gestión del talento humano y la productividad 2014. [Consultado: 10 de marzo de 2021]. Disponible en: https://repository.udem.edu.co/bitstream/handle/11407/385/Gesti%C3%B3n%20del%20cambio%20y%20el%20teletrabajo.pdf?sequence=1

lugares poco poblados cono es las zonas rúlales, estos se encargan de brindar trabajo e impulsar a los habitantes de estos sectores en la creación de empleo y el uso de nuevas tecnologías.

- **Móviles o nómadas**: es una modalidad que le permite al trabajador ejercer sus funciones en el momento que él lo desee, dependiendo principalmente del momento que este lo requiera.

Teniendo en cuenta lo anterior, Burch (1992) menciona las modalidades que son definidas por la consultora británica OVUM, son: Burch, S. (1992). Telecomunicación. Colombia: Legis Editores S.A

- Trabajo en casa
- Trabajadores móviles
- Trabajadores que operan desde un centro de trabajo.

4.2.4.2 Ventajas y desventajas

Como en toda modalidad de trabajo existen las ventajas y desventajas que permite dimensionar si estas se adaptan las necesidades de una empresa u organización, teniendo en cuenta este aspecto se puede tomar tres valores que determina su viabilidad, estos factores son:

- El individuo
- La empresa
- La sociedad

La principal ventaja que representa este modelo de trabajo es su fácil adaptabilidad al mercado cambiante que se encuentra el mundo por la globalización digital, permitiendo que un producto sea mostrado no solo a un nivel local sino internacional sin la necesidad de contar con una infraestructura compleja y costosa para darlo a conocer, es precisamente por este motivo que un sin número de empresas impulsan el desarrollo de nuevas tecnologías que permitan una implementación de este modelo de trabajo.

Pero como en todo proceso cambiar no es fácil y mucho menos el implementar un modelo laboral aun inexplorado en varios aspectos, producto del confinamiento ocurrido a causa del covid-19, se han podido evidenciar de forma clara algunas de sus desventajas, entre las más comunes se encuentran el aislamiento social, falta de organización en los horarios de trabajo, problemas para descansar apropiadamente, el costo en tecnología entre otros.

Existen similitudes en diferentes autores, que dan su opinión de acuerdo con su investigación sobre la modalidad de teletrabajo, un claro ejemplo es Ortiz (1996), quién adopta una postura analizando las ventajas y desventajas de manera muy

detallada y donde sobresalen factores como: flexibilidad, ahorro y productividad. Por otro lado, hablando de las desventajas es importante señalar que autores como el mencionado anteriormente, hace énfasis en el proceso de cambio que tanto para los trabajadores como organizaciones es difícil la adaptación y es entonces donde surgen mal llamadas “desventajas” como dificultad para trabajar en grupo, desvinculación de la entidad, entre otras.

4.2.5 Características del teletrabajador

Las entidades u organizaciones deben realizar un proceso de selección del talento humano, en donde se pueda cualificar al trabajador para la modalidad de teletrabajo, debido a que este debe cumplir una serie de características dentro de su perfil laboral que permitan el buen desempeño de este en las actividades asignadas, así mismo se debe contemplar las características personales como: autogestión, disciplina, constancia, orientación al logro, organización del tiempo y demás que permitan que la persona escogida pueda cumplir con lo esperado.

Telecommuting Guidelines (1998) menciona en su artículo características de un teletrabajador:[24]

- Conocimiento de la modalidad de trabajo y experiencia en la misma
- Habilidades y competencias para desempeñar el cargo, organización del tiempo, planificación de actividades
- Autogestión, disciplina
- Manejo de herramientas que permitan la comunicación asertiva y efectiva con la organización
- Gusto por la modalidad de trabajo

4. Factores que influyen en el teletrabajo

De acuerdo con la opinión de los autores Civit, C. y March, M. (2000) existen unos factores a considerar en el momento de establecer la modalidad de teletrabajo y que son decisivos para las empresas, estos son:

- Factor de la distancia: cuando las actividades laborales requieran presencia física, no debe considerar el teletrabajo como una opción, teniendo en cuenta los resultados esperados de las operaciones empresariales

- Resultados que sean cuantificables: el teletrabajo es una modalidad a distancia que implica un rediseño en la estructura empresarial, con el fin de

[24] Merrie L. Healy, MPH, RNTelecommuting OCCUPATIONAL HEALTH CONSIDERATIONS FOR EMPLOYEE HEATLH AND SAFETY [en línea]. [Consultado: 10 de diciembre de 2022]. Disponible en https://journals.sagepub.com/doi/pdf/10.1177/216507990004800607

incurrir en métodos que impliquen la supervisión del teletrabajador y la medición efectiva del resultado de sus avances laborales

- Manipulación de la información: aquí se tiene en cuenta que, a la hora de implantar el teletrabajo, deben ser actividades en donde la información pueda ser consultada por la empresa y el trabajador y no implique presencia física en el manejo de la misma

- Autonomía: se refiere a la autonomía con la que debe contar el teletrabajador, entre más organizado sea con su planificación y cumplimiento de actividades, será mucho más fácil para la empresa contar con buenos resultados y el seguimiento o supervisión realizada al teletrabajador

- Entrega de resultados y plazos definidos: este apartado está enfocado a la correcta elaboración y cumplimiento de cronograma de actividades del teletrabajador, con el fin que se pueda contar con entregas parciales y totales que demuestren el estricto cumplimiento de sus labores a satisfacción

- Control del trabajo: el teletrabajo es una modalidad que es mucho más fácil implementar en aquellas organizaciones, en donde se pueda contar con flexibilidad horaria y de carga laboral

Civit, C. y March, M. (2000). Implantación del Teletrabajo en la Empresa. España: Gestión 2000.

4.2.6 El cambio en las organizaciones

Todo cambio representa un reto para las empresas u organizaciones, esto se debe al cambio en la forma del funcionamiento de la misma, iniciando por algunos aspectos económicos, tecnológicos, políticos y sociales; como es bien conocido el recurso humano de una empresa u organización es el activo más valioso, y cuando sus valores y objetivos van en la misma dirección hacen que su valor aumente considerablemente.

Es por esto que los departamentos de gestión humana de una empresa u organización debe instruir adecuadamente a sus agentes de cambio con el fin de que estos puedan crear una empatía con el trabajar al momento de asesoras sobre las nuevas condiciones de trabajo y como estas brindaran garantías y beneficios mutuos, permitiendo que los trabajadores acepten estas nuevas propuestas con la mejor aptitud permitiéndoles tener una adaptación cómoda y rápida, sin afectar su desempeño laboral.

Este tipo de propuestas hace un tiempo requerían de una gran inversión por parte de las empresas u organizaciones, debido a que no contaban con estrategias que

les permitiera afrontar este nuevo tipo de cambio, esto fue evidenciado durante el confinamiento del covid-19, al no poder adaptarse a este nuevo cambio perdiendo protagonismo en el mercado, lo cual ocasiono la caída o quiebra de muchas empresas, mientras otras que tenían conocimientos de cómo organizarse adecuadamente, se adaptaron permitiendo sobrevivir e incrementar sus ganancias.

4.2.6.1 Procesos

Todo cambio obedece a un tipo de circunstancia o aspecto que define la naturaleza del mismo, teniendo base este principio se puede determinar el carácter comportamiento que se llevara a cabo durante el desarrollo de los procesos que contribuirán a este cambio, como es el recurso humano, la planificación y puesta en marcha de este, para que un proceso tenga éxito en se debe tener varios factores en cuenta, pero el principal está enfocado en la aceptación del mismo, ya que si existe una resistencia a este todo se desarrollara de forma traumática afectado el éxito del mismo.

Por este motivo cuando se implementa un cambio se debe analizar bien la situación actual de la empresa u organización, verificando con antelación como seria recibido un cambio y que tan favorable seria la actitud con respecto al mismo; teniendo en cuenta esto se debe tener en cuenta el mecanismo que permitan realizar un proceso de aceptación.

En la vida siempre se presentan cambio que alteran el normal comportamiento y suelen sacar de su estado de confort a las personas, en una empresa u organización las cosas no son diferentes, y en muchas ocasiones la gente suele creer que cuando se efectuara un cambio es porque el trabajo que se ha estado desarrollado hasta el momento no ha sido el adecuado o no cumple a satisfacción, este tipo de pensamiento es la primera barrera que se debe superar, esto es expuesto por Lewin (1951) [25], quien teniendo en cuenta que los cambios acarrean diferentes aspectos y procesos, se dio a la tarea de desarrollar tres lineamientos, escalones o bases destinadas a contribuir con los procesos de cambio, este trabajo fue tomado por Schein, E. (1980). Organizational Psychology. Englewood Cliffs, N. J.: Prentice Hall., quien lo profundizo en tres aspectos, el individual, grupal y organización de la siguiente manera:

Descongelación: este es el primer aspecto que se debe tener en cuenta, toda vez que el cambio siempre es necesario para el poder adaptarse a nuevas circunstancias, pero este no siempre es bien recibido, por este motivo que se debe mostrar cuáles serán los beneficios que se obtendrán, pero para lograr esto es necesario evidenciar cuales son las falencias que se presentan en la actualidad y

[25] LEWIN, KURT. Field Theory of Social Science: Selected Theoretical Papers. (Edited by Dorwin Cartwright.) Pp. xx, 346. New York: Harper & Brothers, 1951 [en línea]. [Consultado: 10 de diciembre de 2022]. Disponible en https://journals.sagepub.com/doi/10.1177/000271625127600135

como estas serán solucionados.

Cambio: sin importar el cambio que se quiera efectuar significa que las personas tendrán que adoptar una nueva forma de visualizar, sentir y de interactuar según un nuevo esquema, que solamente cuando es aceptado permitirá crear nuevas pautas que conducirán a desarrollar con éxito las metas propuestas. Para lograr esto es necesario que los nuevos conocimiento y metodologías sean transmitidos de manera fácil y ágil, de forma que estimule el aprendizaje mientras se realiza.

Re congelación: todo cambio es el fruto de un procesos de evolución ligado a circunstancias o factores que cambian el statu quo de un entorno, induciendo al cambio que puede ser de forma natural o de planificada; si este planificado se desarrollara mediante a implementación de procesos en los cuales se invertirán recursos, tiempo y tecnología, que al cabo de un periodo determinado, ya sea a corto, mediano o largo plazo brindara una serie de resultados, los cuales se constataran con los inicuamente planificados, es de anotar que durante estos procesos se llevara un procesos se llevara una seguimiento el cual, servirá de base en caso que los resultados que se estén evidenciados no sean satisfactorios pueda tomarse la decisión de congelar el cambio, para revisar o re direccionar su planteamiento.

Con un entorno tan cambiante como el que se presenta hoy en día, con la implementación de nuevas leyes, un mercado bursátil poco predecible y la aparición de nuevas tecnologías es necesario el tener la disposición y actitud para afrontar estos cambios, generando oportunidades más que la búsqueda de problemas, teniendo en cuenta el tipo de cambio que se presente ya sea interno o externo se deben evaluar cuidadosamente y diagnosticar teniendo en cuenta estos factores.

4.2.6.2 Cambio tecnológico

Siempre ha existido una resistencia al cambio tecnológico, no necesariamente por la implementación que significaba en sí, sino por el cambio que este representaba ya que para muchas personas con la introducción de estos cambios gradualmente siente que serán reemplazados, es por lo que la relación entre el personal y la tecnología debe ser considerada como un encuentro técnico, en el cual el uno sea un complemento del otro. Davis (1979) denominó a la relación entre las personas y la tecnología “sistemas socio técnicos” Davis, L. (1979). Optimizing Organization Plant Design: a complementary Structure for Technical and Social Systems.

Según como dice Davis (1983)14, “el precio que exige la tecnología para el proceso que ofrece, es que las personas deben cambiar” (p. 281) Organizational Dynamics, Autumm. Davis, K. (1983). El Comportamiento Humano en el Trabajo. México: Mc Graw-Hill., lo que supone uno de los principales problemas que se presentan con el

progreso tecnológico radica precisamente en la rapidez con que la tecnología avanza, creando un limitante de adaptación para las personas, ya que no contarían con el tiempo suficiente para comprender y aplicar estas tecnologías en su totalidad a sus actividades laborales.

Este desarrollo tecnológico debe iniciar desde la formación académica, con el fin de afrontar los cambios que se puedan presentar, sin crear traumatismos para las personas o las empresas u organizaciones. Esto supone un amplio impacto, teniendo en cuenta que la evolución de las tecnologías de la información rompe con barreras y el ideal es que transciendan en a los limites organizacionales; es así que se da un cambio importante en la forma de hacer las cosas, desaparece poco a poco la corporeidad y aparece la colaboración a través de herramientas telemáticas que permiten la conexión a distancia en tiempo real, esta es una de las maneras de funcionamiento del teletrabajo[26]

4.2.6.3 Comunicación eficiente.

Ya sea en la sociedad o en una empresa u organización, la interacción entre los individuos que la componen es fundamental para crear un equilibrio que permita a todos sus miembros crecer, y el método empleado para que estos puedan llegar acuerdos es el poder contar con una comunicación eficiente y asertiva que permita que todos tenga un espacio de interlocución en el cual puedan escuchar y ser escuchados.

Es por este motivo que al momento que se desea implementar un cambio sin importar el ámbito que este sea, es necesario que las personas que van a experimentar este cambio puedan contar con un mecanismo que les permuta entender el alcance y las implicaciones que este conlleva, así mismo permitirá que la resistencia al cambio sea mínima y su implantación se exitosa; teniendo en cuenta lo anterior se pueden implementar dos tipos de comunicación como es el formal, el cual está basado en canales directos por medio de los cuales todas las personas involucradas pueden acceder a la información, por otra parte también se puede utilizar los canales informales, estos son empleados dependiendo de del tipo de información que se desee llevar a manos de las personas, un ejemplo de esto es cuando una empresa va hacer el lanzamiento de un nuevo producto y emplea a personas ajenas a la empresa para que compartan una expectativa sobre este, últimamente esto se vio frecuentemente por medio de los llamados influenciadores.

La principal ventaja de emplear una comunicación eficiente y asertiva se ve reflejado

[26] GONZÁLEZ ZULUAGA, Andrea, FLORÉZ LONDOÑO Kelly Danitza y PELÁEZ RAMÍREZ Viviana Vera Gestión Del Cambio Y El Teletrabajo [en línea]. Trabajo De Grado Para Optar El Titulo De Especialistas En Gestión Del Talento Humano Y La Productividad. Universidad de Medellín facultad de ciencias-económico administrativas especialización de gestión del talento humano y la productividad 2014. [Consultado: 10 de marzo de 2021]. Disponible en: https://repository.udem.edu.co/bitstream/handle/11407/385/Gesti%C3%B3n%20del%20cambio%20y%20el%20teletrabajo.pdf?sequence=1

en tiempo y costos, ya que al no tener que invertir grandes cantidades de tiempo y recursos en la implementación de un cambio cuando esta llega de forma clara y concisa a las personas permite en muchos casos que sea aceptado en poco tiempo y su implementación cuente con mínimos inconvenientes.

4.3 MARCO CONTEXTUAL

4.3.1 Las Pymes, el Teletrabajo, y la ciberseguridad en Colombia

Las Pymes en Colombia, de acuerdo a la Ley 590 de 2000, "se entiende por micro, pequeña y mediana empresa, toda unidad de explotación económica, realizada por persona natural o jurídica, en actividades empresariales, agropecuarias, industriales, comerciales o de servicios, rural o urbana" [27] y se clasifican así:

Cuadro 1. Pymes

TIPO	PERSONAL (Cantidad de Trabajadores)	ACTIVOS TOTALES (valor en smmlv)
Microempresa	Entre 1 a 10	Inferiores a 501
Pequeña Empresa	Entre 11 a 50	Mayores a 501 y menores a 5.001
Mediana	Entre 51 a 200	Entre 5.001 y 15.000

Fuente: COLOMBIA. Departamento Administrativo de la Función Pública. LEY 590 (10, julio, 2000). Por la cual se dictan disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresa [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 44.078 de Julio 12 de 2000. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=12672

Estas representan aproximadamente el "90% del sector productivo en Colombia y así mismo generando el 35% PIB y el 80% del empleo en nuestro país"[28]. No obstante, se vieron impactadas negativamente durante la cuarentena y confinamiento obligatorio decretado por el Gobierno Nacional y la propagación del COVID-19, presentando bajos ingresos y falta de liquidez financiera, lo cual provoco enviar a sus trabajadores a CASA y asumiendo nuevos desafíos organizacionales, logísticos e infraestructura para la realización de sus trabajos, conllevando a la aplicación de la modalidad del TELETRABAJO.

Se comprende que al presentarse este cambio inesperado, no todas las empresas y pymes se encuentran preparadas para asumir esta modalidad laboral, toda vez

[27] COLOMBIA. Departamento Administrativo de la Función Pública. LEY 590 (10, julio, 2000). Por la cual se dictan disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresa [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 44.078 de Julio 12 de 2000. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=12672

[28] COLOMBIA. Ministerio del Trabajo. "MiPymes representan más de 90% del sector productivo nacional y generan el 80% del empleo en Colombia": ministra Alicia Arango. [en línea]. Santa Fe de Bogotá, D.C. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.mintrabajo.gov.co/prensa/comunicados/2019/septiembre/mipymes-representan-mas-de-90-del-sector-productivo-nacional-y-generan-el-80-del-empleo-en-colombia-ministra-alicia-arango

que se requiere adoptar un modelo digital y con lo que este conlleva, es decir, que no solo es tener un ordenador, conexión a internet y otros aplicativos necesarios para desarrollar este, sino que también se debe tener en cuenta los conceptos de conectividad, comunicación, codificación y ciberseguridad, pero la poca cultura digital y capacidad tecnológica que existe en la empresas y las pymes en la actualidad hace que al aplicar el Teletrabajo se presenten innumerables riesgos logísticos y tecnológicos.

Como se indicó anteriormente la ciberseguridad es una de las piezas fundamentales a la hora de aplicar la modalidad del Teletrabajo en cualquier organización, pero este es un de los puntos más débiles que tienen las Pymes, toda vez que estas centran o colocan toda su atención en crecer y que funcionen sus negocios y no tienen en cuenta o no tienen dentro sus prioridades la Ciberseguridad. Así mismo esto se debe aún pensamiento que sea venido mantenido en las Pymes durante un tiempo, el cual es que, al ser una Pyme, no atraerían o no estarían en la mira de los ciberdelincuentes, sin embargo, el pasar por alto este problema podría ocasionar graves consecuencias, ya que los Ciberdelincuentes no distinguen a la hora de realizar sus ataques entre grandes organizaciones o pequeñas, pymes o personas jurídicas o naturales.

Por lo anterior, se hace necesario e indispensable que las Pymes, para adaptarse a este nuevo modelo digital que conozcan de los riesgos, amenazas y vulnerabilidades que se pueden presentar en esta transformación, el cómo pueden prevenir y/o mitigarlos, pero esto solamente se puede garantizar una guía base para el mejoramiento de la Ciberseguridad, la cual en el presente documento se irá desarrollando

4.4 MARCO LEGAL

4.4.1 Ley 1221 de 2008

El 16 de julio del 2008, se promulga la ley 1221, la cual define el teletrabajo como “una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo”. (Artículo 2, Ley 1221 de 2008), posterior a esto en el año 2012 se expide el decreto 0884, que se encarga de reglamentar esta ley.

Las características que define en teletrabajo como una actividad laboral que se efectúa en un lugar diferente del sitio de ubicación de la organización, empleado las tic, las cuales facilitan el cumplimiento de las funciones o asignaciones laborales.

Con la implementación de este modelo laboral se vio en la necesidad de

implementar canales eficientes de comunicación, una gestión, control y seguimiento adecuados a esta modalidad, teniendo en cuenta que la ley 1221 de 2008, en donde se identifican las siguientes áreas o espacios para ejecutar el teletrabajo así:

- **Autónomos**: hace referencia a aquellos trabajadores que mediante la implementación de las tecnologías de la información y la comunicación TIC, hace de cualquier espacio disponible su lugar de trabajo.
- **Móviles:** a diferencia de los autónomos, los móviles no cuentan con un espacio establecido, y se basa su trabajo en la implementación de dispositivos móviles.
- **Suplementarios:** este término es uno de los más aplicados durante el confinamiento por motivo del covid-19 durante el final del año 2020 y en los inicios del 2021, esto se debe a que los espacios en las empresas u organizaciones, no eran tan amplias para mantener la distancia entre los empleados, por este motivo se implementó este modelo que permitía que un grupo de trabajadores asistir a las oficinas unos días determinados y los otros desde sus hogares.

Por medio del ministerio de trabajo y el SENA (servicio nacional de aprendizaje), se implementó programas en los cuales se ofrecen una serie de beneficios aquella pyme, que vincularán a nuevas personas a al mercado laboral empleado este tipo de modalidad.

4.4.2 Decreto 884 de 2012

Con la promulgación de la ley 1221 del 2008, en el año 2012 sale el decreto 884, por medio del cual se reglamenta esta ley, en este decreto se establecen las condiciones que se tendrán en cuenta entre empleado y jefe, definiendo sus obligaciones ya sean en entidades públicas o del sector privado, el principal fundamento que introdujo este decreto, está basado en voluntariedad, igualdad y reversibilidad que se aplica en este modelo.

4.4.3 Resolución 2886 de 2012

Con la introducción de esta nueva modalidad de trabajo se dio a la creación de una red nacional por medio de la cual se fomentará el teletrabajo, teniendo en cuenta esto se dicta la resolución 2886 de 2012 por medio de la cual se definirá que tipo de entidades integraran esta red.

Esta red nacional tiene como fin principal el fomento del empleo, por este motivo se realizarán reuniones mensuales en las cuales se determinarán acuerdos y estrategias destinadas a dar a conocer las ventajas, esto será de manera descentralizada permitiendo que en la departamentos y municipios se puedan adaptar políticas y medidas de acuerdo a sus necesidades, teniendo un enfoque

sobre la población vulnerable.

Desde la promulgación de esta resolución en el 2012, se ha visto un incremento constante iniciando con un alrededor de 31.500 en el 2012 llegando a 122 mil TELETRABAJADORES a finales del 2018; pero es imposible hablar del incremento excepcional que sufrió esta modalidad de trabajo a casusa del confinamiento por covid-19, en donde se vio los grandes beneficios que esta modalidad trae consigo, al mismo tiempo que las dificultades que esta trae consigo en aspectos tercios y de ciberseguridad.

5 MARCOS LEGALES Y TÉCNICOS QUE REGULAN EL TELETRABAJO Y TRABAJO REMOTO

5.1 EXAMINAR LOS DIFERENTES MARCOS LEGALES Y TÉCNICO VIGENTE ENTRE EL TELETRABAJO Y TRABAJO REMOTO PARA SU ADOPCIÓN EN PYMES COLOMBIANAS.

5.1.1 Marco Legal y Técnico Teletrabajo en Colombia

5.1.1.1 Decreto 1072 de 2015

El aspecto principal que define las condiciones laborales es el tipo de contrato, y para evitar que se presenten condiciones laborales desfavorables en el decreto 1072 del 2015 en su artículo 2.2.1.5.3 define cuales son los requerimientos básicos, teniendo como base los siguientes aspectos:

Se debe tener en cuenta los aspectos tecnológicos asociados a los requerimientos del servicio, además del ambiente y espacio determinado para esto

Es pertinente el establecer un cronograma de actividades en el cual se identifiquen los días y horarios en los cuales se dará desarrollo a lo planteado.

Para el sitio de trabajo se establecerán unas pautas que servirán de guía en caso de cualquier incidente que pueda conllevar a un accidente laboral, identificando las responsabilidades de las partes.

Establecer responsabilidad sobre el manejo y custodia de la información suministrada y resultante del trabajo establecido a sí mismo la forma adecuada para la entrega de la misma al finalizar las actividades establecidas previamente.

En todo empleo existen una serie de responsabilidades inherentes a las obligaciones contractuales, pero para el teletrabajador se agrega una, que toma una importancia significativa, y es la de la seguridad informática, al no encontrarse laborando en las instalaciones del empleador, el teletrabajador debe de cumplir con una serie de recomendaciones que brindaran seguridad al momento de desarrollar las actividades laborales.

Es necesario tener en cuenta que al igual que un trabajo normal un teletrabajador debe de identificar el tipo de contrato por medio del cual se creara su vínculo laboral con su empleador, el cual puede ser:

- Contrato de trabajo a término fijo
- Contrato de trabajo a término indefinido

- Contrato por jornada laboral
- Contrato por duración de obra o labor asignada

Una de las principales ventajas con las que cuenta esta modalidad de trabajo se estipula en la ley 1221 de 2008 su artículo 6; «A los teletrabajadores, dada la naturaleza especial de sus labores no les serán aplicables las disposiciones sobre jornada de trabajo, horas extraordinarias y trabajo nocturno»[29] No obstante, la jornada laboral debe ser definida para efectos de delimitar la responsabilidad de la ARL como lo señala el artículo 2.2.1.5.3 del decreto 1072.

Adicional a esto en el parágrafo del mismo artículo se establece: «Cuando el teletrabajo sea ejecutado donde sea verificable la 8 jornada laboral, y el teletrabajador a petición del empleador se mantiene en la jornada laboral más de lo previsto en el artículo 161 del Código Sustantivo del Trabajo y de la Seguridad Social, o le asigna más trabajo del normal, el pago de horas extras, dominicales y festivos se le dará el mismo tratamiento de cualquier otro empleado»[30] En igual sentido se pronuncia el artículo 2.2.1.5.10 del decreto 1072 de 2015.

Con base en lo anterior el teletrabajador tendrá un máximo, si así lo estipula el contrato de 8 horas laborales dentro de las cuales se debe especificar si serán en un horario establecido o si por el contrario contara con una libertad de horario para desarrollarlas, si se presenta que este cuenta con una libertad horaria para elaborar su trabajo y este opta por realizarlas en horas de la noche esto no dará lugar a recargo nocturno; de igual forma esto se aplica para días feriados, esto cambiara si estos son estipulados por el empleador.

en relación con el tiempo de trabajo y la remuneración económica esta puede ser de dos tipos, en primer lugar no debe ser inferior al salario mínimo mensual vigente establecido por el gobierno nacional, o por el contrario a convenir por obra o trabajo ejecutado, esto son aspectos que debe analizar el trabajador antes de firmar un contrato mediante la modalidad de teletrabajo, según las últimas disposiciones dictadas por el gobierno nacional a través del ministerio de trabajo, los trabajadores que se encuentran mediante la modalidad de teletrabajo, tendrán acceso al subsidio de transporte pero en su caso será denominado como subsidio de telecomunicación, el cual está destinado a ayudar en los gastos de conectividad y apoyo al pago de servicio de luz.

[29] COLOMBIA. Congreso de la República de Colombia. LEY 1221 (16, julio, 2008). Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 47052 de julio 16 de 2008. [Consultado: 10 de abril de 2021]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=31431

[30] COLOMBIA. Congreso de la República de Colombia. LEY 1221 (16, julio, 2008). Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 47052 de julio 16 de 2008. [Consultado: 10 de abril de 2021]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=31431

5.1.1.2 Circular 027 de 2019

Durante los último años nuevas modalidades de trabajo han comenzado una revolución laboral en la cual se ha implementado la tecnología como base a su forma de trabajo, este es el caso del teletrabajo que durante los últimos 6 años ha presentado un incremento constante hasta llegar a un 200%, y con los efectos ocasionados por la pandemia COVID 19, este modelo de trabajo creció de manera exponencial, por esta razón el gobierno nacional el 12 de abril del 2019, se expide la circular 027 para "TRABAJADORES Y EMPLEADORES DEL SECTOR PUBLICO Y PRIVADO ADMINISTRADORAS DE RIESGOS LABORALES"[31], la cual dicta las siguientes precisiones:

- Las visitas al puesto de trabajo: es necesario concertar por las partes el cronograma de una serie de visitas, en las cuales se identificaran una serie de características que permitirán evaluar la conveniencia de ejercer el teletrabajo, entre las características a tener en cuenta es físicas, biológicas, psicosocial entre otras, y atendiendo lo dispuesto en el artículo 2.2.1.5.9 del decreto 1072 de 2015, el empleador debe contar con una guía de riesgos profesionales y en base a la información obtenida se podrá diligenciar el formulario de afiliación para teletrabajo como se especifica en la resolución 3310 del 2018.

  Los aspectos que se tendrán en cuenta al momento de la afiliación, el lugar de trabajo, las actividades que se ejecutaran, el riesgo que estas representan y el horario dentro del cual se desarrollaran las actividades. Esta información permitirá general un reporte el cual se identifiquen las condiciones laborales.

- Una de las principales dificultades es el identificar quien es el encargado de proveer los equipos y herramientas, esto fue reglamentado mediante el artículo 6 en su numeral 7 la cual dicta que "los empleadores deberán proveer y garantizar el mantenimiento de los equipos de los teletrabajadores, conexiones, programas, valor de la energía, desplazamientos ordenados por él, necesarios para desempeñar sus funciones".[32]

  Esto acompañado del artículo 57 del código sustantivo del trabajo estable, en su numeral 1 "son obligaciones especiales del patrono el poner a disposición de los teletrabajadores, salvo estipulación en contrario, los

[31] COLOMBIA. Ministerio del Trabajo. CIRCULAR 0017 (24, febrero, 2020). Lineamientos minimos a implementar de promoción y prevención para la preparación, respuesta y atención de casos de enfermedad por covid-19 (antes denominado coronavirus) [en línea]. Santa Fe de Bogotá, D.C.: [Consultado: 10 de abril de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=107276

[32] COLOMBIA. Congreso de la República de Colombia. LEY 1221 (16, julio, 2008). Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 47052 de julio 16 de 2008. [Consultado: 10 de abril de 2021]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=31431

instrumentos adecuados y los materiales primos necesarios para la realización de las labores".

En concordancia con lo expuesto se puede concluir que el empleador y el trabajador acordaran las condiciones del desarrollo de las actividades de acuerdo a lo establecido en las leyes, decretos y normas existentes.

En 1973 se presentó la crisis una crisis petrolera, que trajo consigo un sin número de dificultades, entre las cuales laborales, es en este momento cuando **JACK NILLES**, propone la idea de "llevar el trabajo al trabajador", [33]dando así nacimiento al concepto telecommunting. Con el paso del tiempo y loa avances en tecnología y el ingreso de la internet o World Wide Web, se abrieron más caminos que permitieron explorar esta modalidad de trabajo, pero fue hasta después del 11 de septiembre del 2001 cuando esta modalidad de trabajo creo un avance significativo; gracias a este movimiento américa latina comenzó a explorar esta forma de trabajo que les permitía una reducción de costos significativa.

A medida que el tiempo ha transcurrido esta modalidad de trabajo fue tomando cada vez más auge y esto llevo a los diferentes países a comenzar una reglamentación sobre esta modalidad, España forma el plan concilia que regula el teletrabajo en el 2006, y Colombia en el 2008 crea la ley 1221 en su artículo 2, donde define esta actividad modo de remuneración y manejo de la información y tecnologías de la comunicación, que posteriormente en el año 2012 se realiza una reglamentación parcial a la ley 1221.

Pero esto no era suficiente al ser una modalidad de trabajo poca explorada para lo cual en el año 2020 se establece por parte del ministerio de tecnológicas de la información y comunicaciones, el libro blanco que contiene el ABC de los elementos y parámetros del teletrabajo en Colombia, este compendio está dividido en 4 capítulos de la siguiente manera:

- Conceptos clave
- Implementación del teletrabajo en las organizaciones
- Tecnología para teletrabajar
- Consideraciones jurídicas y legales del teletrabajo

Cada capítulo desarrolla las temáticas más importantes desde los aspectos básicos a los más complejos, lo que lleva a evidenciar como esta modalidad de trabajo surge con el fin de ayudar a superar una crisis laboral como la que se ha estado presentando a nivel mundial por efectos del covid-19, por otro lado, diferentes organismos y especialistas con el paso de los años han aportado conceptos o referencias que han ayudado a construir los esquemas sobre para abordar el teletrabajo, por ejemplo:

[33] 360es.com. Llevar el trabajo al trabajador, y no el trabajador al trabajo [en línea]. 360es.com. [Consultado: 10 de abril de 2021]. Disponible en: https://360es.com/es/llevar-el-trabajo-al-trabajador-y-no-el-trabajador-al-trabajo/

Tabla 1. Conceptos y Definiciones

	CONCEPTO O DEFINICIÓN
Martínez-Cárdenas, Cote-Rangel, Dueñas, & CamachoRamírez (2017)	Habla que, al ser una actividad laboral reciente, y por este motivo existen zonas grises que no están contempladas en la legislación naciente para reglamentar el teletrabajo, una de las más frecuentes es la de no contar con un horario establecido que defina los momentos de descanso o familiares con los laborales.
Alzate & Giraldo (2017)	Afirman que con el desarrollo tecnológico cada día se acerca el momento en el cual con un ordenador o un dispositivo móvil se pueda acceder de manera rápida y sin importar el lugar a las actividades laborales, lo cual permite ahorrar tiempo en transporte, problemas interpersonales en el lugar de trabajo, ambiente cómodo para el desarrollo de las actividades laborales entre otros.
Osio (2018)	Reconoce el teletrabajo como un trabajo normal con los mismos derechos y deberes por consiguiente debe contar con una remuneración acorde a lo estipulado por la ley o lo acordado por las partes.
Rolon & Sánchez (2018),	Habla sobre como con cualquier actividad, al iniciar es carente de normas o leyes que determinen los derechos y responsabilidades de las partes, pero con el transcurso del tiempo y de las determinaciones adoptadas se va construyendo una base que garantiza equidad entre las partes.
Valencia (2018)	Enumera una serie de beneficios que conlleva el teletrabajo como es: El poder determinar por medio de un cronograma de actividades en qué momento dentro del tiempo establecido desarrollar la(s) actividad(es) propuesta(s). De acuerdo a las condiciones laborales el poder determinar qué tipo de trabajo

	realizar ampliando las oportunidades de crecimiento laboral, al igual que permite ofrecer un servicio a más de una compañía siempre y cuando las estipulaciones laborales lo permitan. En el ámbito personal las principales ventajas son: El poder compartir más tiempo con la familia, mejorando la calidad de vida tanto de la persona como del ambiente familiar. Brinda una oportunidad laboral para las personas que cuentan con condición de discapacidad, al igual que permite la creación de nuevos modelos de empresas en mercados que se comienzan a explorar.
Cifuente & Londoño-Cardozo (2020),	Afirman que su principal impacto se ve reflejado en el ambiente laboral, ya que este este es más relajado y brinda las condiciones de generar tiempo de calidad con la familia.
Fernández (2020),	Habla que el teletrabajo ha sido una alternativa muy favorable para las empresas que estas iniciando o aquellas que cuentan con una actividad económica que requiere de una flexibilidad en el mane4jo de tiempos y personal, esto sin contar los hechos ocurridos a causa del covi-19, en donde debido a las circunstancias obligo a un sin número de empresas a cambiar su forma de trabajo, lo que despertado en muchas personas opiniones positivas o negativas sobre la implementación del teletrabajo, teniendo este escenario Fernández habla sobre el no hacer juicios en este momento donde el escenario laboral está en constante cambio, ya sea porque se aplicó el teletrabajo, el trabajo remoto, o ya sea por alternancia, y el hacer un juicio de valor teniendo en cuenta los problemas de pandemia no permitirá

	identificar las ventajas y desventajas reales de esta modalidad de trabajo.
En el caso específico de Colombia, antes de la pandemia el teletrabajo según cifras de MinTIC (2020)	Según un estudio realizado por minTic, para marzo del 2020 (antes del confinamiento total a causa del covid-19) se tenía registrado alrededor de 20 mil teletrabajadores en el país, posteriormente durante los tres meses siguiente se fue incrementando de manera exponencial para terminal el año se registraron un incremento alrededor de más de dos millones de nuevos teletrabajadores y sigue en aumento.

Fuente: “elaboración propia”

Teniendo en cuenta lo anterior, la herramienta más importante es la tecnología, ya que esta será el vínculo del trabajador con la empresa u compañía, sobre todo en el manejo de la información, ya sea porque esta se maneja de forma diaria o en grandes volúmenes en un tiempo determinado, ya sea que esto se realice por medio de una aplicación o varias de estas, convirtiendo al teletrabajo en un universo de posibilidades y oportunidades tanto para trabajadores y empresas de abrir nuevos mercados y servicios, cambiando la forma de percibir el mundo laboral.

5.1.2 Marco legal y técnico trabajo remoto en Colombia

Con los acontecimientos ocasionados por el covid-19, comenzaron a surgir una serie de conceptos que si bien no son nuevos eran desconocidos para muchas personas, este es el caso del teletrabajo que fue originalmente comparado con el trabajo remoto; con la nueva realidad que se presentó en el país y el mundo entero era necesario la implementación de estrategias que diera la libertad a los empleados de laboral desde sus hogares ya sea por unos días de la semana de terminados o de forma permanente, es en este momento donde se desvinculo el concepto de teletrabajo con el de trabajo remoto, obligando al gobierno nacional la creación de un concepto base donde se identifiquen los derechos y obligaciones por parte del empleador y el trabajador.

Este lapso de tiempo permitió ver las ventajas y desventajas que representa esta modalidad de trabajo, el principal inconveniente que se encuentra sobre la mesa es que esta modalidad está planteada para ser una medida transitoria, que se adoptó por necesidad a una realidad determinada, por otra parte la legislación vigente y la que se ha tramitado y se está tramitando deja de lado una serie de aspectos que dejan una serie de vacíos que se prestan para creas desventajas para las partes participantes.

2. **Modalidades de trabajo remoto.**

Analizando la información y la legislación existente se puede inferir que el trabajo remoto no se puede comparar con el teletrabajo ya que el primero se podría tomar como el género, mientras que el segundo se puede determinar con una de sus modalidades; se debe entender que la expresión trabajo remoto es empelada para denominar una serie de actividades que no se encuentran reglamentadas como es el caso del teletrabajo, trabajo a domicilio o trabajo en casa entre otras; en España se expide el real decreto 28 el 2020 donde se identifica el trabajo a distancia (en Colombia denominado trabajo remoto), donde dice que la "forma de organización del trabajo o de realización de la actividad laboral conforme a la cual esta se presta en el domicilio de la persona trabajadora o en el lugar elegido por esta, durante toda su jornada o parte de ella, con carácter regular" [34](Artículo 2-a).

Por otra parte, dice que el teletrabajo es "aquel trabajo a distancia que se lleva a cabo mediante el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación" [35](Artículo 2-b).

A continuación, se presentan las siguientes modalidades

Tabla 2. Modalidades

Modalidad	Definición
Trabajo a Domicilio	Forma de trabajo que se consagro en el código sustantivo del trabajo en su artículo 89, es una normatividad que se encuentra en vigencia, pero durante los últimos años ha dejado de estar en uso activo, a diferencia del teletrabajo esta modalidad de trabajo ya que emplea herramientas de información y comunicación ya sea solo o con la ayuda de amigos o familiares, enfocándose en las herramientas más que en el servicio.

[34] ESPAÑA. Jefatura del Estado. Real Decreto-ley 28 (22, septiembre, 2020). de trabajo a distancia [en línea]. España: «BOE» núm. 253, de 23/09/2020. [Consultado: 10 de abril de 2021]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2020-11043#a2

[35] ESPAÑA. Jefatura del Estado. Real Decreto-ley 28 (22, septiembre, 2020). de trabajo a distancia [en línea]. España: «BOE» núm. 253, de 23/09/2020. [Consultado: 10 de abril de 2021]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2020-11043#a2

Teletrabajo	Una modalidad de trabajo que genera empleo empleado los medios de comunicación y herramientas tecnológicas, con las cuales desempeña sus actividades, teniendo en cuenta esto las TIC proclaman la ley 1221 del 2008 y el decreto 884 del 2012 donde se busca reglamentar esta modalidad de trabajo, en donde las partes conozcan sus deberes y derechos. Esta modalidad de trabajo ha tenido su auge durante la pandemia covid-19, ya que por las circunstancias de confinamiento muchas empresas han buscado una modalidad en la que puedan seguir trabajando, es ahí donde el teletrabajo entro en escena, ya que permite que los trabajadores puedan realizar sus actividades laborales desde sus hogares, siempre contando con las medidas que permitan ejercerlas de forma adecuada (para lo cual cuenta con el aval de las aseguradoras de riesgos profesionales).
Trabajo en Casa	Es una medida que se puede confundir con el teletrabajo, pero la gran diferencia es que esta medida no cuenta con una reglamentación sobre los deberes y derechos de las partes, lo cual permite que no se respeten los límites de cargas laborales. Durante la pandemia de covid-19 un sin número de trabajadores aceptaron la modalidad de trabajo en casa, que con el transcurso del tiempo se fue evidenciando como se presentaron una serie de inconveniencias por parte de una o de las dos partes involucradas, en

	este momento se han comenzado una serie de debates en el congreso de la república, en donde se reglamenten al menos los conceptos básicos. Es de anotar que esta modalidad de trabajo esta siento tomada de manera transitoria, y es muy probable que en el momento que se pueda regresar a un estado de normalidad estable, esta tendera a desaparecer o disminuir en gran medida.
Trabajo Remoto	Esta es una modalidad de trabajo en donde el empleador destina que uno o varios de sus trabajadores presten sus servicios en lugares remotos, esto quiere decir que puede ser fuera del área de influencia de la compañía (como es el caso de un nuevo departamento o fuera del país) todo contando con el apoyo en caso de riesgo por parte de las ARL, que de seguridad tanto a la empresa como a los trabajadores.
Nómadas Digitales	Con el avance tecnológico que se ha presentado durante los últimos años, se ha comenzado a ver una nueva modalidad de trabajo, en el cual da una libertad amplia a sus trabajadores para que estos puedan ejercer sus labores desde cualquier lugar del mundo, estos son denominados nómadas digitales, ya que sin importar el lugar de residencia (esto puede ser cualquier lugar del mundo), mientras cuenten con un dispositivo con acceso a internet estos tendrán la posibilidad de efectuar sus labores. Dentro de este grupo existen un grupo de individuos que han

	logrado un reconocimiento a nivel mundial, a los cuales se le han denominado como influencer, quienes con el acceso a internet y diversas plataformas (generalmente de redes sociales), desde las cuales llegan a un sin número de personas y con su influencia hacen que un producto o servicio pueda ser visto y contratado por sus seguidores generando un gran impacto en el mercado.

Fuente: “elaboración propia”

Propuesta en curso para la post-pandemia

En el año 2020, el 31 de diciembre se expidió la ley 2069, “de Emprendimiento, Una ley para el fomento y desarrollo cooperativo y de la economía solidaria”, [36]en sus artículos se busca la fomentación de empleo por medio de la creación de empresas y la consolidación de pymes; entre la regulación se puede encontrar sobre el trabajo en casa, cuya modalidad de trabajo se fue implementada durante el confinamiento del covid-19, esta modo laboral fue confundido con el teletrabajo que fue reglamentado en la ley 1221 de 2008, su principal diferencia está centrada en la implementación de medios de comunicación y protocolos de seguridad para los empleados.

Con la nueva normalidad que se presenta tanto a nivel nacional como mundial, es necesario la creación de nuevos escenarios que permitan la fomentación de empleo y esto se presenta como una oportunidad por medio de la cual reactivar la economía manteniendo la productividad y la estabilidad de los hogares en tiempos de pandemia.

Teniendo en cuenta lo anterior el senado de la república de Colombia busca aprobar un proyecto de ley que se encargue de regular la modalidad de trabajo en casa, en donde se tendrán aspectos como las condiciones, derechos y obligaciones de los trabajadores; así mismo se identificara los elementos necesarios que permitirán el buen ejercicio de las labores contractuales, para lo cual la empresa entregara estos implementos; y todo lo anterior y demás aspectos serán consagrados de manera escrita por medio de un contrato firmado y legalizado por las partes.

[36] COLOMBIA. Congreso de la República de Colombia. LEY 2069 (31, diciembre, 2020). "por medio del cual se impulsa el emprendimiento en Colombia [en línea]. Santa Fe de Bogotá, D.C.: [Consultado: 10 de abril de 2021]. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%202069%20DEL%2031%20DE%20DICIEMBRE%20DE%202020.pdf

El senado de la república de Colombia dio aprobación al proyecto de ley 352 del 2020 y el 429 del 2020 en la cámara de representantes, que se encarga de la regulación de del trabajo en casa y dista otras disposiciones en el uso de esta figura; pero es necesario entender que esta es una figura ocasional, excepcional y especial, y que con la implementación de esta ley se busca proteger a los trabajadores y empleadores al crear un vínculo formal que garantice derechos y obligaciones de las partes.

5.1.3 Análisis comparativo entre Teletrabajo y Trabajo Remoto

Cuadro 2. Análisis comparativo entre Teletrabajo y Trabajo Remoto

	NORMATIVIDAD LEGAL VIGENTE	**DIFERENCIAS**	**SIMILITUDES**
TELETRABAJO	• Ley 1221 de 2008 • Decreto 884 de 2012 • Resolución 2886 de 2012 • Decreto 1072 de 2015 • Circular 027 de 2019	• Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo	• Se tiene remuneración o salario por las actividades laborales realizadas • Se tiene derecho a jornadas o espacios de descanso • Se trata al empleado con dignidad e igualdad

		• La organización tiene el deber de provisionar de equipos necesarios para garantizar el cumplimiento de las actividades laborales tales como conexión, equipos de cómputo, pago servicios de energía entre otros • La organización tiene el deber de garantizar que el lugar de trabajo se acople con lo establecido en los sistemas de salud y seguridad en el trabajo. • Esta modalidad se presenta como un acuerdo por escrito por las partes. Así mismo este contrato se debe	

		presenta ante ARL • Esta modalidad de teletrabajo se encuentra incluida en el reglamento de trabajo.	
TRABAJO REMOTO	• Circular 21 del 17 de marzo de 2020 por MINTRABAJO • Circular 41 del 2 de junio de 2020 por MINTRABAJO : lineamientos para adoptarlo durante tiempos de pandemia • Ley 352 de 2020 en Senado y 429 de 2020 en Cámara: Se encuentra a espera de sanción presidencial para promulgación y aplicación, la reciente ley aprobada por el Senado la cual tiene como fin regular el 'trabajo en casa o trabajo remoto'	• Se presenta por mandato excepcional del Gobierno Nacional dentro del marco de la emergencia sanitaria covid-19, situación temporal y ocasional teniendo como objetivo el buen desarrollo de las actividades laborales en el domicilio de los trabajadores. • Las organizaciones no se encuentran obligadas legalmente hasta el momento de	

		proporcionar equipos, herramientas. • Actualmente no se encuentra regulado el rol con las ARL.	

Fuente: “elaboración propia”

6 RIESGOS Y AMENAZAS QUE AFECTAN A LA CIBERSEGURIDAD EN LA MODALIDAD DEL TELETRABAJO EN LAS PYMES COLOMBIANAS

6.1 EVALUAR LOS RIESGOS Y AMENAZAS QUE AFECTAN A LA CIBERSEGURIDAD EN LA MODALIDAD DEL TELETRABAJO EN LAS PYMES COLOMBIANAS MEDIANTE LA APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN.

6.1.1 Ciberataques en la modalidad del Teletrabajo

El teletrabajo es uno de los grandes retos desde el año 2020, revolucionando la manera como las empresas a nivel nacional se han tenido que organizar, para llevar a cabo sus procesos operacionales, sin afectar su productividad y su posición en el mercado vigente. Así mismo, se han buscado formas de descentralizar la información y manejar los recursos tecnológicos de una manera más optima

De acuerdo con las cifras presentadas por la fiscalía general de la nación en el periodo comprendido entre marzo y noviembre del año 2020, se observa un aumento en ciberataques en un 98%, uno de los más comunes es la suplantación en donde se busca el robo de datos personales de la víctima y es el delito con más crecimiento en un 372% con respecto a años anteriores, otras prácticas de los ciberdelicuentes fueron el phishing, spoofing y pharming que atacaron a las empresas[37]

Estas cifras anteriormente mencionadas, son respaldadas por Comparitech, especializada en servicios informáticos, quién menciona que Colombia se encuentra en el puesto 39 en el ranking mundial de ciberseguridad. Además, esta entidad asegura que es necesario desarrollar estrategias de seguridad en un corto plazo

Una de estas estrategias a implementar tiene que ver con el factor múltiple de autenticación, que permite realizar el proceso de validación. Existen herramientas como por Microsoft que cuenta con una predicción de ataques, monitoreo de fugas de información, control de dispositivos asociados, etc.

Realmente lo que se busca es implementar políticas, procedimientos y técnicas que puedan generar alertar tempranas, se pueda auditar periódicamente y así mismo, realizar sensibilización a los usuarios sobre entornos seguros de la información, a

[37] PORTAFOLIO. Cifras de ciberseguridad en Colombia prenden alarmas al cierre de 2020 [en línea]. portafolio.co [Consultado: 10 de abril de 2021]. Disponible en: https://www.portafolio.co/tendencias/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020-547412

esto se le denomina “higiene cibernética” y es responsabilidad de las organizaciones, mediante la gestión de diferentes herramientas, así como del talento humano y gestión eficiente con que se cuente.

El año 2021, será un reto en Colombia en cuanto a ciberseguridad teniendo presente el actuar del gobierno nacional frente a la emergencia sanitaria por COVID – 19, que seguirá obligando a la mayoría de colombianos a trabajar desde casa. Los diferentes estudios realizados, muestran que en Colombia se realizaron más de 32.000 reportes de ciberataques cifra que es muy preocupante para el desarrollo tecnológico y de las empresas a nivel nacional y que constituye un factor de riesgo para los activos de información.

A continuación, se presenta el porcentaje de crecimiento en cuanto a delitos informáticos en Colombia, con el fin de contar con un mejor panorama de la situación vivida:

Tabla 3. Crecimiento delitos informáticos en Colombia

Tipo de delito	**Porcentaje de crecimiento con respecto al año 2019**	**Número de casos reportados**
Suplantación de sitios web	372%	3.800
Violación de datos personales	190%	6.159
Hurto por medios informáticos	39%	12.000

Fuente: “elaboración propia”

Las anteriores cifras, registran el incremento de actividad cibercriminal en el país, que cuenta con más de 5.400 millones de intentos de ciberataques en el periodo comprendido entre enero y junio de 2020, cifras que muestran el margen de criminalidad comparándolas con 15.000 millones de amenazas presentadas en el mismo periodo en toda Latinoamérica y el caribe, la mayoría de ataques o intentos de los mismos, son los denominados “fuerza bruta”, sin embargo, los delincuentes han cambiado sus formas de operar y pueden llegar a utilizar herramientas más sofisticadas, para obtener su cometido.

Los ataques de “fuerza bruta”, son acciones repetitivas que, si se revisan cuidadosamente, se encuentra que el criminal busca descifrar el algoritmo que guarda las credenciales del usuario y en Colombia es muy común encontrar este

tipo de ataques o intentos de los mismos con una cantidad cercana a los 818 millones solo mencionando el primer semestre de 2020.

Con la aparición de la emergencia sanitaria por COVD – 19 y la preocupación del trabajo desde el hogar o teletrabajo, se encuentra que no son suficientes los mecanismos utilizados actualmente para la protección de datos, las cifras demuestran que Colombia, se encuentra en un proceso de crecimiento en cuanto a ciberseguridad se refiere, sin embargo, es necesario seguir analizando la problemática y seguir integrando diferentes herramientas en este tema.

6.1.2 Normatividad vigente de la ciberseguridad en Colombia

La legislación colombiana ha ido evolucionando, incluyendo normatividad que apoye la protección de datos y haga frente a los diversos delitos informáticos. A continuación, se mencionará la legislación de manera cronológica:

Constitución Política de Colombia 1991:

“ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.”[38]

“Ley 527 de 1999 – Comercio Electrónico “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”[39]

[38] COLOMBIA. Asamblea Nacional Constituyente. Constitución Política de la República de Colombia (20, julio, 1991). [en línea]. Santa Fe de Bogotá, D.C.: Gaceta Constitucional No. 116 de 20 de julio de 1991 última actualización Diario Oficial No. 51.635 - 15 de abril 4 de 2021 [Consultado: 10 de abril de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html#1

[39] COLOMBIA. Congreso de la República de Colombia. LEY 527 (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial No. 43.673, de 21 de agosto de 1999 [Consultado: 10 de abril de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

"Ley 603 de 2000 - Control de Legalidad de Software"[40]

"Ley 1266 de 2008- Habeas Data Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"[41]

"Ley 1341 de 2009- Sociedad de la Información y las TIC's Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones –TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones"[42]

"Ley 1273 de 2009 – "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones." ARTÍCULO 1o. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos" "Articulado del 269A al 269J. [43]

Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009 Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones."[44]

"Documento CONPES 3701 de 2011 Lineamientos de política para ciberseguridad y ciberdefensa"[45]

---

[40]COLOMBIA. Congreso de la República de Colombia. LEY 603 (27, julio, 2000). Por la cual se modifica el artículo 47 de la Ley 222 de 1995. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial No 44.108, de 31 de julio 2000 [Consultado: 10 de abril de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0603_2000.html

[41] COLOMBIA. Congreso de la República de Colombia. LEY ESTATUTARIA 1266 (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial No. 47.219 de 31 de diciembre de 2008 [Consultado: 10 de abril de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

[42] COLOMBIA. Congreso de la República de Colombia. LEY 1341 (30, julio, 2009). Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial No. 47.219 de 31 de diciembre de 2008 [Consultado: 10 de abril de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

[43] COLOMBIA. Congreso de la República de Colombia. LEY 1273 (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial No. 47.223 de 5 de enero de 2009 [Consultado: 10 de abril de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html#:~:text=El%20que%2C%20sin%20orden%20judicial,y%20dos%20(72)%20meses.

[44]COLOMBIA. Congreso de la República de Colombia. RESOLUCION 2258 (23, diciembre, 2009). Por la cual se modifican los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1.8 y 2.4 de la Resolución CRT 1740 de 2007.. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial 47572 de diciembre 23 de 2009 [Consultado: 10 de abril de 2021]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=38498

[45]COLOMBIA. Consejo Nacional De Política Económica Y Social República De Colombia Departamento Nacional De Planeación Documento CONPES 3701 (14 de julio de 2011). POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. [en línea].

"Ley 1581 de 2012- Protección de Datos Personales Por la cual se dictan disposiciones generales para la protección de datos personales."[46]

"Decreto reglamentario 1377 de 2013- Protección de datos Personales Reglamentar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales."[47]

"Circular 052 de 2007 (Superintendencia Financiera de Colombia) Fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de Medios y canales de distribución de productos y servicios para clientes y usuarios."[48]

Norma Técnica NTC-ISO/IEC Colombiana 27001 El estándar para la seguridad de la información ISO/IEC 27001, especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).[49]

Santa Fe de Bogotá, D.C.: [Consultado: 10 de abril de 2021]. Disponible en: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

[46] COLOMBIA. Congreso de la República de Colombia. LEY 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales.. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial No. 48.587 de 18 de octubre de 2012 [Consultado: 10 de abril de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[47] COLOMBIA. Ministerio De Comercio, Industria Y Turismo. Decreto 1377 (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012 [en línea]. Santa Fe de Bogotá, D.C.: [Consultado: 10 de abril de 2021]. Disponible en: http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf

[48]COLOMBIA. Superintendencia Financiera De Colombia. Circular Externa 052 (octubre, 2007). capitulo décimo segundo: requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios [en línea]. Santa Fe de Bogotá, D.C.: [Consultado: 10 de abril de 2021]. Disponible en: https://www.enlaceoperativo.com/articulo/circular-externa-052-de-2007/

[49] ISOTOOLS. Sistemas de Gestión de Riesgos y Seguridad ¿Qué es la ISO 27001?. [en línea]. Edición. Bogotá D.C. [Consultado10 de marzo de 2021]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001#:~:text=ISO%2027001%20es%20una%20norma,los%20sistemas%20que%20la%20procesan.&text=La%20Gesti%C3%B3n%20de%20la%20Seguridad,en%20la%20norma%20ISO%2027002.

6.1.3 Identificación y Evaluación de riesgos y amenazas que afectan a la Ciberseguridad en la modalidad del Teletrabajo en Colombia.

Teniendo en cuenta la importancia de los activos de información que se emplean en las actividades de propias del teletrabajo, tales como hardware, software, almacenamiento, bases de datos, comunicaciones, procedimientos y recursos humanos asociados; se hace necesario implementar una metodología que permita hacer una gestión de riesgos y amenazas que afectan a estos activos.

De acuerdo a lo anterior se utilizaría la metodología MAGERIT, la cual permitirán hacer una identificación y evaluación de riesgo y amenazas, que afectan a los activos de información que se emplean en las actividades de propias del teletrabajo (Ver ANEXO A).

Así las cosas, a continuación, en la siguiente Tabla se presentarán la clasificación de los tipos activos de información de conformidad con a lo estandarizado por la metodología MAGERIT.

Tabla 4.Tipos activos de información

CATEGORÍA DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	UBICACIÓN	RESPONSABLE
[D] DATOS	Base de datos Backups	Se generan copias de seguridad de la actividad realizada	Servidores de la organización	Organización / teletrabajador
[S] SERVICIOS	Página Web	Servicio de información de la organización contratado con	Servidor web de la organización	Organización

		proveedor de dominios		
	Correo Electrónico / CHAT´S	Servicio de mensajería utilizado como puente de comunicación con los demás usuarios de la organización		
	VPN	Servicio de red segura utilizado como puente de comunicación entre los servidores de la organización y la terminal u ordenador del usuario		
[SW] SOFTWARE	Antivirus	Aplicación que permite tener una protección contra software maliciosos	Equipos de computo	Teletrabajador
	Paquete ofimático	Aplicaciones para creación, modificación y lectura de archivos de		

		texto, presentaciones y hojas de cálculo.		
	Aplicación web	Software utilizado para el buen desarrollo de las actividad del usuario que tienen que ver propiamente con la funciones de la organización		
[HW] EQUIPAMIENTO INFORMÁTICO	Laptop personales	Dispositivos de cómputo para el desarrollo de las actividades laborales	Domicilio del teletrabajador	Teletrabajador
[COM] REDES DE COMUNICACIONES	Router	Dispositivos de red encargados de la interconexión de la red de datos conexión	Domicilio del teletrabajador	Teletrabajador
	Internet			
[L] INSTALACIONES	Domicilio del trabajador	Lugar designado por la organización para el	Domicilio del teletrabajador	Teletrabajador

	desarrollo de las actividades laborales del tele trabajador

Fuente: “elaboración propia”

6.1.3.1 ANALISIS DE RIESGOS

Una vez realizado el proceso de identificación y clasificación de los activos que se pueden ser empleados en la modalidad del Teletrabajo, se continuara con el análisis de riesgos existentes para cada uno de estos, de conformidad con la metodología MAGERIT.

A continuación, se iniciará con el dimensionamiento con respecto a la valoración, el permite establecer los atributos que hacen valioso un activo con el objetivo de valorar las consecuencias de la materialización de una amenaza. ANEXO B FINAL DEL DOCUMENTO

A partir de los criterios de valoración (ANEXO C), los cuales son la escala para medir el nivel de daño que se puede presente en una organización, se realizará la valoración y análisis de riesgos.

Tabla 5. Valoración y análisis de riesgos

CATEGORÍA DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	UBICACIÓN	RESPONSABLE	DIMENSIONES				
					D	**I**	**C**	**A**	**T**
[D] DATOS	Base de datos	Se generan copias de seguridad de la actividad realizada	Servidores de la organización	Organización / teletrabajador	A	A		A	
	Backups				A	M		B	

[S] SERVICIOS	Página Web	Servicio de información de la organización contratado con proveedor de dominios	Servidor web de la organización	Organización	M	M		M
	Correo Electrónico / CHAT´S	Servicio de mensajería utilizado como puente de comunicación con los demás usuarios de la organización			A	M	A	A
	VPN	Servicio de red segura utilizado como puente de comunicación entre los servidores de la organización y la terminal u ordenador del usuario			A	M	A	A
[SW] SOFTWARE	Antivirus	Aplicación que permite tener una protección contra software maliciosos	Equipos de computo	Teletrabajador	A	A		
	Paquete	Aplicaciones			A	A		

	ofimático	para creación, modificación y lectura de archivos de texto, presentaciones y hojas de cálculo.						
	Aplicación web	Software utilizado para el buen desarrollo de las actividad del usuario que tienen que ver propiamente con la funciones de la organización			A	A	M	
[HW] EQUIPAMIENTO INFORMÁTICO	Laptop personales	Dispositivos de cómputo para el desarrollo de las actividades laborales	Domicilio del teletrabajador	Teletrabajador	M	M		
[COM] REDES DE COMUNICACIONES	Router	Dispositivos de red encargados de la interconexión de la red de datos conexión	Domicilio del teletrabajador	Teletrabajador	M	M		M
	Internet				A	M		

[L] INSTALACIONES	Domicilio del trabajador	Lugar designado por la organización para el desarrollo de las actividades laborales del tele trabajador	Domicilio del teletrabajador	Teletrabajador	B	B

Fuente: “elaboración propia”

Ahora bien, una vez que realizo el dimensionamiento con respecto a la valoración, continuamos con la identificación de cada una de las amenazas según la metodología MAGERIT y que aplican a los activos anteriormente identificados.

Tabla 6. Identificación de amenazas

CATEGORÍA DEL ACTIVO	NOMBRE DEL ACTIVO	AMENAZAS
[D] DATOS	Base de datos	[E.2] Errores del administrador [[A.11] Acceso no autorizado
	Backups	[E.1] Errores de los usuarios [E.2] Errores del administrador
[S] SERVICIOS	Página Web	[I.8] Fallo de servicios de comunicaciones
	Correo Electrónico / CHAT´S	[I.8] Fallo de servicios de comunicaciones [E.8] Difusión de software dañino

		[A.5] Suplantación de la identidad del usuario [A.14] Interceptación de información
	VPN	[I.8] Fallo de servicios de comunicaciones [E.8] Difusión de software dañino [A.5] Suplantación de la identidad del usuario [A.14] Interceptación de información
[SW] SOFTWARE	Antivirus	[E.20] Vulnerabilidades de los programas(software) [E.21] Errores de mantenimiento / actualización de programas (software)
	Paquete ofimático	[E.21] Errores de mantenimiento / actualización de programas (software) [E.1] Errores de los usuarios
	Aplicación web	[E.21] Errores de mantenimiento / actualización de programas (software) [E.1] Errores de los usuarios [I.8] Fallo de servicios de comunicaciones
[HW] EQUIPAMIENTO INFORMÁTICO	Laptop personales	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.5] Avería de origen físico o lógico
[COM] REDES DE COMUNICACIONES	Router	[I.1] Fuego [I.2] Daños por agua [I.5] Avería de origen físico o lógico [E.4] Errores de configuración
	Internet	[I.6] Corte del suministro eléctrico [I.8] Fallo de servicios de

		comunicaciones [I.9] Interrupción de otros servicios y suministros esenciales
[L] INSTALACIONES	Domicilio del trabajador	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales

Fuente: “elaboración propia”

Se continua con la valoración de las amenazas de acuerdo a dos atributos: Degradación: nivel afectación que tendría el activo y Probabilidad nivel de probabilidad que tiene una amenaza sobre el activo (ver anexo D).

Tabla 7. Valoración de las amenazas

CATEGORÍA DEL ACTIVO	NOMBRE DEL ACTIVO	AMENAZAS	PROBABILIDAD	DEGRADACIÓN				
				D	**I**	**C**	**A**	**T**
[D] DATOS	Base de datos	[E.2] Errores del administrador [[A.11] Acceso no autorizado	A	A	A		A	
	Backups	[E.1] Errores de los usuarios [E.2] Errores del administrador	A	A	M		B	
[S] SERVICIOS	Página Web	[I.8] Fallo de servicios de	M	M	M		M	

		comunicaciones					
	Correo Electrónico / CHAT´S	[I.8] Fallo de servicios de comunicaciones [E.8] Difusión de software dañino [A.5] Suplantación de la identidad del usuario [A.14] Interceptación de información	A	A	M	A	A
	VPN	[I.8] Fallo de servicios de comunicaciones [E.8] Difusión de software dañino [A.5] Suplantación de la identidad del usuario [A.14] Interceptación de información	A	A	M	A	A
[SW] SOFTWARE	Antivirus	[E.20] Vulnerabilidades de los programas(software) [E.21] Errores de mantenimiento / actualización de	M	A	A		

		programas (software)					
	Paquete ofimático	[E.21] Errores de mantenimiento / actualización de programas (software) [E.1] Errores de los usuarios	A		A	A	
	Aplicación web	[E.21] Errores de mantenimiento / actualización de programas (software) [E.1] Errores de los usuarios [I.8] Fallo de servicios de comunicaciones	A		A	A	M
[HW] EQUIPAMIENTO INFORMÁTICO	Laptop personales	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.5] Avería de origen físico o lógico	M		M	M	
[COM] REDES DE COMUNICACIONES	Router	[I.1] Fuego [I.2] Daños por agua [I.5] Avería de	M		M	M	M

		origen físico o lógico [E.4] Errores de configuración			
	Internet	[I.6] Corte del suministro eléctrico [I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios y suministros esenciales	M	A	M
[L] INSTALACIONES	Domicilio del trabajador	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales	B	B	B

Fuente: “elaboración propia”

Estimación del Impacto y Riesgo Potencial

Estimación del impacto potencial: consiste en la medida del daño sobre el activo derivado de la materialización de una amenaza.

Cuadro 3. IMPACTO POTENCIAL vs DEGRADACION

IMPACTO POTENCIAL	DEGRADACION				
	MB	B	M	A	MA

ACTIVO	MA	M	M	A	MA	MA
	A	B	M	A	MA	MA
	M	B	B	M	A	A
	B	MB	B	B	M	A
	MB	MB	MB	MB	B	B

Fuente: “elaboración propia”

Tabla 8. IMPACTO POTENCIAL

CATEGORÍA DEL ACTIVO	NOMBRE DEL ACTIVO	AMENAZAS	IMPACTO POTENCIAL				
			D	**I**	**C**	**A**	**T**
[D] DATOS	Base de datos	[E.2] Errores del administrador [[A.11] Acceso no autorizado	A	A		A	
	Backups	[E.1] Errores de los usuarios [E.2] Errores del administrador	A	M		B	
[S] SERVICIOS	Página Web	[I.8] Fallo de servicios de comunicaciones	M	M		M	
	Correo Electrónico / CHAT´S	[I.8] Fallo de servicios de comunicaciones	A	M	A	A	

		[E.8] Difusión de software dañino [A.5] Suplantación de la identidad del usuario [A.14] Interceptación de información				
	VPN	[I.8] Fallo de servicios de comunicaciones [E.8] Difusión de software dañino [A.5] Suplantación de la identidad del usuario [A.14] Interceptación de información	A	M	A	A
[SW] SOFTWARE	Antivirus	[E.20] Vulnerabilidades de los programas(software) [E.21] Errores de mantenimiento / actualización de programas (software)	A	A		
	Paquete ofimático	[E.21] Errores de mantenimiento /	A	A		

		actualización de programas (software) [E.1] Errores de los usuarios				
	Aplicación web	[E.21] Errores de mantenimiento / actualización de programas (software) [E.1] Errores de los usuarios [I.8] Fallo de servicios de comunicaciones	A	A	M	
[HW] EQUIPAMIENTO INFORMÁTICO	Laptop personales	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.5] Avería de origen físico o lógico	M	M		
[COM] REDES DE COMUNICACIONES	Router	[I.1] Fuego [I.2] Daños por agua [I.5] Avería de origen físico o lógico [E.4] Errores de configuración	M	M		M

	Internet	[I.6] Corte del suministro eléctrico [I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios y suministros esenciales	A	M
[L] INSTALACIONES	Domicilio del trabajador	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales	B	B

Fuente: “elaboración propia”

Estimación del riesgo potencial: riesgo a la medida del daño probable sobre un sistema.

Cuadro 4. RIESGOS POTENCIAL vs PROBABILIDAD

RIESGOS POTENCIAL		PROBABILIDAD				
		MB	B	M	A	MA
IMPACTO	MA	M	M	A	MA	MA
	A	B	M	A	MA	MA
	M	B	B	M	A	A
	B	MB	B	B	M	A
	MB	MB	MB	MB	B	B

Fuente: “elaboración propia”

Tabla 9. RIESGO POTENCIAL

CATEGORÍA DEL ACTIVO	NOMBRE DEL ACTIVO	AMENAZAS	RIESGO POTENCIAL				
			D	**I**	**C**	**A**	**T**
[D] DATOS	Base de datos	[E.2] Errores del administrador [[A.11] Acceso no autorizado	A	A		A	
	Backups	[E.1] Errores de los usuarios [E.2] Errores del administrador	A	M		B	
[S] SERVICIOS	Página Web	[I.8] Fallo de servicios de comunicaciones	M	M		M	
	Correo Electrónico / CHAT´S	[I.8] Fallo de servicios de comunicaciones [E.8] Difusión de software dañino [A.5] Suplantación de la identidad del usuario [A.14]	A	M	A	A	

		Interceptación de información				
	VPN	[I.8] Fallo de servicios de comunicaciones [E.8] Difusión de software dañino [A.5] Suplantación de la identidad del usuario [A.14] Interceptación de información	A	M	A	A
[SW] SOFTWARE	Antivirus	[E.20] Vulnerabilidades de los programas(software) [E.21] Errores de mantenimiento / actualización de programas (software)	A	A		
	Paquete ofimático	[E.21] Errores de mantenimiento / actualización de programas (software) [E.1] Errores de los usuarios	A	A		
	Aplicación	[E.21] Errores de	A	A	M	

	web	mantenimiento / actualización de programas (software) [E.1] Errores de los usuarios [I.8] Fallo de servicios de comunicaciones			
[HW] EQUIPAMIENTO INFORMÁTICO	Laptop personales	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.5] Avería de origen físico o lógico	M	M	
[COM] REDES DE COMUNICACIONES	Router	[I.1] Fuego [I.2] Daños por agua [I.5] Avería de origen físico o lógico [E.4] Errores de configuración	M	M	M
	Internet	[I.6] Corte del suministro eléctrico [I.8] Fallo de servicios de comunicaciones	A	M	

		[I.9] Interrupción de otros servicios y suministros esenciales		
[L] INSTALACIONES	Domicilio del trabajador	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales	B	B

Fuente: “elaboración propia”

Una vez que se ha realizado la identificación y valoración de los posibles riesgos y amenazas que se pueden presentar en la modalidad del Teletrabajo, se hacen necesarios implementar protocolos y lineamientos que contribuyan a minimizar los riesgos, para lo cual es indispensable el brindar una capacitación a los teletrabajadores sobre la implementación de buenas prácticas de ciberseguridad con el fin de poder mitigar y prevenir estos riesgos y amenazas.

7 GUÍA BASE PARA EL MEJORAMIENTO DE LA CIBERSEGURIDAD EN LA MODALIDAD DEL TELETRABAJO PARA PYMES EN COLOMBIA

7.1. PRÓLOGO

En la modalidad de teletrabajo los dispositivos utilizados para tal fin pueden ser controlados o monitoreados por la organización o terceros autorizados, con el fin de evitar inconvenientes de seguridad de la información. Con el avance de la tecnología y sus múltiples usos para desarrollar las tareas, es indispensable pensar en el aseguramiento de la información como activo de valor empresarial y que no caiga en manos de terceros que pueden ocasionar daños y/o perdidas no solo materiales, sino financieras y operativas.

Es importante mencionar que, en la modalidad de teletrabajo existe la conexión remota a través de varios métodos y el uso de aplicaciones que permiten realizar esta acción, lo que permite que los usuarios de una empresa puedan acceder fácilmente a los recursos informáticos de la entidad desde cualquier ubicación, de acuerdo al manejo de perfiles y permisos asignados previamente y de acuerdo a la necesidad.

En el desarrollo de la presente guía, se explicará la importancia del teletrabajo como alternativa legal de trabajo y se darán pautas para realizar una conexión segura que salvaguarde la información y permita el desarrollo de las actividades laborales de una manera más eficiente y segura.

7.1.1 LEGISLACIÓN COLOMBIANA SOBRE EL TELETRABAJO

Según el Decreto 1227 de 2022 “por el cual se modifican los artículos 2.2.1.5.3, 2.2.1.5.5, 2.2.1.5.8 y 2.2.1.5.9, y se adicionan los artículos 2.2.1.5.15 al 2.2.1.5.25 al Decreto 1072 de 2015, Único Reglamentario del Sector Trabajo, relacionados con el Teletrabajo.”[50]

Este decreto trata en su Artículo 1° el contrato o vinculación de teletrabajo, sus requisitos y normatividad vigente de acuerdo con lo estipulado en el artículo 39 del Código Sustantivo del Trabajo y de la Seguridad Social y las garantías a que se refiere el artículo 6° de la Ley 1221 de 2008.

Con este decreto el ministerio de trabajo tiene como objetivo introducir cambios en la legislación del teletrabajo, para que la implementación de este se lleve a cabo de una manera segura y sencilla, que permita también dar solución a algunos temas que no estaban claros en esta figura a nivel jurídico.

Así mismo, este decreto trata la reversibilidad, flexibilidad, equipos y herramientas del teletrabajo, entre otras disposiciones, aparte de las modificaciones a los artículos anteriormente mencionados en este apartado.

Dentro del contrato de teletrabajo aparte de las especificaciones propias dadas por la ley para su suscripción, existen requisitos adicionales tales como:

- ✓ Las características técnicas de los equipos y programas informáticos, así como las restricciones y responsabilidades de incumplimiento.
- ✓ La descripción del tipo de modalidad de teletrabajo que se va a ejecutar durante el contrato vigente y la estipulación de la jornada del trabajador
- ✓ Las políticas y medidas de ciberseguridad que debe conocer el trabajador y su estricto cumplimiento
- ✓ Los requisitos mínimos que debe tener el trabajador en su puesto de trabajo para la ejecución a satisfacción de la labor contratada; aspectos tecnológicos y de seguridad y salud en el trabajo

Existen así mismo, otros aspectos relevantes como las obligaciones por parte del trabajador y el empleador que se deben tener en cuenta en este tipo de modalidad

[50] COLOMBIA. Ministerio del Trabajo. DECRETO 1227 (18, julio, 2022). por el cual se modifican los artículos 2.2.1.5.3, 2.2.1.5.5, 2.2.1.5.8 y 2.2.1.5.9, y se adicionan los artículos 2.2.1.5.15 al 2.2.1.5.25 al Decreto 1072 de 2015, Único Reglamentario del Sector Trabajo, relacionados con el Teletrabajo [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. No. 52.099 18 de julio de 2022. [Consultado: 20 de septiembre de 2022]. Disponible en: https://www.suin-juriscol.gov.co/viewDocument.asp?id=30044448

garantizando los derechos y deberes de cada de las partes y la importancia de su estricto cumplimiento, con el fin de no acarrear complicaciones jurídicas por incumplimiento dentro de las cláusulas pactadas en el marco del contrato celebrado.

7.1.2 OBJETIVOS DE SEGURIDAD EN LA MODALIDAD DE TELETRABAJO

Con la regulación del teletrabajo, se hace necesario que los usuarios finales o trabajadores, conozcan cuales son los objetivos de seguridad para salvaguardar la información, que a fin de cuentas es un activo de alto valor para la organización o empresa. dentro de este orden de ideas es imprescindible conocer que la seguridad de la información, está basada y se articula sobre 5 dimensiones sobre los cuales se aplican las medidas de protección, a continuación, se da a conocer cada una de ellas:

Disponibilidad: es la capacidad de asegurar la fiabilidad y el acceso oportuno a los datos y/o información, además de recursos cuando se necesiten.

Autenticidad: es la garantía que la información es fidedigna, que provenga de la fuente de origen que dice provenir o que fue enviada.

Integridad: es mantener la información sin alteraciones de ningún tipo, que su modificación sea autorizada en debido caso.

Confidencialidad: es salvaguardar la información de su publicación sin previa autorización y solo puede ser leída o tratada la información o datos por personal con autorización, de acuerdo a permisos de perfil.

Trazabilidad: es la propiedad de la organización de rastrear su información a través de diversos mecanismos y certificar que solo la misma puede realizar este proceso.

Además de estos pilares, como la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad, cabe resaltar que se debe tener en cuenta el cumplimiento estricto de la ley y de las políticas de SGSI de la entidad en la cual el trabajador o usuario está vinculado laboralmente.

7.1.3 MÉTODOS DE ACCESO DEL TELETRABAJO

En esta era de modernidad y de cambios donde ya no es necesario estar presencialmente en las instalaciones de una empresa para desempeñar las labores de un cargo, sino que, al contrario, existe la posibilidad de adaptar un puesto de trabajo desde el cual se acceda remotamente a las aplicaciones de la organización.

Ahora bien, existen distintas formas en las que los empleados que se encuentran laborando en la modalidad de TELETRABAJO pueden acceder remotamente, entre las más comunes y utilizadas son VPN y VDI

7.1.3.1 VPN

Sus siglas en ingles Virtual Private Network, que español significan red privada virtual, es un tipo de tecnología de red que proporciona una extensión de forma segura de la red LAN sobre una red no controlada o pública. Una red VPN lo que realmente hace es cifrar su contenido o tráfico dentro de una red pública como internet, es crear un disfraz que dificulta el rastreo de la información y posible pérdida de esta a manos de terceros.

7.1.3.1.1 ESTRUCTURA DE LA VPN

Una VPN es una estructura tipo cliente – servidor, que crea un túnel que permite mantener una conexión segura y a la vez privada. Este tipo de red permite tener una comunicación y buen uso de los recursos informáticos de la entidad al encontrarse disponibles en otras ubicaciones fuera de las instalaciones principales.

A continuación, se mostrarán los principales tipos de VPN:

7.1.3.1.2 VPN DE SITIO A SITIO

Denominada en inglés VPN site to site, se utiliza mayormente para realizar la conexión o comunicación de un sitio con uno o más de un sitio de forma remota. En este tipo de VPN se requieren dos dispositivos tipo servidores VPN, uno en cada sitio, este tipo de conexión no necesitan instalar algún tipo de software en el dispositivo cliente

Esta estructura cuenta con dos tipos de implementaciones, una de ellas establecida en internet y otra basada en extranet; la primera, se utiliza cuando la empresa tiene más de una ubicación remota y se configura la VPN para que una cada red LAN que está separada a una sola red WAN y al segunda se utiliza cuando la empresa tiene relación muy cercana con otras compañías en donde cuentan con un cliente, proveedor, se construye una red VPN extranet que logre conectar todas las red LAN de esa empresa.

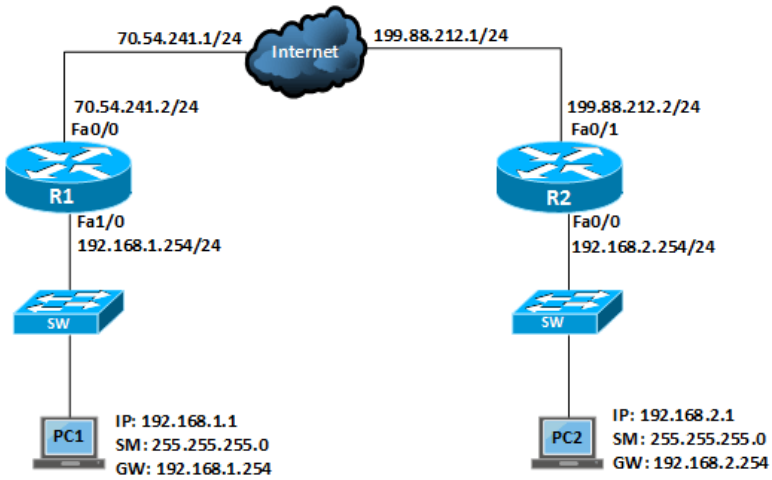
Figura 1. VPN de sitio a sitio

Fuente: JP Jones. VPN de sitio a sitio [imagen]. Top10VPN. [Consultado: 18 de noviembre de 2022]. Disponible en: https://www.top10vpn.com/es/que-es-una-vpn/tipos-de-vpn/

Dentro de las VPN sitio a sitio existen 3 formas de implementarlas:

1. Túnel Ipsec: denominada muchas veces VPN router a router, se utiliza para combinar sitios y de esta manera conectar a una persona a una red privada dentro de redes de acceso remoto

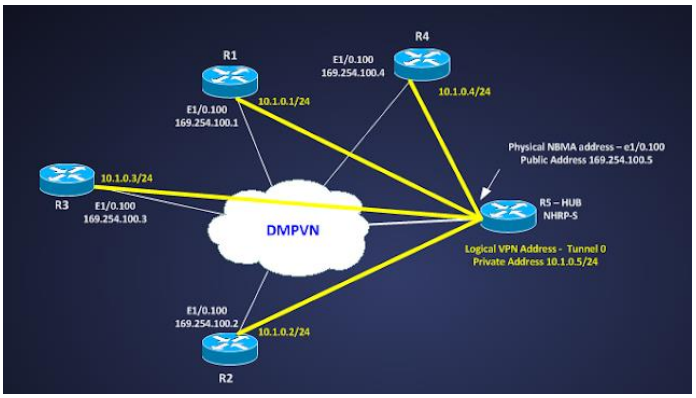
Figura 2. Configure Site to Site IPSec VPN Tunnel in Cisco IOS Router



Fuente: mustbegeek. Configure Site to Site IPSec VPN Tunnel in Cisco IOS Router [imagen]. mustbegeek. [Consultado: 18 de noviembre de 2022]. Disponible en: https://www.mustbegeek.com/configure-site-to-site-ipsec-vpn-tunnel-in-cisco-ios-router/

2. VPN dinámica multipunto – DMVPN: en este caso se permite conectar a distintas oficinas de una misma empresa al router principal utilizando las direcciones IP dinámicas

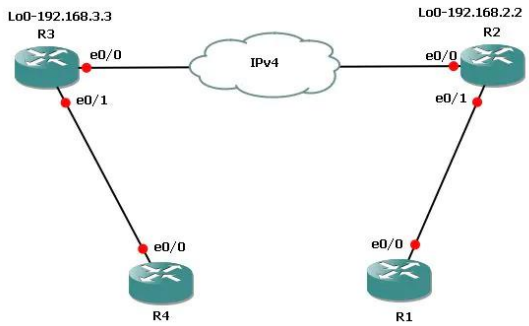
Figura 3. Operación de DMVPN



Fuente: Torrico Gumucio, Jose R, Conociendo Dynamic Multipoint VPN (DMVPN) [imagen]. community.cisco.com. [Consultado: 18 de noviembre de 2022]. Disponible en: https://community.cisco.com/t5/blogs-routing-y-switching/conociendo-dynamic-multipoint-vpn-dmvpn/ba-p/3101118

3. VPN de capa 3 (L3VPN): se basa este modelo en la conmutación de etiquetas multiprotocolo que dentro de sus beneficios ofrecen conectividad global, teniendo en cuenta que se enrutan los paquetes mediante cualquier medio de transporte o transmisión ya sea microondas, fibra óptica, entre otros. Además, se utiliza cualquier protocolo

Figura 4. VPN L3 dinámicas con túneles mGRE en redes IP solamente (no MPLS) Diagrama de la red



Fuente: cisco, C VPN L3 dinámicas con túneles mGRE en redes IP solamente (no MPLS) Diagrama de la red imagen]. cisco.com. [Consultado: 18 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/ios-nx-os-software/layer-3-vpns-l3vpn/116725-configure-mgre-00.html

7.1.3.1.3 VPN DE ACCESO REMOTO O CLIENTE – PROVEEDOR

Este tipo de comunicación es la más utilizada para la configuración de los dispositivos entre el trabajador y la empresa, para tener el acceso necesario a los recursos informáticos y tener una conexión segura que salvaguarde la información, de acuerdo con los perfiles y permisos asignados.

Características:

Se necesita instalar un dispositivo tipo concentrador o Gateway
Requiere un dispositivo software o cliente VPN

Figura 5. VPN de acceso remoto

Fuente: JP Jones. VPN de acceso remoto [imagen]. Top10VPN. [Consultado: 18 de noviembre de 2022]. Disponible en: https://www.top10vpn.com/es/que-es-una-vpn/tipos-de-vpn/

7.1.3.1.4 VENTAJAS DE UNA VPN

Cifrado: es una de las ventajas que tienen las conexiones VPN, debido a que se necesita de una clave para acceder a la información, este tipo de cifrado del tráfico de la información en redes públicas es bastante beneficioso para las entidades

Identidad oculta: las redes tipo VPN pueden ocultar su dirección IP o disfrazarla en las redes no controladas o públicas, lo que permite un tráfico de información más seguro de sitio a sitio

Cifrado de protocolos: la VPN puede ayudar en el momento de la configuración de las cookies, que permite no dejar rastro en los historiales de navegación y de esta manera, impedir que terceros puedan obtener la información necesaria que les de el acceso a un sistema y perpetuar un posible ataque.

Autenticación: las redes tipo VPN utilizan métodos de autenticación que pueden ser variados, con el fin de evitar que cualquier persona pueda iniciar sesión, solamente aquellos que tienen los privilegios lo podrán hacer

7.1.3.2 INFRAESTRUCTURA DE ESCRITORIOS VIRTUALES - VDI

Son máquinas virtuales que se gestionan como escritorios virtuales para los trabajadores en entornos controlados por las entidades para las cuales laboran. Este tipo de entornos virtuales facilitan el teletrabajo, donde le trabajador se

encuentra fuera de las instalaciones de la empresa, así como a aquellos que tienen bastante movilidad como agentes comerciales entre otros.

La virtualización del escritorio ofrece que sea un entorno amigable para el trabajador, debido a que este puede visualizar el escritorio y disponer de las mismas aplicaciones que utiliza en el ordenador de la oficina, pero esta vez desde cualquier dispositivo accediendo a través del navegador web

Figura 6. Arquitectura genérica de VDI

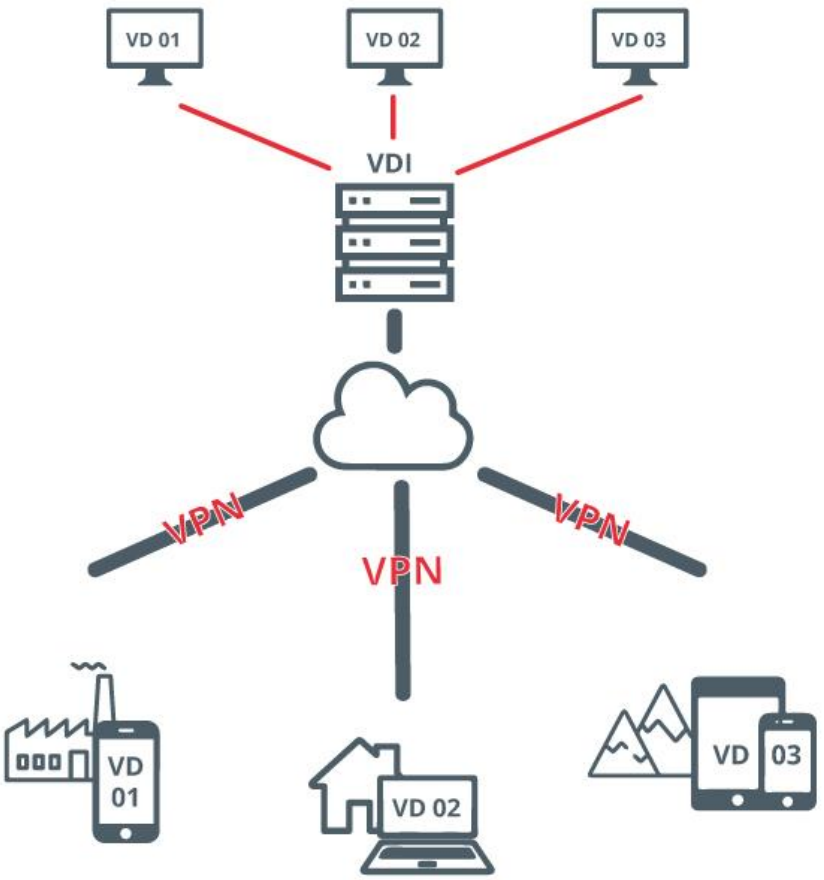
Fuente: .ITSITIO. Arquitectura genérica de VDI [imagen]. ITSITIO [Consultado: 18 de noviembre de 2022]. Disponible en: https://www.itsitio.com/mx/ifx-networks-provee-escritorios-virtuales-desde-la-nube/

7.1.3.2.1 TIPOS DE VDI

7.1.3.2.1.1 VDI en un servidor propio

Este tipo de conexión es el control que se tiene sobre la administración y no depende de terceros, ni de la autorización a estos.

Figura 7. VDI propio o como servicio «DaaS»

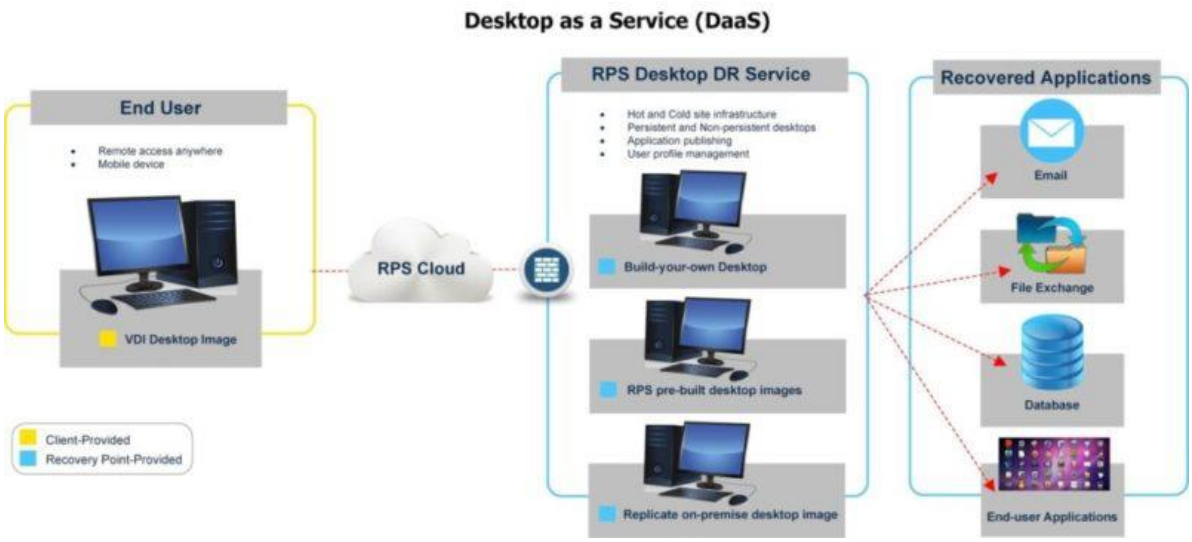


Fuente: incibe. VDI propio o como servicio «DaaS» [imagen]. Incibe [Consultado: 18 de noviembre de 2022]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/sistemas-vdi-covid-19

7.1.3.2.1.2. VDI DaaS (Desktop as a Service)

Este tipo de servicio debe contratarse de manera externa tanto para la implementación como para su mantenimiento, básicamente es el mismo principio de escritorio virtual guardando los protocolos y políticas utilizadas para esta conexión, sin embargo, debe firmarse un acuerdo de confidencialidad de la información al ser tratado con terceros

Figura 8. Desktop as a Service (DaaS)



Fuente: recoverypoint Desktop as a Service (DaaS) [imagen]. recoverypoint [Consultado: 18 de noviembre de 2022]. Disponible en: https://www.recoverypoint.com/vdi/

7.1.3.2.2 VENTAJAS DE VDI

- ✓ Ofrece movilidad para los usuarios
- ✓ Facilidad en el acceso remoto y seguridad
- ✓ Ahorro costo – beneficio
- ✓ Gestión centralizada

7.1.4 AMENAZAS DEL TELETRABAJO

Dentro de la modalidad del Teletrabajo, existen amenazas que tienen relación con la ciberseguridad, el ámbito tecnológico y propiamente del teletrabajo. A continuación, se presentarán aquellas amenazas que infringen en la seguridad de la información y pueden ocasionar pérdidas materiales, tecnológicas y financieras y que de acuerdo con INCIBE (Instituto Nacional de Ciberseguridad) recuerda su importancia:

- ➢ Ausencia de controles de seguridad física: es importante gestionar y aplicar las medidas que sean necesarias para el monitoreo y mantenimiento de los dispositivos utilizados en el teletrabajo, debido a que quedan expuestos a lugares no acreditados y en muchas circunstancias a la manipulación de terceros no autorizados por las entidades, por ejemplo: hoteles, en casa, etc.

- Problemas de configuración: los dispositivos utilizados deben ser configurados por especialistas, teniendo en cuenta que el software que garantiza el uso de varias aplicaciones para el teletrabajo debe tener una configuración adecuada.

- Inseguridad en redes: otro de los mayores problemas que acarrea el teletrabajo es la seguridad en las redes que se utilizan y que son consideradas inseguras al no encontrarse bajo la supervisión de la empresa. Por lo anterior, se recomienda utilizar VPN y no hacer uso de redes públicas

- Acceso no autorizado: es uno de los mayores inconvenientes a la hora de estar en la modalidad de teletrabajo, porque desde el trabajador hasta un ciberdelincuente puede tener acceso a los sistemas operativos a través de la red, por lo que se recomienda métodos o mecanismos robustos en la autenticación del sistema y en ocasiones que sea una autenticación doble.
- Falta de capacitación: no se debe desvirtuar esta parte, el trabajador de acuerdo con las políticas de formación de la empresa, debe estar en disposición de brindar capacitación o formación en tiempos prudenciales sobre el manejo y actualización de los dispositivos utilizados para desempeñar su labor y el cuidado de estos.

- Actualización de software: no tener actualizado el software en los dispositivos cliente como de servidores, es un riesgo muy alto para la empresa y así mismo, la instalación indebida de software no autorizado.

- Pérdida, hurto o destrucción de los dispositivos: los dispositivos utilizados en teletrabajo y otras modalidades fuera de las instalaciones de las empresas se caracterizan por ser portátiles y de bajo peso, están expuestos a diversos riesgos como hurto o pérdida, por lo que es importante asegurar la información contenida para evitar inconvenientes.

- Seguridad en aplicaciones colaborativas: las aplicaciones colaborativas están sujetas a riesgos de transferencia de información no adecuada y de virus, por su forma de manejo, es conveniente realizar una configuración adecuada al ser utilizadas y activar firewall que garanticen la seguridad de la información a tratar.

- Almacenamiento en la nube o cloud: los servicios de almacenamiento en la nube son de los más utilizados en la actualidad con el trabajo híbrido y teletrabajo, pero representan amenaza para la información, sino son configurados de manera adecuada y con los parámetros de autorización necesarios de acuerdo a las políticas de seguridad de la empresa.

7.1.5 SEGURIDAD CLIENTE – SERVIDOR (SOFTWARE)

Dentro del teletrabajo como cualquier otra modalidad fuera de instalaciones corporativas necesita establecer seguridad tanto en los dispositivos cliente como en aquellos que son servidores y que permiten tener acceso a los recursos corporativos, por eso se hace necesario el control en la autenticación y la implantación de medidas de seguridad con el fin de proteger la información de la empresa y la continuidad del negocio.

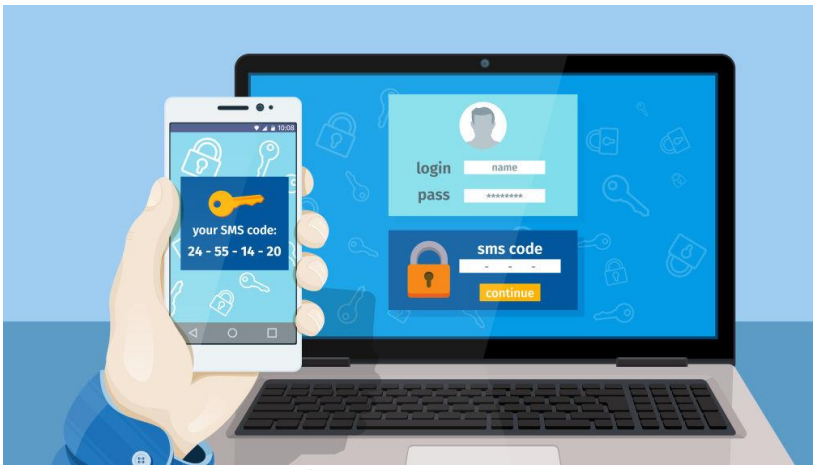
Es necesario tener presente que los dispositivos tipo servidor, deben mantenerse actualizados, con la configuración que se ha definido para su correcto uso y que solamente puedan ser gestionados por los administradores autorizados. Por lo anterior, debe evaluarse cada cierto tiempo las posibles vulnerabilidades que puedan comprometer al servidor y su seguridad.

7.1.5.1 SEGURIDAD Y ACCESO REMOTO SERVIDOR

Los recursos informáticos a los cuales se tiene conexión de carácter remoto solo deben estar disponibles para las personas autorizadas y que hacen uso de estos, con el fin de garantizar la restricción de acceso, estos dispositivos deben realizar la autenticación o reconocimiento del teletrabajador antes de quedar en completa disponibilidad cualquier recurso corporativo, sin olvidar los permisos asignados previamente a cada trabajador. Esto permite que en caso de verse comprometida la seguridad y la perdida de contraseñas que puedan dar acceso a recursos informáticos, se dé el debido tratamiento preventivo.

En lo posible las organizaciones deben mantener un tipo de autenticación en dos pasos o mutua, lo que permite tener mayor control de la situación y una mayor legitimidad de las operaciones, en este tipo de autenticación es posible generar un certificado digital para el servidor y el dispositivo cliente y una vez realizado este paso, vendría una serie de controles de idoneidad, detección, etc, que permiten verificar la legitimidad del cliente y estar en constante monitoreo para la prevención de incidentes de seguridad

Figura 9. La autenticación en dos pasos: protege tu cuenta en un minuto



Fuente: compromiso.atresmedia La autenticación en dos pasos: protege tu cuenta en un minuto [imagen]. compromiso.atresmedia [Consultado: 18 de noviembre de 2022]. Disponible en: https://compromiso.atresmedia.com/levanta-la-cabeza/lineas-accion/privacidad-legislacion/autenticacion-dos-pasos-protege-cuenta-minuto_201904125cb06cdd0cf27daea8ef5359.html

7.1.5.2 SEGURIDAD Y ACCESO REMOTO CLIENTE

En las conexiones remotas también existen las configuraciones realizadas al software que da el acceso remoto, estas pueden ser realizadas por personal experto de la organización de manera remota y que de hecho es la mejor opción, para que el usuario del software cliente no pueda manipular la configuración del dispositivo. Así mismo, se debe asegurar que la gestión remota este debidamente cifrada en cuanto a comunicaciones de red se refiere y como se explicaba en el anterior apartado realizar la autenticación mutua.

Las organizaciones o empresas deben considerar la posibilidad de tener asistencia técnica a los teletrabajadores, con el fin que puedan acceder al soporte de sus dispositivos a cargo de manera remota y dar resolución a los posibles problemas que se puedan presentar en los mismos.

7.1.6 ASEGURAMIENTO DE EQUIPOS (HARDWARE)

De acuerdo con el artículo 9 de Decreto 884 de 2012 acerca del teletrabajo indica que: “las Administradoras de Riesgos Profesionales -ARP, en coordinación con el Ministerio del Trabajo, deberán promover la adecuación de las normas relativas a higiene y seguridad en el trabajo a las características propias del teletrabajo. Las Administradoras de Riesgos Profesionales deberán elaborar una guía para prevención y actuación en situaciones de riesgo que llegaren a presentar los teletrabajadores, y suministrarla al teletrabajador y empleador”[51].

[51] COLOMBIA. Ministerio de Salud Y Protección Social. DECRETO 884 (30, abril, 2012). Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. No. 48417 de abril

El Ministerio de las TIC recomienda que cada organización debe garantizar que los equipos asignados a los trabajadores en la modalidad de teletrabajo cuenten con las medidas de protección necesarias para la ejecución de la actividad contratada.

Existe la guía creada por el Ministerio de trabajo en conjunto con Fasecolda, denominada “Guía técnica para la promoción de la salud y la prevención de los riesgos laborales en el teletrabajo”, en donde tiene un apartado dedicado a la parte tecnológica y que a continuación se ven algunos ítems para la prevención e intervención de factores de riesgo:

- No desconectar los equipos a la fuerza, halando el cable

  Figura 10. No desconectar los equipos a la fuerza, halando el cable

Fuente: Jiménez García Natividad Riesgos Y Medidas Preventivas Delante De Los Riesgos Electricos [imagen]. slideplayer.es [Consultado: 18 de noviembre de 2022]. Disponible en: https://slideplayer.es/slide/9042998/

- Utilizar extensiones o multitomas certificadas, que permitan tener la continuidad del polo a tierra, para evitar generar cortocircuito y sobrecargas eléctricas

  Figura 11. Multitoma

30 de 2012. [Consultado: 16 de octubre de 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=47216#:~:text=El%20objeto%20del%20presente%20decreto,privado%20en%20relaci%C3%B3n%20de%20dependencia.

Fuente: questinter.com Multitomas (Regletas) eléctricas para montaje en Rack [imagen]. slideplayer.es [Consultado: 18 de noviembre de 2022]. Disponible en: https://www.google.com/url?sa=i&url=http%3A%2F%2Fwww.questinter.com%2Fportafolio-multitomas-electricas&psig=AOvVaw15hh-VkDJRGaUic5BuALHW&ust=1669078413063000&source=images&cd=vfe&ved=0CBAQjRxqFwoTCJiDt-OHvvsCFQAAAAAdAAAAABAF

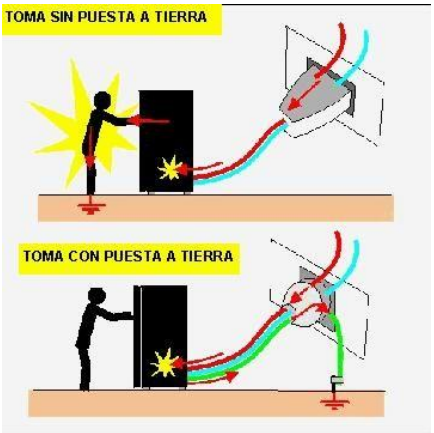
- Establecer de acuerdo con la norma zonas de paso y organización adecuada de cableado, cumpliendo con todos los parámetros de seguridad, como guayas, canaletas, etc.

Figura 12. Gestión del cableado

Fuente pinterest.es Gestión del cableado [imagen]. pinterest.es [Consultado: 18 de noviembre de 2022]. Disponible en: https://www.pinterest.es/pin/303570831107571400/

- Todas las tomas corrientes deben tener polo a tierra en donde se pueda conectar de manera segura los dispositivos de computo

Figura 13. Polo a tierra



Fuente Areatecnologia. Puesta A Tierra [imagen]. Areatecnologia. [Consultado: 18 de noviembre de 2022]. Disponible en: https://www.areatecnologia.com/electricidad/puesta-a-tierra.html

- Verificar siempre el buen estado del cableado a utilizar tanto de los cables de poder como del cableado de poder, HDMI, tipo USB

Figura 14. Puertos y conectores de una computadora

Fuente Tecnologia-informatica. Puertos y conectores de una computadora [imagen]. tecnologia-informatica.com [Consultado: 18 de noviembre de 2022]. Disponible en: https://www.tecnologia-informatica.com/conectores-computadora-equipos-audio-video/

- Verificar el correcto estado del equipo de cómputo y todos sus periféricos

Figura 15. Equipo de cómputo y todos sus periféricos

Fuente compubit.com.co. ¿Cuáles son los equipos electrónicos de computo que no pueden faltar en tu hogar? Part 2 [imagen]. compubit.com.co. [Consultado: 18 de noviembre de 2022]. Disponible en: https://compubit.com.co/cuales-son-los-equipos-electronicos-de-computo-que-no-pueden-faltar-en-tu-hogar-part-2/

7.1.7 CONTROLES

En la norma NIST SP 800-53 Revisión 4 se mencionan los controles necesarios que soportan el teletrabajo empresarial, el acceso remoto y las tecnologías BYOD, los cuales permiten tener presente el aseguramiento de los dispositivos utilizados en estos tipos de modalidad de trabajo, así mismo, es una manera de tener una base firme sobre la cual formular políticas de seguridad que puedan ser más efectivas y eficaces.

A continuación, se presentan los controles relacionados con el teletrabajo y/o acceso remoto:

Tabla 10.Controles NIST SP 800-53 Revisión 4

Control NIST SP 800-53	**Teletrabajo y/o Acceso Remoto**
AC-17, acceso remoto	Este control documenta todos los requisitos del acceso remoto, la autorización antes de permitir las conexiones, monitoreo y control de acceso remoto, cifrado de conexiones, entre otros
AC-19, Control de Acceso para Dispositivos Móviles	Este control es para los dispositivos móviles que deben ser controlados por la organización y para la autorización de conexión de estos a sistemas organizacionales
CP-9, Respaldo del Sistema de Información	Este control específico trata la realización de la copia de seguridad que puede ser remota o local
IA-2, Identificación y Autenticación (Organizacional Usuarios)	Este control hace uso de autenticación única o de tipo multifactor para los usuarios que utilizan acceso remoto, aquí se sugiere el uso de contraseñas robustas, certificados digitales y/o tokens de autenticación de hardware.
IA-3, Identificación de dispositivos y Autenticación	Autenticación mutua para verificar la legitimidad de un servidor de acceso remoto antes de proporcionar acceso a los recursos organizacionales

IA-11, Reautenticación	Autenticación después de un tiempo de inactividad que puede oscilar entre 30 minutos y 8 horas, dependiendo lo configuración por la entidad. Esto permite que las organizaciones confirmen que la persona que tiene el acceso a recursos de manera remota está debidamente autorizada.
RA-3, Evaluación de riesgos	Se debe realizar evaluación de riesgo para la formulación de métodos seguros de acceso remoto, acceso a las aplicaciones, entre otros servicios
SC-7, Protección de límites	Control y monitoreo de subredes y establecimiento de límites de conexión para mantener las redes públicas fuera de las redes internas
SC-8, Confidencialidad e integridad de la transmisión	Este control implica los diversos métodos de protección de la confidencialidad, integridad y disponibilidad mediante la criptografía

7.1.7.1 CONTROLES DE CIBERSEGURIDAD

Dentro de los controles de la norma, se enumeran las subcategorías dentro del marco de ciberseguridad que permiten el aseguramiento del teletrabajo empresarial, el acceso remoto y las tecnologías BYOD

Tabla 11.Controles de ciberseguridad

Marco de Ciberseguridad Subcategoría	Teletrabajo/Acceso Remoto/Implicaciones BYOD
ID.GV-1: Se establece la política de seguridad de la información organizacional	Políticas de seguridad informática sobre el teletrabajo de la organización

ID.RA-5: Las amenazas, vulnerabilidades, probabilidades e impactos se utilizan para determinar el riesgo	Revisión de riesgos en la parte de acceso remoto
PR.AC-1: Se gestionan identidades y credenciales para dispositivos y usuarios autorizados	Este control trata la autenticación única o multifactor para el acceso remoto para la verificación de autenticación de hardware
PR.AC-3: Se gestiona el acceso remoto	La organización debe gestionar todos los procesos y las tecnologías de acceso remoto
PR.AC-5: Se protege la integridad de la red, incorporando la segregación de la red cuando corresponda	Segmentación de redes para mantener los componentes de acceso públicos fuera de las redes internas
PR.DS-2: Los datos en tránsito están protegidos	Métodos de criptografía para la protección de la información en acceso remoto
PR.IP-4: Se realizan, mantienen y prueban periódicamente respaldos de información	Realizar la copia de seguridad de forma local o remota

CONCLUSIONES

Se realizó un análisis de las políticas de seguridad informática existentes dentro del marco colombiano y las leyes dispuestas para el desempeño del teletrabajo en el país, para entender el contexto en el cual se iba a profundizar con el desarrollo de la presente monografía. Además de llegar a la conclusión que pese a los esfuerzos del estado colombiano en conjunto con las empresas Pymes en el país, no ha sido posible llegar a una total mitigación de los delitos informáticos que se cometen con el auge del uso de la tecnología y acceso remoto implementado por las organizaciones, con el fin de llevar a otro nivel el crecimiento empresarial y la continuidad del negocio

Se realizó un análisis de los riesgos que marcan las estadísticas colombianas, frente a la ciberseguridad, en donde se utilizó la metodología MAGERIT para el análisis y gestión de riesgos de los sistemas de información, mostrando de esta manera la tendencia que se tiene en la actualidad y el impacto generado en las organizaciones, lo que permite tener bases para toma de mejores decisiones y de la implementación de una política de seguridad más robusta al interior de la operación de las PYMES.

Se desarrolla como resultado de la presente monografía una Guía, en la cual su objetivo es incentivar a las Pymes en la construcción de mejores prácticas en cuanto a seguridad informática se refiere, con el propósito de salvaguardar la información en su triada de confidencialidad, disponibilidad e integridad, teniendo presente que la información es un activo de alto valor para los diferentes procesos de una organización. Por esta razón, se dan pautas para el acceso remoto, la seguridad de dispositivos y aplicaciones y se da a conocer la normatividad vigente nacional e internacional sobre ciberseguridad y seguridad informática, para la implementación de políticas que se ajusten a la necesidad de cada entidad, de acuerdo con la naturaleza y recursos de estas.

El paso a paso de la configuración tanto de dispositivos o equipamiento hardware como de aplicaciones software en el planteamiento de la modalidad de teletrabajo, dependerá de las necesidades de cada empresa, de los manuales y procedimientos que se dispongan para tal fin y de la construcción de políticas SGSI, recordando que las guías técnicas y lineamientos son base primordial para realizar estos procedimientos y para la construcción de manuales específicos según se considere

RECOMENDACIONES

Se debe realizar una revisión, análisis y actualización de acuerdo con la necesidad de las empresas PYMES en Colombia, de las leyes y normas colombianas frente a la protección de datos y de la información, con respecto al teletrabajo con el fin de salvaguardar la información en su triada y contemplar medidas o estrategias necesarias que permitan las buenas prácticas del uso de la información y de las nuevas tecnologías.

La formulación de una política de seguridad de la información más robusta, eficiente y eficaz dependerá del análisis de riesgos realizado por cada organización, de acuerdo con sus estándares, procedimientos, lineamientos y modalidad de operación, sin embargo, se hace totalmente necesario que para un óptimo resultado se pueda implementar la metodología MAGERIT que facilita el análisis de riesgos, además de ser una de las más confiables y utilizada a nivel internacional.

La guía de recomendaciones es una forma de dar orientación a las PYMES sobre cuáles son los métodos que se pueden implantar en una modalidad de teletrabajo de manera segura, mitigando de esta manera la posible materialización de los riesgos actuales sobre los activos de información tanto físicos como digitales, mostrando las ventajas y desventajas de cada uno, su manera a nivel general de funcionamiento y configuración, que sirve como parte de un informe que se puede presentar a las altas direcciones de una entidad para revisar y analizar la viabilidad financiera y operativa del correcto manejo e implementación de esta modalidad de trabajo con sus pros y contras, para la toma de decisiones encaminadas al cumplimiento de metas y objetivos corporaciones.

Es necesario impartir capacitación a nivel interno de las empresas colombianas, sobre las políticas de seguridad informática y ciberseguridad implementadas para lograr mitigar, prevenir o corregir los daños causados por los delitos informáticos.

BIBLIOGRAFÍA

1. Asociación Colombiana de Ingenieros de Sistemas. Ciberseguridad: la aliada de las PyMEs durante la realidad actual (julio, 2020) [en línea]. acis.org.co [Consultado: 10 de marzo de 2021]. Disponible en: https://www.acis.org.co/portal/content/noticiasdelsector/ciberseguridad-la-aliada-de-las-pymes-durante-la-realidad-actual
2. Bruce Schneier. [en línea]. wikipedia.org [Consultado: 10 de marzo de 2021]. Disponible en: https://es.wikipedia.org/wiki/Bruce_Schneier#:~:text=A%20Schneier%20se%20deben%20frases,personas%2C%20procesos%20y%20tecnolog%C3%ADa%22
3. CARIDAD Migdalia Josefina y VIRVIESCAS PEÑA John Anderson. El teletrabajo como estrategia laboral competitiva en las PYME colombianas [en línea]. researchgate.net. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.researchgate.net/publication/322493981_El_teletrabajo_como_estrategia_laboral_competitiva_en_las_PYME_colombianas
4. COLOMBIA. Departamento Administrativo de la Función Pública. LEY 590 (10, julio, 2000). Por la cual se dictan disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresa [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 44.078 de Julio 12 de 2000. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.teletrabajo.gov.co/622/w3-article-8098.html
5. COLOMBIA. Ministerio de Tecnologías de la Información y las Comunicaciones. Todo lo que se debe saber sobre el teletrabajo. [en línea]. Santa Fe de Bogotá, D.C. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126148:Todo-lo-que-se-debe-saber-sobre-el-teletrabajo
6. COLOMBIA. Ministerio del Trabajo. CAPÍTULO 4 CONSIDERACIONES JURÍDICAS Y LEGALES DEL TELETRABAJO. [en línea]. Santa Fe de Bogotá, D.C. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.teletrabajo.gov.co/622/propertyvalues-7939_descargable_1.pdf
7. COLOMBIA. Ministerio del Trabajo. Marco Jurídico. [en línea]. Santa Fe de Bogotá, D.C. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=12672
8. COLOMBIA. Ministerio del Trabajo. “MiPymes representan más de 90% del sector productivo nacional y generan el 80% del empleo en Colombia”: ministra Alicia Arango. [en línea]. Santa Fe de Bogotá, D.C. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.mintrabajo.gov.co/prensa/comunicados/2019/septiembre/mipym

es-representan-mas-de-90-del-sector-productivo-nacional-y-generan-el-80-del-empleo-en-colombia-ministra-alicia-arango

9. COLOMBIA. Ministerio del Trabajo. Recomendaciones sobre Ciberseguridad. [en línea]. Santa Fe de Bogotá, D.C. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.teletrabajo.gov.co/622/w3-article-126328.html
10. COLOMBIA. Ministerio del Trabajo. Retos para la implementación. [en línea]. Santa Fe de Bogotá, D.C. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.teletrabajo.gov.co/622/w3-article-8366.html
11. GONZÁLEZ ZULUAGA, Andrea, FLORÉZ LONDOÑO Kelly Danitza y PELÁEZ RAMÍREZ Viviana Vera Gestión Del Cambio Y El Teletrabajo [en línea]. Trabajo De Grado Para Optar El Titulo De Especialistas En Gestión Del Talento Humano Y La Productividad. Universidad de Medellín facultad de ciencias-económico administrativas especialización de gestión del talento humano y la productividad 2014. [Consultado: 10 de marzo de 2021]. Disponible en: https://repository.udem.edu.co/bitstream/handle/11407/385/Gesti%C3%B3n%20del%20cambio%20y%20el%20teletrabajo.pdf?sequence=1
12. IIUNAM. Seguridad Informática en el Hogar [video]. YouTube, IIUNAM. (13 abril 2018). 1:37:30 minutos. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.youtube.com/watch?v=J_F72OXgiy0
13. InfoJobs. La Ciberseguridad en tu empresa: teletrabajo y medidas de protección [video]. YouTube, InfoJobs. (2020). 37:21 minutos. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.youtube.com/watch?v=hVr16NFrQFY&t=2s
14. Instituto Nacional De Ciberseguridad. Ciberseguridad en el teletrabajo: una guía de aproximación para el empresario [en línea]. incibe.es [Consultado: 10 de marzo de 2021]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf
15. Instituto Nacional De Ciberseguridad. Ciberseguridad para la empresa (1/4) [video]. YouTube, INCIBE. (20 noviembre 2015). 3:24 minutos. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.youtube.com/watch?v=EHjmxujXIaQ
16. Instituto Nacional De Ciberseguridad. Políticas de seguridad para la pyme [video]. YouTube, INCIBE. (6 de agosto de 2018). 3:34 minutos. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.youtube.com/watch?v=oado7fL4fz0
17. iso27000.es. SGSI. ¿Qué es un SGSI?- Integridad. [en línea]. iso27000.es. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.iso27000.es/sgsi.html

18. iso27000.es. SGSI. ¿Qué es un SGSI?. [en línea]. iso27000.es. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.iso27000.es/sgsi.html
19. ISOTOOLS. Sistemas de Gestión de Riesgos y Seguridad ¿Qué es la ISO 27001?. [en línea]. Edición. Bogotá D.C. [Consultado10 de marzo de 2021]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/
20. JUÁREZ, César. Las 80 mejores frases sobre la Tecnología [en línea]. Psicología y Mente. [Consultado: 10 de marzo de 2021]. Disponible en: https://psicologiaymente.com/reflexiones/frases-tecnologia#:~:text=Si%20piensas%20que%20la%20tecnolog%C3%ADa,(Bruce%20Schneier)
21. NIÑO WILCHES, Yamith Andrés. Importancia de la implementación del concepto de ciberseguridad organizacional en las organizaciones tipo Pymes [en línea]. Master en Gestión de Organizaciones. Bogotá D.C. Universidad Militar Granada Facultad De Ciencias Económicas Maestría En Gestión De Organizaciones Bogotá, D.C. 2015. [Consultado: 10 de marzo de 2021]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/7325/Importancia%20de;jsessionid=1121A9100F1C84F9AFA3B98DE608009F?sequence=1
22. OISS – Organización Iberoamericana de la Seguridad Social. Informe Sobre El Teletrabajo/Trabajo No Presencial [en línea]. oiss.org [Consultado: 10 de marzo de 2021]. Disponible en: https://oiss.org/wp-content/uploads/2020/07/INFORME-SOBRE-EL-TELETRABAJOTRABAJO-NO-PRESENCIAL.pdf
23. ORJUELA TORRES. Yeshica El teletrabajo puede abrir puertas a ciberataques [en línea]. En: *El Tiempo*, 25 de marzo 2020. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/el-teletrabajo-puede-abrir-puertas-a-ciberataques-477240
24. PORTAFOLIO. ¿Cómo proteger su compañía de ciberataques en tiempos de teletrabajo? [en línea]. portafolio.co [Consultado: 10 de marzo de 2021]. Disponible en: https://www.portafolio.co/tendencias/como-proteger-su-compania-de-ciberataques-en-tiempos-de-teletrabajo-539729
25. Principios de la seguridad informática: consejos para la mejora de la ciberseguridad - Confidencialidad de la información [en línea]. En: UNIR REVISTA 30 de abril 2020. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.unir.net/ingenieria/revista/principios-seguridad-informatica/#:~:text=Proteger%20la%20informaci%C3%B3n%20significa%20garantizar,la%20disponibilidad%20de%20la%20informaci%C3%B3n .
26. Quanti Channel. La Ciberseguridad en tu empresa: teletrabajo y medidas de protección [video]. YouTube, Quanti Channel. (30 octubre 2019).

12:21 minutos. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.youtube.com/watch?v=RAqR2l97wJE

27. RAMÍREZ MONTEALEGRE, Benjamín José. Medición de madurez de CiberSeguridad en MiPymes colombianas [en línea]. Tesis presentada como requisito parcial para optar al título de: Magíster en Ingeniería – Telecomunicaciones Universidad Nacional de Colombia Facultad de Ingeniería, Área Curricular de Ingeniería de Sistemas e Industrial Bogotá, Colombia 2016. [Consultado: 10 de marzo de 2021]. Disponible en: https://repositorio.unal.edu.co/bitstream/handle/unal/57956/80245271.2016.pdf?sequence=1&isAllowed=y
28. RODRÍGUEZ ARROYO Hugo Alfonso Importancia De Controlar Todas Las Amenazas Detectadas A Través De Magerit V.3 E Iso/Iec 27002 Según Análisis De Ataques Informáticos En Latinoamérica [en línea]. Monografía. universidad nacional abierta y a distancia unad escuela de ciencias básicas, tecnología e ingeniería especialización en seguridad informática barranquilla 2019. [Consultado: 10 de marzo de 2021]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/31879/harodriguezar.pdf?sequence=1&isAllowed=y
29. Semana. Ciberseguridad: los riesgos que puede traer el teletrabajo [en línea]. semana.com [Consultado: 10 de marzo de 2021]. Disponible en: https://www.semana.com/management/articulo/los-riesgos-del-teletrabajo-en-ciberseguridad/284349/
30. VerSprite. La Ciberseguridad en tu empresa: teletrabajo y medidas de protección [video]. YouTube, VerSprite. (22 enero 2021). 25:51 minutos. [Consultado: 10 de marzo de 2021]. Disponible en: https://www.youtube.com/watch?v=CQJeivbLyY4
31. COLOMBIA. Congreso de la República de Colombia. LEY 1221 (16, julio, 2008). Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 47052 de julio 16 de 2008. [Consultado: 10 de abril de 2021]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=31431
32. COLOMBIA. Ministerio del Trabajo. CIRCULAR 0017 (24, febrero, 2020). Lineamientos mínimos a implementar de promoción y prevención para la preparación, respuesta y atención de casos de enfermedad por covid-19 (antes denominado coronavirus) [en línea]. Santa Fe de Bogotá, D.C.: [Consultado: 10 de abril de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=107276
33. 360es.com. Llevar el trabajo al trabajador, y no el trabajador al trabajo [en línea]. 360es.com. [Consultado: 10 de abril de 2021]. Disponible en: https://360es.com/es/llevar-el-trabajo-al-trabajador-y-no-el-trabajador-al-trabajo/

34. ESPAÑA. Jefatura del Estado. Real Decreto-ley 28 (22, septiembre, 2020). de trabajo a distancia [en línea]. España: «BOE» núm. 253, de 23/09/2020. [Consultado: 10 de abril de 2021]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2020-11043#a2
35. COLOMBIA. Congreso de la República de Colombia. LEY 2069 (31, diciembre, 2020). "por medio del cual se impulsa el emprendimiento en Colombia [en línea]. Santa Fe de Bogotá, D.C.: [Consultado: 10 de abril de 2021]. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%202069%20DEL%2031%20DE%20DICIEMBRE%20DE%202020.pdf
36. COLOMBIA. Asamblea Nacional Constituyente. Constitución Política de la República de Colombia (20, julio, 1991). [en línea]. Santa Fe de Bogotá, D.C.: Gaceta Constitucional No. 116 de 20 de julio de 1991 última actualización Diario Oficial No. 51.635 - 15 de abril 4 de 2021 [Consultado: 10 de abril de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html#1
37. COLOMBIA. Congreso de la República de Colombia. LEY 527 (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial No. 43.673, de 21 de agosto de 1999 [Consultado: 10 de abril de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html
38. COLOMBIA. Congreso de la República de Colombia. LEY 603 (27, julio, 2000). Por la cual se modifica el artículo 47 de la Ley 222 de 1995. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial No 44.108, de 31 de julio 2000 [Consultado: 10 de abril de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0603_2000.html
39. COLOMBIA. Congreso de la República de Colombia. LEY ESTATUTARIA 1266 (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial No. 47.219 de 31 de diciembre de 2008 [Consultado: 10 de abril de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html
40. COLOMBIA. Congreso de la República de Colombia. LEY 1341 (30, julio, 2009). Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial No. 47.219 de 31 de diciembre de 2008 [Consultado: 10 de abril de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

41. COLOMBIA. Congreso de la República de Colombia. LEY 1273 (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial No. 47.223 de 5 de enero de 2009 [Consultado: 10 de abril de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html#:~:text=El%20que%2C%20sin%20orden%20judicial,y%20dos%20(72)%20meses.
42. COLOMBIA. Congreso de la República de Colombia. RESOLUCION 2258 (23, diciembre, 2009). Por la cual se modifican los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1.8 y 2.4 de la Resolución CRT 1740 de 2007.. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial 47572 de diciembre 23 de 2009 [Consultado: 10 de abril de 2021]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=38498
43. COLOMBIA. Consejo Nacional De Política Económica Y Social República De Colombia Departamento Nacional De Planeación Documento CONPES 3701 (14 de julio de 2011). POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. [en línea]. Santa Fe de Bogotá, D.C.: [Consultado: 10 de abril de 2021]. Disponible en: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf
44. COLOMBIA. Congreso de la República de Colombia. LEY 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales.. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial No. 48.587 de 18 de octubre de 2012 [Consultado: 10 de abril de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
45. COLOMBIA. Ministerio De Comercio, Industria Y Turismo. Decreto 1377 (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012 [en línea]. Santa Fe de Bogotá, D.C.: [Consultado: 10 de abril de 2021]. Disponible en: http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf
46. COLOMBIA. Superintendencia Financiera De Colombia. Circular Externa 052 (octubre, 2007). capitulo décimo segundo: requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios [en línea]. Santa Fe de Bogotá, D.C.: [Consultado: 10 de abril de 2021]. Disponible en: https://www.enlaceoperativo.com/articulo/circular-externa-052-de-2007/
47. ISOTOOLS. Sistemas de Gestión de Riesgos y Seguridad ¿Qué es la ISO 27001?. [en línea]. Edición. Bogotá D.C. [Consultado10 de marzo de 2021]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-

27001#:~:text=ISO%2027001%20es%20una%20norma,los%20sistemas%20que%20la%20procesan.&text=La%20Gesti%C3%B3n%20de%20la%20Seguridad,en%20la%20norma%20ISO%2027002.

48. SMYTHSYS IT CONSULTING. Qué es el Pharming. Cómo detectarlo y cómo evitarlo. [video]. Youtube. (11 diciembre 2019). 2:22. [Consultado: 10 de abril de 2021]. Disponible en: https://www.youtube.com/watch?v=TNWQ52-Cgmw

49. GONZÁLEZ Yolanda. ¿Cómo proteger tu página web del defacement? [en linea]. 2 julio, 2020 [Consultado: 10 de abril de 2021]. Disponible en https://protecciondatos-lopd.com/empresas/defacement/

50. ASOCIACIÓN ESPAÑOLA DE BANCA. Campaña contra el vishing o fraude telefónico [video]. Youtube. (11 septiembre 2019). 2:22. [Consultado: 10 de abril de 2021]. Disponible en: https://www.youtube.com/watch?v=Y5dKotmyAWA

51. MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [en línea]. Edita: © Ministerio de Hacienda y Administraciones Públicas, octubre 2012.- NIPO: 630-12-171-8. [Consultado: 10 de abril de 2021]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

52. pmg-ssi.com Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad [en linea]. 1 febrero, 2018 [Consultado: 20 de septiembre de 2022]. Disponible en https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

53. bancosantander ¿Qué es la disponibilidad informática? [en linea]. [Consultado: 20 de septiembre de 2022]. Disponible en https://www.bancosantander.es/glosario/disponibilidad-informatica#:~:text=Centr%C3%A1ndonos%20en%20el%20campo%20de,lo%20necesitan%20para%20desenvolver%20sus

54. pmg-ssi.com Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad [en linea]. 1 febrero, 2018 [Consultado: 20 de septiembre de 2022]. Disponible en https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

55. latam.kaspersky.com ¿Qué es una VPN y cómo funciona? [en linea]. [Consultado: 20 de septiembre de 2022]. Disponible en https://latam.kaspersky.com/resource-center/definitions/what-is-a-vpn

56. vmware.com Infraestructura de escritorios virtuales (VDI) [en linea]. [Consultado: 20 de septiembre de 2022]. Disponible en https://www.vmware.com/es/topics/glossary/content/virtual-desktop-infrastructure-vdi.html

57. portalempresarial Cuáles son las 4 Mayores Amenazas del Home Office para las Empresas [en linea]. [Consultado: 12 de octubre de 2022]. Disponible en https://portalempresarial.org/recursos-humanos/legislacion-gestion-humana/cuales-son-las-4-mayores-amenazas-del-home-office-para-las-empresas/#:~:text=P%C3%A9rdida%20de%20Control%20y%20Comunicaci%C3%B3n,empresa%20y%20reduce%20la%20productividad.

58. Muyseguridad Diez amenazas a superar para lograr un teletrabajo seguro [en linea]. [Consultado: 12 de octubre de 2022]. Disponible en https://www.muyseguridad.net/2021/08/21/diez-amenazas-teletrabajo-seguro/

59. .latinpymes LA CIBERSEGURIDAD, RETO DE LAS PYMES [en linea]. [Consultado: 12 de octubre de 2022]. Disponible en https://www.latinpymes.com/la-ciberseguridad-reto-de-las-pymes/

60. asomovil Use bien sus equipos en teletrabajo para reducir los riesgos laborales [en linea]. [Consultado: 18 de octubre de 2022]. Disponible en https://www.asomovil.org/use-bien-sus-equipos-en-teletrabajo-para-reducir-los-riesgos-laborales/

61. COLOMBIA. Ministerio de Salud Y Protección Social. DECRETO 884 (30, abril, 2012). Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. No. 48417 de abril 30 de 2012. [Consultado: 16 de octubre de 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=47216#:~:text=El%20objeto%20del%20presente%20decreto,privado%20en%20relaci%C3%B3n%20de%20dependencia.

62. scolalegal modificaciones-relacionadas-con-el-teletrabajo-decreto-1227-de-2022 [en linea]. [Consultado: 18 de octubre de 2022]. Disponible en https://scolalegal.com/modificaciones-relacionadas-con-el-teletrabajo-decreto-1227-de-2022/

63. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. [en línea]. Edición. NIST Special Publication 800-46 Revision 2 Lugar de publicación: July 2016 [Consultado: 23 de octubre de 2022]. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

ANEXOS

Anexo A. Tipos de activos

ACTIVOS	DESCRIPCIÓN
,m	Copias de Respaldo, datos de control de acceso, código fuente.
[K] CLAVES CRIPTOGRÁFICAS	Claves privadas de firmas.
[S] SERVICIOS	Página Web, Correo electrónico.
[SW] SOFTWARE	Sistemas operativos, Sistemas aplicativos, Antivirus.
[HW] EQUIPAMIENTO INFORMÁTICO	Equipos de escritorio, Equipos móviles, Enrutadores.
[COM] REDES DE COMUNICACIONES	Red telefónica, Alámbrica, Inalámbrica, Telefonía, Internet.
[Media] SOPORTE DE INFORMACIÓN	Discos de almacenamiento de información.
[AUX] EQUIPAMIENTO AUXILIAR	Fuentes de alimentación, Equipos de Climatización, de destrucción.
[L] INSTALACIONES	Oficinas, Edificios, Vehículos.
[P]PERSONAL	Usuarios internos, Externo, Administradores Todos los trabajadores de la empresa.

Fuente: libro II-MAGERIT MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [en línea]. Edita: © Ministerio de Hacienda y Administraciones Públicas, octubre 2012.- NIPO: 630-12-171-8. [Consultado: 10 de abril de 2021]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Anexo B. Dimensionamiento con respecto a la valoración,

[D] Disponibilidad: consiste en la propiedad de los activos de estar accesibles cuando los requieran.
[I] Integridad: Propiedad que garantiza que la información no ha sido alterada de manera no autorizada
[C] Confidencialidad: consiste en NO revelar información, ni poner en disposición, a terceros o procesos no autorizados.
[A] Autenticidad de los usuarios: Propiedad que garantiza la fuente de la que proceden los datos.
[T] Trazabilidad: Propiedad consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad

Fuente: libro II-MAGERIT. MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [en línea]. Edita: © Ministerio de Hacienda y Administraciones Públicas, octubre 2012.- NIPO: 630-12-171-8. [Consultado: 10 de abril de 2021]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Anexo C. Criterios de valoración,

VALOR			CRITERIO
10	EXTREMO	E	Daño extremadamente grave
9	MUY ALTO	MA	Daño muy grave
6-8	ALTO	A	Daño grave
3-5	MEDIO	M	Daño importante
1-2	BAJO	B	Daño menor
0	DESPRECIABLE	D	Irrelevante a efectos prácticos

Anexo D. Degradación, Probabilidad

Degradación:

MUY ALTO	MA	Casi seguro	Fácil
ALTO	A	Muy alto	Medio

MEDIO	M	Posible	Difícil
BAJO	B	Poco probable	Muy difícil
MUY BAJO	MB	Muy raro	Extremadamente difícil

Probabilidad

100	MA	Muy frecuente	A diario
10	A	Frecuente	Mensualmente
1	M	Normal	Una vez al año
1/10	B	Poco frecuente	Casa varios años
1/100	MB	Muy poco frecuente	siglos