TRABAJO DE GRADO

TECNOLOGÍAS DEL TELETRABAJO PARA PYMES, ASPECTOS DE SEGURIDAD

ANDRÉS MAURICIO RICO MENESES

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020

TRABAJO DE GRADO

TECNOLOGÍAS DEL TELETRABAJO PARA PYMES, ASPECTOS DE SEGURIDAD

ANDRÉS MAURICIO RICO MENESES

Trabajo de grado presentado para optar al título de Especialista en Seguridad de la Información

Docente

ALFONSO LUQUE ROMERO
MSC EN SISTEMAS DE INFORMACIÓN

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020

Todas las palabras que he dicho
Siempre estás en ellas

A mi familia y a todas aquellas personas que con su apoyo esfuerzo y dedicación me han llevado hasta donde he llegado

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Es evidente el cambio de paradigma debido a los eventos recientes, se han establecido nuevas necesidades entre ellas la continuidad laboral en tiempos de pandemia. Ya que el mundo moderno no había tenido que lidiar con una situación de tales proporciones[1], ha sido necesario y en tiempo récord agilizar la integración del teletrabajo no cómo una herramienta para casos puntuales de trabajo administrativo de poco valor, sino como la base del trabajo actual. Crear y adaptar empresas a esta nueva experiencia es una labor traumática por decirlo menos, independientemente de la región la mayoría de pequeñas y medianas empresas no conciben el teletrabajo como una manera de generar resultados, sino de compensar labores para aquellas personas que no pueden presentarse físicamente a la oficina.

Realizar esta adaptación en las empresas, particularmente las pequeñas y medianas o PYMES que en el panorama regular no estaban preparadas para estos sistemas, requiere de todas las herramientas disponibles, y quizás una a las que se debe prestar mayor atención es la seguridad; la implementación del teletrabajo y herramientas colaborativas somete a las empresas a enfrentar nuevas vulnerabilidades, que posiblemente no estén preparadas para afrontar; visibilizar estos riesgos es la función de este trabajo, establecer los orígenes y las posibles soluciones, elegir de manera adecuada las herramientas de acuerdo al nicho laboral, objetivo, misión, visión y demás que permitan aumentar la productividad de las empresas.

Esta es la razón de este proyecto, encaminar a las PYMES quienes son particularmente vulnerables en los escenarios regulares, y en este nuevo panorama son aún más propensas a perder la información. Por encima de las demás empresas. Cualquier herramienta que pueda ayudar en la toma de decisiones es necesaria y bien recibida.

[1] CARREÑO DUEÑAS, Dalia. (2016). Contexto general de la virtualidad. En D. Carreño Dueñas. Pensar el derecho como derecho virtual (pp. 12). Bogotá: Universidad Católica de Colombia

2. GENERALIDADES

1. LÍNEA DE INVESTIGACIÓN

Esta investigación se realiza bajo la línea de investigación de “Software inteligente y convergencia tecnológica” avalado por la Universidad Católica de Colombia.

2. PLANTEAMIENTO DEL PROBLEMA

Las actuales circunstancias nos han llevado a utilizar las herramientas del teletrabajo, estas mismas circunstancias no permitieron una instrucción apropiada, una socialización acertada para la mayoría de las empresas PYMES que seis meses atrás no contemplaban estas de una manera viable para realizar labores administrativas y/o técnicas, las implementaciones en este campo han tenido un crecimiento exponencial, así como sus ataques a las plataformas y tecnologías[2], peligra la confidencialidad y la integridad de los sistemas y la información de las empresas.

Ante el panorama de seguridad corporativo actual en Colombia[3], la baja penetración de los sistemas de seguridad para proteger la información y controlar el acceso a los sistemas internos de cada compañía, el teletrabajo agrega un nuevo aspecto en consideración a la seguridad.

Es necesario e igualmente importante estudiar los entornos del teletrabajo, analizar sus vulnerabilidades que decanten las soluciones apropiadas a cada entorno teniendo en cuenta sus limitaciones económicas, ambientes corporativos, funciones, minimizando las vulnerabilidades existentes mediante buenas prácticas y la socialización correspondiente.

1. ANTECEDENTES DEL PROBLEMA

Según el informe de tendencias del cibercrimen Colombia 2019 – 2020 se reportaron 717 casos de ransomware en el país[4], tomando en cuenta que solamente se reportan entre un 10% y un 20% frente a la dimensión del delito, se estima un total de ataques entre 3,500 y 4,000 durante 2019, sumado a que un 83% de las

[2] RODRÍGUEZ A, Javier H. & TORRES C, Wilmer A. (2019). Análisis de riesgos de seguridad de la información del área IT de la empresa Royal Services S.A. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información. Bogotá, Colombia. Pág. 10

[3] FORERO O, Bryan, PAVA C, Jonier. & SARMIENTO, James. (2018). Diagnóstico de seguridad y privacidad de la información en la alcaldía municipal de Icononzo-Tolima. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información. Bogotá, Colombia

[4] CCIT Informe de las tendencias del cibercrimen en Colombia (2019-2020). Bogotá D.C., 2019

empresas del país carecen de protocolos de respuesta a la violación de políticas de seguridad de la información. Estos son datos relevantes, ya que el crecimiento y la pérdida total de sistemas de información se ha constituido en una amenaza estructurada y latente para la continuidad del negocio; hasta hace tres años el segmento de ataques informáticos no contemplaba ataques transversales a la estructura de información, (computadores, servidores, equipos de almacenamiento, y recuperación) por igual.

El sitio especializado en aplicaciones y compañías Crunchbase, reporta un crecimiento del 698% de descargas de la aplicación Zoom con más de 40 millones en los últimos 30 días. Los ciberdelincuentes no miran qué tan robusto es un sistema para atacarlo, sino su popularidad[5]; esta panorámica expuesta muestra la tendencia de ataques del 2020, este crecimiento sumado a la actual necesidad de distanciamiento y confinamiento harán una fuente redituable de dinero para los criminales. Y si bien como empresas no es posible eliminar las vulnerabilidades si es posible mejorar sus prácticas reduciendo los riesgos

Ante las recientes vulnerabilidades publicadas para las plataformas de comunicaciones Zoom, CVE-2019-13450, CVE-2020-11469, CVE-2020-11470, CVE-2020-11500, cisco WebEx teams CVE-2020-3131, CVE-2020-3155, Microsoft teams CVE-2020-0815 se hace necesario evaluar el uso de esta plataforma tanto en sus vulnerabilidades técnicas, como en sus prácticas de uso corporativo. No solo por las implicaciones de seguridad y afectación de infraestructuras, sumado a la perdida de información, sino también a las afectaciones a las que se expone una empresa al ser presa de un ataque tal como sucedió en la universidad de Antioquia ante 170 participantes[6]. Este tipo de vulnerabilidades pueden afectar la imagen corporativa tanto de la empresa como de sus clientes; la responsabilidad de resguardar la confidencialidad de la información se extiende a las presentaciones y debe pensar en los presentadores y en los participantes.

A estos antecedentes se deben agregar los comportamientos típicos de los usuarios, como por ejemplo el uso de equipos comunitarios, redes sin seguridad, equipos sin actualizar, falta de sistemas operativos actualizados en empleados como en empresas, falta de políticas de conexión (ejemplo notificado por el reporte de amenazas Fortinet Q4, en el cual se reportó una aplicación falsa de customización de teclado que permitía a los criminales capturar información bancaria y tuvo 40 millones de descargas)[7], protocolos técnicos de acceso remoto, protocolo de reuniones virtuales, políticas de seguridad implementadas en ambientes virtuales, ya que es un escenario totalmente nuevo; la masificación del

[5] TAMAYO. Laura. Si usa Zoom, ¿debería preocuparse por su seguridad? El colombiano. 20 de abril de 2020
[6] NOTICIAS CARACOL. Universidad de Antioquia denuncia que su cuenta de Zoom fue hackeada en plena videoconferencia. Medellín, 17 de abril de 2020
[7] FORTINET. Threat Landscape Report Q4 2019. Sunnyvale, 2019

teletrabajo en empresas pequeñas y medianas que no habían contemplado esto de manera regular y constante, lo que plantea retos a nivel de estimación de riesgos, análisis de vulnerabilidades, metodologías e investigaciones sobre el uso adecuado y acertado de tecnologías de comunicación hacia la oficina, y entre los empleados. Diseñando soluciones en la medida de sus infraestructuras[8], ya que realizar una inversión inconveniente a estas tecnologías va a desencadenar en mayores riesgos de seguridad a los existentes, mayor dificultad de los empleados para realizar sus labores, nuevos vectores de ataque. Es importante tomar en cuenta el tipo de labor que desarrollaran los empleados, cuanta información y cuantos sistemas afectan sus labores diarias, ya que debe ser la meta de estos momentos debe ser la conservación de las actividades laborales fuera de las empresas.

2. PREGUNTA DE INVESTIGACIÓN

¿Cómo elegir las tecnologías del teletrabajo para PYMES que representen menor exposición al riesgo de seguridad?

3. VARIABLES DEL PROBLEMA

- El impacto en una organización por la vulnerabilidad de la aplicación y/o tecnología analizada, para determinar qué tanta afectación puede tener una empresa en caso de elegir la aplicación con dicha vulnerabilidad.

- La cantidad de vulnerabilidades acumuladas en una aplicación y/o tecnología que representen un riesgo significativo para la información.

3. JUSTIFICACIÓN

Para Mayo de 2019 “el Ministerio de las telecomunicaciones e información (MinTIC) asegura que en Colombia más de 12.912 empresas funcionan en la modalidad del teletrabajo y tan solo en Bogotá 63.995 personas laboran bajo de esta manera”[9]; las actuales circunstancias han obligado a cambiar el panorama radicalmente, el teletrabajo se ha convertido en un rublo de vital importancia para la operación de las empresas, el mundo se ha contraído en una manera sin precedentes en los tiempos modernos, con un aumento desmesurado de usuarios en teletrabajo aumentan los riesgos y se potencializan las amenazas; la aceleración de las empresas PYMES[10] hacia el teletrabajo obliga a contemplar y tomar todas las

[8] BARACALDO RINCÓN, Laura P. (2019). El outsourcing en las entidades públicas de Colombia. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Derecho. Bogotá, Colombia. Pág.6
[9] ARIAS. Diana. 12,912 empresas han implementado el teletrabajo en Colombia. Enter.co. Bogotá D.C. 17 de mayo de 2019.
[10] GONZÁLEZ S, Rony M. & COLO M., José H. (2019). Diseñar un modelo para implementar un sistema de gestión de seguridad de la información para una PYME del sector privado. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información. Bogotá, Colombia. Pág. 9

precauciones para elegir cual es el sistema más conveniente, cuál es el más seguro en relación costo-beneficio, y cuáles son las consideraciones para adoptar las tecnologías necesarias para implementar esta metodología de trabajo a distancia[11]

La situación vulnerable de las empresas hace que se tomen decisiones basadas en la inmediatez, primando la urgencia sobre la importancia, se incrementan los riesgos y las vulnerabilidades a las ya existentes; adoptando herramientas que pueden ser sub utilizadas o desproporcionadas, superando los costos a los beneficios; la creación de este análisis de vulnerabilidades se condensa en una guía práctica para la adopción correcta de las herramientas, contemplando factores los siguientes factores: crecimiento, seguridad y control de estas herramientas para poder brindar las garantías tanto a los trabajadores como a las empresas del uso correcto de estas.

El teletrabajo es la respuesta laboral a estos tiempos que requieren aumentar el distanciamiento social, disminuir la concentración de personas, mantener la producción, el trabajo y la economía; manteniendo segura a la población. Actualmente las empresas están obligadas a cambiar la manera de trabajar, a establecer nuevos y mejores sistemas administrativos, donde prime la salud de las personas sobre cumplir horarios, reemplazando el trabajo constante por resultados óptimos, estableciendo mejores métricas de productividad, reduciendo los recursos físicos en una empresa, siendo la nueva piedra angular del trabajo y todo lo que ello requiera. Un mejoramiento de archivos tanto físicos como digitales, ordenamiento y reducción de procesos, mejoramiento de la cadena de producción y entrega.

Esta crisis genera nuevas oportunidades, a repensar en lo que hace la empresa con el tiempo de sus trabajadores, cómo hacerles mejor la vida, cómo hacer que sean más productivos, cómo aprovechar más su tiempo; la tecnología permite una integración impensable hace 10 años; estudios del instituto Nacional de seguridad de España colocaban a Colombia en un promedio de consumo de internet de 76 kb/s en el 2015, cinco años después perfectamente se podría pensar en diez veces esa velocidad por persona, una penetración del 113% en el mercado móvil[12], muestran evidentemente el crecimiento de la economía.

[11] PORRAS SOTO, Edgar F. (2019). Las plataformas móviles una mirada al contrato laboral en Colombia. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Derecho. Bogotá, Colombia. Pág. 14.

[12] INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). Internacionalización Ficha Colombia. León 2015

3. OBJETIVOS

1. OBJETIVO GENERAL

Aportar elementos de juicio para elegir las herramientas del teletrabajo (conectividad remota y trabajo colaborativo), acordes a las necesidades de cada empresa PYMES de acuerdo con sus funciones, propósitos e infraestructura.

2. OBJETIVOS ESPECÍFICOS

- Listar vulnerabilidades en las tecnologías del teletrabajo y delimitarlas en un entorno empresarial tipo PYMES para determinar sus implicaciones al momento de adoptar las mismas.

- Evaluar las vulnerabilidades que se pueden encontrar en la modalidad de teletrabajo, enfocándose en aquellas que impactan las labores internas, el trabajo colaborativo, y las reuniones virtuales.

- Establecer las recomendaciones para mitigar los riesgos en las labores desarrolladas a través del teletrabajo.

4. MARCOS DE REFERENCIA

1. MARCO CONCEPTUAL

El concepto de teletrabajo es ampliamente conocido y no es relativamente reciente en la historia moderna de la sociedad; a través de la conceptualización de sus formas y las tecnologías que usa para el desarrollo de las actividades, se definirán los límites de información y la intención de desarrollo de este trabajo; por lo tanto, se aislará lo relacionado a la parte psicológica, social, buenas prácticas, tratando de enfocar los conceptos al área de seguridad, conservación e integridad de la información[13].

La definición de teletrabajo nace de la transformación de otro término: tele conmutación definido durante la crisis del petróleo de 1973 por el físico Jack Nilles, como una solución a reducir costos operativos realizando labores de conmutación de información desde los hogares, este concepto obtuvo unos niveles elevados de rendimiento y de reducción de costos en energía, aire acondicionado, transportes y demás; posteriormente en 1990 junto a un equipo de trabajo desarrolló un proyecto elaborado del teletrabajo[14]. Con la llegada y la masificación del internet, sumado al aumento de las labores computacionales, la reducción de procesos análogos cerca del año 2000 se pudo contemplar realizar labores completamente alejado de la oficina acuñando el termino teletrabajo

La organización internacional del trabajo OIT define de varias maneras en su manual de buenas prácticas al teletrabajo de la siguiente forma:" El teletrabajo es la forma de organizar y realizar el trabajo a distancia mediante la utilización de las TIC en el domicilio del trabajador o en lugares o establecimientos ajenos al empleador"[15] pero más allá de su definición, el ministerio de las TIC en Colombia establece las características asociadas al teletrabajo[16]:

- Una actividad laboral que se lleva a cabo fuera de la organización en la cual se encuentran centralizados todos los procesos

[13] ARÉVALO C., Ligia, FERNÁNDEZ M., Edwin N. & ZAMBRANO R., Ángela (2016). Diseño del plan de recuperación de desastres (D.R.P.) para la compañía Agencia de Aduanas Profesional nivel 1 SIAP sede Bogotá. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Especialización en Seguridad de la Información. Bogotá, Colombia Pag 14

[14] KITAMURA. Ryuichi, NILLES. Jack M., CONROY Patrick, & FLEMING David M. Telecommuting as a Transportation Planning Measure: Initial Results of California Pilot Project. Transportation Research Record 1285. págs. 98 - 104. 1990.

[15] OFICINA INTERNACIONAL DE TRABAJO. Manual de buenas prácticas en teletrabajo. Buenos Aires. 2011.

[16] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. LIBRO BLANCO El ABC del teletrabajo en Colombia. Bogotá D.C. 2017

- La utilización de tecnologías para facilitar la comunicación entre las partes sin necesidad de estar en un lugar físico determinado para cumplir sus funciones

- Un modelo organizacional diferente al tradicional que replantea las formas de comunicación interna de la organización y en consecuencia genera nuevos mecanismos de control y seguimiento a las tareas.

De esta manera se cambian los conceptos de cumplimiento de tareas metas y métricas para mejorar el nivel de efectividad de las labores del trabajador, más allá de llegar a un sitio y cumplir su horario.

Por otro lado, ICONTEC establece en NTC-ISO-IEC 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos al teletrabajo como un objetivo de control y lo expresa de la siguiente manera: "Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo"[17]. Adicionalmente, en la norma ISO 27002 se expresa en una forma consistente a la norma 27001 en afrontar el teletrabajo como un objetivo de control tal como lo expone JJ Chaverra en el artículo El teletrabajo y la seguridad de la información personal:

> "La norma GTC-ISO-IEC 27002:2015 Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información. Está compuesta por 14 dominios, 35 objetivos de control y 114 controles e incluye en el dominio 6: Organización de la seguridad de la información, y también dos puntos sobre los dispositivos para la movilidad y el teletrabajo, las políticas para dispositivos móviles y las políticas para el teletrabajo [18]"

Definido el concepto del teletrabajo se establecen 3 modalidades del teletrabajo: autónomo, suplementario, y móvil[19] en los cuales autónomo es la realización de las labores a través de las tecnologías de información entregando los resultados para evaluación de un superior; en el suplementario el trabajador mínimo 2 días a la semana realiza labores remotas complementarias a sus labores desarrolladas en las instalaciones; y por último el trabajo móvil son las actividades desarrolladas puerta a puerta utilizando dispositivos de comunicación móvil bajo plataformas GSM

[17] NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001. Pág. 13. Bogotá D.C. 2013.
[18] CHAVERRA MOJICA. John J. El teletrabajo y la seguridad de la información empresarial. Medellín. 04 de junio de 2015. pág. 115.
[19] CRUZ CASTILLO, Jhon F., GUZMÁN BAYONA, Jesly S., HURTADO CONTRERAS, Maite C. & MELO VARGAS, Yudy D. (2018). Análisis de la factibilidad del modelo del teletrabajo en la entidad financiera BA para el área de servicio al cliente. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ciencias Económicas y Administrativas. Programa de Economía. Especialización en Formulación y Evaluación Social y Económica de Proyectos. Bogotá, Colombia. Pág. 16.

que permiten entregar información de la labor realizada y el lugar donde se realiza[20]. Independientemente de su modalidad el teletrabajo tiene dos funciones primarias, la realización de las labores con sus respectivos informes y entregables, y la comunicación interna (reuniones, comités, capacitaciones, etc.) se definen estas dos funciones para establecer las tecnologías relacionadas; adicionalmente es necesario establecer el tipo de usuario del teletrabajo, relacionado con los niveles de acceso a los sistemas, la intervención en los mismos, si estas labores intervienen en niveles operarios, financieros, estratégicos, directivos, ya que a mayor nivel de intervención mayor seguridad debe ser integrada para estas labores; los niveles son:

- Nivel operativo: aquel empleado que tiene acceso a los sistemas de información, para labores de mercadeo, operación, compras, ventas u similar puede tener acceso público o privado

- Nivel financiero: aquellas operaciones que se deben realizar ante entidades financieras, pagos de nómina y proveedores, impuestos; estas operaciones requieren de elevación de seguridad, únicamente mediante canales privados, y con niveles de múltiple autenticación.

- Nivel Estratégico: contiene toda la información anterior, más todos los datos críticos de la compañía, estados financieros, proyecciones de ventas, operaciones y contratos con clientes; este nivel debe ser tratado de ser necesario con niveles de encriptación en ambas partes (origen-destino) con niveles de autenticación multi-factor.

- Nivel Directivo: en este nivel no debe ser manejado en teletrabajo puesto que es el principal objetivo de espionaje corporativo, esta información no debe ser colaborativa y debe estar resguardada con todos los sistemas de seguridad disponibles.

Para realizar las labores mencionadas en teletrabajo se debe definir los canales y medios de comunicación:

- Canales de comunicación pública: las labores operativas puedes ser realizadas bajo comunicación pública, portales laborales los cuales poseen sistemas de autenticación de 1 o dos niveles para realizar las labores internas de un sistema de información, esto supone una arquitectura robusta de información de la empresa interna o externa dependiendo de sus presupuestos.

[20] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. LIBRO BLANCO El ABC del teletrabajo en Colombia. Bogotá D.C. 2017.

- Canales de comunicación privada: se refiere principalmente a las VPN (Red Virtual Privada) la cual establece una comunicación entre el empleado y la oficina principal, esta comunicación se establece mediante los siguientes protocolos, que son la manera de cifrar la información y que no sea púbica para cualquier persona que trate de capturar esta conexión:

    - PPTP Protocolo de Túnel punto a punto, uno de los primeros sistemas de cifrado de información apoyado por Microsoft, es estándar desde 1995 y es considerado uno de los más agiles y a la vez más inseguros recomendado únicamente para labores de baja complejidad, mucha carga de información, paquetes de datos grandes, los sistemas de comunicación PPTP utiliza un sistema de usuario y contraseña el cual es guardado tanto en el software de VPN como en su contraparte en el dispositivo de comunicación, bien sea servidor o enrutador, la encriptación de 128 bits se utiliza en la comunicación no en la transferencia de paquetes lo que representa una debilidad y un posible vector de ataque[21]

    - L2TP Layer 2 Tunneling Protocol, cómo tal L2TP no ofrece encriptación va de la mano de un protocolo conocido como IPsec para realizar una encriptación por paquetes, cada paquete de información lleva imbuido una porción del hash generado para el usuario y contraseña el cual es recibido en la oficina desencriptado AES-256 bits de manera simétrica, este protocolo puede ser usado mediante certificados de seguridad (una entidad que genera una llave asegurando que el sitio, los servidores, y la conexión sean seguras) o mediante una contraseña la cual si bien es más económica que un certificado es más insegura, entre sus desventajas está el bloqueo por parte de firewalls ya que maneja un protocolo UDP, y una velocidad inferior a PPTP

    - SSTP Protocolo de Túnel de Puerto Seguro utiliza encriptaciones de 2048 en la autenticación y es obligatorio el uso de un certificado SSL/TLS su llave de conexión utiliza una encriptación adicional de 256 bit en los paquetes haciéndolo imposible de atacar para extracción de información, permite múltiples conexiones hasta 1,000 usuarios simultáneos, sus costos de implementación dificultan a las pequeñas y medianas empresas volverlo un protocolo de masiva utilización.

[21] EXPRESS VPN. 2020. https://www.expressVPN.com/es/what-is-VPN/protocols/pptp

- IKEV2 Llave Intercambiable de Internet 2da Versión, otro protocolo cuyas características no le permiten encriptar por sí mismo y utiliza el protocolo IPSEC utiliza un cifrado en las llaves AES-256 bit y SHA2-384, utilizado masivamente en el mercado móvil ya que se adapta a los cambios de red y conserva la conexión por mayor tiempo que los otros protocolos[22].

- Canales de comunicación pública no centralizada: se refiere a todos los programas que permiten la conexión a las oficinas de trabajo bajo conexiones de un tercero, TeamViewer, log mein son los más utilizados requieren de un software en cada lado, un número de identificación y una contraseña, la autenticación se realiza mediante la verificación de los servidores en la nube que establecen el canal de comunicación no directo entre empleado y máquina utilizan sistemas de encriptación invisibles y no configurables para el usuario, sin embargo, estos programas requieren un pago por maquina conectada y de pago en servicios en la nube por mensualidad o anualidad, utiliza sistemas de conexión [23] seguros más no encriptados y bajo los riesgos que esto conlleva.

Establecidos los canales de comunicación para la realización de las labores del teletrabajo se definen las tecnologías para realizar el trabajo colaborativo (reuniones, comités, entrega de resultados) se definirán las tecnologías expuestas en el cuadrante mágico de Gartner.

Figura 1. Cuadrante de Gartner en soluciones de reuniones Q3 2019

[22] CASTELLANO, Jenifer. Solvetik. 16 de octubre de 2017. https://www.solvetic.com/page/recopilaciones/s/seguridad/caracteristicas-protocolos-VPN-openVPN-sstp-l2tp-ikev2-pptp

[23] ANGARITA P., Cristian A. & GUZMÁN F., Camilo (2017). Protocolos para la mitigación de ciberataques en el hogar. Caso de estudio: estratos 3 y 4 de la ciudad de Bogotá. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información. Bogotá, Colombia Pág. 10.

Se realiza una descripción breve de las tecnologías utilizadas para realizar el trabajo colaborativo:

- ZOOM: una aplicación cloud[24] que integra video y comunicaciones hasta 1,000 personas por sala, con una aplicación stand alone, acceso web o app es capaz de conectar a las personas registradas trasmitir imagen, compartir la imagen del presentador o algún participante, tiene capacidades de calendario lo que permite la organización de tiempo de los empleados en una agenda integrada a las cuentas de correo comunes, ha tenido un crecimiento acelerado en los años recientes volviendo muy popular su utilización.

- MICROSOFT TEAMS, parte de las soluciones integrales, Microsoft desarrolla una herramienta capaz de compartir no solo las características de Zoom sino también intervención de documentos, planeación labores todo integrado a su plataforma de office 365 con una capacidad de 10,000 usuarios es una herramienta de mayor nivel que su contraparte.

- CISCO WEBEX TEAMS, ofrece una mayor conectividad e integración a telefonía IP y a las infraestructuras cisco reservado para grandes clientes con infraestructuras robustas ya que soporta 40,000 usuarios en una reunión.

Descritas las herramientas para desarrollar teletrabajo se debe enumerar y explicar brevemente los tipos de ataque que estarían enfocados los usuarios del teletrabajo y su objetivo siempre será el económico, bien sea minimizando la competencia, obteniendo información crítica (espionaje industrial) obtención de datos bancarios para fraudes, o simplemente la suspensión de actividades que desemboca en alguno de los objetivos anteriormente descritos, los vectores de ataque (fuentes de riesgos) son:

- Phishing terminó ingles que se refiere a obtener datos críticos de una organización mediante correos electrónicos solicitando falsamente información sensible, engañando al usuario para acceder a vínculos falsos que pueden ser réplicas de sitios oficiales, o portales de descarga de códigos maliciosos para capturar y transmitir información.

[24] GONZÁLEZ GARCÍA, Manuel F. (2018). Definición de estrategias de adopción de la cuarta revolución industrial por parte de las empresas en Bogotá, aplicables a PYMES en Colombia. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería Industrial. Bogotá, Colombia. Pág. 39.

- Bombing, interrupciones a las reuniones virtuales, aprovechando vulnerabilidades de las plataformas de comunicación, intervienen una reunión, desacreditando a los anfitriones y evitando la entrega de información pertinente, estas vulnerabilidades permiten obtener información de los participantes, grabación de las sesiones de manera no autorizada, afectación del buen nombre y demás.

- Hacking, el acceso no autorizado a infraestructuras mediante los canales dispuestos para teletrabajo, esta práctica tiene muchas condiciones para ser exitosa, requiere obtención de datos de acceso o uso de ingeniería social para obtener las credenciales y los datos relevantes para realizar una conexión exitosa a una organización.

2. MARCO TEÓRICO

Robert Morgan, experto en administración de negocios y autor del libro "Teleworking: An Assessment of the Benefits and Challenges" expresa entre muchas la siguiente teoría: "el teletrabajo no solo coadyuva a que la empresa optimice un balance financiero – reducción de costos de funcionamiento- sino también a incluir nuevos talentos laborales a una comunidad o mercado segmentado, caracterizado por la inclusión de nuevas formas de venta, marketing, compra e intercambio"[25]; estas nuevas formas de hacer negocios contienen una parte del empleador creando las herramientas y las condiciones de seguridad necesarias para conservar los tres pilares de la información (disponibilidad, integridad, confidencialidad), y del parte del trabajador siguiendo los protocolos de seguridad, realizando buenas prácticas del teletrabajo, creando una simbiosis que beneficie a la industria y al trabajador, el primero con mejores índices de productividad y al segundo con una mejor calidad de vida.

Hacia este camino de beneficio mutuo para ambas partes (empleador-trabajador) Oscar Jiménez director de proyectos de Great Place to Work en Colombia considera fundamental la relación de confianza entre ambas partes, la generación de nuevas competencias de liderazgo, y la cultura del trabajo presencial al virtual[26]; estas directrices le permitirán tanto a las empresas reducir sus medidas disciplinarias, a recibir elementos productivos de calidad de empleados comprometidos con la empresa ya que el nivel de responsabilidad es mayor entre un empleado presencial que un empleado en teletrabajo, en el cual es su propio inspector de calidad, depende de sus conocimientos y recursividad para resolver problemas que en otros casos podría acudir a superiores que solventaran tales problemas.

[25] MORGAN, Robert. Teleworking: An Assessment of the Benefits and Challenges. European Business Review. Vol. 16 No 4. págs. 344-357. 2004.
[26] REVISTA LUCIERNAGA. Comunicación organizacional en torno al teletrabajo. Medellín. Vol. 16, No 18, págs. 61-71. 2017.

Los retos para las empresas que debieron someterse aceleradamente a implementar sistemas del teletrabajo[27] son muchos; han tenido que adaptarse sobre la marcha cambiando las maneras de medir la productividad, cambiar los controles disciplinarios, controlar las comunicaciones internas que cumplan los objetivos de alto nivel; y, bajo estos parámetros el concepto de Michael Antony Clark. “un nuevo concepto empresarial, cuya determinación comercial y éxito empresarial depende de la agilidad disciplinar, analítica y praxeológica del cuerpo gerencial” donde estas habilidades gerenciales deben contemplar la seguridad de la información cómo un elemento transversal de toda esta transformación, ante esto expone Edwar Morales Osorio: “La seguridad informática se debe ver como un proceso preventivo y defensivo dentro del negocio y sería ideal que se convirtiera en un proceso transversal en cualquier negocio”[28] está integración es de vital importancia y es la razón principal de esta investigación, analizar las tecnologías actuales, comerciales más populares para realizar las labores del teletrabajo bajo los dos enfoques explicados en el marco conceptual; determinar los riesgos involucrados al utilizar una u otra herramienta permitiría a los departamentos de TI y gerencias evaluar las opciones y tomar medidas para mitigar los riesgos.

3. MARCO JURÍDICO

En Colombia la definición y clasificación de empresas tipo PYMES se encuentra reglamentada por la Ley 590 de 2000 y sus modificaciones en la Ley 905 de 2004 en las que se define y categorizan según el número de trabajadores y el valor de los activos, siendo las microempresas una unidad de explotación económica con menos de 10 trabajadores, la pequeña empresa comprende entre los 11 y 50 trabajadores y la mediana empresa es la que cuentan con un personal entre 51 y 200 trabajadores[29].

El teletrabajo se encuentra amparado bajo las normas expresas en la Ley 1221 del 2008 y el decreto 884 del 2012, adicionalmente, se exponen los 5 acuerdos para la implementación del teletrabajo en el sector privado:

- Voluntariedad: debe existir una solicitud clara y escrita por parte del empleado para realizar las labores de manera remota, está es bidireccional y debe ser aceptada o rechazada voluntariamente por la parte ofertante.

[27] DIAZGRANADOS, Carlos (2018). Precisiones conceptuales e implementación práctica del teletrabajo. En L. A. Diazgranados Quimbaya, L. F. Vallecilla Baena, C. M. Diazgranados Quimbaya, S. Gómez Escobar, J. D. Montenegro Timón & J. E. Almanza Junco. (pp. 71-93). Bogotá: Editorial Universidad Católica de Colombia

[28] OSORIO MORALES, Eduar. logopoliskpo. 21 de junio de 2018. http://logopoliskpo.com/2018/06/21/seguridad-de-la-informacion-en-pymes/

[29] OSORIO MORALES, Eduar. logopoliskpo. 21 de junio de 2018. http://logopoliskpo.com/2018/06/21/seguridad-de-la-informacion-en-pymes/

- Acuerdo o contrato: se debe crear un anexo al contrato en el que se expresan las condiciones en que operará el teletrabajador y la compañía.

- Modificación del reglamento interno: se debe incorporar un capítulo referente al teletrabajo, en el que cubra los aspectos de las restricciones de uso de programas, la protección de datos personales, y las sanciones al incumplimiento de dichas normas.

- Seguridad Social: cómo cualquier trabajador, la persona que labore en teletrabajo tiene derecho a su seguridad social integral.

- Reversibilidad: es la capacidad del trabajador de retornar a sus labores en sitio, garantizar por parte del empleador las condiciones para ese retorno cuando este no ha sido contratado bajo la modalidad del teletrabajo.

En cuanto a la normatividad vigente en Colombia para la seguridad de la información, que es la meta principal de esta investigación, se adhiere a las leyes expuestas y referenciadas en el plan de seguridad y privacidad de la información del ministerio de comunicaciones, las cuales se describen a continuación:

- **Ley 44 de 2093.** Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).

- **Ley 527 de 2099.** Por 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.

- **Ley 594 de 2000.** Por medio de la cual se expide la Ley General de Archivos.

- **Ley 1266 de 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.

- **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.

- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.

- **Ley 2015 de 2018.** Por la cual se modifica la Ley 23 de 2082 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

4. MARCO GEOGRÁFICO

Esta labor se realiza en la verificación de vulnerabilidades de las plataformas de trabajo colaborativo y accesos remotos, no tiene un sitio determinado para ser revisadas las condiciones de una empresa.

5. MARCO DEMOGRÁFICO

La investigación no requiere el estudio de una población específica y no es necesario plantear las características de esta.

6. ESTADO DEL ARTE

No hay opiniones divididas, no existe polémica, ni posiciones distantes, todas las personas del medio de seguridad concuerdan con la necesidad urgente de aplicar medidas y políticas para reducir las amenazas[30] y evitar desenlaces conocidos por la seguridad informática; nuevas herramientas acarrean nuevos riesgos, nuevas vulnerabilidades y prácticas para determinar la mejor utilización de los recursos. Este estado del arte expone los puntos de vista comunes de expertos en seguridad

Tony Anscombe CSE de eset antivirus expone al respecto sobre seguridad del teletrabajo en tiempos de cuarentena “Dividir la organización en unos pocos grupos con diferentes requisitos y el tratamiento de las necesidades de cada uno para lograr el éxodo masivo puede parecer un enfoque simplista, pero probablemente sea esencial dada la urgencia en algunos casos.“ y probablemente sea el enfoque correcto reducir los niveles de acceso[31], debe ser la primera trinchera en estos tiempos a menor acceso menor riesgo; adicionalmente es importante capacitar en las buenas prácticas para el uso correcto de estas herramientas de uso obligatorio en tiempos de distanciamiento social.

[30] SÁNCHEZ S., Andrés F. & RODRÍGUEZ R., Rafael E. (2018). Desarrollo de un modelo para calcular el nivel de seguridad en sitios Web, basado en el top 10 de vulnerabilidades más explotadas en 2017 según el marco de referencia OWASP. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información. Bogotá, Colombia Pág. 14

[31] MELO CAMPOS, Angie R. (2019). Regulación de las nuevas formas de empleo que surgen por medio de las plataformas digitales. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Derecho. Bogotá, Colombia

Jesús Yáñez Abogado IT de ECIJA expone en su artículo una serie de recomendaciones de las cuales abe recalcar la siguiente: “es necesario abandonar los usuarios genéricos por varios motivos fundamentales. Entre estos, destaca la seguridad, ya que, si dispone de usuarios genéricos, no va a poder saber quién entra realmente al sistema.”. Cómo uno de los principales pilares de la seguridad la individualización del trabajador es vital para trazabilidad de riesgos, ataques y vulneraciones a los sistemas, el anonimato es cómplice del criminal; es muy importante esta práctica cómo base y control de todos los procesos del teletrabajo y de manera trasversal cómo se expuso en apartados anteriores. Debe ser una política general de acceso a todos los sistemas de manera individual, pero conservando el equilibrio y ajustando a los accesos multi-factor para realizar la verificación del trabajador en la compañía.

5. METODOLOGÍA

1. FASES DEL TRABAJO DE GRADO

La metodología utilizada en este trabajo de grado se realizará en base a los principios del marco de gobierno de TI COBIT 2019, ya que se enfoca para las pequeñas y medianas empresas PYME no se realizará un sistema riguroso de uso de COBIT; utilizando sus ventajas se ajustará en los siguientes pasos

- Recolección de vulnerabilidades en tecnologías relacionadas con teletrabajo, basándose en los reportes generados por la base de datos NVD, agrupados por su función (en el caso de las tecnologías de comunicación) o por género (en el caso de las tecnologías de trabajo remoto).

- Tabulación de la información recolectada en la cual se extraerá las plataformas afectadas, fecha de publicación, las condiciones en las cuales se materializa la vulnerabilidad según las pruebas hechas por NVD al momento de publicar el reporte.

- Realización de un análisis de las vulnerabilidades cotejando sus impactos tanto en peligrosidad como penetración a las organizaciones mediante el establecimiento de puntos en común, tendencias, picos de reportes en un determinado periodo.

- Establecimiento de recomendaciones basadas es los análisis de vulnerabilidades transversales acotando aquellas que puedan influir en otra tecnología.

2. INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

Se utiliza la matriz de riesgos para establecer las amenazas de las herramientas del teletrabajo basadas en el estudio de descargas App Annie aquellas aplicaciones de reuniones que han tenido un crecimiento al uso tradicional tal como se puede observar en la imagen

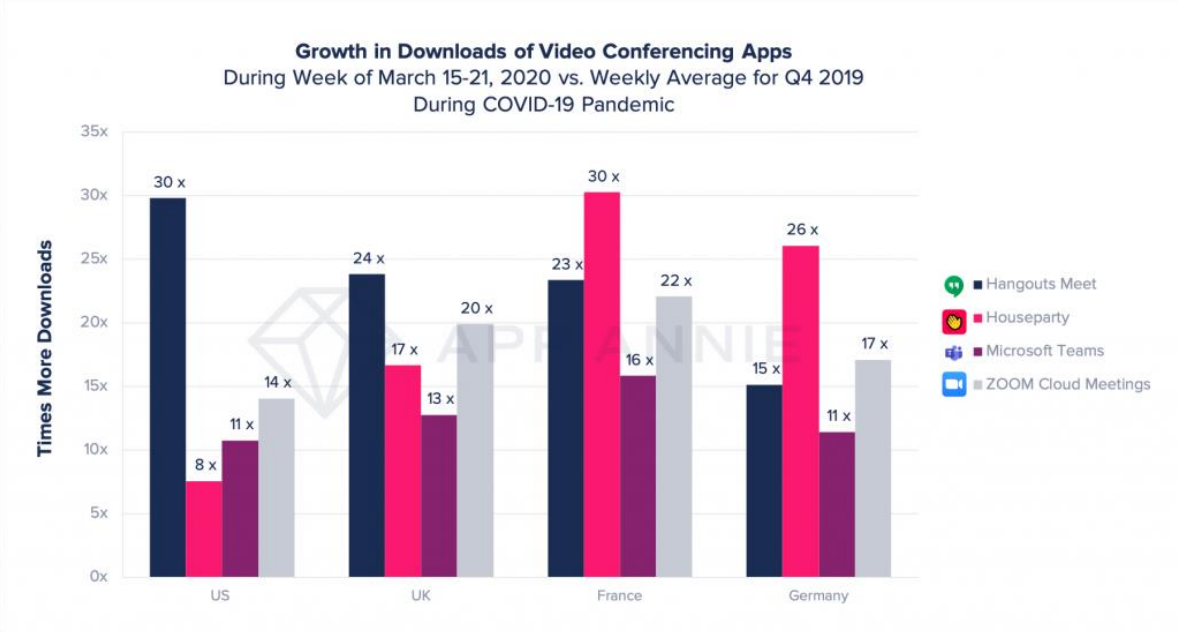

Figura 2. Crecimiento de descargas de aplicaciones de reuniones Q4 2019 fuente: https://www.appannie.com/en/insights/market-data/video-conferencing-apps-surge-coronavirus/

Para determinar que aplicaciones pueden ofrecer mayor nivel de seguridad a las PYMES es necesario realizar un análisis trasversal de las vulnerabilidades, analizar más allá de una revisión de la falla, para este análisis de vulnerabilidades se utilizan dos métodos, el primero de ellos fue la realización de un estudio estadístico de cada reporte utilizando Microsoft Power BI®; este estudio permitió promediar, establecer tendencias y decantar cuales reportes deben de tomar nuestra atención. El segundo fue el establecimiento de escenarios de riesgo individuales y compuestos que pudieran determinar en qué momentos las vulnerabilidades pueden tener una relevancia mayor al combinar ciertas tecnologías permitiría escalar riesgos, acrecentarlos o reducirlos combinando probabilidades; estos escenarios se realizaron en formatos de escenario de riesgos COBIT 5 v2013.

3. POBLACIÓN Y MUESTRA

El proyecto no está orientado a una población determinada por ende no se realiza un estudio poblacional.

4. ALCANCES Y LIMITACIONES

Se realizará un documento analizando las amenazas actuales publicadas documentadas y registradas en la base de datos de vulnerabilidades CVE de Mitre de las tecnologías del teletrabajo administrativo comercial (Zoom meeting, Microsoft Teams, Google Meet, Cisco WebEx Teams) para determinar su escala de seguridad en relación costo/beneficio; estas aplicaciones se ponderan sobre otras basadas en el estudio realizado por App Annie el cual determinó la cantidad de descargas durante una semana del 15 al 21 de marzo estableciendo un marcado crecimiento y popularidad; creando un marco comercial de asesoría, así como un documento con las mejores prácticas para los colaboradores, administradores IT, junto con sus perspectivas de uso; no incluye pruebas de ataque a las plataformas de manera teórica o práctica, tampoco se analizará códigos de programación de dichas plataformas al igual que someterlo a pruebas ambientales en entornos controlados. Este análisis trasversal permite totalizar las vulnerabilidades, estudiar sus picos de descubrimiento y el tiempo que se han tomado para detectar y publicar las mencionadas vulnerabilidades

De igual forma es importante recalcar los aspectos medioambientales del trabajo en casa, y los aspectos de seguridad que conllevan. Típicamente se ha recomendado elevar las condiciones de seguridad en los hogares mediante prácticas básicas; uso de antivirus pagado en los equipos, la individualización de estos para cada miembro del hogar, entre otros. Sin embargo, estas prácticas no pueden ser medidas o estudiadas mediante las variables y los objetos de estudio presentados en este trabajo.

6. PRODUCTOS A ENTREGAR

1. Evaluación de vulnerabilidades de tecnologías del teletrabajo para PYMES

2. Resultados de los análisis de escenarios de riesgo de las herramientas del teletrabajo

3. Trabajo de grado en el cual se entregan las conclusiones de los análisis de las herramientas analizadas

4. Articulo IEEE Sobre la seguridad de la información en el teletrabajo

7. ENTREGA DE RESULTADOS E IMPACTOS

Para desarrollar un enfoque hacia los riesgos de cualquier tecnología al alcance presupuestal de las PYMES, que no requieran una implementación compleja, o un cambio de infraestructura total, migraciones a la nube, administración de servidores en AWS o implementaciones que superan los niveles técnicos; en segunda instancia para determinar el nivel de seguridad, y a un nivel más específico las vulnerabilidades registradas en la base de datos de vulnerabilidades NVD desde el primero de enero del año 2000 hasta la fecha de levantamiento según el cronograma; ahora si bien la base de datos almacena de manera secuencial todas las vulnerabilidades registradas tiene métodos de búsqueda, estos métodos de búsqueda permitieron establecer las tecnologías buscando las palabras, VPN, ZOOM, WEBEX, GOOGLE CLOUD, MIKROTIK, FORTINET, IPSEC, VPN, y RDP; se excluyeron todas las vulnerabilidades que no tuvieran que ver con las tecnologías requeridas para PYMES, ej.: WORDPRESS.

El paso siguiente para desarrollar el estudio, consistió en la tabulación de la información la cual arrojó 190 vulnerabilidades entre las dos aristas propuestas (teletrabajo y comunicación). Estas fueron clasificadas por la palabra clave de búsqueda en la base de datos, se establecieron datos tales como la fecha de publicación de la vulnerabilidad, la plataforma afectada en el reporte. Al ser una base de datos interactiva que permite ser reanalizada, se colectó el informe de seguridad de la vulnerabilidad y se anexó al informe final como datos adjuntos ya que estos reportes pueden modificar las puntuaciones y ser reinterpretadas o reclasificadas y crearían un conflicto al no tener documentos de referencia. Los datos que no tienen un campo definido en el reporte fueron extraídos de la descripción de la vulnerabilidad en su idioma original.

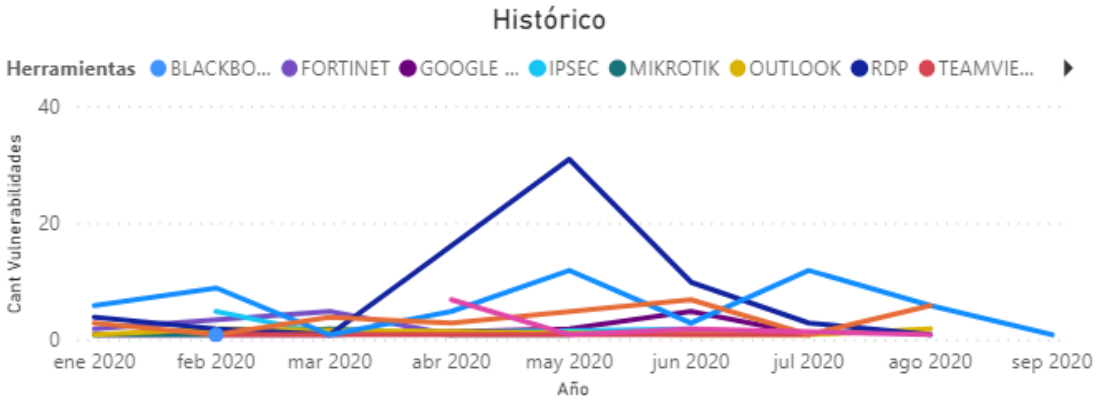

Figura 3. Histograma de vulnerabilidades en el año fuente: Anexo 3 Bi Vulnerabilidades.

Se puede observar un crecimiento de la cantidad de vulnerabilidades reportadas durante los tiempos de aislamiento mundial por la pandemia que aceleró los

procesos de teletrabajo y comunicaciones no presenciales, mostrando un pico para las tecnologías de escritorio remoto; únicamente al visibilizar las vulnerabilidades en contexto con otras fue posible determinar la fragilidad de una tecnología en contexto con otras tecnologías.

Realizada la tabulación se procedió a realizar el informe de inteligencia de negocios a las vulnerabilidades tabuladas (Consultar anexo 3 BI Vulnerabilidades), este estudio permitió no solo determinar en qué campos se afectaban más las vulnerabilidades (integridad, disponibilidad, confiabilidad); se estudian las tendencias estableciendo los picos de vulnerabilidades por tecnología durante el periodo extraído, cuales plataformas son más afectadas por las vulnerabilidades lo que expone cuales requieren mayor atención en caso de una implementación y, dependiendo del enfoque de la empresa cual es el campo que más debe proteger.

Se pudo establecer en los parámetros de búsqueda en la base de datos NVD conceptos preconcebidos en temas de seguridad. El primero de ellos las tecnologías abiertas siguen teniendo más vulnerabilidades o las empresas no invierten tanto en seguridad para encontrar tantas vulnerabilidades. WEBEX es una plataforma con 25 vulnerabilidades de seguridad activas; las mayores vulnerabilidades están para el sistema operativo Mac OS, la mayoría de sus vulnerabilidades afectan la disponibilidad del sistema y al ser un sistema hibrido entre nube y sistemas internos no es posible ser protegido por sistemas de seguridad perimetral (Consultar anexo 3 BI Vulnerabilidades); únicamente el establecimiento de políticas y procedimientos de seguridad pueden mitigar las amenazas producidas por las vulnerabilidades. Generado el informe se procedió a establecer los escenarios de riesgo, en los que se utilizaron las vulnerabilidades más relevantes de cada tecnología, aquellas que tuvieran mayor impacto y aquellas que tuvieran un mayor nivel de explotación; se decantaron 23 escenarios de riesgo; estos estudios llevaron a una descripción de seguridad por cada tecnología cómo se relaciona a continuación:

ZOOM por su parte, es una aplicación que presenta 5 vulnerabilidades activas en su mayoría para sistemas operativos Windows, sus vulnerabilidades son severas o catastróficas si no se realizan las correcciones necesarias. Dentro de las vulnerabilidades estudiadas se trabajó bajo la suposición de tener la vulnerabilidad Zoombombing que afectó cientos de reuniones bajo esta plataforma, los datos y estadísticas aún son confusos dado que las empresas afectadas no reportaron en la mayoría de sus casos dichos ataques, la vulnerabilidad que permitió estos ataques fue la vulnerabilidad CVE-2019-13567 reportada el 7 de diciembre del año 2019 y que fue explotada en marzo del presente año; esta vulnerabilidad fue expresada en función de la versión de Zoom 4.4 para Mac OS, lo que deja una ventana de 4 meses entre la vulnerabilidad, la supuesta reparación mediante versiones más modernas, y el uso comercial del ataque que desencadenó en Zoombombing. Esto nos plantea un escenario preocupante a todas luces por los siguientes motivos:

- No se están haciendo las pruebas necesarias para verificar una vulnerabilidad, más allá de las explicaciones oficiales.

- No se toman medidas de seguridad cuando se expone una vulnerabilidad.
- No es suficiente con la exposición de la vulnerabilidad, la corrección y el respectivo parche, se debe analizar a nivel de seguridad de las posibilidades de estas vulnerabilidades.

Se obviaron todos los aspectos relevantes, todos los protocolos que debieron ser establecidos una vez identificada la vulnerabilidad. Zoom evitó durante 40 días que estuvo en auge la vulnerabilidad, en establecer la encriptación de la comunicación, aspecto que afectaba la velocidad de las reuniones, pero debía incrementar la seguridad. Este escenario conduce a la siguiente pregunta; ¿se están tratando correctamente las vulnerabilidades? No sólo por los fabricantes responsables de las fallas de seguridad, sino también por los usuarios quienes apropian la tecnología sin unos protocolos definidos, unas reglas de seguridad establecidas que mitigaran la vulnerabilidad.

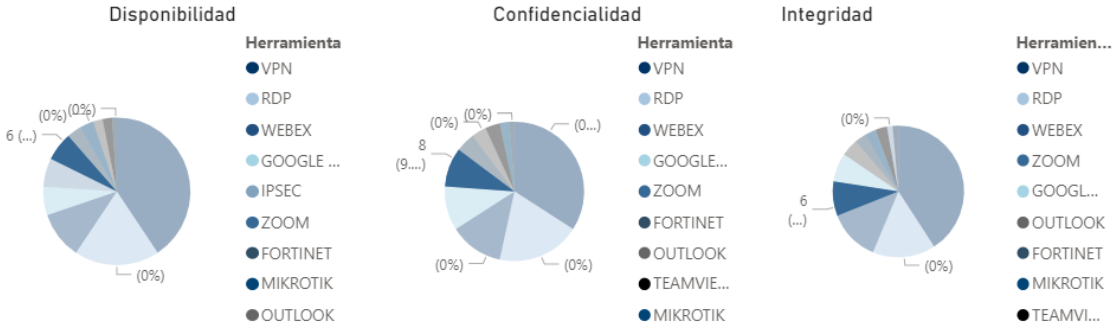

Figura 4. Afectación de las vulnerabilidades de Zoom en los tres pilares de seguridad fuente: Anexo 3 Bi Vulnerabilidades

En la imagen podemos observar cuantas vulnerabilidades de la plataforma Zoom afectan en alta medida a los pilares de seguridad de la información; 6 de estas afectaban la disponibilidad que se traduce en interrupción del servicio de reuniones, 8 vulnerabilidades afectaban la confidencialidad en alta medida que se interpreta como fuga de información durante una reunión, y por último 6 afectaciones a la integridad que se interpreta como intervenciones no autorizadas a una reunión.

El 25% de las vulnerabilidades encontradas fueron en las tecnologías de conexión a escritorio remoto (RDP) de las cuales la mayoría afectan la plataforma abierta Linux en sus distintas versiones y, en una porción compartida importante Windows y Linux, estas vulnerabilidades compartidas afectan a Windows como cliente y Linux como cliente y servidor; RDP es una tecnología vital para el teletrabajo en PYMES puesto que establece un nivel de seguridad en la información superior al uso compartido en nubes gratuitas, permite la elaboración de labores financieras y

contables que no pueden ser ejecutadas de otra manera; si bien no hay reportes tan extensos como los de ZOOM, RDP representa un gran riesgo para las comunicaciones de una PYME ya que estas no poseen múltiples servidores para diferenciar servicios y, al acumular todos los servicios en un solo sistema una vulnerabilidad puede conllevar a fallas catastróficas en la información.

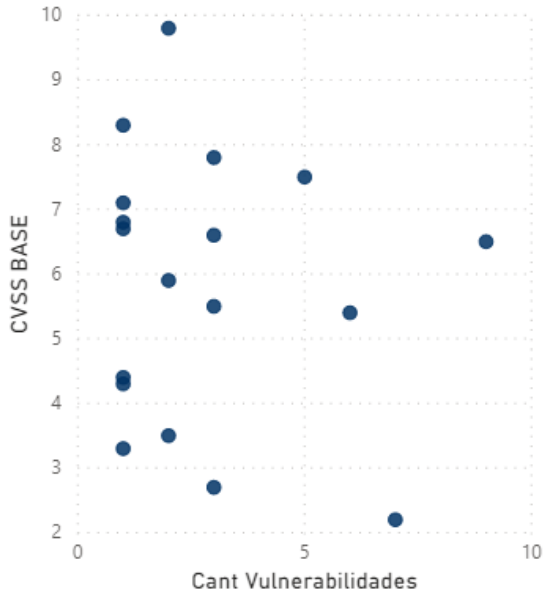

Figura 5. Dispersión de las vulnerabilidades RDP fuente: Anexo 3 Bi Vulnerabilidades.

Aquí se puede observar cuantas vulnerabilidades están por encima del rango de siete puntos, claramente se percibe un mayor volumen en las vulnerabilidades de menor peligrosidad y poder prestar atención a aquellas que afectarían en mayor nivel a las PYMES

El segundo pilar de vulnerabilidades por cantidad reside en la tecnología VPN encargada de establecer comunicaciones privadas para las empresas donde mayoritariamente afecta la disponibilidad más que la integridad y la confiabilidad, las comunicaciones en VPN se establecen con servidores, routers y firewalls que hacen parte de los sistemas de seguridad perimetral de cualquier empresa, en el caso de las PYMES estos sistemas pueden ser integrados por software libre que les otorgue los accesos a la red con unos niveles superiores de seguridad, de estas vulnerabilidades una proporción pertenecen a tecnologías libres como open VPN instalables en servidores Linux, ideal para entornos con bajos costos en licenciamiento e inversamente proporcionales costos de soporte, sumado a las puntuaciones de vulnerabilidad y explotación, se hace necesario mantener un constante seguimiento a las correcciones y las recomendaciones de seguridad por parte del fabricante. Se puede notar a la mayoría de los casos relacionados con este pilar tienen fallas en sus sistemas operativos internos en base Linux o base Unix.

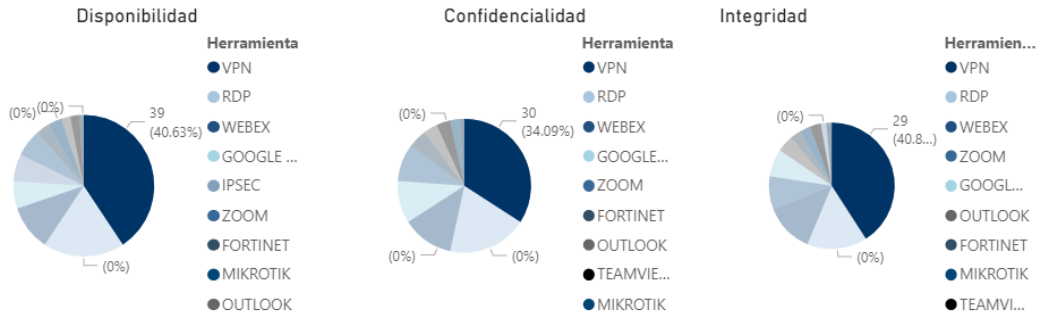

Figura 6. Afectación de las vulnerabilidades de VPN en los tres pilares de seguridad fuente: Anexo 3 Bi Vulnerabilidades

Entre las tecnologías relacionadas con las comunicaciones (RDP y VPN) se contempla el protocolo IPSEC, aunque no existen muchos casos (9) hay que tener seguimiento ya que sus marcas son considerables (4.0). En la figura 6 se puede observar una gran proporción de las afectaciones a los 3 pilares de seguridad donde se contemplan únicamente aquellas que son de nivel mayor y las tecnologías de escritorio remoto son 40.6%, 34% y 40.8% respectivamente.

Para establecer un mercado de soluciones de teleconferencias se estudiaron las otras opciones del mercado según el cuadrante mágico de Garner, entre las cuales se evaluaron Google meet, Microsoft teams, y Cisco Webex; si bien las dos primeras tecnologías no ofrecen un número significativo de vulnerabilidades Webex tiene 25 vulnerabilidades en lo corrido del año 2020, con un pico de notificación de siete vulnerabilidades en el mes de junio, su impacto está en el orden de los seis puntos y el nivel de explotación de las mismas en cuatro puntos; cabe resaltar que las vulnerabilidades de la tecnología afectan tanto a clientes como servidores y toda la infraestructura comprometida en el proceso; al igual que ZOOM, sus vulnerabilidades pueden comprometer los tres campos de seguridad.

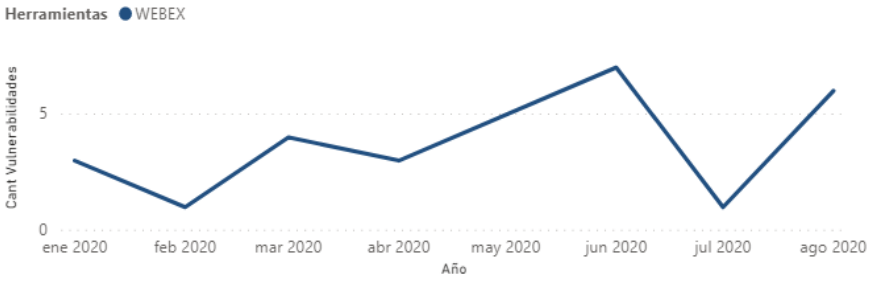

Figura 7. Histograma de vulnerabilidades del programa WEBEX durante el año 2020 fuente: Anexo 3 Bi Vulnerabilidades

ESTABLECIMIENTO DE ESCENARIOS DE RIESGO

Realizado los estudios de inteligencia de negocios para las vulnerabilidades se utilizaron los casos más significativos a nivel de impacto para establecer los escenarios de riesgo, esto permitirá acercar a una PYME en la adquisición de herramientas para el teletrabajo. Se establecieron 23 escenarios de riesgos individuales describiendo bajo cuales condiciones se puede materializar una vulnerabilidad, dependiendo de la cantidad de vulnerabilidades que cumplieran con los niveles establecidos (7.5 o superior), se edificaron entre tres y cinco escenarios de riesgo por cada herramienta del teletrabajo; determinando si puede ser de origen accidental o intencional, si puede ser ejecutado por un usuario sin permisos o con credenciales superiores, todos los escenarios de riesgo son multiplataforma, lo cual es un requisito para una vulnerabilidad grave o catastrófica. Los escenarios de riesgo son la herramienta principal para las PYMES, al comparar estos con las situaciones actuales de la empresa, si una de sus herramientas para teletrabajo junto con sus demás sistemas pueden cumplir los requisitos para ser víctimas de la vulnerabilidad descrita en el escenario descrito; es necesario tener en cuenta que en este punto se verificaron las vulnerabilidades de manera individual, y las variables medioambientales, de infraestructura y humanas no son tomadas en cuenta.

Los tres primeros escenarios corresponden a vulnerabilidades relacionadas con ZOOM, en las cuales no sólo se pueden interrumpir las reuniones debido a una debilidad en el cifrado de las videollamadas, sino también mediante el uso de mensajes arbitrarios enviar malware que puede tomar control de los equipos en la reunión; el último escenario describe un escalamiento de privilegios para clientes con sistema IOS que permitiría el uso privilegiado para la instalación de malware y, tomando en cuenta el estatus de estos equipos puede acceder a esferas directivas o gerenciales de las PYMES. Los siguientes cuatro escenarios corresponden a CISCO Webex en los cuales se puede acceder a la plataforma sino se tiene correctamente configurado el sistema de tokens; así mismo, una empresa que utilice la plataforma unificada de comunicaciones Zimbra puede afectarse mediante un ataque de puertos cruzados valiéndose de la vulnerabilidad zimlet. También puede darse el evento que una persona recibe una grabación de una reunión modificada con malware insertado a una persona de la organización, si bien la infraestructura de cisco es costosa para los valores que pudiera manejar una PYME, tan solo necesita adquirir una licencia cliente como parte de un negocio con un cliente más estructurado. Los siguientes tres escenarios correspondieron a fallas de plataforma Fortinet por uso no controlado de recursos, llevado por una configuración por defecto (un caso que se extiende a muchas tecnologías usadas por PYMES). Un escenario especialmente particular es la vulnerabilidad IPSEC presentada en un router NIP6800 que puede ser de uso por una PYME a través de su proveedor de servicios de internet, este escenario afecta las comunicaciones por tiempo indeterminado de materializarse esta vulnerabilidad. Los últimos 9 escenarios de

riesgo corresponden a las vulnerabilidades de las distintas herramientas utilizadas para conexión a escritorio remoto (RDP) que pueden funcionar desde servidores Microsoft, Linux, routers y demás. Si bien los escenarios de RDP son serios debido al acceso a la información de las PYMES, también se debe considerar el uso multitarea que se establecen para los sistemas de datos, por ende, cualquier vulnerabilidad que permita tomar control o interrumpir un sistema de escritorio remoto se debe tomar en cuenta que va a acceder a toda la información que pueda contener el servidor. (Consultar Anexo 3 Tecnologías del teletrabajo – Escenarios de Riesgo).

ESTABLECIMIENTO DE ESCENARIOS DE RIESGO COMPUESTOS

Si bien una vulnerabilidad tiene unas implicaciones en la seguridad que deben ser consideradas en singularidad, es necesario correlacionar las vulnerabilidades como un conjunto, estableciendo las afectaciones que tiene por ejemplo el sistema de seguridad perimetral sobre las demás tecnologías dentro de una Pyme, cuanto afectan las vulnerabilidades de RDP a un sistema sin seguridad perimetral; estas circunstancias determinaron el nivel de importancia de las tecnologías en un promedio acumulado de la siguiente manera:

	HERRAMIENTA	INFLUENCIA
SEGURIDAD PERIMETRAL	MIKROTIK	35%
	FORTINET	35%
TRABAJO REMOTO	VPN	25%
	RDP	22%
REUNIONES NO	ZOOM	5%
	WEBEX	5%

Figura 8. Influencia de las tecnologías de teletrabajo en la seguridad de una PYME fuente: Anexo 1 Tabla de vulnerabilidades.

Las tecnologías de comunicación tienen poca influencia en los escenarios compuestos ya que son sistemas mixtos o completamente abocados a la nube y no pueden ser protegidos por la seguridad perimetral, o las comunicaciones mediante canal VPN, y ya que son temas multimedia, las tecnologías de escritorio remoto no pueden ser aplicados. Se realizaron agrupaciones de vulnerabilidades según su descubrimiento, así dos informes no pueden ser acumulados ya que pertenecen al mismo evento y, cuando son continuas es porque se desenvuelven más vulnerabilidades de uno solo. Para estos escenarios compuestos se utilizaron las vulnerabilidades de mayor número, las que pueden afectar más a una PYME; se pudo determinar bajo los porcentajes que la suma de las combinaciones, 2 reportes en el grupo de tecnologías de seguridad perimetral, 26 reportes para las tecnologías

de escritorio remoto, y por último cinco vulnerabilidades de comunicaciones VPN, que permitió realizar 312 combinaciones que determinaron una vulnerabilidad acumulada en promedio de 7.4 con un mínimo de 7.1 y un tope de 8.0, esta información nos permite inferir que la combinación de herramientas en función de la seguridad hace menos vulnerable una PYME.

Dentro de los escenarios compuestos se contemplaron los sistemas operativos que le permiten a una PYME contemplar su plataforma base de operación, si bien debe elegir por temas de presupuesto y mantenimiento, es un componente importante estudiar si la tecnología que adquiere para seguridad perimetral o VPN o escritorio remoto tiene una afectación particular a la plataforma que tienen sus equipos entre otros ejemplos.

8. NUEVAS ÁEAS DE ESTUDIO

Se ha estudiado todos los temas relacionados a la seguridad para las PYMES, y en caso de utilizar el teletrabajo no como herramienta en tiempos de aislamiento sino como fuente estable de labores, se somete a consideración evaluar todas las variables que puedan comprometerse en el desarrollo de esta misma, tales como: BYOD (trabaja con equipos propios), asignación de recursos a teletrabajo, establecimiento de canales seguros y, dependiendo del nivel dedicados para la comunicación y desarrollo de labores estratégicas o niveles más críticos.

El levantamiento de informes fue hecho enteramente a mano, mediante la extracción de palabras claves, análisis de reportes, parametrización de sistemas operativos, clasificación mediante información inferida en el reporte; es posible realizar esta extrapolación de los reportes de NIST de manera automática, utilizando machine learning, IA, o tecnologías que pudieran alimentar los reportes y tendencias de manera automática expandiendo este tipo de análisis en business intelligence a otras escenas de la seguridad de la información.

9. CONCLUSIONES

Después de realizar los análisis respectivos, el establecimiento de los escenarios, y conjugar las vulnerabilidades en conjunto sobresalta un tema por encima de los aspectos técnicos, la administración de vulnerabilidades cómo parte de las labores de un usuario o un área encargada; se está administrando de la manera incorrecta; típicamente un cliente de una tecnología las adquiere, la configura, la usa, y eventualmente la actualiza. Se ha dejado de lado todas las pruebas de seguridad más allá de las entregadas por búsqueda de vulnerabilidades de parte del fabricante, y es necesario llegar a un ambiente de pruebas controladas para establecer dentro del contexto corporativo que se encuentre la herramienta que pueda afectar a otros sistemas, otros usuarios y otros niveles.

Este tipo de pruebas se puede efectuar en todos los niveles corporativos: tanto como usuarios, redistribuidores, y proveedores; la responsabilidad no debe recaer únicamente en este último, la aplicación de recomendaciones de seguridad debe volverse mandataria, el seguimiento de las vulnerabilidades y la alerta de estas debe ser tomada en prioridad con su respectivo seguimiento que evite la materialización de un ataque que afecte la información que a la final es el esfuerzo de este campo la prevención de perdida de sistemas e información.

El reto para las empresas pequeñas y medianas PYME consiste en proyectar sus necesidades en un balance entre costo-beneficio y seguridad; cuanto puede invertir en el monitoreo y los ajustes a las herramientas que decida elegir, que tanto tiempo y recursos puede asignar para determinar que tanto pueden comprometer sus sistemas y su información para asimilar los nuevos escenarios laborales que se presentan en el momento, donde el teletrabajo, el trabajo colaborativo en línea y las reuniones no presenciales no son sólo una medida ante los eventos recientes, sino una nueva manera de ejercer las labores administrativas y operarias no productivas de las empresas, donde el 90% de las labores son a distancia; estos análisis son la respuesta a resolver las inquietudes de seguridad de una herramienta y realizar una elección ajustada a sus necesidades y presupuestos.

10. BIBLIOGRAFÍA

ANGARITA P., Cristian A. & GUZMÁN F., Camilo (2017). Protocolos para la mitigación de ciberataques en el hogar. Caso de estudio: estratos 3 y 4 de la ciudad de Bogotá. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información. Bogotá, Colombia Pág. 10.

ARÉVALO C., Ligia, FERNÁNDEZ M., Edwin N. & ZAMBRANO R., Ángela (2016). Diseño del plan de recuperación de desastres (D.R.P.) para la compañía Agencia de Aduanas Profesional nivel 1 SIAP sede Bogotá. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Especialización en Seguridad de la Información. Bogotá, Colombia Pag 14.

ARIAS Diana. 12.912 empresas han implementado el teletrabajo en Colombia Enter.co. Bogotá D.C.17 de mayo de 2019.

BARACALDO RINCÓN, Laura P. (2019). El outsourcing en las entidades públicas de Colombia. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Derecho. Bogotá, Colombia. Pág. 6

CARREÑO DUEÑAS, Dalia. (2016). Contexto general de la virtualidad. En D. Carreño Dueñas. Pensar el derecho como derecho virtual (pp. 12). Bogotá: Universidad Católica de Colombia

CASTELLANO. Jenifer. Solvetic.16 de octubre de 2017. Internet: https://www.solvetic.com/page/recopilaciones/s/seguridad/caracteristicas-protocolos-VPN-openVPN-sstp-l2tp-ikev2-pptp.

CCIT. Informe de las tendencias del cibercrimen en Colombia (2019-2020). Bogotá D.C., 2019.

CHAVERRA MOJICA. John J. El teletrabajo y la seguridad de la información empresarial. Medellín. 04 de junio de 2015. pág. 115.

CLARK MICHAEL. Antony. Teleworking in the Countryside. Routledge, 2000.

CRUNCHBASE crunchbase.com. 28 de abril de 2020. Internet: https://www.crunchbase.com/organization/Zoom-video-communications#section-investors.

CRUZ CASTILLO, Jhon F., GUZMÁN BAYONA, Jesly S., HURTADO CONTRERAS, Maite C. & MELO VARGAS, Yudy D. (2018). Análisis de la factibilidad del modelo del teletrabajo en la entidad financiera BA para el área de

servicio al cliente. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ciencias Económicas y Administrativas. Programa de Economía. Especialización en Formulación y Evaluación Social y Económica de Proyectos. Bogotá, Colombia. Pág. 16

DIAZGRANADOS, Carlos (2018). Precisiones conceptuales e implementación práctica del teletrabajo. En L. A. Diazgranados Quimbaya, L. F. Vallecilla Baena, C. M. Diazgranados Quimbaya, S. Gómez Escobar, J. D. Montenegro Timón & J. E. Almanza Junco. (pp. 71-93). Bogotá: Editorial Universidad Católica de Colombia

EXPRESS VPN. ExpressVPN.com. 01 de mayo de 2020. Internet: https://www.expressVPN.com/es/what-is-VPN/protocols/pptp.

FORERO O, Bryan, PAVA C, Jonier. & SARMIENTO, James. (2018). Diagnóstico de seguridad y privacidad de la información en la alcaldía municipal de Icononzo-Tolima. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información. Bogotá, Colombia

FORTINET. Threat Landscape Report Q4 2019. Sunnyvale, 2019.

GONZÁLEZ S, Rony M. & COLO M., José H. (2019). Diseñar un modelo para implementar un sistema de gestión de seguridad de la información para una PYME del sector privado. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información. Bogotá, Colombia. Pág. 9

GONZÁLEZ GARCÍA, Manuel F. (2018). Definición de estrategias de adopción de la cuarta revolución industrial por parte de las empresas en Bogotá, aplicables a PYMES en Colombia. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería Industrial. Bogotá, Colombia. Pág. 39.

INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). Internacionalización Ficha Colombia. - León, 2015.

KITAMURA. Ryuichi, NILLES. Jack M., CONROY Patrick, & FLEMING David M. Telecommuting as a Transportation Planning Measure: Initial Results of California Pilot Project. Transportation Research Record 1285. págs. 98 - 104. 1990

MELO CAMPOS, Angie R. (2019). Regulación de las nuevas formas de empleo que surgen por medio de las plataformas digitales. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Derecho. Bogotá, Colombia.

MINISTERIO DE TECNOLOGÍAS DE A INFORMACIÓN Y LAS

COMUNICACIONES. Pacto por el teletrabajo. 07 de mayo de 2020. Internet: https://www.teletrabajo.gov.co/622/w3-article-8423.html.

_____. Pacto por el Teletrabajo. 07 de mayo de 2020. Internet : https://www.teletrabajo.gov.co/622/w3-article-8098.html.

_____. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Bogotá, 2020.

_____. LIBRO BLANCO El ABC del teletrabajo en Colombia. Bogotá D.C., 2017.

MORGAN. Robert. Teleworking: An Assessment of the Benefits and Challenges, European Business Review. 2004. no 4, Vol. 16. págs. 344-357.

NOTICIAS CARACOL. Universidad de Antioquia denuncia que su cuenta de Zoom fue hackeada en plena videoconferencia. Noticias Caracol. 17 de mayo de 2020.

OFICINA INTERNACIONAL DE TRABAJO. Manual de buenas prácticas en teletrabajo. Buenos Aires, Unión Industrial Argentina, 2011.

OSORIO MORALES. Eduar. logopoliskpo. 21 de junio de 2018. Internet : http://logopoliskpo.com/2018/06/21/seguridad-de-la-informacion-en-PYMES/

PORRAS SOTO, Edgar F. (2019). Las plataformas móviles una mirada al contrato laboral en Colombia. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Derecho. Bogotá, Colombia. Pág. 14.

REVISTA LUCIERNAGA. Comunicación organizacional en torno al teletrabajo Revista Luciérnaga. 2017. 18. Vol. 9. - págs. 61-71.

RODRÍGUEZ ARÉVALO, Javier H. & TORRES CALDERÓN, Wilmer A. (2019). Análisis de riesgos de seguridad de la información del área IT de la empresa Royal Services S.A. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información. Bogotá, Colombia. Pág. 10.

SÁNCHEZ S., Andrés F. & RODRÍGUEZ R., Rafael E. (2018). Desarrollo de un modelo para calcular el nivel de seguridad en sitios Web, basado en el top 10 de vulnerabilidades más explotadas en 2017 según el marco de referencia OWASP. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información. Bogotá, Colombia Pág. 14

SYDOW. Lexi. App Annie. 30 de marzo de 2020. Internet : https://www.appannie.com/en/insights/market-data/video-conferencing-apps-surge-coronavirus

TAMAYO. Laura. Si usa Zoom, ¿debería preocuparse por su seguridad? El colombiano. 20 de abril de 2020.

YÁÑEZ. Jesús. Expansión.com. 12 de marzo de 2020. Internet : https://www.expansion.com/juridico/opinion/2020/03/12/5e6a108ce5fdea0b688b4601.html