ANÁLISIS DEL ESTADO DE EMERGENCIA SANITARIA- COVID 19 Y LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD INFORMÁTICA EN EL USO DE CANALES ELECTRÓNICOS Y LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS EN AMBIENTES DE TRABAJO EN CASA

CLARA INÉS MUÑOZ SÁNCHEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
POPAYÁN
2021

ANÁLISIS DEL ESTADO DE EMERGENCIA SANITARIA- COVID 19 Y LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD INFORMÁTICA EN EL USO DE CANALES ELECTRÓNICOS Y LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS EN AMBIENTES DE TRABAJO EN CASA

CLARA INÉS MUÑOZ SÁNCHEZ

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

Yenny Stella Núñez
Directora trabajo de grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
POPAYÁN
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Popayán, 11 de diciembre de 2021

DEDICATORIA

Este trabajo de grado lo dedico primero a Dios por darme la sabiduría, a mis papás aunque no están conmigo, continúan siendo mi inspiración, guía y deseo de superación, a los profesores, amigos y compañeros por haber sido un pilar fundamental para el logro de este trabajo.

AGRADECIMIENTOS

A Dios el único sabio, que con su infinita bondad nos dio vida, salud, sabiduría, paciencia y compromiso para lograr la meta propuesta.

A la Ingeniera Yenny Stella Núñez por sus conocimientos, enriquecedores aportes para que este trabajo tuviese éxito.

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar.

A mi sobrina Dirley Yuliana Muñoz Sánchez , quien compartió sus conocimientos, aportes y contribuyó con el desarrollo del proyecto.

CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

GLOSARIO

Ciberataque: “Es un intento organizado causado por una o varias personas para provocar daños a un sistema informático o red. Estos ataques informáticos se aprovechan de alguna debilidad o vulnerabilidad del software o hardware”[1].

Coronavirus: “El coronavirus es un grupo de virus que causan enfermedades que van desde el resfriado común hasta enfermedades más graves como neumonía, síndrome respiratorio de Oriente Medio (MERS) y síndrome respiratorio agudo grave (SARS). Cabe destacar que la cepa de coronavirus (2019-nCoV) que ha causado el brote en China es nueva y no se conocía previamente”[2].

Digitalización: “La digitalización es un proceso mediante el cual, algo real (físico, tangible) es pasado a datos digitales para que pueda ser manejado por una computadora (de naturaleza, a su vez, digital), modelándolo, modificándolo, y aprovechándolo para otros propósitos distintos de su cometido o función originales”[3].

Documento electrónico: “Es la información generada, enviada, recibida, almacenada y comunicada por medios electrónicos, ópticos o similares”[4].

---

[1] UREÑA, Francisco. Ciberataques, la mayor amenaza actual. Documento de Opinión 09. 2015

[2] PERALTA, Antonio .Infección por SARS-CoV2, epidemiología, manifestaciones clínicas, inmunología: tratando de entender la enfermedad. Revista de Investigación Universitaria en Salud, 2020, vol. 2, p. 15-23.

[3]SORO, José. La digitalización de documentos en la Administración de Justicia. Ibersid: revista de sistemas de información y documentación (ISSNe 2174-081X; ISSN 1888-0967), 2014, vol. 8, p. 49-53.

[4] LÓPEZ, Valentín. Valor probatorio del documento electrónico. Informática y Derecho: revista iberoamericana de Derecho informático.1995. (8), 133-174.

Pandemia: Se llama pandemia a la propagación mundial de una nueva enfermedad. Se produce una pandemia de gripe cuando surge un nuevo virus gripal que se propaga por el mundo y la mayoría de las personas no tienen inmunidad contra él. Por lo común, los virus que han causado pandemias con anterioridad han provenido de virus gripales que infectan a los animales[5].

[5] RAMONET, Ignacio. La pandemia y el sistema-mundo. Le Monde Diplomatique, 2020, vol. 25, no 04.

RESUMEN

En el marco de la emergencia sanitaria, por la llegada al país del coronavirus Covid 19, el presidente de la república mediante la expedición de diversas normas y medidas ha decretado el aislamiento preventivo en todo el territorio colombiano, lo anterior, con el propósito de prevenir la expansión de la enfermedad, garantizar el distanciamiento social y tomar acciones respecto a la atención de usuarios, gestión y trámite de documentos y otros servicios que prestan las entidades de la administración pública en sus diferentes niveles, entidades privadas que cumplen funciones públicas, archivos privados de interés público y los demás organismos regulados por la ley 594 de 2000.

En virtud de lo anterior, se implementó el trabajo en casa mediante dispositivos digitales y las tecnologías de la información y las comunicaciones, con el fin de evitar la interrupción y garantizar la continuidad y confianza en los servicios.

Palabras clave: Ciberataque, coronavirus, digitalización, documento electrónico, pandemia

ABSTRACT

In the framework of the health emergency, due to the arrival in the country of the Covid 19 coronavirus, the president of the republic through the issuance of various norms and measures has decreed preventive isolation throughout the Colombian territory, the foregoing, with the purpose of preventing the spread of the disease, guarantee social distancing and take actions regarding the attention of users, management and processing of documents and other services provided by public administration entities at different levels, private entities that perform public functions, private archives of public interest and the other organisms regulated by law 594 of 2000.

By virtue of the foregoing, work at home was implemented using digital devices and information and communication technologies, in order to avoid interruption and guarantee continuity and trust in services.

Keywords: Cyber attack, coronavirus, digitization, electronic document, pandemic

INTRODUCCIÓN

Desde el inicio de la cuarentena en el país en marzo de 2021, las empresas debieron implementar protocolos, directrices de trabajo en casa, de acuerdo con las medidas preventivas o directivas estatales las cuales restringieron el contacto personal.

Algunas organizaciones ya estaban familiarizadas con el teletrabajo, así que el impactó fue leve, para las que obligatoriamente les tocó enviar a sus empleados a casa, es cuando se aprecia el teletrabajo más grande y masivo en el país.

El teletrabajo ha demostrado ser una herramienta importante para garantizar la continuidad operativa, pero la mayoría de compañías carecen de una estrategia consecuente para el trabajo digital, como organizar a los equipos y puntualizar los cuidados que se deben tener a nivel de ciberseguridad, en virtud de lo anterior, los ataques cibernéticos se incrementaron, existen estudios en que los correos electrónicos y sitios web son los medios de comunicación más relevantes a la hora de generar un ataque, debido a que el 96% de los ciberataques inician con un sencillo e-mail.

Se plantea analizar las medidas de seguridad informática asociadas al uso de canales electrónicos y gestión de documentos electrónicos en ambientes de trabajo en casa o teletrabajo.

Identificar un peligro cibernético es tan sólo el primer paso. Tomar medidas contra las amenazas y crímenes del ciberespacio es un reto aún mayor para las organizaciones

En virtud de lo anterior, esta investigación se basa en evaluar los riesgos, amenazas, normativa expedida y las medidas que han asumido las entidades frente al trabajo en casa, referente a la ciberseguridad en el uso de los recursos digitales en la red y uso de canales electrónicos

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Una vez el gobierno declara el estado de emergencia económica, social y ecológica en todo el territorio nacional debido a la llegada del nuevo Coronavirus y se ordena aislamiento preventivo obligatorio, teniendo en cuenta que uno de los activos más importante de las entidades es la información, la cual deben custodiarla y gestionarla, estas inician a prestar sus servicios mediante el trabajo en casa, debido a que las relaciones con las personas naturales y jurídicas debe continuar, produciendo múltiples documentos internos y externos con firmas digitalizadas o escaneadas y utilizando como medio de transmisión el correo electrónico, en virtud de lo anterior se deduce que estos documentos electrónicos generados no cumplen con los principios de seguridad informática, como integridad, disponibilidad y confiabilidad, aunado a este tema los funcionarios no están formados para coadyuvar con la seguridad de la información, incluso algunas compañías no le prestan atención al tema tal vez por desconocimiento o carencia de recursos económicos.

La realidad actual demanda nuevos recursos para salvaguardar la información, por lo tanto es imprescindible que las organizaciones actúen y busquen estrategias para evitar la alteración y la vulnerabilidad de uno de sus activos más importantes, pues existe una gran brecha entre la protección del documento electrónico y el soporte papel.

Para atender esta situación atípica, la alcaldía de Bogotá, expide un guía denominada “Lineamientos para el uso de documentos electrónicos en la contingencia generada por la emergencia sanitaria COVID-19, en la cual orienta

directrices y establece lineamientos para mitigar riesgos asociados al uso de documentos electrónicos en los ambientes de trabajo en casa" [6] hace énfasis en la implementación de herramientas para seguridad informática, uso adecuado de canales electrónicos, producción de documentos electrónicos de archivo, uso de firmas electrónicas y firmas digitales.

Según el centro de ciberseguridad Gamma Ingenieros[7], para la implementación de trabajo en casa se debe contar con una política corporativa donde se tenga en cuenta la forma de acceder a la información de la empresa, los medios de almacenamiento para la información producida, el soporte técnico en caso de que se presente alguna novedad, entrenar a los funcionarios sobre riesgos a que se expone la información de la empresa , pues puede ser víctima con más facilidad de muchas amenazas existentes.

En un webinar realizado por Certicámara S.A, el líder Valimail y Grupo de Emergencias Cibernéticas de Colombia (COLCERT), denominado "robo de identidades que no te engañen", se evidenciaron que los correos electrónicos y sitios web son los medios de comunicación más relevantes a la hora de generar un ataque, debido a que el 96% de los ciberataques inician con un sencillo e-mail, asimismo resaltaron que el 11,7 corresponde a phishing, este ataque oscila entre 10 y 12 minutos.

[6] ARIAS, Álvaro. Lineamientos para el uso de documentos electrónicos en la contingencia generada por la emergencia sanitaria Covid-19. Bogotá, 2020.

[7] CENTRO DE CIBERSEGURIDAD GAMMA INGENIEROS ¿Qué debe tener en cuenta para teletrabajar sin poner en riesgo sus datos y dinero? Citado por RCN.Radio.Bogotá, 2020

El problema radica en que las personas están forzadas a laborar desde casa, con el propósito de cortar el contagio del Covid – 19, por lo que el sector empresarial modificó obligatoriamente su modelo de trabajo, así pues los funcionarios se ven obligados a usar sus propios recursos tecnológicos, dispositivos y equipos personales, utilizando sistemas operativos y antivirus desactualizados, los cuales son más asequibles a un ciberataque, debido a que los controles de seguridad desde casa son mucho más frágiles que en los escenarios corporativos.

De acuerdo con el estudio "Digital Workplace Report, realizado por NTT Ltd, el 60% de las compañías en el mundo carecen de una estrategia consecuente para el trabajo digital, como organizar a los equipos y puntualizar los cuidados que se deben tener a nivel de ciberseguridad"[8].

En virtud de lo anterior, se plantea analizar las medidas de seguridad informática asociadas al uso de canales electrónicos y gestión de documentos electrónicos en ambientes de trabajo en casa o teletrabajo.

1.2 FORMULACIÓN DEL PROBLEMA

Qué medidas respecto a la seguridad de la información ha implementado el sector empresarial con el fin de proteger los activos?

[8] NIPPON TELEGRAPH AND TELEPHONE CORPORATION. Digital Workplace Report, citado por revista gerencia. Pwc. Las nuevas amenazas al teletrabajo. Chile: 2020.

2 JUSTIFICACIÓN

El autor Álvaro Gómez[9], en su obra Enciclopedia de la Seguridad Informática, define el concepto de seguridad informática como: “cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema, de acuerdo con lo anterior, hoy por hoy se hace imprescindible incluir y capacitar en competencias y debilidades en ciberseguridad a los ciudadanos y funcionarios del sector público como privado.

La Organización Mundial de la Salud el 11 de marzo de 2020 declaró el nuevo coronavirus como pandemia, la cual ha desatado una crisis de gran relevancia a nivel mundial, con ello el crecimiento y uso de tecnologías y su transversalidad en cada uno de los sectores, asimismo el aumento de ciberataques, debido a que las amenazas de seguridad informática en estos tiempos son más ininteligibles.

Teniendo en cuenta que el tema de la ciberseguridad avanza a pasos gigantes, en Colombia en el año 2011 se expidió el CONPES 3701 Lineamientos de Política para ciberseguridad y ciberdefensa para contrarrestar las amenazas cibernéticas del entorno digital, después, en el año 2016 el CONPES 3854, Política Nacional de Seguridad Digital, se enfatizaron en la gestión de riesgos, con el propósito de ofrecer seguridad en el ciberespacio no sólo a los habitantes sino a las organizaciones. Posteriormente, en el año 2020 se formula el documento CONPES 3995, Política Nacional de Confianza y Seguridad Digital, este analiza el escenario de usuarios

[9] GÓMEZ, Álvaro. Enciclopedia de la seguridad informática. 2007, vol 1266 de Alfaomega Grupo Editor, pp 664.ISBN 9701512669, 9789701512661

en el país respecto al uso de internet en diferentes factores: acceso a internet, capacidad de prevención y defensa frente a posibles ciberataques.

"Un estudio en el CSOC -Centro de Operaciones de Ciberseguridad de Claro, presentó cifras por ciberataques durante la pandemia, (marzo - noviembre) se registró un incremento superior al 98%. El delito con mayor número de denuncias es la suplantación de sitios web, con un crecimiento del 372%, seguido se encuentra violación de datos personales, con más de 6.159 casos registrados, posteriormente, se resalta el hurto por medios informáticos con un 39% de crecimiento,"[10].

De acuerdo con el entorno actual, el propósito de la investigación es orientar a las organizaciones sobre las diversas herramientas o técnicas para la seguridad de la información en ambientes de trabajo en casa, asimismo mejorar las prácticas de seguridad informática en los empleados.

[10] RODRÍGUEZ, Flavio. Centro de Operaciones de Ciberseguridad de Claro, Citado por Portafolio, Cifras de ciberseguridad en Colombia prenden alarmas al cierre de 2020.Bogotá : 2020

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar del estado de emergencia sanitaria- Covid 19 y la implementación de medidas de seguridad informática en el uso de canales electrónicos y la gestión de documentos electrónicos en ambientes de trabajo en casa o teletrabajo en las organizaciones estatales

3.2 OBJETIVOS ESPECÍFICOS

- Evaluar los diferentes riesgos y amenazas frente al teletrabajo y al uso de recursos digitales en la red.

- Examinar la normativa expedida por el país frente a la emergencia sanitaria causada por el Covid 19 junto con los lineamientos de seguridad digital vigentes en Colombia, respecto a la utilización de canales y recursos electrónicos por parte de las organizaciones.

- Establecer las medidas de seguridad informática que han asumido las diferentes entidades frente al trabajo en casa teniendo en cuenta el uso de canales electrónicos y la gestión de documentos digitales.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Según Aguilera[11], se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad.

La acción primordial de la seguridad informática es disminuir riesgos, estos se generan a partir de dispositivos extraíbles, canales electrónicos, virus, no hacer copias de seguridad y usuarios, entre otros. En virtud de lo anterior la seguridad se divide en tres grupos: infraestructura, información y usuarios.

La infraestructura, suele suceder que es el medio más inspeccionado, sin embargo, no significa que sea el que corre menos riesgos, depende de las actividades que se ejecutan. Se deben involucrar eventos reales, como los de un acceso no permitido, robo de identidad, robo del equipo, factores antropogénicos, desastres naturales.

[11] AGUILERA, seguridad informática, Citado por ROMERO CASTRO Martha Irene, FIGUEROA MORÁN Grace Liliana Y VERA NAVARRETE Denisse Soraya. Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. Editorial Área de Innovación y Desarrollo,S.L. Alcoy: 2018.p. 14-15.

La información es considerada como uno de los principales activos, la cual es imprescindible salvaguardarla, incluso algunos autores mencionan que es el oro de la seguridad informática.

Los usuarios son calificados como el eslabón más débil de la cadena, porque a ellos es muy difícil controlarlos, un usuario puede cometer ciertos errores con o sin intención, quienes pueden ocasionar grandes pérdidas respecto a la información, por tal razón, en la mayoría de los casos el sistema y la información deben de protegerse del mismo usuario.

En relación con lo anterior, se evidencia que en la seguridad informática no sólo se debe tener en cuenta la infraestructura y la información, también es importante darle relevancia al usuario, de nada sirve contar con sistemas robustos de seguridad si el usuario es totalmente indiferente y no se lo tiene en cuenta en las organizaciones frente a estos aspectos.

Colombia ha sido hasta ahora uno de los pocos países que a nivel mundial ha reglamentado el teletrabajo mediante la ley 1221 DE 2008, en el fomento del teletrabajo se deben tener en cuenta los siguientes componentes: Infraestructura de telecomunicaciones. (Mejores Prácticas de seguridad informática), acceso a equipos de computación, aplicaciones y contenidos, divulgación y mercadeo, capacitación, incentivos, evaluación permanente y formulación de correctivos cuando su desarrollo lo requiera.

Existen normas internacionales cuyo objetivo es brindar metodologías y guías de buenas prácticas a las empresas de cómo gestionar la seguridad de la

información. Estas normas son la ISO 27001 e ISO 27002. La norma ISO 27002 en su versión 2013. 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.

Estas normas incluyen políticas de dispositivos que debería considerar una organización, tales como: el registro de los dispositivos móviles, los requisitos de protección física, la restricción de instalación de software, los requisitos de las versiones de software de los dispositivos móviles y para la aplicación de parches, la restricción de la conexión a los servicios de información, los controles de acceso, técnicas criptográficas, protección contra software malicioso, desactivación, eliminación y bloqueo a distancia, copias de seguridad, uso de servicios web y aplicaciones web, acuerdos de licencia de software, la protección contra software malicioso y los requisitos de firewall.[12].

Por otro lado, la norma contiene acciones de control para escenarios como los actuales el teletrabajo, también incluye la utilización de dispositivos electrónicos y comunicaciones. Enfatizando en los riesgos que conlleva realizar acciones administrativas fuera de la organización, incluso tiene en cuenta la seguridad física del medio, aísla los entornos laboral, profesional del privado.

Con base en la exposición anterior sobre las técnicas o herramientas existentes para la seguridad de la información que actualmente se gestiona en ambientes de teletrabajo o trabajo en casa y por algunos canales electrónicos, se requiere

[12] AENOR INTERNACIONAL S.A.U. Tecnología de la Información Técnicas de seguridad Código de prácticas para los controles de seguridad de la información. 2017

urgentemente retomar e implementar planes, estrategias en las organizaciones y cultura digital con el propósito de involucrar la alta gerencia de cómo gestionar la seguridad de sus activos, también la preparación de sus colaboradores en la adquisición de buenas prácticas informáticas, debido a que la mayoría de organizaciones no se encontraban preparadas para abordar con responsabilidad el teletrabajo.

4.2 MARCO CONCEPTUAL

"El 'Libro Blanco: el ABC del Teletrabajo en Colombia' busca facilitar el desarrollo de proyectos de adopción de esta forma de organización laboral en las organizaciones públicas y privadas del país, incluyendo completas guías en materia organizacional, tecnológica y jurídica, basadas en la legislación vigente, el análisis de prácticas internacionales y los resultados de iniciativas desarrolladas en Colombia"[13].

El Ministerio de las TIC como autoridad en el tema de teletrabajo, en su página web explica punto por punto en qué consiste y cómo se debe implementar.

El objetivo de la iniciativa Teletrabajo del Ministerio TIC es la de masificar esta modalidad laboral en el país, como un instrumento para incrementar los niveles de productividad de entidades públicas y organizaciones privadas, generar una movilidad más sostenible, mejorar la calidad de vida de los trabajadores y promover el uso efectivo de las TIC.

[13] MINISTERIO DE LAS TIC. Libro blanco, el ABC del Teletrabajo en Colombia. Bogotá. 2017

La metodología de implementación establece cinco elementos principales: Compromiso institucional (querer hacerlo) Planeación (organizar el proceso - cronograma), autoevaluación (revisión interna frente a los recursos humanos, técnicos, jurídicos y tecnológicos con los que cuenta la organización), adopción e implementación[14]

El grupo Bancolombia es un claro ejemplo del teletrabajo, hoy la mayoría de los empleados de las sedes administrativas está trabajando desde la casa. Desde hace ocho años Bancolombia viene trabajando de manera remota y su proceso ha evolucionado día a día.

Asimismo están en continua capacitación, en uno de sus webinar, se enfocaron en temas relacionados con la ciberseguridad empresarial efectiva, presentando las siguientes técnicas:

1. Definir el apetito de riesgo de la empresa y con base en ello crear la estrategia de ciberseguridad y retroalimentarla.
2. Precisar los focos de trabajo de esa estrategia, la aspiración que se tiene y los temas transversales.
3. Elegir el modelo de seguridad o frameworks de ciberseguridad que sirva como referencia para ser utilizado según la estrategia definida.
4. Poner a las personas en el centro de la estrategia. Hay que cuidar su información (la de los clientes, proveedores, empleado) y, además, son quienes materializan la

[14] MINISTERIO DE LAS TIC. Todo lo que se debe saber sobre el teletrabajo. Bogotá. 2020

estrategia. Las personas son finalmente quienes dan el clic al correo sospechoso o lo eliminan.

5. Garantizar una visibilidad transversal todo el tiempo. La inteligencia y el monitoreo continuo se vuelven factores fundamentales en todo este proceso de protección.

6. Saber priorizar las inversiones en ciberseguridad de acuerdo con el diagnóstico actual de la empresa.[15]

Para finalizar, se mencionó que para conocer si el grado de efectividad de ciberseguridad es positivo en una organización, es imprescindible realizar escaneos de vulnerabilidades y realizar hackeos. Cuando se han detectado las posibles vulnerabilidades se debe priorizarlas y tener en cuenta los riesgos y el factor económico, para su inversión.

De lo anterior se puede deducir, que Colombia es uno de los pocos países en América Latina que tiene normativa respecto al teletrabajo, el Estado ha promulgado a través del Ministerio de las TIC, del Ministerio del trabajo cómo implementar el teletrabajo en las organizaciones, sin embargo la mayoría de las entidades ha hecho caso omiso a estas estrategias y continúa ejerciendo sin recomendaciones pertinentes y sin la seguridad de sus activos.

4.3 MARCO HISTÓRICO

[15] GRUPOBANCOLOMBIA. Medidas de ciberseguridad empresarial por contingencia. Bogotá, 2020

Hoy en día, es inevitable reconocer que los sistemas informáticos son los activos más importantes, debido a nuestro mundo cambiante, la transformación digital y el uso masivo de la tecnología, cada vez los sistemas informáticos adquieren nuevas amenazas.

El trabajo en casa, la utilización intensa de los canales electrónicos y el intercambio de información traen riesgos inminentes a la seguridad de la información, por tal razón es imprescindible proteger, preservar la seguridad, así pues, Yran Marriero Travieso, en su investigación "la Criptografía como elemento de la seguridad informática presenta diferentes mecanismos, dirigidos a garantizar la confidencialidad y autenticidad de los documentos electrónicos, todo ello es parte de la tecnología denominada Criptografía"[16].

En el artículo denominado El teletrabajo y la seguridad de la información empresarial, mencionan que Colombia ha sido hasta ahora uno de los pocos países que a nivel mundial ha reglamentado el teletrabajo con la ley 1221 de 2008, este aspecto se deben tener en cuenta: Infraestructura de telecomunicaciones. (Mejores Prácticas de seguridad informática), acceso a equipos de computación, aplicaciones y contenidos, divulgación y mercadeo, capacitación, incentivos, evaluación permanente y formulación de correctivos cuando su desarrollo lo requiera.

Por otro lado, en Colombia en el año 1999 mediante la "Ley 527 se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de

[16] MARRIERO, Yran. La Criptografía como elemento de la seguridad informática. ACIMED . La Habana.2003. v.11 n.6

las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones"[17].

Esta Ley, establece un marco jurídico integral, pues permite el uso de mensajes de datos en los diferentes escenarios tanto privado como público, el uso de la firma digital, características y requerimientos de las entidades de certificación, certificados digitales, entre otros.

4.4 ANTECEDENTES O ESTADO ACTUAL

Zapata[18], en su trabajo titulado COVID- 19: Estado de emergencia sanitaria, normas gubernamentales y los efectos laborales en Colombia, en donde presenta su investigación sobre los efectos en materia laboral se han derivado de la declaración del Estado de Emergencia Económica, Social y Ecológica en todo el territorio Nacional y de las normas de estado de emergencia que en el marco de este se han elaborado, en razón de la situación de salud pública que tanto a nivel nacional como internacional se ha generado a partir del nuevo coronavirus – COVID-19.

González[19], en su proyecto de grado estudio del estado actual de la seguridad informática en las organizaciones de Colombia en el sector empresarial, desarrolla

[17] CONGRESO DE COLOMBIA. 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. Bogotá, 1999. Diario Oficial No. 43.673 21

[18] ZAPATA, Nataly. COVID- 19: Estado de emergencia sanitaria, normas gubernamentales y los efectos laborales en Colombia. Monografía 2020. Universidad Eafit, Escuela de derecho, Medellín.

[19] GONZALEZ, Jefferson. Estudio del estado actual de la seguridad informática en las organizaciones de Colombia. Proyecto de grado 2020. UNAD, Buga.

un estudio del estado en el que se encuentra actualmente la seguridad informática en Colombia documenta las principales debilidades que actualmente son explotadas por los ciberdelincuentes y los factores que contribuyen al éxito de estos atacantes, se enfoca en revisar algunas de las principales metodologías de hacking ético que están disponibles para implementar en busca de mejorar los niveles de seguridad y empezar a mitigar los riesgos que puedan generar un foco de inseguridad y permitir a un delincuente entrar en los sistemas informáticos y efectuar su ataque de forma exitosa.

Bohórquez y Velásquez[20], en el trabajo de grado denominado, propuesta de seguridad informática para promover la ejecución de teletrabajo en la mesa de ayuda de una empresa de telecomunicaciones, se enfoca en un esquema tradicional de realización del trabajo a una modalidad basada en el teletrabajo, obedece a la necesidad, de ratificar el área, procesos, funciones y actividades relacionadas con la mesa de ayuda de la empresa de Telecomunicaciones previamente identificada como objeto de dicha orientación. El problema central que entra a resolver la presente investigación lo constituye la ausencia de una visión integral y estructurada del sistema de gestión de la seguridad de la información, la cual debe preceder la implantación del teletrabajo para el modelo organizacional asociado a la mesa de ayuda de la Empresa de Telecomunicaciones. Dicha labor se ha visto dilatada debido a que no se han formulado requerimientos y lineamientos de seguridad, que garanticen la disponibilidad, integridad y confidencialidad de la información, al igual que la continuidad en la prestación del servicio al cliente que supondría una modalidad basada en el teletrabajo.

[20] BOHÓRQUE, Astrid y VELÁSQUEZ Magda. Propuesta de seguridad informática para promover la ejecución de teletrabajo en la mesa de ayuda de una empresa de telecomunicaciones. Trabajo de grado 2020. Universidad piloto de Colombia, Bogotá D.C.

4.5 MARCO LEGAL

Las siguientes bases legales respaldan el objeto de estudio, a continuación se presenta la siguiente normativa.

Ley 527 de 1999: Reglamenta y define el acceso y uso de los mensajes de datos, del comercio electrónico, firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 1221 del 2008: Establece el reconocimiento del teletrabajo en Colombia como modalidad laboral, promueve y regula el Teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones. Regula el Teletrabajo suplementario, autónomo y móvil; garantizando los mismos derechos de un trabajador formal. Así mismo, formula política pública de fomento al Teletrabajo.

Decreto 411 del 16 de marzo de 2020, "por el cual se toman medidas transitorias debido a la emergencia sanitaria relacionada con el COVID-19 con respecto al régimen de zonas francas".

Decreto 417 del 17 de marzo de 2020, Por el cual se declara un Estado de Emergencia Económica, Social y Ecológica en todo el territorio Nacional, con ocasión a la pandemia originada por el COVID-19, en todo el territorio nacional, por

el término de treinta (30) días calendario contados a partir de la vigencia de ese mismo Decreto, de acuerdo con las razones expuestas en su parte motiva.

Decreto 457 del 22 de marzo de 2020, Por el cual se imparten instrucciones en virtud de la emergencia sanitaria generada por la pandemia del Coronavirus COVID-19 y el mantenimiento del orden público.
Decreto 464 del 23 de marzo de 2020, Por el cual se disponen medidas con el fin de atender la situación de emergencia económica, social y ecológica de la que trata el Decreto 417 de 2020.

Decreto 806 del 4 de junio de 2020, Por el cual se adoptan medidas para implementar las tecnologías de la información y las comunicaciones en las actuaciones judiciales, agilizar los procesos judiciales y flexibilizar la atención a los usuarios del servicio de justicia, en el marco del Estado de Emergencia Económica, Social y Ecológica.

Documento CONPES 3701 14 de julio de 2011, Lineamientos de Política para ciberseguridad y ciberdefensa. Orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.

Documento CONPES 3854 11 de abril de 2016, Política Nacional de Seguridad Digital, hasta el momento, se ha concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de defensa del país y lucha contra el cibercrimen.

Documento CONPES 3995 1 de julio de 2020, Política Nacional de Confianza y Seguridad Digital, formula una política nacional que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente.

Documento CONPES 4012 30 de noviembre de 2020, Política Nacional de Comercio Electrónico, formula la Política Nacional de Comercio Electrónico que tiene como objetivo impulsar el comercio electrónico en las empresas y la ciudadanía, para aumentar la generación de valor social y económico en el país. Para alcanzar el objetivo trazado, es necesario, primero, generar las capacidades técnicas y económicas para el uso y apropiación del comercio electrónico en el sector empresarial y segundo, en el resto de la sociedad; tercero, aumentar la eficiencia y participación de los operadores postales y logísticos en este ecosistema, y finalmente, desarrollar acuerdos institucionales y actualización normativa para habilitar las innovaciones en el comercio electrónico

5 RIESGOS Y AMENAZAS FRENTE AL TELETRABAJO Y EL USO DE RECURSOS DIGITALES EN LA RED

5.1 Riesgo informático en el Teletrabajo

Con la llegada del Covid-19 gran número de funcionarios en todo el planeta obligatoriamente fueron enviados a la casa para realizar actividades laborales de forma remota. Generalmente, un gran porcentaje de esos funcionarios escasamente cuentan con recursos de seguridad informática, diferentes a los que adquieren cuando están en la oficina.

Por otro lado, la necesidad de las organizaciones de continuar operando y optar por el teletrabajo o trabajo en casa sin ninguna planeación y de improviso, fue imposible capacitar al funcionario en esta modalidad, lo anterior, conlleva a los diferentes activos de información sean vulnerables y amenazados por carecer de un escenario seguro, por lo anterior se presentan los siguientes estadísticas.

Según la revista Portafolio[21] mencionó la pandemia llevó a la mayoría de las empresas a replantear sus modelos de trabajo, acelerando vertiginosamente la incorporación del trabajo remoto y la descentralización de la información corporativa, el aumento del uso de conexiones personales para trabajar o estudiar, este mayor uso de la tecnología y los canales virtuales disparó los ataques de los ciberdelincuentes.

[21] REVISTA PORTAFOLIO. Cifras de ciberseguridad en Colombia prenden alarmas al cierre de 2020.2020

Con engaños y valiéndose del Covid-19, la gran mayoría de empresas se vieron afectadas por ciberataques. Así pues, en el primer trimestre de 2020, la inversión total en ciberseguridad alcanzó los 10.400 millones de dólares.

De acuerdo con el documento construido por el programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE), llamado ciberseguridad en entornos cotidianos, en el que participó Claro, es precisamente, el análisis de diferentes contextos como, trabajo remoto, ciberseguridad en dispositivos móviles, ciberataques a correos electrónicos, entre otros, emite los siguientes datos:

Los ciberdelitos presentados durante el 2020 llegaron a más de 45.000 casos, un incremento del 89% comparado con el año anterior, llegando a ser el año de mayor ascenso en cifras e impacto en Colombia. Durante el periodo denominado COVID (marzo – diciembre 2020), se presentó un incremento del 101%, con más de 37.000 reportes, en el número de noticias criminales instauradas ante la Fiscalía General de la Nación.

El delito que mayores denuncias presentó fue la suplantación de sitios web para capturar datos personales con un crecimiento del 303% comparado con el 2019.

Este delito tiene un vínculo directo con modalidades conocidas, tales como el phishing, spoofing y pharming que afectaron las empresas. Además, hubo 5.440 casos denunciados donde este tipo de ataques fue utilizado por los cibercriminales para capturar datos personales o esparcir malware en las redes corporativas.

El segundo delito con mayor número de denuncias, con 9.487 casos registrados fue la violación de datos personales. Presentó un crecimiento del 174% como consecuencia de la filtración y robo de datos, lo que generó un doble impacto que compromete aspectos operativos, así como legales y de cumplimiento por la pérdida de información sensible.

Le sigue el hurto por medios informáticos con un 37% de crecimiento, registró más de 16.000 casos denunciados. A pesar de poseer datos estadísticos altos, la modalidad que más se destaca es el apoderamiento de credenciales para el acceso a servicios de banca online, con los cuales los cibercriminales, consiguen suplantar al titular del producto bancario y apoderarse del dinero generalmente dispuesto en cuentas bancarias[22].

En virtud de lo anterior, según informe los ciberataques están afectando por igual a múltiples sectores productivos del país, las técnicas más usadas son los ataques de phishing, los cuales se propagan mediante archivos adjuntos maliciosos.

Vale la pena resaltar que varias entidades estatales, quienes prestan servicios en línea fueron atacadas por ciberdelincuentes, como Administración de impuestos y Aduanas, Registraduría Nacional y fiscalía General de la Nación.
Como dice Maddison[23] vicepresidente de FORTINET, la evolución del entorno de trabajo a distancia, la mayor dependencia del uso de dispositivos personales y la

[22] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Seguridad aplicada al fortalecimiento de las empresas (SAFE). Ciberseguridad en entornos cotidianos.2020
[23] MADDISON, Jhon. Nueva investigación de Fortinet indica que las empresas deben adaptarse para afrontar los retos de seguridad del teletrabajo a largo plazo.Sunnyvale.2020

afluencia general de trabajadores fuera de la red corporativa abrieron una oportunidad para una actividad de ciberamenazas sin precedentes.

Las amenazas contienen el phishing y esquemas de compromiso de correo electrónico empresarial y ataques de ransomware. De hecho, el 60% de las empresas reveló un aumento en los intentos de violación de la ciberseguridad durante la transición al trabajo remoto, mientras que el 34% informó de violaciones reales en sus redes.

Así pues, con la suma de funcionarios conectados a la red corporativa desde la casa o de cualquier otro lugar, el incremento de ataques cibernéticos, las organizaciones tienen diversos retos para dar continuidad y funcionamiento al quehacer empresarial, como mejorar la seguridad de las conexiones, capacitación a funcionarios, establece políticas de seguridad, son factores relevantes y retadores en esta evolución.

Jodka y Green[24] miembros del bufete Dickinson Wright, en su artículo denominado "COVID-19 plantea mayores riesgos de ciberseguridad para empleadores y empresas", se refieren a los empleados que trabajan de forma remota quienes pueden crear riesgos para las empresas de las siguientes formas: mayores riesgos del acceso remoto, incluidos los riesgos de seguridad física asociados con el uso de dispositivos personales y de propiedad de la empresa, aumento del phishing y otras estafas, violación de leyes específicas de la industria y del estado.

[24] JODKA Sara y GREEN Caleb. Dickinson Wright. COVID-19 plantea mayores riesgos de ciberseguridad para empleadores y empresas. Detroit. 2020

5.1 Mayores riesgos del acceso remoto

El acceso remoto se basa en el intercambio y la transmisión de información y datos, generalmente a través de Internet. Cuando se trabaja a distancia, los empleados posiblemente manipulan, acceden, discuten o transmiten información confidencial, incluidos secretos comerciales de la empresa, información personal del cliente o datos financieros confidenciales.

El uso de aplicaciones de teleconferencia como Zoom y otras funciones y aplicaciones de videoconferencia, se han vuelto muy populares y comunes respecto al trabajo remoto, pero hay una serie de problemas de privacidad relacionados con la Política de privacidad de Zoom , que se modificó el 29 de marzo de 2020

Los altavoces inteligentes, los asistentes virtuales y los teléfonos inteligentes también representan un riesgo significativo para el teletrabajador inconsciente. Los investigadores y los piratas informáticos blancos han expuesto vulnerabilidades en dispositivos inteligentes como Alexa Echo, Siri y Google Assistant. Los ciberdelincuentes pueden usar ondas de ultrasonido casi silenciosas para activar estos dispositivos inteligentes para que soliciten a los usuarios sus credenciales y contraseñas de usuario, así como para obligar a los dispositivos a ejecutar comandos maliciosos.

Las redes están desbordadas con esquemas de phishing que se aúnan a la pandemia de COVID-19. En febrero de 2020, los ciberdelincuentes lanzaron un sitio web que pretendía ser un mapa de distribución del brote de coronavirus. El mapa malicioso en línea, que estaba ubicado en www.coroa-virus-map [.] Com, contenía una suplantación convincente del mapa legítimo operado por el Centro John

Hopkins de Sistemas, Ciencia e Ingeniería y ofrecía lo que parecía ser un recuento de los casos confirmados y las muertes relacionadas con el brote del virus.

Teniendo en cuenta lo anterior, los ciberdelincuentes están aprovechando la pandemia, confusión y la situación actual de empleados y usuarios para realizar sus ciberataques a través de algunos mecanismos fraudulentos, es por ello que el riesgo en las organizaciones es inevitable, ya que pueden perder información confidencial, financiera, entre otros.

Vale la pena resaltar, que el entorno de trabajo desde la casa significa que los empleados para desarrollar sus actividades laborales deben utilizar sus dispositivos personales o tal vez algunas veces suministrados por la organización, con el propósito de acceder a la información corporativa. Por lo tanto, la organización se está arriesgando a una pérdida de datos o a ataques informáticos en el momento en que permiten que sus funcionarios accedan de forma remota.

Asuntos legales[25], en su artículo sobre "Delito de suplantación de identidad aumentó 409% en 2020 debido a la pandemia" informa que la suplantación de identidad, según datos de la Dijín, creció 409% el año pasado, en plena pandemia del covid-19. El reporte reveló que mientras en 2019 hubo alrededor de 300 casos de este tipo, en 2020 la cifra se disparó a 1.527 reportes.

[25] ASUNTOS LEGALES. Delito de suplantación de identidad aumentó 409% en 2020 debido a la pandemia. Bogotá.2021

Un reporte de la entidad policial también reveló que la suplantación de sitios web creció 358% con 4.353 casos en 2020, a comparación de los 951 reportados el año anterior.

Por otro lado, explican el riesgo que tienen los ciudadanos con sus datos personales y su firma en diferentes documentos que circulan por la red, elementos clave para el delincuente. Afirman que una de las formas de suplantación de identidad más usual es el de personas a través de firmas de un documento escaneado. Dicha rúbrica puede circular por redes hasta que el delincuente tenga acceso a ella y la utilice para sus fines delictivos.

Esta práctica de firmar el documento adhiriéndole la firma manuscrita en formato imagen, se presta para cometer actos fraudulentos, además que no tiene valor probatorio, no se puede evidenciar si la persona quien está firmando el documento es quien dice ser, para ello algunas entidades han optado por darle un porcentaje de seguridad a esta firma con otras técnicas, o algunas han optado por la firma digital.

El portal WeLiveSecurity[26] en su artículo “Resumen con las 10 noticias de seguridad más destacadas que dejó el 2020” hace referencia al protocolo RDP (Remote Desktop Protocol), los intentos de ataque al RDP crecieron durante gran parte del primer semestre de 2020 y continuaron aumentando durante el resto del año. En América Latina este aumento fue durante el tercer trimestre del 141%, con picos de hasta 12 mil ataques diarios a usuarios únicos.

[26] WELIVESECURITY. Resumen con las 10 noticias de seguridad más destacadas que dejó el 2020. 2021

En razón de lo anterior, sucede debido a que los cibercriminales saben muy bien que la mayoría de funcionarios o empleados están trabajando fuera de la infraestructura corporativa y lo hacen desde casa, ellos suponen que algunas organizaciones no brindan la necesaria seguridad informática a los trabajadores, por lo tanto sacan provecho para realizar sus ataques. Por ende, esta realidad laboral incrementó el riesgo de sufrir un incidente de seguridad, más aún para aquellas organizaciones que a la fecha no han tomado medidas de seguridad.

Appgate, compañía mundial especializada en ciberseguridad y prevención de fraude transaccional, dio a conocer los resultados de su informe Fraud Beat 2021, investigación que analiza la forma como la pandemia impactó la seguridad tecnológica en las organizaciones y donde el fraude electrónico es uno de los grandes protagonistas.

5.2 A continuación se presentan casos reales a nivel mundial sobre incidentes que ha traído el trabajo en casa

Como lo manifiesta Camilo Castellanos[27], gerente de seguridad de la información en Mercado Libre, sólo el 10% o 15% de empleados de compañías laboraban de forma remota, debido a la situación actual del COVID-19 ese porcentaje ascendió exponencialmente en el año 2020, asimismo se incrementaron las ciberamenazas, pues al trabajar desde la casa, obedece más del funcionario, de su cuidado y uso de los recursos digitales.

[27] LOS LIBERTADORES FUNDACIÓN UNIVERSITARIA. Era digital: el ciberataque como un arma silenciosa

En lo que se refiere a tipos de ataque, el phishing sigue en subida, sin embargo el Ransomware ha terminado de encaramarse como la más grande amenaza de ciberseguridad en 2020.

Ransonmware, se refiere a ciberataques en los que hackers secuestran los datos de un individuo u organización y piden grandes sumas de dinero a cambio. Se conocen como ransomware y se calcula que en 2021 cada 11 segundos habrá uno.

Colonia Pipeline es uno de los oleoductos más grandes de Los Estados Unidos, provee energía alrededor de unos 50 millones de personas, en mayo de 2021 dejó de operar durante 5 días, como resultado se generó escases de gasolina, pues esta empresa energética fue víctima de un ataque de ransomware quienes tomaron control de su sistema computarizado, los ciberdelincuentes denominados Dark side es un grupo ruso quienes cobraban por la liberación $ 4.00.000 (dólares) en criptomonedas.

El ransonware se ha convertido en un negocio rentable, pues los ciberdelincuentes gozan de anonimato lo que les permite actuar con plena libertad.
FireEye es una de las grandes empresas de ciberseguridad a nivel global, cuenta con clientes como empresas y agencias gubernamentales. La compañía provee herramientas de red team, su misión es simular ataques asimisma para corroborar su defensa y hallar vulnerabilidades. En diciembre 2020 fue víctima de un ataque a su sistema para apoderarse de estas herramientas.

Vacunas contra el COVID-19: Las vacunas contra el coronavirus poseen valor enorme para la salud mundial. Por tal razón la seguridad de las vacunas también se

vio afectada, debido a que en julio del año 2020**,** la Agencia de Seguridad Nacional de Estados Unidos, la autoridad canadiense de ciberseguridad y el Centro de Ciberseguridad Nacional del Reino Unido, anunciaron ataques informáticos dirigidos a científicos británicos, tratando de obtener información secreta sobre las vacunas del COVID-19.

Garmin, es una compañía que se encuentra en todo el planeta, fabrica relojes inteligentes, bandas de gimnasia y otros dispositivos para llevar puestos. En julio de 2020 fue víctima de ataque de ransomware y la hipótesis es que fue infectado con WastedLocker. Las interrupciones iniciaron en sus centros de llamadas y comunicaciones y mediante correo electrónico, así que la compañía optó por cerrar algunos servicios en la nube como como Garmin Connect, Garmin Express y Garmin.com.

Los ciberdelincuentes que atacan con la variante WastedLocker, piden por el rescate 10 millones de dólares.

Canon, es el proveedor líder de soluciones de procesamiento digital de imágenes para los consumidores de todo el mundo. En agosto de 2020 fue víctima de ataque de ransomware, afectando servicios como servidores email, cuentas de Microsoft Teams, el sitio web de la compañía y el servicio de almacenamiento en la nube image.canon. Según Canon la información comprometida oscila alrededor de 10 Tbytes de datos.

El hackeo a Twitter La plataforma social Twitter, en julio del año 2020, debido a un ciberataque se vio obligado a congelar algunas cuentas de personajes famosos.

Algunas de las cuentas que los ciberdelincuentes tuvieron acceso fue la de Barack Obama, Joe Biden, Jeff Bezos, Elon Musk y Bill Gates, publicaron información falsa con el único fin de que los seguidores de estas personas accedieran a un link realizando donaciones mediante la billetera digital de bitcoin.
Por otro lado, se afirma que los estafadores informáticos accedieron a vulnerar la plataforma, debido a que uno de sus empleados se prestó para que los atacantes ingresaran a determinadas herramientas.

Capcom, empresa japonesa desarrolladora y distribuidora de videojuegos fue víctima de ataque en noviembre del año 2020, en este suceso los ciberdelincuentes hurtaron información confidencial tanto de la empresa como sus clientes. El ataque fue perpetrado con ransonware ragnar locker.

Ransonware ragnar locker, son programas maliciosos denominados como malware de rescate.

5.3 Ataques más utilizados durante el covid 19 relacionado con el teletrabajo

A continuación se presentan los grandes hallazgos:
Covid 19: El informe mostró que aproximadamente, 18 millones de malware y correos electrónicos de phishing y más de 240 millones de mensajes basura relacionados con el virus (Covid 19) son enviados diariamente desde Gmail.

Filtración de datos: El año pasado se presentaron aproximadamente 3.950 casos de filtración de datos, casi el 80% sucedió por credenciales robadas o ataques de fuerza bruta.

Phishing: Basado en el informe global de incidentes de Appgate, se produjo un aumento del 345% en usuarios víctimas de engaños a personas haciéndose pasar por una empresa, persona o servicio durante el año pasado.

Malware: Se identificó en una encuesta reciente que el Ransomware es el segundo tipo de malware más común después del Password Dumper.

Hoy por hoy, son verídicas las exponenciales amenazas a las que está expuesta una empresa, por lo tanto deben llevar sus habilidades y estrategias a otro nivel, anticipar el fin delictivo, amenazas y vulnerabilidades. Es la única forma de contrarrestar y está preparado para un ciberataque.

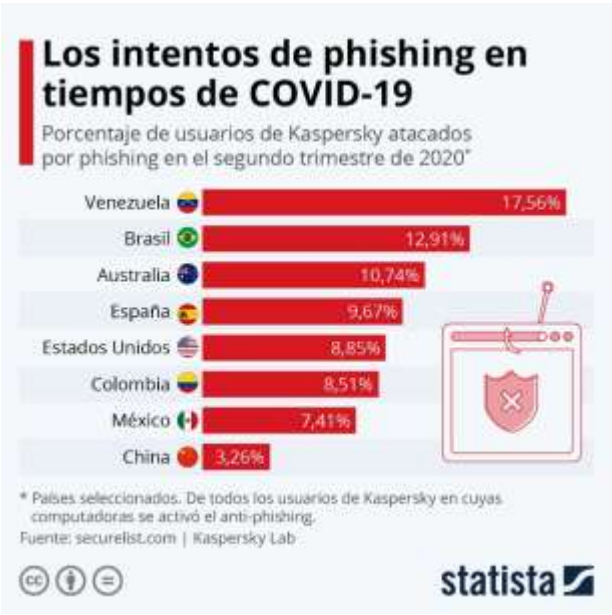
Con la llegada del año 2020, aparece el COVID-19 y se transforma en el agente catalizador de la transformación digital, acelerando la adaptabilidad que los seres humanos venían teniendo a las nuevas formas de trabajo. Junto con su llegada, y con la urgencia de información y distribución de novedades, el phishing acompañado de ransomware relacionado con el COVID-19 aumentó de forma exponencial, tal como se muestra en el gráfico.

Imagen 1 Ataques cibernéticos a partir de la llegada del COVID-19

Fuente: CheckPoint

"Cyber attack trends: 2020 mid-year report", Check Point Software Technologies Ltd., Tel Aviv, Israel, Julio [en línea](Recuperado en 10 noviembre 2021.) Disponible en: https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/.

Imagen 2 Infografía Los intentos de phishing en tiempos de COVID-19



Fuente: PASQUALI,

Marina. Los intentos de phishing en tiempos de COVID-19[En línea]. Ciberdelincuencia. Hamburgo.: Statista GmbH. 2020. (Recuperado en 10 noviembre 2021.) Disponible en https://es.statista.com/grafico/18427/intentos-de-phishing-durante-la-pandemia/

6 NORMATIVAD Y LINEAMIENTOS DE SEGURIDAD DIGITAL VIGENTES EN COLOMBIA, RESPECTO A LA UTILIZACIÓN DE CANALES Y RECURSOS ELECTRÓNICOS

La siguiente normativa, sustenta el objeto de estudio.

6.1 Ley 527 De 1999 uso de medios electrónicos

Ley 527 de 1999 se define el uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establece certificación y se dictan otras disposiciones.

Esta Ley en tiempos de pandemia se aplicó de acuerdo con la necesidad de la entidad en dar continuidad a la gestión y trámite de los documentos organizacionales, actos administrativos entre otros, empezó a gestionar mediante el correo electrónico institucional, de acuerdo como lo dice el Artículos, 6, 7, 8, 9, y 10.

Sin embargo, los medios electrónicos están expuestos a los riesgos propios del internet, como fraude, perdida de datos o Phishing, es relevante que la organización garantice la seguridad de su información mediante respaldo jurídico, buenas prácticas empresariales, buena fe y manejo adecuado de las plataformas.

Por otra parte, con la pandemia del Covid-19, algunas empresas optaron por invertir en seguridad informática y adquirieron firmas digitales, Articulo 28. Atributos jurídicos de una firma digital. Cuando una firma digital haya sido fijada en un

mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

6.2 Ley 1221 de 2008 regulación del teletrabajo en Colombia

Ley 1221 de 2008: por la cual se establecen normas para promover y regular el teletrabajo y se dictan otras disposiciones. Crea la red nacional de fomento al teletrabajo, con el fin de promover y difundir esta práctica en el país e incluye las garantías laborales, sindicales y de seguridad social para los teletrabajadores.

Colombia es uno de los países de américa Latina más adelantados en Teletrabajo. Según cifras del MinTIC, antes de la pandemia existían cerca de 122.000 teletrabajadores, una vez se declara estado de emergencia en el territorio Nacional el 24 de marzo ese número pasó a millones.

Vale la pena mencionar, que el teletrabajo de acuerdo con la Ley de 2008 tiene unas connotaciones diferentes al que los funcionarios de las entidades por pandemia debieron habituarse, debido a que fue la única opción para mantener la continuidad operacional en la mayoría de las industrias.

El Ministerio de Tecnologías de la Información y las Comunicaciones junto con el Ministerio del Trabajo brinda de manera gratuita acompañamiento técnico a entidades públicas y privadas en la implementación del teletrabajo a través de asesorías, conferencias y talleres.

Respecto a la aplicación de la Ley 1221 de 2008, su difusión y aplicación considero ha sido paulatina, a pesar que en el 2020 se declara emergencia sanitaria y confinamiento obligatorio, hasta la fecha no se ha ejecutado de acuerdo con los lineamientos que plantea esta norma, al contrario del trabajo en casa, que tuvo para algunos compañías aspectos acertados como como reducción de gastos locativos, fortalecimiento de la economía, utilización de tecnologías de la información, ahorro servicios públicos entre otros, por otro lado, para los ciudadanos se observa un escenario desalentador respecto a la carga laboral excesiva, aumento de estrés, el uso de sus propios dispositivos, los servicios públicos se incrementaron, espacios del hogar convertidos en oficina.

En virtud de lo anterior, las empresas en el año 2020 continuaron con la figura del trabajo en casa y no el teletrabajo, la mencionada Ley en tiempos de pandemia ha tenido una aplicación reducida y no hoy por hoy no se está implementando.

6.3 Ley 1437 de 2011: por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

De acuerdo con la Ley 1437, las entidades se vieron respaldadas debido a que en el capítulo IV reza la utilización de medios electrónicos y hace énfasis en los procedimientos y trámites administrativos a través de medios electrónicos.

El 25 de enero de 2021 fue sancionada la Ley 2080, por medio de la cual se introducen modificaciones relevantes referentes a los medios tecnológicos en la presente Ley. Se establece la recepción de documentos electrónicos por parte de

las autoridades y se debe contar con un registro electrónico de documentos, que permita controlar la producción documental electrónica tanto enviada como recibida, así mismo garantizar la seguridad de la información.

Por otra parte, la entidad deberá contar con una sede electrónica.

Como elemento fundamental en la normatividad relacionada con la supresión de trámites, se requiere integrar a la sede electrónica los otros elementos, enunciados en el Decreto 2106 de 2019 art. 14. “Integración a la sede electrónica”. Este establece que: las autoridades deberán integrar a su sede electrónica todos los portales, sitios web, plataformas, ventanillas únicas, aplicaciones y soluciones existentes, que permitan la realización de trámites, procesos y procedimientos a los ciudadanos de manera eficaz.[28]

De acuerdo con lo anterior, las entidades han asumido el reto de habilitar canales digitales con el objetivo de dar continuidad a la gestión y trámite, garantizando el registro y radicación de los documentos electrónicos y reduciendo trámites presenciales. Sin embargo, aún existen falencias en la seguridad de la información, debido a que la mayoría continúan usando la firma digitalizada sin ninguna protección, dicha firma es vulnerable, no goza de integridad, no repudio y confiabilidad, pues no se puede asegurar que quien firma es quien dice ser.

[28] ARCHIVO GENERAL DE LA NACIÓN. Requisitos para la gestión documental en sedes electrónicas, ventanillas únicas y portales transversales. Bogotá. 2021

Vale la pena resaltar, la capacitación continua sobre seguridad digital a los funcionarios, aún no se adquiere conciencia de este tema relevante, tal vez diversas entidades han sido afortunadas y no ha sufrido ataques informáticos, por tal razón ha hecho caso omiso o han dado poco valor a este aspecto, porque de nada sirve tener la mejor infraestructura de seguridad informática, los mejores sistemas y tecnología si la vulnerabilidad se encuentra en los funcionarios, quienes son el punto débil de la organización, para ello utilizan diferentes técnicas conocidas como ingeniería social, phishing o pharming.

6.4 Ley 2088 de 12 de mayo de 2021: por la cual se regula el trabajo en casa y se dictan otras disposiciones

La Ley trae aspectos importantes para el objeto de estudio, debido a que orienta directrices que se deben cumplir para el trabajo en casa y enfatiza que el trabajo en casa no es lo mismo que el teletrabajo, pues este último está regulado mediante la Ley 1227 de 2008.

El Ministerio del Trabajo aclara que los trabajadores que desarrollen sus funciones desde su domicilio no son considerados como teletrabajadores.

La Ley resalta que el trabajador puede usar sus propios equipos para desempeñar sus funciones, siempre que medie acuerdo con el empleador. Si no se llega al mencionado acuerdo, el empleador suministrará los equipos, sistemas de información, software o materiales necesarios para el desarrollo de la función o labor contratada, de acuerdo con los recursos disponibles para tal efecto.

La Ley busca una posible solución a la situación actual, sin embargo a la fecha la mayoría de empleados sin ningún tipo de concertación con la empresa han venido utilizando sus propios dispositivos electrónicos para realizar actividades laborales,

la Ley ha tenido una progresiva aceptación, pero no se está aplicando de manera apropiada, pues existe una seria confusión entre el teletrabajo y trabajo en casa.

Respecto al factor tecnológico, se ha logrado mayor acceso a las tecnologías, manejo de aplicaciones, la información se envía con mayor rapidez, disminución tráfico de vehículos, también incremento de ciberataques, precisamente por la utilización de los dispositivos electrónicos propios.

En esta situación se debe propender por la seguridad de la informática, debido a que el empleado va estar por fuera de la oficina y tendrá acceso remoto a la información de la entidad, la cual posiblemente pueda sufrir ataques informáticos mientras realice sus labores.

Decretos

6.5 Decreto no. 491 del 28 de marzo de 2020, el gobierno nacional adoptó medidas de urgencia para garantizar la atención y prestación de los servicios por parte de las autoridades públicas, estableciendo en su artículo 11 lo siguiente:

De las firmas de los actos, providencias y decisiones. Durante el período de aislamiento preventivo obligatorio las autoridades a que se refiere el artículo 1 del presente Decreto, cuando no cuenten con firma digital, podrán válidamente suscribir los actos, providencias y decisiones que adopten mediante firma autógrafa mecánica, digitalizadas o escaneadas, según la disponibilidad de dichos medios.

Decreto ineludible para la investigación, debido a que varias entidades en Colombia al carecer de la firma digital optaron por la firma digitalizada con el propósito de garantizar la prestación de servicios.

Es de resaltar que la firma digitalizada o escaneada no es propiamente un mecanismo técnico o tecnológico y sus inconvenientes redundan en la dificultad a la hora de demostrar su confiabilidad por su bajo nivel de seguridad por ende las entidades que utilizan esta firma son responsables de adoptar las medidas internas necesarias para garantizar la seguridad de los documentos que se firmen por este medio, debido a que la rúbrica de una persona es fácilmente suplantable, así como la imagen de esta, sin control alguno, puede ser copiada y pegada virtualmente sobre cualquier documento.

Firma escaneada

Ya que la firma electrónica pueden ser datos biométricos que permitan identificar a una persona y la escritura entra en esta categoría, al ser un rasgo que permite identificar a una persona, el firmar un contrato y escanearlo o incluir la firma escaneada en el contrato para luego compartirlo por medios electrónicos puede ser considerada como un tipo de firma electrónica.

La firma escaneada no es propiamente un mecanismo técnico o tecnológico y sus inconvenientes redundan en la dificultad a la hora de demostrar su confiabilidad por su bajo nivel de seguridad, pues la rúbrica de una persona es fácilmente

suplantable, así como la imagen de esta, sin control alguno, puede ser copiada y pegada virtualmente sobre cualquier documento[29].

Directivas

- Directiva presidencial No 2 del 12 de marzo de 2020 - Medidas para atender la contingencia generada por el covid-19, a partir del uso de las tecnologías de la información y las telecomunicaciones.

Teniendo en cuenta la directiva presidencial impartida para organismos y entidades de la rama ejecutiva del orden nacional y territorial, las directrices del presidente Duque frente al trabajo en casa por medio del uso de las tic y el uso de herramientas colaborativas, han provocado la utilización de plataformas virtuales sin ningún tipo seguridad y privacidad, sobre todo para cientos de usuarios que a la fecha le eran desconocidas.
En el caso de la Plataforma Zoom, se ha convertido en una de las plataformas con mayor uso, asimismo, este auge generó el ataque cibernético denominado zoombombing, hace referencia a la persona que sin invitación alguna ingresa a la sala virtual y comparte información inadecuada, ya sea en reuniones empresariales o sector educativo.

De acuerdo con lo expuesto anteriormente, en algunas entidades, aún se carece de conciencia, cuidado, cultura sobre la seguridad y privacidad de la información, ya que no basta sólo con orientar charlas y realizar guías sobre el tema, se debe

[29] ASUNTOS LEGALES. Firma digital o escaneada, una decisión basada en la seguridad

fortalecer el talento humano, quien es el principal causante y anzuelo para perpetuar un ataque cibernético.

- Directiva No 07, 27 de agosto de 2020 Presidencia de la Republica. Retorno gradual y progresivo de los servidores públicos y contratistas a las actividades laborales y de prestación de servicios de manera presencial.

- Directiva Presidencial No 03 del 15 de Marzo de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

Las directivas presidenciales son claves en la investigación, nos invitan a hacer uso de las TIC, portales de conocimiento, redes sociales, plataformas colaborativas para adelantar reuniones, capacitaciones con el propósito de evitar el contacto en las oficinas y reducir el número de funcionarios realizando actividades presenciales, en virtud de lo anterior, el aumento de ciberataques en el mundo aumentó exponencialmente, es por ello que el gobierno nacional orienta lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos, para que las entidades busquen implementar modelos que permitan la protección y ciberseguridad de sus activos

- Norma técnica colombiana NTC/ISO 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información, mediante la norma técnica se puede realizar seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).

7 MEDIDAS DE SEGURIDAD INFORMÁTICA QUE HAN ASUMIDO LAS DIFERENTES ENTIDADES FRENTE AL TRABAJO EN CASA

Con la publicación de la edición 2020 del informe “Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe” pone en evidencia que la región de América Latina y el Caribe aún no está suficientemente preparada para enfrentar los ataques que se producen en el ciberespacio. Únicamente 7 países de los 32 analizados en este reporte cuentan con un plan de protección de su infraestructura crítica, y 20 han establecido algún tipo de grupo de respuesta a incidentes, llamado CERT o CSIRT, según sus siglas en inglés. Esto limita la capacidad de identificar ataques y responder oportunamente a los mismos.

Como lo menciona Urrutia[30], Secretaria de Seguridad Multidimensional de la OEAA, tanto las personas como las instituciones están expuestas a la incertidumbre y la impredecible naturaleza del delito cibernético. Los esfuerzos para hacerlo deben ser de naturaleza multidimensional, porque se requiere una variedad de factores para construir una cibersociedad resistente.

De acuerdo con lo anterior, la llegada de la pandemia ha fomentado el teletrabajo a nivel mundial y se implantó de forma apresurada, convirtiéndose en el blanco perfecto para los ciberataques, debido a que algunas organizaciones no estaban preparadas en cuanto al equipamiento y conocimiento de seguridad para realizar actividades laborales en el contexto actual.

[30] BANCO INTERAMERICANO DE DESARROLLO, Citado por URRUTIA Farah. Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el CARIBE. 2020

En Colombia, una vez se decreta en marzo el aislamiento social, el teletrabajo se intensificó, así pues las comunicaciones por correo electrónico también crecieron, llegando a ser un medio importante para enviar programas maliciosos.

A continuación se exponen algunas organizaciones, las cuales han tomado medidas de seguridad frente al teletrabajo o trabajo en casa en esta coyuntura.

Alcaldía Mayor de Bogotá[31], expidió la guía sobre lineamientos para el uso de documentos electrónicos en la contingencia generada por la emergencia sanitaria COVID-19. En este documento establecen lineamientos técnicos para mitigar los riesgos asociados al uso documentos electrónicos en los ambientes de trabajo en casa en razón de la actual emergencia ocasionada por el COVID-19.

Con el fin de propiciar un canal seguro para la conectividad y Gestión de Documentos Electrónicos de Archivo en condiciones de trabajo en casa y/o teletrabajo, se realizan una serie de recomendaciones con respecto al uso adecuado de canales electrónicos haciendo énfasis sobre la implementación de herramientas para seguridad informática, lo cual permitirá mitigar riesgos asociados al uso indebido y perdida de información durante la gestión de Documentos Electrónicos de Archivo

[31] ARIAS , Álvaro y Garzón Jhon. Guía lineamientos para el uso de documentos electrónicos en la contingencia generada por la emergencia sanitaria Covid-19. Bogotá. 2020

La empresa Claro, cuenta con soluciones de seguridad y ciberseguridad las cuales permiten prevenir el riesgo de fuga de información y proteger el bien más valioso que es la información, frente al creciente volumen de amenazas cibernéticas, con soluciones de DLP (Data Loss Prevention) desde los siguientes frentes:

- Web - Dispositivos extraíbles
- Servidores de archivos
- Carpetas compartidas
- Correo electrónico
- Monitor de Red y accesos a aplicaciones

La protección de los datos inicial se realiza a través de la instalación de Equipo Especializado de red y Equipo especializado de correo, que permiten tener un control 360 de las actividades que desarrollan los colaboradores de las compañías incluso en el teletrabajo, validando usabilidad del correo electrónico, navegación web, uso de aplicaciones de mensajería instantánea y compartir archivos, todo controlado y auditado bajo la capa de seguridad en la red.

El siguiente paso es la protección de los datos, para ello usan un Agente que controla todo el almacenaje de información en dispositivos externos como USB, discos duros, Smartphone, CDs, DVDs e incluso las mismas impresiones de información, enviando mensajes de alerta en pantalla a los funcionarios de la empresa, recordando la confidencialidad de la información y evitando su almacenaje.

Banco Bilbao Vizcaya Argentaria (BBVA)[32], a pesar de que el teletrabajo se está convirtiendo en una práctica habitual, para las organizaciones sigue siendo un desafío que desde casa se tomen todas las medidas necesarias para proteger la seguridad de la información corporativa. Vanesa Gil funcionaria de BBVA y experta en ciberseguridad afirma que es esencial, que los empleados sean conscientes de los riesgos a los que están expuestos a la hora de trabajar fuera de la oficina. A continuación alguna recomendaciones:

La red wifi de nuestras viviendas es uno de los elementos fundamentales a tener en cuenta, debido a que constituye un punto de entrada a través del cual usuarios maliciosos podrían acceder a nuestra información. Para protegerla, algunas de las acciones que debemos llevar a cabo son cambiar el nombre de la red y modificar la contraseña de la misma, estableciendo una que sea robusta.

Para evitar que un usuario malicioso acceda a la información que se gestiona a través de dispositivos conectados a la red, como ordenadores, smartphones o tabletas, lo ideal es mantener el 'software' y las 'apps' actualizadas, emplear un antivirus también actualizado y utilizar diferentes usuarios para cada persona y finalidad.

Cuando se utilice dispositivos personales, recomienda trabajar con herramientas corporativas y evitar trabajar en local, almacenar información en los mismos y utilizar memorias extraíbles.

[32] BANCO BILBAO VIZCAYA ARGENTARIA- BBVA. Cómo teletrabajar de forma segura desde casa. 2021

Utilizar contraseñas robustas y diferentes en cada dispositivo, modificarlas periódicamente, establecer un doble factor de autenticación y recordar que nunca se deben compartir.

"Grupo Bancolombia, es la primera compañía de Colombia en habilitar la mayor cantidad de empleados trabajando desde casa. En poco tiempo esta compañía logró que 19,500 a 22,000 empleados en el país pudieran trabajar bajo un esquema flexible con todas las herramientas y controles de seguridad necesarios"[33].

En ese sentido, habilitaron herramientas de trabajo remoto para empleados y aliados, que incluyeron la entrega de unos 4,000 equipos y 2,000 diademas. Así, el 100% de los equipos ágiles usaron herramientas de automatización, manteniendo su productividad y la continuidad del negocio.

Vale la pena mencionar que para Bancolombia los esquemas flexibles de trabajo no significaron una novedad, ya que ellos desde 2012 implementaron el teletrabajo, lo que les permitió adaptarse con facilidad, gracias a un camino recorrido, lleno de aprendizajes y en el que más de 3.300 empleados ya los acompañaban**.**

Sugieren algunas herramientas útiles para teletrabajar:

Microsoft Office 365: contiene servicio de correo, teleconferencias, sitios de entorno comunicacional, además de sus acostumbradas hojas de cálculo y

[33] GRUPOBANCOLOMBIA. Claves para implementar el teletrabajo en medio del coronavirus. 2020

herramientas de edición, y lo mejor es todo en línea, permitiendo que varios equipos trabajen al tiempo.

Slack: es una solución creada para bajar el uso del correo electrónico, además de ser un centro de colaboración para aumentar la productividad. Integra aplicaciones libres para el tratamiento de datos e información.

Telegram: es competencia directa de WhatsApp y su principal diferenciador es la posibilidad de trabajar con archivos de alto volumen de datos (permite compartir hasta por 1.5 gigas). Es posible acceder desde cualquier tipo de dispositivo y permite crear grandes grupos de comunicación, logrando tener hasta 2000 miembros en un solo grupo de chat.

Por último, el Ministerio de las Tic[34] con la publicación de la Resolución 1519 de 2020 desarrolló las bases para impulsar la transformación digital de las entidades públicas, a partir de cambios en los sitios web y las nuevas sedes electrónicas de las entidades.

El documento contiene cuatro anexos, el primero desarrolla las directrices de accesibilidad web; el segundo incorpora nuevos estándares de transparencia y divulgación de contenidos; el tercero dispone medidas en materia de seguridad digital, y el cuarto dispone condiciones sobre datos abiertos.

[34] MINISTERIO DE LAS TIC. Nuevas medidas para la transformación digital de los sitios web de las entidades públicas definió el Ministerio de las TIC. Resolución 1519 de 2020. Bogotá. 2020

Sobre la seguridad digital web, trae nuevos requisitos. El avance de la digitalización también implica que los sujetos obligados deban garantizar la disponibilidad de los sitios web y, en especial, la seguridad digital, la seguridad de la información y la privacidad de los datos.

A nivel mundial, España se encuentra liderando el cuarto puesto en relación con la ciberseguridad, sin embargo los ataques en el sector educativo se han incrementado significativamente alrededor del 300% precisamente por la pandemia, de esta manera las instituciones se enfrentan a un reto formativo, de inversión y prevención. El aislamiento provocó que las instituciones se obligaran a orientar clase en línea, utilizando los dispositivos electrónicos privados, uso masivo de correo electrónico, redes sociales, nuevas plataformas, factores que dispararon ataques cibernéticos a esto se suma la falta de presupuesto, capacitación y carencia de habilidades tecnológicas del talento humano y alumnado.

En virtud de lo anterior, para especialistas en el tema, consideran imprescindible entrenar a la comunidad educativa con el propósito de aplacar ataques, invertir en herramientas tecnológicas, realizar pruebas de penetración, inteligencia artificial, ya que estos escenarios no son pasajeros[35].

Willy Zamudio, gerente de TI del SENATI[36], presenta diversos pasos, los cuales están siendo implementados en su empresa, además advierten un ciberataque y la manera de proteger la información.

[35] COMPUTERWORLD. La educación, en el punto de mira de los ciberdelincuentes.2021

[36] ANDINA. ¿Cómo prevenir un ciberataque en tu empresa? Lima. 2021

Se debe proteger los equipos de cómputo, utilizando antimalware, EDR y aplicando actualizaciones. Se debe utilizar solo software aprobado por la compañía.

Se debe tener cuidado con los correos electrónicos. Evitar hacer click en enlaces o descargas de archivos desconocidos.

Evitar el uso de dispositivos externos en las computadoras corporativas sin antes haber realizado el procedimiento de limpieza de virus o archivos malintencionados.

Tener en cuenta de construir contraseñas largas, por lo menos ocho caracteres, incluir signos, números y mayúsculas. Entre más extensa la contraseña, más difícil de romperse. Vale la pena recordar, no utilizar la misma contraseña para todos tus equipos y servicios.

Se debe abstener de conectar dispositivos personales a redes empresariales sin aviso.

Es relevante contar con un experto en ciberseguridad, que garantice la confidencialidad, integridad y confiabilidad de la data.

8 CONCLUSIONES

Se evaluaron los diferentes riesgos y amenazas frente al teletrabajo y el uso de recurso digitales en la red, se evidenció la vulnerabilidad de los activos de información, uso inadecuado de plataformas virtuales, uso de dispositivos personales, falta de capacitación al talento humano, aumento ataques cibernéticos, los cuales se propiciaron debido al trabajo en casa, por la necesidad de que la organización continuara operando.

Se presentó la normatividad y lineamientos de seguridad digital vigentes en Colombia, respecto a la utilización de canales y recursos electrónicos, para llevar a cabo la implementación de la normativa es relevante el compromiso de la alta dirección, construir procedimientos tanto para infraestructura como aplicaciones y educar al servidor público con el propósito de reaccionar con anticipación en caso de una amenaza digital.

Las medidas de seguridad informática que han asumido las diferentes entidades frente al trabajo en casa, evidenciaron que América Latina no está suficientemente preparada para enfrentar los ataques que se producen en el ciberespacio, pues la llegada de la pandemia fomentó el teletrabajo a nivel mundial y se implantó de forma apresurada, convirtiéndose en el blanco perfecto para los ciberataques.

9 RECOMENDACIONES

Implementar un sistema de gestión de seguridad de la información que cumpla con un estándar reconocido internacionalmente como ISO 27001, que ayuda a las organizaciones a fortalecer la seguridad de los datos y mitigar el riesgo de violaciones de datos, aborda la gestión de activos, seguridad operativa, control de acceso, gestión de incidentes, seguridad de recursos humanos y seguridad física.

Ajustar las políticas y los marcos legales y todas las partes interesadas de la sociedad civil, así como los sectores públicos y privado, deben trabajar para crear una cultura de ciberconciencia y capacitar a profesionales calificados para construir una estrategia de ciberseguridad, es un esfuerzo continuo y complejo.

Involucrar a la alta dirección de la organización, concientizar, culturizar y hacer entender que el cibercrimen es un trabajo que implica aunar esfuerzos, junto con las entidades de control, Policía Nacional, que cuenta con el Centro de Capacidades para la Ciberseguridad de Colombia “C4” y hacen un constante seguimiento a este tipo de casos.

10 BIBLIOGRAFÍA

ACOSTA ARGOTE, Cristian Delito de suplantación de identidad aumentó 409% en 2020 debido a la pandemia. *Asuntos: legales.* [En línea]. Bogotá. 12 Abril 2021, [Consultado 10 de mayo de 2021]Disponible en: https://www.asuntoslegales.com.co/actualidad/delito-de-suplantacion-de-identidad-aumento-409-en-2020-debido-a-la-pandemia-3151651#:~:text=Judicial-,Delito%20de%20suplantaci%C3%B3n%20de%20identidad%20aument%C3%B3%20409,2020%20debido%20a%20la%20pandemia&text=La%20suplantaci%C3%B3n%20de%20identidad%2C%20seg%C3%BAn,se%20dispar%C3%B3%20a%201.527%20reportes.

AGUILERA, seguridad informática En: Martha Irene, ROMERO CASTRO et al. Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. Alcoy, Alicante, España, Editorial área de innovación y desarrollo, s.l2018, 1, pp. 14-15.978-84-949306-1-4

ANDINA, Agencia peruana de noticias. ¿Cómo prevenir un ciberataque en tu empresa?. *Agencia peruana de noticias.* [En línea]. Lima. 7 Noviembre2021, [Consultado 10 de mayo de 2021]. Disponible en: https://andina.pe/agencia/noticia-empresas-conoce-recomendaciones-a-fin-evitar-ciberataques-868527.aspx

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA. Requisitos para la gestión documental en sedes electrónicas, ventanillas únicas y portales transversales. Guía de requisitos. Bogotá D. C.: 2021. 36 p. [Consultado 15 de noviembre de 2021]. Disponible en:

https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/Guia_Requisitos_GD_en_SedesElectronicas.pdf

ARIAS, Álvaro y Garzón Jhon. Guía lineamientos para el uso de documentos electrónicos en la contingencia generada por la emergencia sanitaria Covid-19. Guía. Bogotá D. C.: 2020. 45 p. [Consultado 27 de mayo de 2021]. Disponible en: https://secretariageneral.gov.co/sites/default/files/documentos/guia-de-lineamientos-para-el-uso-de-documentos-electronicos_2020.pdf

BANCO BILBAO VIZCAYA ARGENTARIA- BBVA. Cómo teletrabajar de forma segura desde casa. *Ciberseguridad.* [En línea]. España. 15 Febrero 2021, [Consultado 5 de noviembre de 2021]. Disponible en: https://www.bbva.com/es/como-teletrabajar-de-forma-segura-desde-casa/

BANCO INTERAMERICANO DE DESARROLLO, Reporte de ciberseguridad 2020En: Farah, URRUTIA. Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el CARIBE. EUA: BID, 2020. pp. 12-13.

BOHÓRQUEZ, Astrid y VELÁSQUEZ Magda. Propuesta de seguridad informática para promover la ejecución de teletrabajo en la mesa de ayuda de una empresa de telecomunicaciones. Trabajo de grado especialización en seguridad informática. Bogotá.: Universidad piloto de Colombia. Facultad de Postgrados2015. 147 p. (Recuperado en 25 de Junio de 2021.) Disponible en http://polux.unipiloto.edu.co:8080/00002858.pdf

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Seguridad aplicada al fortalecimiento de las empresas (SAFE). *Ciberseguridad en entornos cotidianos. Estudios.* [En línea]. Bogotá. Diciembre 2020, [Consultado 6 de junio de 2021]. Disponible en: https://www.ccit.org.co/estudios/ciberseguridad-en-entornos-cotidianos-estudio-del-cibercrimen-2020/

CASTILLO, Alejandra. Las nuevas amenazas al teletrabajo. [En línea]. PWC Chile Revista Gerencia. Chile.: 2020. (Recuperado en 20 de Octubre de 2021.) Disponible en https://www.pwc.com/cl/es/prensa/prensa/2020/Las-nuevas-amenazas-al-teletrabajo.html

CENTRO DE CIBERSEGURIDAD GAMMA INGENIEROS. COVID-19: recomendaciones de ciberseguridad para trabajo en casa. *Blog Cyberacademy.* [En línea]. Bogotá. 27 Abril 2020, [Consultado 15 de mayo de 2021]. Disponible en: https://gammacyberacademy.com/blog/f/covid-19-recomendaciones-de-ciberseguridad-para-la-medida-de-tra

CHAVERRA Mojica, J. J., Restrepo Vélez, H. de J., & Pérez García, J. F. El teletrabajo y la seguridad de la información empresarial. *Revista CINTEX.* [En línea]. Medellín. 2015, vol. 20, nro. 1. p. 111– 121. [Consultado 13 de junio de 2021]0122-350X. Disponible en: https://revistas.pascualbravo.edu.co/index.php/cintex/article/view/33

COLOMBIA. CONGRESO DE COLOMBIA. Ley 1221 (16, Julio, 2008). Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras

disposiciones. Diario Oficial. Bogotá, D.C., 2008. , no. 47052. p. 11 - 13(Consultado en 30 de Julio de 2021.) Disponible en http://svrpubindc.imprenta.gov.co/diario/view/diarioficial/detallesPdf.xhtml

COLOMBIA. CONGRESO DE COLOMBIA. Ley 1437 (18, Enero, 2011). Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Diario Oficial. Bogotá, D.C., 2011. , no. 47956. p. 1 - 28. (Consultado en 3 de Agosto de 2021.) Disponible en http://svrpubindc.imprenta.gov.co/diario/view/diarioficial/detallesPdf.xhtml

COLOMBIA. CONGRESO DE COLOMBIA. Ley 2088 (12, Mayo, 2021). Por la cual se regula el trabajo en casa y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2021. , no. 51672. p. 1 - 3. (Consultado en 11 de Septiembre de 2021.) Disponible en http://svrpubindc.imprenta.gov.co/diario/view/diarioficial/detallesPdf.xhtml

COLOMBIA. CONGRESO 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. Diario Oficial. Bogotá, D.C., 1999. , no. 43673. p. 21(Consultado en 18 de Agosto de 2021.) Disponible en http://svrpubindc.imprenta.gov.co/diario/view/diarioficial/detallesPdf.xhtml

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 100 (23, Diciembre, 1993). Por la cual se crea el sistema de seguridad social integral y se dictan otras disposiciones.

Diario Oficial. Bogotá, D.C., 1993. , no. 41148. p.1-168.(Consultado en 27 de Agosto de 2021.) Disponible en http://svrpubindc.imprenta.gov.co/diario/view/diarioficial/detallesPdf.xhtml

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN Y OTROS. CONPES 4012 (30, Noviembre, 2020). Política nacional de comercio electrónico. Bogotá, D.C., 2020. 77 p. (Consultado en 3 de Septiembre de 2021.) Disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4012.pdf

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. CONPES 3995 (1, Julio, 2020). Política nacional de confianza y seguridad digital. Bogotá, D.C., 2020. 51 p. (Consultado en 18 de Junio de 2021.) Disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

COLOMBIA. MINISTERIO DE INTERIOR Y DE JUSTICIA Y OTROS. CONPES 3701 (14, Julio, 2011). Lineamientos de política para ciberseguridad y ciberdefensa. Bogotá, D.C., 2011. 43 p. (Consultado en 22 de Septiembre de 2021.) Disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

COLOMBIA. MINISTERIO DE JUSTICIA Y DEL DERECHO. Decreto 491 (28, Marzo, 2020). Por el cual se adoptan medidas de urgencia para garantizar la atención y la prestación de los servicios por parte de las autoridades públicas y los particulares que cumplan funciones públicas y se toman medidas para la protección laboral y de los contratistas de prestación de servicios de las entidades públicas, en el marco del Estado de Emergencia Económica, Social y Ecológica. Diario Oficial.

Bogotá, D.C., 2020. , no. 51270. p. 4 - 7(Consultado en 11 de Octubre de 2021.) Disponible en
http://svrpubindc.imprenta.gov.co/diario/view/diarioficial/detallesPdf.xhtml

COLOMBIA. MINISTERIO DE JUTSICIA Y DEL DERECHO. Decreto 806 (4, Junio, 2020). Por el cual se adoptan medidas para implementar las tecnologías de la información y las comunicaciones en las actuaciones judiciales, agilizar los procesos judiciales y flexibilizar la atención a los usuarios del servicio de justicia, en el marco del Estado de emergencia Económica, Social y Ecológica. Diario Oficial. Bogotá, D.C., 2020. , no. 51335. p. 61 - 68. (Consultado en 19 de Octubre de 2021.) Disponible en
http://svrpubindc.imprenta.gov.co/diario/view/diarioficial/detallesPdf.xhtml

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Y OTROS. CONPES 3854 (11, Abril, 2016). Política nacional de seguridad digital. Bogotá, D.C., 2016. 91 p. (Consultado en 12 de Agosto de 2021.) Disponible en
https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

COLOMBIA. MINISTERIO DE TECNOLOGíAS DE LA INFORMACiÓN Y LAS COMUNICACIONES. Decreto 464 (23, Marzo, 2020). Por el cual se disponen medidas con el fin de atender la situación de emergencia económica, social y ecológica de la que trata el Decreto 417 de 2020. Bogotá, D.C., 2020. No aparece publicado en el Diario oficial. 8 p.(Consultado en 6 de Septiembre de 2021.) Disponible en
https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20464%20DEL%2023%20DE%20MARZO%20DE%202020.pdf

COLOMBIA. MINISTERIO DE TECNOLOGíAS DE LA INFORMACiÓN Y LAS COMUNICACIONES. Resolución 1519 (24, Agosto, 2020). Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos. Diario Oficial. Bogotá, D.C., 2020. , no. 51521. p. 1 - 78(Consultado en 21 de Noviembre de 2021.) Disponible en
http://svrpubindc.imprenta.gov.co/diario/view/diarioficial/detallesPdf.xhtml

COLOMBIA. MINISTERIO DEL INTERIOR. Decreto 457 (22, Marzo, 2020). Por el cual se imparten instrucciones en virtud de la emergencia sanitaria generada por la pandemia del Coronavirus COVID-19 y el mantenimiento del orden público. Diario Oficial. Bogotá, D.C., 2020. , no. 51264. p. 1 - 4 (Consultado en 13 de Agosto de 2021.) Disponible en
http://svrpubindc.imprenta.gov.co/diario/view/diarioficial/detallesPdf.xhtml

COLOMBIA. PRESIDENCIA DE LA REPUBLICA. Decreto 411 (16, Marzo, 2020). Por el cual se toman medidas transitorias debido a la emergencia sanitaria relacionada con el COVI 0-19 con respecto al régimen de zonas francas. Diario Oficial. Bogotá, D.C., 2020. , no. 51258. p. 34 - 35. (Consultado en 9 de Julio de 2021.) Disponible en
http://svrpubindc.imprenta.gov.co/diario/view/diarioficial/detallesPdf.xhtml

COLOMBIA. PRESIDENCIA DE LA REPUBLICA. Decreto 417 (17, Marzo, 2020). Por el cual se declara un Estado de Emergencia Económica, Social y Ecológica en todo el territorio Nacional. Diario Oficial. Bogotá, D.C., 2020. , no. 51259. p. 1 - 5

(Consultado en 21 de Mayo de 2021.) Disponible en http://svrpubindc.imprenta.gov.co/diario/view/diarioficial/detallesPdf.xhtml

COMPUTER WORLD UNIVERSITY. Los ciberataques cuestan al sector educativo una media de 2,34 millones de euros. *La excelencia de la profesión TI.* [En línea]. España. 05Noviembre 2021, [Consultado 4 de junio de 2021]. Disponible en: https://www.computerworlduniversity.es/ciberseguridad/los-ciberataques-cuestan-al-sector-educativo-una-media-de-234-millones-de-euros

DAPRE COLOMBIA Normativa. Directivas. [En línea]. Normativa. Bogotá.: 2021. (Recuperado en 10 de Noviembre de 2021.) Disponible en https://dapre.presidencia.gov.co/normativa/directivas

DAVILA PERALTA, Antonio Eduardo. Infección por SARS-CoV2, epidemiología, manifestaciones clínicas, inmunología: tratando de entender la enfermedad. *Revista de Investigación Universitaria en Salud.* [En línea]. La Plata, Argentina. 18 Mayo 2020. vol. 2, p. 15-23[Consultado 16 de octubre de 2021]Disponible en: https://publicaciones.uap.edu.ar/index.php/revistaRIUS/article/view/908

ESPITIA, Daniel. Nueva investigación de Fortinet indica que las empresas deben adaptarse para afrontar los retos de seguridad del teletrabajo a largo plazo. *Los Libertadores Fundación Universitaria.* [En línea]. Bogotá. 14 Septiembre 2020, [Consultado 8 de julio de 2021]. Disponible en: https://www.ulibertadores.edu.co/era-digital-el-ciberataque-como-un-arma-silenciosa/

GÓMEZ, Álvaro. Enciclopedia de la seguridad informática. España. Alfaomega Grupo Editor2007. 828 p. ISBN 9701512669, 9789701512661[Consultado 10 de diciembre de 2021]. Disponible en: https://www.ra-ma.es/libro/enciclopedia-de-la-seguridad-informatica-2a-edicion_48115/

GONZALEZ, Jefferson. Estudio del estado actual de la seguridad informática en las organizaciones de Colombia. Proyecto de grado Especialización en seguridad informática. Buga. Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería2020. 90 p. (Recuperado en 8 de Noviembre de 2021.) Disponible en https://repository.unad.edu.co/bitstream/handle/10596/36669/jgonzalezlon.pdf?sequence=1&isAllowed=y

GRUPO BANCOLOMBIA. Equipo Editorial. Medidas de ciberseguridad en la empresa por parte de líderes. *Capital Inteligente.* [En línea]. Medellín. 30Julio 2020. [Consultado 13 de junio de 2021]Disponible en: https://www.grupobancolombia.com/wps/portal/empresas/capital-inteligente/especiales/preguntas-y-respuestas-webinar-ie/ciberseguridad-en-empresas-por-pandemia-contingencia

GRUPOBANCOLOMBIA. 5 Claves para implementar el teletrabajo en medio del coronavirus. [En línea]. Tendencias. Medellín.: 2020. (Recuperado en 9 de Septiembre de 2021.) Disponible en https://www.bancolombia.com/wps/portal/negocios/actualizate/tendencias/teletrabajo-en-colombia-en-medio-del-coronavirus

GRUPOBANCOLOMBIA. Medidas de ciberseguridad empresarial por contingencia. [En línea]. Capital inteligente. Medellín.: 2020. (Recuperado en 11 de Noviembre de 2021.) Disponible en https://www.bancolombia.com/wps/portal/empresas/capital-inteligente/especiales/preguntas-y-respuestas-webinar-ie/ciberseguridad-en-empresas-por-pandemia-contingencia/!ut/p/z1/pZBBb4MwDIV_UuwkhOTIRkkCNBCxjC6XiVOFtHU9VP39zRDrYdLYpPlm-Xu23yORHEg8Tdf5OF3mj9P0lvqXKF6pVhYbjk4KlYHvbadLa-lThWRcAPihCiDxL3qO4tFwCa027QMUJuNQOcZA8v_pRbboN9aPvxmM2_ZGEhdEaFUg_TyhZBrsRBC73KMGtgJbEW1uaOgK3J_swkDBG8aZ61qT9_w7oCsnwA-VlM_lXrEaV-CeA5Q-gwKlNn1tdb__AmpU1mACJPAEiMY1tkw5DTk5v4cQDjDb2R5vS2lnRw!!

HARÁN, Juan Manuel. Resumen con las 10 noticias de seguridad más destacadas que dejó el 2020. [En línea]. WELIVESECURITY. Bratislava.: Eslovenia, 2021. (Recuperado en 18 de Junio de 2021.) Disponible en https://www.welivesecurity.com/la-es/2021/01/05/las-10-noticias-seguridad-informatica-mas-destacadas-2020/

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Documentación, Presentación de tesis, trabajos de grado y otros trabajos de investigación NTC 1486Bogotá D.C.: El Instituto, 2008. 41 p. [Consultado 8 de julio de 2021]. Disponible en https://academia.utp.edu.co/seminario-investigacion-II/files/2017/03/Norma_Tecnica_Colombiana_NTC_1486_completa_archivo.pdf

JODKA Sara y GREEN Caleb. COVID-19 plantea mayores riesgos de ciberseguridad para empleadores y empresas. [En línea]. Mibiz reportes de

negocios. Detroit. Dickinson Wright. 2020. (Recuperado en 6 de Noviembre de 2021.) Disponible en https://mibiz.com/sponsored-content/covid-19-poses-increased-cybersecurity-risks-to-employers-and-businesses

LÓPEZ, Valentín. Valor probatorio del documento electrónico. *Informática y Derecho: revista iberoamericana de Derecho informático.* [En línea]. España. 1995. vol. 8, p. 133-174. [Consultado 29 de agosto de 2021]1136-288X. Disponible en: https://dialnet.unirioja.es/servlet/revista?codigo=1710

LOS LIBERTADORES FUNDACIÓN UNIVERSITARIA. Era digital: el ciberataque como un arma silenciosa. [En línea]. Noticias. Bogotá.: 2020. (Recuperado en 4 de Julio de 2021.) Disponible en https://www.ulibertadores.edu.co/era-digital-el-ciberataque-como-un-arma-silenciosa/

MARRIERO, Yran. La Criptografía como elemento de la seguridad informática. *ACIMED.* [En línea]. La Habana, Cuba. 2003, vol. 11 nro. 6. [Consultado 26 de julio de 2021] ISSN 1024-9435. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012

MINISTERIO DE TECNOLOGíAS DE LA INFORMACiÓN Y LAS COMUNICACIONES. Normativa. Compilación jurídica sector Tic. Covid 19. [En línea]. Normativa. Bogotá.: 2021. (Recuperado en 10 de Octubre de 2021.) Disponible en https://www.mintic.gov.co/portal/inicio/Normatividad/

MINISTERIO DE TECNOLOGíAS DE LA INFORMACiÓN Y LAS COMUNICACIONES. Todo lo que se debe saber sobre el teletrabajo. [En línea]. Bogotá. 12 Marzo 2020, [Consultado 28 de septiembre 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

MINISTERIO DE TECNOLOGíAS DE LA INFORMACiÓN Y LAS COMUNICACIONES, Ministerio del Trabajo & Colombia Digital. Libro blanco. El ABC del teletrabajo en Colombia. Bogotá: Colombia digital2001. 97 p. [Consultado 10 de diciembre de 2021]. Disponible en: https://teletrabajo.gov.co/622/articles-8228_archivo_pdf_libro_blanco.pdf

MUSA, Nadya. Firma digital o escaneada, una decisión basada en la seguridad. *Asuntos : legales.* [En línea]. Bogotá. 09Abril 2020, [Consultado 14 de septiembre de 2021]. Disponible en: https://www.asuntoslegales.com.co/consultorio/firma-digital-o-escaneada-una-decision-basada-en-la-seguridad-2989926

NIMTIC. Nuevas medidas para la transformación digital de los sitios web de las entidades públicas definió el Ministerio de las TIC. Resolución 1519 de 2020. [En línea]. Bogotá. 17 Diciembre 2020, [Consultado 3 de agosto de 2021]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/161060:Nuevas-medidas-para-la-transformacion-digital-de-los-sitios-web-de-las-entidades-publicas-definio-el-Ministerio-de-las-TIC

NIPPON TELEGRAPH AND TELEPHONE CORPORATION. Las nuevas amenazas al teletrabajo. Digital Workplace Report, citado por revista gerencia. *Pwc.* [En línea]. Chile. 2020. [Consultado 16 de octubre de 2021]. Disponible en: https://www.pwc.com/cl/es/prensa/prensa/2020/Las-nuevas-amenazas-al-teletrabajo.html

OFICINA DE CIBERSEGURIDAD DEL INTERNAUTA. Guía de ciberataques. Guía. España.: Gobierno de España. Vicepresidencia Primera del Gobierno. ND. 46 p.[Consultado 27 de mayo de 2021]Disponible en: https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

PASQUALI,
Marina. Los intentos de phishing en tiempos de COVID-19. [En línea]. Ciberdelincuencia. Hamburgo.: Statista GmbH. 2020. (Recuperado en 3 de Junio de 2021.) Disponible en
https://es.statista.com/grafico/18427/intentos-de-phishing-durante-la-pandemia/

PONTIFICIA UNIVERSIDAD JAVERIANA. Manual de normas Icontec. [En línea]. Recurso centro de escritura. Cali.: Colombia. 2018. (Recuperado en 12 de Junio de 2021.) Disponible en
https://www.javerianacali.edu.co/centro-escritura/recursos/manual-de-normas-icontec

PORTAFOLIO. Cifras de ciberseguridad en Colombia prenden alarmas al cierre del 2020 _ Tendencias _ Portafolio. *Portafolio.* [En línea]. Bogotá. 10Diciembre 2020, [Consultado 31 de octubre de 2021]. Disponible en:
https://www.portafolio.co/tendencias/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020-547412

RAMONET, Ignacio. Ante lo desconocido… La pandemia y el sistema-mundo. *Le Monde Diplomatique en español.* [En línea]. La Habana, Cuba. 25Abril 2020, vol.

25nro. 4. [Consultado 5 de octubre de 2021]. Disponible en: https://mondiplo.com/la-pandemia-y-el-sistema-mundo

RODRÍGUEZ, Flavio. El DANE fue un blanco de un ataque cibernético. Centro de Operaciones de Ciberseguridad de Claro, Citado por Portafolio, Cifras de ciberseguridad en Colombia prenden alarmas al cierre de 2020. *Portafolio.* [En línea]. Bogotá. 10 Noviembre 2021, [Consultado 15 de noviembre de 2021]. Disponible en: https://www.portafolio.co/economia/gobierno/dane-fue-blanco-de-hackeo-o-ataque-cibernetico-558379

ROMERO CASTRO, Martha Irene et al. Introducción a la seguridad informática y el análisis de vulnerabilidades. In Introducción a la seguridad informática y el análisis de vulnerabilidades. Alcoy, Alicante, España: Editorial Área de Innovación y Desarrollo, S.L. 2018. 124 p.978-84-949306-1-4[Consultado 4 de diciembre de 2021]. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

SORO, José. La digitalización de documentos en la Administración de Justicia. *Ibersid: revista de sistemas de información y documentaciónIbersid.eu.* [En línea]. Zaragoza, España. 27 Junio 2014vol. 8, p. 49-53. [Consultado 15 de noviembre de 2021]ISSN 1888-0967. Disponible en: https://www.ibersid.eu/ojs/index.php/ibersid/article/view/4179/3794

UNE ASOCIACION ESPAÑOLA DE NORMALIZACION Tecnología de la información, Técnicas de seguridad, Código de prácticas para los controles de seguridad de la información. ISO / IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015España.: Norma Española2017. 5 p. [Consultado 8 de julio de 2021]Disponible en https://academia.utp.edu.co/seminario-investigacion-II/files/2017/03/Norma_Tecnica_Colombiana_NTC_1486_completa_archivo.pdf

URUEÑA, Francisco J. Ciberataques, la mayor amenaza actual. *Documento Opinión Instituto Español de estudios estratégicos.* [En línea]. España. 16 Enero 2015. 18 p. [Consultado 18 de octubre de 2021]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

VALBUENA, Sindy. ¿Qué debe tener en cuenta para teletrabajar sin poner en riesgo datos. RCN Radio. *RCN Radio.com.* [En línea]. Bogotá. 19 Marzo 2020 [Consultado 15 de mayo de 2021]. Disponible en: https://www.rcnradio.com/tecnologia/que-debe-tener-en-cuenta-para-teletrabajar-sin-poner-en-riesgo-sus-datos-y-dinero

ZAPATA, Nataly. COVID- 19: Estado de emergencia sanitaria, normas gubernamentales y los efectos laborales en Colombia. Monografía. Medellín.: Universidad EAFIT, Escuela de derecho, 2020. 109 p. [Consultado 6 de junio de 2021]Disponible en: https://repository.eafit.edu.co/bitstream/handle/10784/17110/Nataly_ZapataMoreno_2020.pdf?sequence=2&isAllowed=y