IMPORTANCIA DE LAS BUENAS PRÁCTICAS EN CIBERSEGURIDAD EN EL TRABAJO REMOTO DE ENTIDADES PÚBLICAS DE COLOMBIA EN ÉPOCA DE PANDEMIA

MYRIAM ORTIZ OSORIO

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

IMPORTANCIA DE LAS BUENAS PRÁCTICAS EN CIBERSEGURIDAD EN EL TRABAJO REMOTO DE ENTIDADES PÚBLICAS DE COLOMBIA EN ÉPOCA DE PANDEMIA

MYRIAM ORTIZ OSORIO

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

EDUARD MANTILLA TORRES
Director Trabajo de Grado

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

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

A David, mi hijo y hermana Alieth. Han sido fuente inspiradora en este proyecto y motivación para lograr la culminación, contra todos los inconvenientes presentados.

AGRADECIMIENTOS

Agradezco a los docentes de la Universidad Nacional Abierta y a Distancia -UNAD, que han hecho parte del desarrollo de mis estudios, en especial al Ingeniero Edward Mantilla ya que con sus observaciones y conocimientos ha aportado de manera significativa para la evolución no sólo de este documento, sino que también de mi crecimiento profesional.

Igualmente agradezco de manera especial a mi gran amigo Miguel Ángel Torres, quien con su apoyo incondicional, conocimiento técnico y voluntad aportó a la culminación de este objetivo.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

pág.

GLOSARIO

AMENAZA: Objeto o acción que puede impactar negativamente la seguridad informática.

CIBERSEGURIDAD: Conjunto de medidas de tipo documentales, procedimentales o técnicas que permiten salvaguardar un activo en el ciberespacio.

CISO: Se denomina así al colaborador de una organización encargado de ajustar las posibles decisiones en materia de seguridad, políticas y programas, con los objetivos organizacionales.

CONFIDENCIALIDAD: Se define como la certeza de que la información solo se utilizará para los medios que fue autorizada y que ninguna persona no autorizada tendrá acceso a la misma.

DISPONIBILIDAD: Se denomina a la garantía que se da de que la información será accesible en todo momento.

INTEGRIDAD: Garantía que se brinda de que la información no ha sido alterada.

PANDEMIA: Enfermedad de propagación global

POLÍTICA: Lineamiento de alto nivel sobre un tema específico que describe la posición de una organización.

RIESGO: El riesgo es la posibilidad de materialización de una amenaza.

SEGURIDAD: Conjunto de garantías que se otorgan en la protección de un activo.

TRABAJO REMOTO: Relativo a ejecutar actividades laborales de manera virtual, con ayuda de dispositivos electrónicos y/o pc

VPN: Red virtual privada que permite establecer conexión entre dos redes diferentes de forma segura.

VPS: Es un servidor virtual privado donde un mismo servidor físico es dividido en varios servidores virtuales.

VULNERABILIDAD: Toda aquella debilidad presente en un sistema informático que produce un riesgo para la seguridad de la información comprometiendo con esto la integridad.

RESUMEN

La situación generada por la transmisión del virus Covid-19 (Coronavirus), que fue declarada pandemia, llevo a las organizaciones no sólo de Colombia, sino a nivel global a implementar el trabajo remoto de forma masiva y casi espontánea, sin tener la oportunidad de implementar los controles necesarios con anticipación.

En ese orden de ideas proteger la información se hace fundamental, debido a que el incremento de las conexiones eleva los riesgos de ataques cibernéticos que ya se venían presentando y que con el transcurso de la pandemia se han incrementado.

Ahora bien, teniendo en cuenta las entidades públicas de Colombia, como caso de estudio, es necesario realizar un análisis que refleje el estado real en las nuevas condiciones, así como revisar qué medidas han tomado las áreas de tecnología de las instituciones para solventar y asegurar de alguna manera los riesgos y las posibles vulnerabilidades que se hayan generado en los sistemas informáticos de las entidades, por las razones expuestas anteriormente.

Es de mencionar que, aunque en su mayoría las instituciones cuentan con una infraestructura con un nivel de seguridad considerable no contaban con tan alto porcentaje de acceso remoto por sus empleados, ni ellos estaban tecnológicamente preparados para asumir adecuadamente esta nueva modalidad laboral. Asimismo, se genera la necesidad de disponer de mayor procesamiento y conectividad y habilitar acceso no solo a las aplicaciones sino también a datos.

Esto implica, entre otros temas, que se revisen las políticas de seguridad implantadas por las entidades públicas para el trabajo remoto y que permita reflejar el impacto que pueda tener la seguridad de la información, que se analicen los diferentes entornos tanto a nivel remoto como trabajo en sitio, que visualice los posibles riesgos en cada uno de ellos y finalmente, se hace necesario, relacionar una serie de buenas prácticas y recomendaciones que permitan incrementar de manera eficiente la Seguridad Informática.

Palabras clave: Buenas prácticas, Entidad, Pandemia, Seguridad, Trabajo Remoto.

ABSTRACT

The situation generated by the spread of the Covid-19 virus (Coronavirus), which was declared a pandemic, led organizations to implement remote work in a massive and almost spontaneous way, without having the opportunity to implement the necessary controls in advance.

In this context, the protection of information is vital, since as network connections increase, cyber risks such as malware, data theft or leakage and phishing increase, one of the most used attack vectors in 2019 by the cybercriminals and that with the course of the pandemic have increased.

In the case of public entities in Colombia, it is necessary to carry out an analysis that reflects the real state in the new conditions, as well as to review what measures have been taken by the institutions technology areas to solve and in some way ensure risks and risks. Possible vulnerabilities that have been generated in the entities computer systems, for the reasons stated above.

It is worth mentioning that, although most of the institutions have an infrastructure with a considerable level of security, they did not have such a high percentage of remote access by their employees, nor were the technologically prepared to adequately assume this new work modality. Likewise, there is need for greater processing and connectivity and enable access not only to applications but also to data.

This implies, among other issues, that the security policies implemented by public entities for remote work are reviewed and that it allows to reflect the impact that information security nay have, that the different environments are analyzed both remotely and at work on site, which visualizes the possible risks in each one of them and finally, it is necessary to relate a series of good practices and recommendations that allow an efficient increase in Information Security.

Keywords: Goog practices, Entity, Pandemic, Remote Work, Security

INTRODUCCIÓN

Es evidente que el año 2020 ha sido el inicio de grandes cambios sin precedentes a nivel mundial, la declaración de pandemia por el brote de coronavirus, ha obligado a tomar medidas drásticas de confinamiento que, a su vez, gran parte de la fuerza laboral debió quedarse en casa y trabajar a distancia o mediante acceso remoto. Tanto las empresas que ya venían realizando actividades con esta modalidad como las que no, enviaron sus empleados a casa y de esta forma se generó el experimento de teletrabajo más extenso y masivo de la historia, en condiciones óptimas en algunos casos como en otros no tanto.

En las entidades públicas de Colombia, objeto de este estudio, no ha sido diferente la situación, aunque es de resaltar que en un contexto como el que se vive ahora por cuenta del COVID-19, el trabajo remoto sin duda ha sido un instrumento de gran aporte para la continuidad laboral.

No obstante, así como ha sido un aporte, también ha generado grandes retos a nivel tecnológico y de seguridad informática, por el crecimiento descontrolado de ataques cibernéticos a los que han sido sometidas las entidades por el aumento significativo de conexiones, uso de redes, acceso a aplicaciones de forma remota, que no estaba contemplada en esa magnitud. De acuerdo con las últimas estadísticas del Centro Cibernético de la Policía Nacional, en los primeros meses de pandemia se detectaron aproximadamente 17.211 denuncias por delitos informáticos, representando un aumento del 59% en relación con los mismos meses del 2019.[1] Estas estadísticas lo que demuestra es una real amenaza a la seguridad de la información en las instituciones.

Para dar respuesta al panorama planteado, se han establecido tres objetivos específicos que llevarán a reflejar como primera instancia una revisión de políticas de ciberseguridad para identificar cuáles están aplicando las entidades públicas. Seguidamente se realizará un análisis que muestre las diferencias del trabajo remoto vs. trabajo en sitio en las actuales circunstancias y por último se dispondrá de unas recomendaciones de buenas prácticas en esta modalidad laboral para las entidades públicas de Colombia, que evidenciarán la importancia de dichas prácticas en la ciberseguridad para el trabajo remoto.

Sin duda, el aprovechamiento y consulta de los diferentes documentos que se han generado recientemente por expertos del tema tanto en ciberseguridad como de teletrabajo y buenas prácticas tanto a nivel de investigación como académico, será un gran aporte al desarrollo de este documento, que permitirá integrar diferentes puntos de vista, así como avances temáticos y tecnológicos.

[1] CENTRO CIBERNÉTICO POLICÍA NACIONAL. Bogotá, D.C. [En línea]. 2020. Disponible en: https://caivirtual.policia.gov.co/

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

El 11 de marzo de 2020, la Organización Mundial de la Salud (OMS), consideró el nuevo brote por un coronavirus (Covid-19), como Pandemia. Dicho brote inició en la provincia de Hubei (China), con alto riesgo de propagación a nivel mundial[2].

Este nuevo contexto mundial ha obligado a todos los gobiernos, sector salud, sociedad, organizaciones empresariales y los mismos ciudadanos a asumir responsabilidades y drásticos cambios en el entorno tanto familiar como laboral, para lograr controlar la propagación del virus. Dentro de las medidas tomadas para poder contrarrestar los efectos, se estableció no sólo en Colombia, sino también en diferentes países del mundo el trabajo remoto.

Ahora bien, teniendo en cuenta el contexto actual, debido a la reciente Pandemia del Covid 19, se ha generado una carga masiva y simultánea de trabajo remoto, que ha obligado a las entidades públicas de Colombia a cuestionarse si realmente se está preparado para enfrentar los temas relevantes a la ciberseguridad y se tiene en uso un protocolo de buenas prácticas o si por el contrario, esta nueva modalidad laboral se puede convertir en un foco de vulnerabilidades, al habilitar el trabajo remoto al total de empleados, dado que en su mayoría los equipos no son de la entidad sino que son de propiedad del empleado y que no se encontraban configurados de la manera apropiada para estos casos.

Cabe resaltar, que ya antes se estaba tomando en cuenta esta forma de trabajo como iniciativa del gobierno, buscando adoptar esta tendencia con la finalidad de bajar los índices de desempleo y hay muchas entidades públicas que ya lo venían realizando, sin embargo, no se tenía contemplado de manera generalizada, como sucedió en las actuales circunstancias por la Pandemia.

Como referente también se va a tener en cuenta el Estudio que presentó la Federación Colombiana de Gestión Humana (ACRIP), el cual revela que, en Colombia en promedio, una de cada dos empresas no cuenta con las políticas o procedimientos de trabajo remoto establecido previamente a la pandemia, sin embargo un 11,2% si contaban con procedimientos de actividades para teletrabajo.[3]

---

[2]ORGANIZACIÓN PANAMERICANA DE LA SALUD – OPS. [En línea] 2020. Disponible en: https://www.paho.org/es/tag/enfermedad-por-coronavirus-covid-19?topic=All&d%5Bmin%5D=&d%5Bmax%5D=&page=25

[3]PORTAFOLIO. Empleados admiten que ahora trabajan más. [En línea]. 2020. Disponible en: https://www.portafolio.co/negocios/empresas/que-tan-preparadas-estaban-las-empresas-colombianas-para-el-trabajo-remoto-541592

Desde otra perspectiva, teniendo en cuenta una gran parte de usuarios, en este caso empleados se conectan a través de redes personales inalámbricas, lo cual puede generar vulnerabilidades, dado que en su mayoría las redes inalámbricas se encuentran totalmente desprotegidas. Muchas de las redes personales sólo incorporan el protocolo WEP (Wired-Equivalente Privacy) como medida de protección, que han demostrado ser inseguras, lo cual las convierte muy vulnerables y fáciles de acceder para un atacante conectar a una WLAN[4].

Es por lo anterior, que estos riesgos han permitido que los líderes de la seguridad de la información tomen las medidas pertinentes para abordar el tema de manera eficaz para enfrentar los desafíos de la Ciberseguridad y fortalecer las buenas prácticas. Dado que también es importante mencionar que sin estas herramientas que permiten el acceso remoto las entidades públicas no hubieran podido mantenerse competitivas ni cumplir con sus objetivos misionales en las circunstancias descritas, aunque eso haya significado un riesgo de seguridad informática.

Recientemente en una publicación de la Revista Dinero, el Jefe de Soluciones de Industria del Centro de Ciberseguridad del WEF, Georges de Moura, manifestó que el proceso precipitado hacia la virtualidad al que obligó la pandemia del Covid-19, exige que los líderes mundiales, así como sus organizaciones, precisen mecanismos para mitigar los riesgos en materia de cibernética y así como también se debe acelerar la transformación digital con la finalidad de obtener los beneficios que logren el equilibrio entre agilidad, escalabilidad, eficiencia, rentabilidad y ciberseguridad[5].

Para sintetizar lo anterior, en la tabla 1 se presenta un resumen de los referentes que se tuvo en cuenta como apoyo para este planteamiento.

[4] ÁLVAREZ MARAÑÓN, Gonzalo. Seguridad informática para empresas y particulares. Madrid etc, Spain: McGraw-Hill (2004). España. [En línea]. Recuperado en Pp. 20 – 41. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/50050?page=1

[5] REVISTA DINERO. alerta sobre aumento dramático de riesgos en ciberseguridad tras la pandemia. WEF. [En línea]. Disponible en: [https://www.dinero.com/internacional/articulo/aumento-dramatico-de-riesgos-en-ciberseguridad-tras-la-pandemia/286804

Tabla 1. Referentes de Investigación

Título	Autores	Año	País	Descripción
Reporte CIBERSEGURIDAD, Riesgos, Avances y el camino a seguir en América Latina	Banco Interamericano de Desarrollo	2020		El reporte describe de forma detallada el estado actual en tema de ciberseguridad en todos los países de América Latina y El Caribe y en el cual evidencia que sólo 7 de los 32 países cuenta con un plan de protección a su infraestructura.
Insight Report Cyber Information Storing: Bulding Collective Security	World Economic Forum -WEF	2020	Switzerland	El documento refleja los problemas que enfrenta el mundo el día de hoy, en ciberseguridad, relata cómo se ha transformado en esta última década la tecnología. Enfatiza la ciberseguridad como un pilar de una sociedad digitalmente resiliente y hace referencia al impacto potencial de los ataques de hoy en día, debido a la pandemia.
Informe sobre el Teletrabajo/trabajo no presencial	Organización Iberoamericana de Seguridad Social	2020	España	El documento presenta en detalle la relación de medidas tomadas por cada uno de los países iberoamericanos sobre el teletrabajo frente a la COVID-19.
Manual de Gobierno Digital. Implementación de la Política Digital Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2)	Ministerio de Tecnologías de la Información y las Comunicaciones	2019	Colombia	El documento contiene la Política de Gobierno Digital que da lineamientos y acciones en esta temática para todas entidades públicas de Colombia.
Medición del Teletrabajo en Entidades Públicas de Colombia.	Centro Nacional de Consultoría	2019	Colombia	El Informe presenta importantes estadísticas como resultado de una encuesta hecha en octubre de 2019 a las entidades públicas, en relación a la percepción e inclusión del teletrabajo.

Fuente: elaboración propia

1.2 FORMULACIÓN DEL PROBLEMA

Dentro de ese orden de ideas del ítem anterior, se ve reflejada la necesidad por parte de las entidades públicas de Colombia de hacerle frente al desafío de la Ciberseguridad y de la necesidad de buenas prácticas para el trabajo remoto, ya que uno de los objetivos es propiciar confianza tanto a nivel interno como externo de la organización, proyectando un manejo seguro de la información, pero que por la alta demanda de acceso remoto en estos momentos, se ha contemplado como un riesgo que hay que enfrentar y se vuelve un reto.

Siendo las cosas así, surge el siguiente interrogante:

¿Cómo a partir de la aplicación de buenas prácticas en las entidades públicas, puede contribuir en la reducción de brechas de seguridad en el trabajo remoto?

2 JUSTIFICACIÓN

Evidenciar la importancia de las buenas prácticas en ciberseguridad para el trabajo remoto de las entidades públicas de Colombia, es un factor relevante dada la situación actual de pandemia por el Covid-19.

La habilitación del trabajo remoto de manera masiva en la mayoría de las organizaciones ha expuesto la seguridad informática a exposición de diferentes riesgos debido a la improvisación general y repentina.

La Ciberseguridad desde esta nueva perspectiva global en el trabajo remoto, se vuelve un papel fundamental para todos, su implementación de manera correcta no solo permitirá confianza y sostenibilidad en esta modalidad laboral, sino que gracias a ella se puede proteger los datos de las constantes amenazas, las cuales ya han sido exponencialmente notorias por los múltiples ciberataques ocurridos en este último año específicamente en las entidades públicas de Colombia, objeto de este estudio.

La Seguridad de la información tiene diversos conceptos definidos, uno de ellos lo define como la temática que se encarga de la gestión de los riesgos de los sistemas informáticos. Es decir, que, a través de la aplicación de sus principios, se implementarán tanto en la infraestructura como en los aplicativos informáticos medidas de seguridad que buscan contrarrestar amenazas que se encuentran expuestas en los activos de la organización: la información y los elementos hardware y software que la soportan.[6]

Cada día se presentan nuevas maneras de atentar contra la privacidad y seguridad de la información de las entidades, delitos informáticos que cada vez son más frecuentes y que ponen en riesgo la confidencialidad, integridad y disponibilidad de los datos.

Tecnológicamente, se pretende disponer de unas buenas prácticas de ciberseguridad para el trabajo remoto, teniendo en cuenta que son parte fundamental para cumplir el objetivo de la disminución de los riesgos tecnológicos como de seguridad para la información, así como un factor de protección y sostenibilidad en el proceso de las organizaciones, del estado y la sociedad. Éstas dependerán de las características de cada entidad, de sus posibilidades y nivel de madurez. Sin embargo, las presentadas aquí constituyen una batería de contramedidas que seguramente disminuirán los niveles de riesgo y harán que la organización pueda operar en forma casi normal durante el período que dure esta

[6] ÁLVAREZ MARAÑÓN, Gonzalo. Seguridad informática para empresas y particulares. Madrid etc, Spain: McGraw-Hill (2004). [En línea]. España. Recuperado en Pp. 20 – 41. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/50050?page=1

modalidad laboral y luego de su implementación definitiva, consolidando una defensa sólida en la lucha contra ataques y vulneraciones informáticas**.**

Asimismo, es importante mencionar que las tecnologías de la información están en una constante evolución, que obliga a las organizaciones a mantener al día la actualización de todos sus componentes y a la academia a procurar que sus programas estén también actualizados para que contribuyan a la idoneidad de los profesionales de esta rama y que dicho conocimiento sea plasmado de manera precisa y segura en el entorno informático.

Por último, cabe resaltar que la Ciberseguridad es de crucial relevancia en cualquier organización y más si se desea mantener un alto nivel de competitividad que genere confiabilidad en todos los aspectos de la seguridad de la información para la entidad como para su clientes.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Construir un documento monográfico que permita reseñar la importancia de buenas prácticas en ciberseguridad para el trabajo remoto en época de pandemia en entidades públicas de Colombia

3.2 OBJETIVOS ESPECÍFICOS

- Esquematizar cuáles son las políticas y buenas prácticas que se están aplicando en el trabajo remoto en las entidades públicas colombianas con el fin establecer su impacto en las dimensiones de la seguridad de la información

- Analizar las diferencias de trabajo remoto y trabajo en sitio para determinar cuáles pueden ser los riesgos que se relacionan con la ciberseguridad en cada una de las modalidades.

- Establecer una serie de recomendaciones de buenas prácticas de ciberseguridad que puedan ser aplicadas para el trabajo remoto en entidades públicas colombianas, con el fin de contribuir en la reducción de brechas de inseguridad.

3.3 MARCO TEÓRICO

Como fue reportado por la Organización Mundial de la Salud (OMS), el 11 marzo de 2020, la propagación de virus por el coronavirus, fue declarada como Pandemia[7] y hace un llamado a todas las naciones para que sean adoptadas las medidas que sean necesarias, urgentes y contundentes, para frenar dicha propagación.

Esta declaración lo que busca es promover la salud pública. Sin embargo, es claro que la afectación es a un nivel general para todos los sectores, como son el social, económico, laboral, entre otros.

Este nuevo hecho, obliga a todos los países a asumir grandes retos y drásticos cambios tanto del sector salud, sociedad y en todas las comunidades en general como en las organizaciones empresariales, con el fin buscar la disminución de propagación del virus. Una de las medidas más contundentes fue establecer el trabajo remoto, no sólo en Colombia, sino que a nivel mundial. Colombia lo formaliza a través del Ministerio del Trabajo expidiendo la Circular 0041 del 2 de junio de 2020 de la Presidencia de la República, en el cual menciona que para solventar la contingencia del COVID-19, se debe impulsar la prestación del servicio por medio del trabajo en casa o teletrabajo con la ayuda de tecnologías de la información y las telecomunicaciones -TIC.[8]

Sin lugar a duda, la pandemia logró reestructurar entre otros temas, la forma de laboral y la tecnología se convirtió en un instrumento indispensable que permitió facilitar la nueva dinámica del trabajo.

Muchas organizaciones se cuestionan y se reinventan pensando en que este precedente cambiará por siempre la forma de trabajo en oficina como se conocía anteriormente y se deberá buscar su fortalecimiento cada día, sobre todo a nivel de seguridad de la información.

Al respecto Paola Villafuerte[9], menciona que, a largo plazo, el trabajo individual terminará realizando de forma remota en un 100%. Así como también se recalca que la evolución de la tecnología facilitó el generar la nueva dinámica de trabajo

---

[7] ORGANIZACIÓN MUNDIAL DE LA SALUD -OMS – [En línea]. 2020. Disponible en: https://www.who.int/es/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19 11-march-2020

[8] PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Circular 0041 de 2020. [En Línea]. Disponible en: https://www.mintrabajo.gov.co/documents/20147/60876961/Circular+0041-2020.PDF/98d19065-352d-33d2-978e-9e9069374144?t=1591222484807

[9] OBSERVATORIO DE INNOVACIÓN EDUCATIVA. La pandemia como un catalizador de una nueva cultura laboral. Paola Villafuerte. [En línea]. México. 2020. Disponible en: https://observatorio.tec.mx/edu-news/trabajo-remoto-postcovid19

remoto, dado que para eso es necesario un buena computadora y conectividad a internet.

Las cifras de aumento en esta nueva modalidad, se incrementaron hasta en 400%[10], según lo menciona, Jonnatan Arango, en el portal de Económicas.News, en un artículo relativo al trabajo en casa, en el cual también hace referencia a lo mencionado por el presidente de la Asociación de Gestión Humana, Acrip del Valle, en el sentido de que estas circunstancias como la de la cuarentena, lleva a tomar medidas de trabajo de remoto a las empresas que no tenían como prioridad esto y que de alguna manera se vieron forzadas hacerlo sin mucha experiencia.

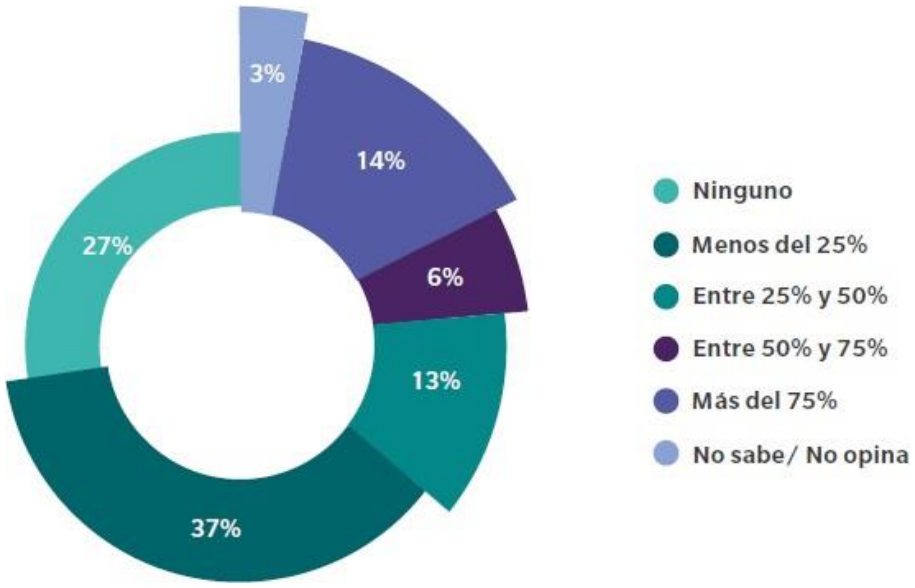
Según el último informe presentado por Microsoft y Marsh, evidencian que más de un 30% de las organizaciones de América Latina tuvieron un incremento del 31% de ataques cibernéticos a raíz de la pandemia por Coronavirus[11].

El informe está soportado por los resultados obtenidos mediante la encuesta sobre Riesgos Cibernéticos originados en tiempos de pandemia que se realizó en más de18 países. Entre los temas más relevantes del informe se menciona que de las empresas que implementaron el trabajo remoto de manera instantáneamente permitieron que aproximadamente el 70% de sus empleados trabajaran con equipos personales, lo que aumentó ampliamente la exposición a diferentes tipos de eventos cibernéticos, así como solo el 27% trabaja con los dispositivos de la organización. La figura 1 muestra dichos resultados.

[10] ARANGO, JONNATAN. Portal Económicas.News. 2020. [En línea]. Disponible en: https://economicas.news/2020/05/27/trabajo-desde-casa-en-colombia-con-mas-de-seis-millones-de-personas-por-la-pandemia/

[11] MARSH. MICROSOFT. Estado del Riesgo Cibernético en Latinoamérica en Tiempos de COVID-19. Octubre. 2020. [En línea]. Octubre 2020. Disponible en: https://coronavirus.marsh.com/mx/es/insights/research-and-briefings/report-cyber-risk-in-latin-america-in-times-of-covid19.html

Figura 1. Porcentaje del Total de Empleados trabajando con dispositivos personales y no de la organización.



Fuente: Encuesta de Marsh y Microsoft sobre Riesgo Cibernético en tiempos de Covid.

Los resultados también muestran que las organizaciones en algunos casos, tomaron las medidas pertinentes relacionadas con el incremento de presupuesto que ayudara a la implementación de controles que ayudara a mitigar de alguna forma los riesgos presentados. Sin embargo, no es una acción generalizada, por el contrario, se evidencian aún organizaciones que al no percibir situaciones de riesgo no toman medidas de protección, pero por el contrario debe ser por falta de herramientas o mecanismos necesarios que no detectan situaciones de riesgo.[12] Asimismo, con los resultados del informe se percibe la necesidad, de que las organizaciones cuenten con un seguro que cubra los riesgos cibernéticos, pero sólo el 17% de las empresas encuestadas manifestó contar con dicho seguro.

En materia de seguridad y por orden de prioridad se encontró que la protección de datos es lo que más busca protegerse, luego el acceso de manera remota y como última prioridad está la concientización de los riesgos a los empleados

[12] Ibid., p. 3

Otro referente a tener en cuenta también, son los resultados de la encuesta global hecha por la firma Morning Consult a nombre de IBM, la cual buscaba sustraer los comportamientos en materia digital en medio de la pandemia[13].

Dentro de los resultados se identificaron algunos comportamientos que llaman la atención como es la creación nueva en promedio de 15 cuentas en línea por persona encuestada, lo que lleva la creación de millones de cuentas nuevas y que probablemente no serán desactivadas ni eliminadas generando una huella digital más, pero como menciona el director de IBM, esto puede conllevar a un alto costo de la privacidad y seguridad de los datos.[14]

En el caso de los colombianos encuestados mostraron que el 50% conserva las contraseña de las cuentas en la memoria, mientras un 29% guardan las contraseñas en papel. Igualmente, aproximadamente dos terceras partes de los encuestados utilizan el protocolo de autenticación multifactor.

Por otro lado, las organizaciones deben asegurar la implementación de controles que eviten el acceso no autorizado y que se puedan encriptar los datos confidenciales.

Una de las grandes recomendaciones que finalmente hace IBM en relación con los resultados de la encuesta, es considerar la evolución de una seguridad de Confianza cero, lo que fortalecerá de manera significativa la seguridad de la información de las organizaciones, así como adoptar una gran serie de buenas prácticas.

Por su parte Colombia también presenta datos importantes de ciberseguridad del último año a través del Análisis realizado por parte de la Cámara Colombiana de Informática y Telecomunicaciones – CCIT con base en informes y tendencias sobre el tema tanto a nivel nacional como global.

Al respecto del análisis mencionado anteriormente, el presidente ejecutivo de la CCIT, hace referencia entre otros temas, a la importancia de que tanto las organizaciones como los empleados sean conscientes y responsables con la ciberseguridad, dada la virtualidad acrecentada en medio de la pandemia lo que

[13] MORNING CONSULT. IBM SECCURITY. IBM Consumer Survey: Security Side: Effects Of the Pandemic. [En línea]. Junio 2021. Disponible en: https://filecache.mediaroom.com/mr5mr_ibmnews/191177/Pandemic%20Security%20Side%20Effects%20Global%20Survey_IBM%20Analysis.pdf

[14] Ibid., p. 2

hace más atractivo para los delincuentes y el enfoque debe ser dirigido a la protección del activo más valioso en cualquier entidad como son los datos.[15]

El análisis o estudio también señala de acuerdo con las cifras presentadas por la fiscalía general, que el ciberataque más reportado este último año y hasta mediados del 2021, fue la Violación de Datos Personales con más de 6500 casos, que en comparación con el 2020 se incrementó en más del 100%[16]. La técnica más usada por los delincuentes sigue siendo a través del envío masivo de correo electrónico phishing.

La siguiente o segunda tendencia de ataque denunciada con un 33% es la suplantación de sitios WEB, siendo el foco para la explotación de vulnerabilidades de los sistemas operativos que se encuentran en muchos casos desactualizados.

La modalidad que ocupa el tercer puesto con mayor incremento en comparación al 2020, es el Acceso Abusivo a Sistema Informático. Este ataque está asociado a intrusos que en muchos casos pertenecen a la misma organización y que a través de escritorio remoto o puertas traseras, haciendo uso a través de usuarios con privilegios de nivel alto.

En el mismo informe Juan Hover González, del centro de operaciones de la firma Claro, menciona la evolución en las técnicas para la extorsión de datos. Ahora, más del 70% de los ataques detectados fueron dirigidos a organizaciones con alto valor e igualmente a funcionarios con nivel de responsabilidad alta. Las cifras en cuanto a alertas reportadas también tuvieron un alto crecimiento relacionadas en SIEM (IPS, DDoS, NBA, AD).[17]

Otro punto importante mencionado en el Análisis de la CCIT, es la detección de más de 70000 exploits en uso en todo el país. Lo que da mayor facilidad de acceso a los ciberdelincuentes en su materialización. En la tabla 2 se presentan los exploits más utilizados en 2021.

[15] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Evaluación, Retos y Amenazas a la Ciberseguridad. [En línea]. 2021. Disponible en: https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf
[16] Ibid., p. 16
[17] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES.. Evaluación, Retos y Amenazas a la Ciberseguridad. [En línea]. 2021. Disponible en: https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf

Tabla 2. Listado Exploits Colombia 1Q Colombia

Conteo total **Exploit: 79.822**	% Global **Exploit 1.68%**
PHPUnit.Eval-stdin.PHP.Remote.Code.Exe...	40.13%
ThinkPHP.Controller.Parameter.Remote.Co...	40.09%
NETGEAR.DGN1000.CGI.Unauthenticated...	39.19%
Dasan.GPON.Remote.Code.Execution	38.56%
D-Link.Devices.HNAP.SOAPAction-Header...	37.17%
PHP.CGI.Argument.Injection	35.71%
PHP.Diescan	35.4%
Drupal.Core.Form.Rendering.Component.R...	34.29%
vBulletin.Routestring.widgetConfig.Remote...	33.98%
ThinkPHP.Request.Mehot.Remote.Code.E...	33.94%

Fuente: CCIT – Diagramación Estudio Evaluación, retos y Amenazas a la Ciberseguridad.

De acuerdo a la tabla anterior en su mayoría 5 están enfocados en PHP (Lenguaje de Programación), siendo uno de los más usados en Colombia. A tal detalle según el motor de búsqueda Shodan6, que existen más de 10000 sitios con este lenguaje de programación, generando un alto impacto de acuerdo con las vulnerabilidades encontradas en el mismo.

En ese sentido, la firma Claro, también hace énfasis en la importancia de suministrar mejores prácticas que permitan identificar y asumir proactivamente las vulnerabilidades antes que sean aprovechadas por los ciberdelincuentes. Entre las recomendaciones que dan están las siguientes, entre otras no mencionadas.

- Incrementar la validación de la identidad, habilitando el multiple-factor de autenticación.
- Implementar la detección y respuesta
- Elaborar las políticas de cumplimiento
- El servicio de correo debe tener toda la seguridad implementada.
- Tener herramientas de gestión de vulnerabilidades.

Por otro lado, otros autores mencionan que el teletrabajo hoy en día es una realidad, no sólo por la circunstancias de la pandemia, sino que refiere también diversos beneficios relacionados con la productividad, sostenibilidad, así como la eficiencia y la satisfacción laboral, sin embargo, no es una forma de trabajo generalizada y

estructurada tanto en compañías y organizaciones debido a la percepción que se tienen al respecto[18].

En el caso de las empresas que han adoptado el teletrabajo se convierte en una modalidad que mejora en gran parte la calidad de vida de los empleados y facilita la armonía entre el ambiente familiar y laboral, adicional que se puede contar con una mayor flexibilidad, lo que permite ser tan funcionales trabajando desde casa al igual que en la oficina. Son múltiples los beneficios que el teletrabajo aporta a las empresas como modalidad laboral donde los principales factores que influyen en la implementación son: la cultura organizacional, la confianza con el trabajador, la seguridad de la información, la normatividad y la inversión desde diferentes conceptualizaciones. El teletrabajo plantea cambios y obstáculos a los que se deben enfrentar las organizaciones, no obstante, la implementación de buenas prácticas a nivel de ciberseguridad para el acceso remoto se vuelve un punto fundamental.

El teletrabajo ha sido implementado desde varios años en diferentes países. En el caso de Colombia esta modalidad, está normatizada mucho antes de la pandemia por la Ley 1221 de 2008. Sin embargo, dada la crisis sanitaria se implementó la figura de "trabajo en casa" (o trabajo remoto), la cual está definida como "ocasional, temporal y excepcional", de acuerdo a lo definido en la Circular 041 de 2020. Es así, que el Ministerio del Trabajo, menciona que "se estima que más de 6 millones de personas hacen uso en este momento de la figura de trabajo en casa"[19].

Ahora bien, si se tiene en cuenta el auge del trabajo remoto, por tema de Pandemia, un informe de Gartner[20] menciona que una encuesta reciente, el 76% de las empresas ya tienen también políticas BYOD para sus empleados, sin embargo, las empresas que ya contaban con esta tendencia antes de la pandemia Covid-19, están mejor preparadas para pasar a una modalidad laboral completamente remota. Es importante mencionar que las políticas BYOD son una tendencia que permite a los trabajadores usar sus propios equipos personales para poder realizar las actividades diarias. Sin embargo, a pesar de registrar un aumento en la productividad, genera alarma respecto al riesgo que implica sobre la seguridad de la información de la institución.

En el nuevo contexto, es importante traer en mención lo expresado por los autores del artículo Riesgos y Ciberseguridad en las Empresas[21], en relación a que las organizaciones, así como los gobiernos implementen medidas de ciberseguridad y

[18] VARGAS, Osma, 2013. Machuca et al, 2014.
[19] MINISTERIO DE LAS TICS. Efectivas han sido las medidas implementadas por el Gobierno para proteger el empleo en Colombia. 2020.
[20] GARTNER. Tendencias favorecidas por la pandemia. [En línea]. 2020. Disponible en: https://www.ituser.es/seguridad/2020/09/dos-tendencias-de-ciberseguridad-con-impactaran-en-la-empresa-en-esta-decada
[21] SANTIAGO, ENRIQUE. ALLENDE, J., SANCHEZ. Revista Tecnología y Desarrollo. Riesgos de Ciberseguridad en las empresas. 2017. Madrid. España.

tratamiento de riesgo para la infraestructura tecnológica como para los procesos, para evitar su exposición a la cantidad de amenazas y objetivos del cibercrimen que en esta época se han incrementado sustancialmente. Igualmente hacen énfasis de que las organizaciones implementen medidas y tratamientos de gestión de riesgos de Ciberseguridad tanto para los procesos como para la infraestructura tecnológica lo que ayudará a prevenir amenazas que de no hacerlo se comprometería seriamente los activos de información.

También Navia Barmpaliou del Foro Económico Mundial manifiesta que esta pandemia marcará una línea primordial a nivel global y generará una dependencia de la Infraestructura Digital[22].

Por último, se hace referencia a la conclusión del informe de la CEPAL[23], sobre la Ciberseguridad en tiempos de Covid, en el cual indica que el mundo cada vez será más digital con tecnologías disruptivas y muy exigentes, pero a la vez expuestas a ciberataques. Se debe imponer esfuerzo para reducir la ocurrencia de esas posibilidades con medidas efectivas no solo sobre la tecnología, sino que abarque procesos y recurso humano sin importar el tamaño de la organización.

3.4 MARCO CONCEPTUAL

La definición de Ciberseguridad tiene diversos conceptos, pero todos apuntan al mismo interés que es protección. Para el caso de ISACA, está definida como Protección de activos de información, que busca el tratamiento de las amenazas que generan riesgo a la información que es almacenada, procesada y dirigida por los Sistemas de Información que se encuentran interconectados[24].

Ahora, viéndolo de una manera práctica, la ciberseguridad nació con el interés de que las empresas protejan sus entornos informáticos de diversas amenazas y Riesgos.

En segunda instancia, el riesgo está determinado como la posibilidad de que una amenaza se provoque, es decir que un pc puede ser atacado o que la probabilidad de que el ataque se produzca por dicha vulnerabilidad existente en el sistema, pero a la vez el riesgo permite realizar análisis de vulnerabilidades.[25]

---

[22] OEA. Reporte CIBERSEGURIDAD, Riesgos, Avances y el camino a seguir en América Latina. 2020.

[23] CEPAL. Boletín FAL No. 382 La ciberseguridad en tiempos de COVID-19 y el tránsito hacia una inmunidad. 2020.

[24] PORTAL WELIVESECURITY. Ciberseguridad o Seguridad de la Información. [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

[25] FUNDAMENTOS DESEGURIDAD INFORMÁTICA. Avenía Delgado, Carlos Arturo. Bogotá D.C., Fundación Universitaria del Área Andina. 2017

En ese orden de ideas, también es importante mencionar el concepto de la Gestión de Riesgo de la Ciberseguridad, el cual está entendido como la labor de proteger la confidencialidad, disponibilidad e integridad tanto de una infraestructura, datos personales y activos de información.

Sin lugar a duda la gestión del riesgo en la Ciberseguridad es uno de los grandes retos de las entidades públicas, los activos de la información en los últimos años y específicamente en este último de época de pandemia han sido sometidos a innumerables amenazas demostrando que para los delitos cibernéticos no existen fronteras ni jurisdicciones. Lo cual convierte la gestión del riesgo como medida definitiva y de cooperación internacional.

El desafío es enorme, si se tiene en cuenta que la tecnología evoluciona constantemente y margina los progresos de regulación. Los riesgos cibernéticos se acoplan a la regulación cambiante, lo cual hace necesario aunar esfuerzos que permitan desarrollar marcos y se puedan gestionar con principios alineados con flexibilidad.[26] Proteger los activos es algo que definitivamente debe ejecutarse por medio una gestión de riesgos, que permitirá garantizar una mejor seguridad o en su defecto disminuir las posibilidades de que esas amenazas logren materializarse.

También es importante considerar el concepto de la política de seguridad, el cual según ISO 27001:2013, busca implementar un marco de referencia o actuación organizacional que busca salvaguardar la información[27]. Igualmente, IBM, hace mención a la lista de directrices, procedimientos o normas que buscan garantizar un cumplimiento de dicha instrucciones técnicas con la finalidad de proteger la seguridad informática.[28]

El trabajo remoto que se ha incrementado a raíz de esta nueva realidad ha abierto brechas de inseguridad a las organizaciones poniendo en jaque el manejo y gestión de la Ciberseguridad.

Esta modalidad de trabajo remoto estuvo considerada hasta el 2 de agosto de 2021, como actividades que se realizan fuera del lugar del trabajo, sin afectación a la empresa y que son de común acuerdo con el empleador, podía ser por horas, semanal o de forma simultánea con presencia en la oficina, apoyado con tecnologías de la Información y la comunicaciones. A partir del 3 de agosto de 2021 quedó reglamentada esta nueva tendencia laboral, por ley expedida por el Gobierno

[26] OEA. Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina. [En línea]. 2019. Disponible en: https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

[27] NORMAS ISO. ISO 27001 Seguridad de la Información. [En línea]. Disponible en: https://www.normas-iso.com/iso-27001/

[28] IBM. La Política de Seguridad. [en línea]. Disponible en: https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives

Colombiano, la cual busca fomentar campañas de socialización para que las entidades tanto privadas como públicas puedan implementar el trabajo remoto y evidenciando las ventajas que puede generar para la economía y mejorar la tasa de desempleo en Colombia[29].

Por otro lado, el Teletrabajo, está definido por la Organización Internacional del trabajo – OIT, como: "Una forma de trabajo que se efectúa en un lugar fuera de las instalaciones de la organización, que no tiene contacto con más personal de la oficina y que, con la tecnología facilita la comunicación¨[30], y en Colombia esta práctica laboral está reglamentada en la Ley 1221 del 2008.

Dentro de este contexto de la Ciberseguridad en el trabajo remoto se hace fundamental también mencionar conceptualmente el término de buenas prácticas, el cual no solo se refiere a esa práctica sino al resultado generado como parte de su uso acertado. Las buenas prácticas enfocadas a la ciberseguridad no sólo garantizan una mejor seguridad a la información o a una red, también aportan a una mejor gestión de la infraestructura. Para esto es importante tener en cuenta las acciones que implementen técnicas de control y que ayudan a la prevención de ciberataques.

Como resalta la firma Deloitte[31] en su artículo sobre Ciberseguridad en medio de una pandemia global, es Importante que las organizaciones se capaciten y preparen a sus empleados para que de manera idónea enfrenten los posibles riesgos de ciberseguridad propios del trabajo remoto, así como también las vulnerabilidades presentadas en los diferentes sistemas y definidas como debilidades que pueden ser aprovechadas por los ciberdelincuentes.

Una vulnerabilidad informática es una debilidad del software o aplicación que puede comprometer la seguridad y causar daños enormes. Dichas debilidades pueden aparecer en cualquier elemento físico de una equipo en el software o sistema operativo.

Asimismo, se hace necesario brevemente explicar los diferentes tipos de ataque que están dirigidos a los usuarios del trabajo remoto:

---

[29] PRESIDENCIA DE LA REÚBLCA DE COLOMBIA. Ley 2121 del 3 de agosto de 2021, "Por medio de la cual se crea el Régimen de Trabajo Remoto y se establecen normas para promoverlo, regularlo y se dictan otras disposiciones. [En línea]. 2021. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%202121%20DEL%203%20DE%20AGOSTO%20DE%202021.pdf

[30] DI MARTINO, Vittorio. 2004. El teletrabajo en América Latina y el Caribe. Ginebra. Fuente: www.idrc.ca (Consultado el: 01-02-2010).

[31] DELOITTE, Consideraciones generales de Ciberseguridad en medio de una pandemia global. Bogotá, D.C. 2020.

Phishing, está definido como una modalidad en la que atacante crea un sitio web, un archivo falso o un enlace y de esta forma engaña a una persona haciéndole creer que está a un lugar oficial.

- Bombing, denominado así a las interrupciones de reuniones virtuales debido a vulnerabilidades de la plataforma de comunicación, lo cual permite obtención de datos e información de los participantes, grabación no autorizada de las sesiones.
- Hacking, acceso no autorizado a una red por medio de herramientas de conexión remota, para ser exitosa esta práctica requiere captar los datos de acceso o uso de ingeniería social para una conexión exitosa a la infraestructura de la organización
- Ransomware: Programa dañino que encripta los ficheros informáticos y limitando el acceso a determinadas partes o archivos del sistema que infecta se encarga de explotar las debilidades de un sistema para tomar el control, este se transmite a través de páginas web infectadas, aunque el método más común es con archivos adjuntos en correos electrónicos, el comportamiento es como el de un troyano o gusano.

Finalmente, la Seguridad de la Información está definida entre otros conceptos, como el conjunto de procedimientos humanos y técnicos y medidas que protegen la integridad, disponibilidad y confidencialidad de la información[32].

3.5 MARCO HISTÓRICO

La modalidad de trabajo remoto está concebida desde hace más de 45 años, cuando Jack Nilles, ingeniero de la NASA, decide optar por esta posibilidad, para amortiguar la crisis energética que estaba atravesando en esos momentos los Estados Unidos[33].

En 1992 en Washington fue creado un proyecto piloto denominado Interagencial de Teletrabajo, que tenía como finalidad difundir el uso de telecentros externos para diferentes agencias. Luego en el año 1994, el 20 de septiembre fue declarado como “El día del teletrabajo de los empleados”, y así emprendió más fuerza el concepto.

En 1995 la agencia ESPN, realizó una transmisión de un juego de beisbol por radio, basada en el protocolo HTTP que confirmaría de esta forma la posibilidad real del teletrabajo.

[32] ESCRIVÁ GASCÓ, Gonzalo. (2013). Seguridad informática. Macmillan Iberia, S.A.
[33] UNIVERSIDAD ESTATAL A DISTANCIA. Programa de Teletrabajo. Costa Rica. [En línea]. Disponible en: https://www.uned.ac.cr/viplan/teletrabajo/que-es-teletrabajo/historia

En 2008, Microsoft lanzó la tecnología Streaming, que dio lugar a que las empresas se centraran en este tipo de transmisión, hasta incluir plataformas para reuniones a través de la web y zonas de colaboración para trabajadores remotos.

En el mismo año, Colombia expide la Ley (1221 de 2008) que define y regula el teletrabajo en este país.

En 2010, Estados Unidos a través del Congreso, expide la Ley de mejora del Teletrabajo para impulsar la modalidad.

El 1 de mayo del 2012, Colombia firma el Decreto 0884, a través del cual reglamenta la Ley del teletrabajo para los Servidores Públicos, como una forma de organización laboral.

EL 28 de marzo de 2020, a través del Decreto 491, denominado Emergencia Sanitaria, Colombia formaliza el trabajo remoto para solventar la situación causada por la Pandemia del Coronavirus.

Finalmente, en materia de regulación en el mes de agosto de 2021, el gobierno colombiano formalizo el trabajo remoto a través de la Ley 2121.

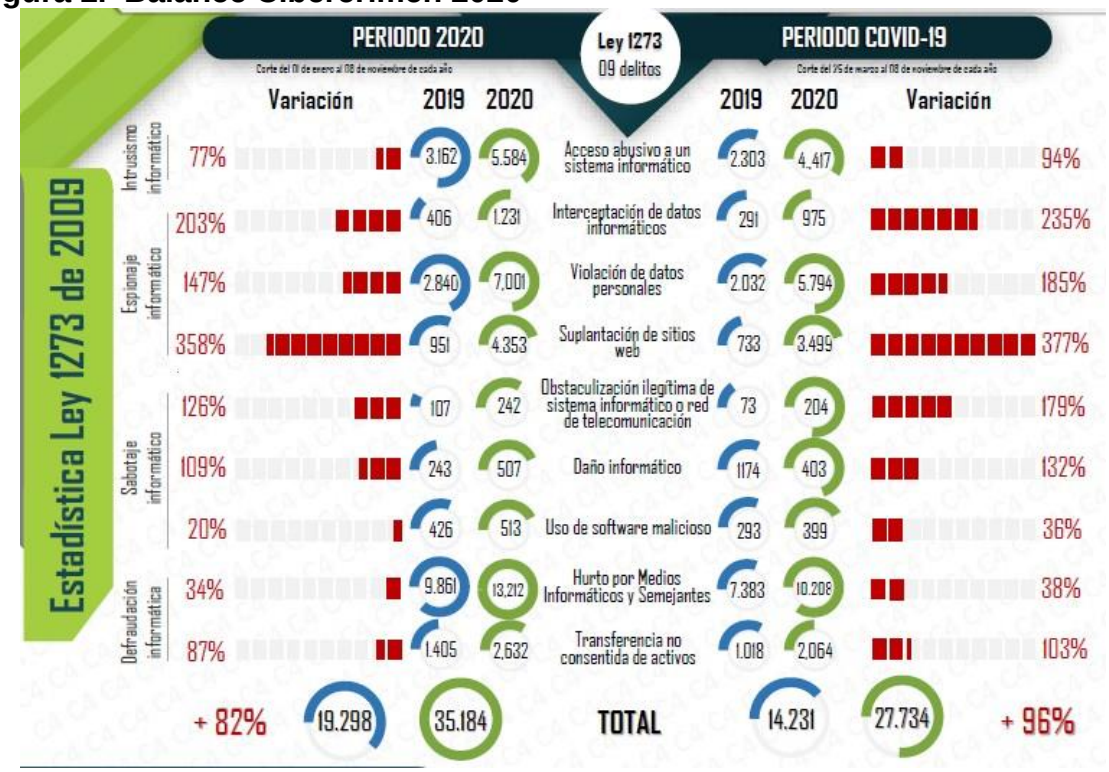
A medida que avanza la propagación del virus del COVID-19 a nivel mundial, los gobiernos y empresas enfocan sus acciones en garantizar no sólo el bienestar de los ciudadanos, empleados y clientes, sino que también han tenido que fortalecer las acciones y controles de protección a la seguridad de la información, dado que, así como se ha intensificado la enfermedad se ha incrementado al mismo tiempo los delitos informáticos.

Las Naciones Unidas, así como Interpol, ponen a consideración el alarmante incremento de ataques en la web registrados en los primeros 6 meses del año. La ONU, confirmó que debido a la pandemia los ataques a organizaciones de salud y correos maliciosos se incrementaron en un 600%.[34]

Por su parte, en Colombia de acuerdo a las estadísticas más recientes del Centro Cibernético de la Policía Nacional, estos delitos han aumentado en un 96%, en lo correspondiente al período desde el inicio de la pandemia hasta noviembre de 2020, respecto a todo el año 2019, como se muestra en la figura 2, a manera de resumen.

34 REVISTA DINERO. La ciberseguridad, el talón de Aquiles de las empresas en cuarentena. [En línea]. Disponible en: https://www.dinero.com/empresas/articulo/panorama-sobre-la-ciberdelincuencia-en-el-mundo--infografia/303546

Figura 2. Balance Cibercrimen 2020



Fuente: Centro Cibernético Policial.

Analizando la figura 2, se evidencia, por ejemplo, que la intrusión pasó de un 77% a un 94%, en el ítem de violación de datos personales en el 2019, se contabilizaron 2032 casos y en el 2020 período de Covid se reportaron 5794 casos, lo que representa un 185% de incremento. Otro punto de afectación importante ha sido la suplantación de sitios web, en el cual en el 2019 fueron 733 casos y en el 2020 el incremento ha sido exponencialmente afectado con 3499 casos, llegando a un 377% de incremento. Estas cifras, así como las otras representadas, lo que demuestran es el aumento de uso masivo e intensificado tanto de operaciones digitales como incremento laboral tecnológico[35], debido a la pandemia.

De igual forma, el periódico el Portafolio, hace referencia a un estudio de TrasUnion, que menciona a Colombia, y en el cual destaca el "phishing" como el fraude más común a nivel mundial y también menciona que el 27% de los encuestados manifestaron haber sido víctimas de este tipo de robo en lo que lleva de pandemia.[36]

[35] CENTRO CIBERNÉTICO POLICIAL. Balance cibercrimen. Bogotá.. [En línea]. 2020. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

[36] PORTAFOLIO. Delitos informáticos, la otra pandemia en tiempos del coronavirus. [En línea]. 2020. Disponible en: https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642

También, se menciona que del 21% de los encuestados manifestó haber sido estafado por terceros, es decir mediante enlaces de origen de páginas web legítimas de comercio en línea, por el contrario, el 19% indicó ser víctima por medio de supuestos fondos de recaudos para caridad.

Por otro lado, según el portal Reset y las estadísticas presentadas por SAFE las entidades institucionales más atacadas o suplantadas durante el período que llevamos de pandemia en su orden han sido[37]:

- La Dirección de Impuestos y Adunas Nacionales 57%
- La fiscalía general de la Nación: 12%
- Asociaciones de tránsito 10%
- Policía Nacional Colombiana 9%
- Ministerio de salud 7%.

Otra modalidad de delito que también se ha intensificado en estos últimos años y desde luego también se ha visto implementada en época de pandemia, es el llamado ransomware, que específicamente es malware o software malicioso que secuestra bases de datos de forma encriptada, correspondiente a información sensible de las empresas.

Los delincuentes lo que hacen es extorsionar a los empresarios a cambio de liberar la información encriptada o de lo contrario llegan hasta eliminar dicha información.

Esto lo que evidencia es la importancia de la protección tanto de la infraestructura ya sea física y lógica como de la seguridad de la información, más allá de tener en cuenta los activos son un elemento relevante para las organizaciones.

En este orden de ideas, resulta imperante tener en cuenta las técnicas y buenas prácticas del uso de la estructura física y lógica de las entidades oficiales de Colombia a través del trabajo remoto generado en gran demanda, como es el caso de hoy en día por el tema de la propagación del Coronavirus, que ayuden a proteger la ciberseguridad de las instituciones.

3.6 MARCO LEGAL

Teniendo en cuenta la reglamentación colombiana, desde el año 2008, el gobierno colombiano reglamentó el teletrabajo a través de la Ley 1221, en la cual determina el teletrabajo como: una forma de organización laboral, que radica en el desempeño de actividades remuneradas o prestación de servicios a terceros con utilización de tecnologías de la información y la comunicación – TIC como medio de

[37] PORTAL RESET. Ciberseguridad en Colombia y el mundo. [En línea]. Disponible en: https://resetmarketingdigital.com/ciberseguridad-en-colombia-y-mundo-cifras

comunicación entre el trabajador y la empresa, sin necesidad de la presencia física del trabajador en un sitio específico de trabajo[38].

En este contexto, se da por entendido que el acceso a la tecnología y conectividad es esencial para el desarrollo de las actividades laborales de trabajo remoto.

Por otro lado, cabe resaltar el Decreto 884 de 2012[39], a través del cual se establece en los artículos 13 y 14 las acciones al componente tecnológico, relacionados con el trabajo remoto.

Igualmente, se debe tener en cuenta que la seguridad digital sea ha convertido en un eje esencial en avance tecnológico en Colombia, lo que ha permitido poner al país a la vanguardia en los últimos años en el ámbito digital con estrategias como la creación de la Política de Ciberseguridad y Ciberdefensa (CONPES 3701 y 3854)[40].

Cabe considerar también, que dadas las circunstancias de la Pandemia por COVID-19, el gobierno colombiano ha formalizado el trabajo remoto para esta situación a través del Decreto 491 de 2020[41], denominado Emergencia Sanitaria y dentro del cual establece entre otros temas las medidas a tomar en cuenta para facilitar los medios tecnológicos a los servidores públicos y así como otras disposiciones relacionadas al tema.

Asimismo, el 3 de agosto del 2021 se firmó la Ley 2121[42], en la cual queda establecida para ejecutar el trabajo remoto, se crean mecanismos para incentivarlo y regularlo, lo que busca la Ley es darle un ámbito de aplicación unos principios generales y crear una política pública del trabajo remoto que establezca entre otros, la jornada laboral.

---

[38] DNP. Articulo 3703. [En línea:]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3703_documento.pdf

[39] MINTIC. Decreto 884 de 2012. [En línea]. Disponible en: https://www.mintic.gov.co/portal/inicio/3638:Decreto-884-de-2012

[40] DNP. Conpes 3854. [En línea]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

[41] FUNCIÓN PÚBLICA. Decreto 491 de 2020. Emergencia Sanitaria Covid-19. [En línea]. Disponible en: https://www.funcionpublica.gov.co/documents/418537/616038/2020-04-07-Preguntas-decreto-491-cap-2.pdf/59b4ecb3-19b5-212e-d0d8-d0cd3b8b9e78?t=1586745515202

[42] PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Ley 2121 del 3 de agosto de 2021. [En línea]. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%202121%20DEL%203%20DE%20AGOSTO%20DE%202021.pdf

Finalmente es importante también traer a colación la Ley de 1273 de 2009, “de la protección de la información y de los datos”[43]. Dicha ley busca preservar los sistemas que sean utilizados a través de tecnologías de la información y las comunicaciones, así como reglamentar las conductas relacionadas con el manejo de los datos personales.

[43] REPÚBLICA DE COLOMBIA. Ley 1273 de 2009. [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

4 DESARROLLO DE LOS OBJETIVOS

4.1 OBJETIVO 1: ESQUEMATIZAR CUÁLES SON LAS POLÍTICAS Y BUENAS PRÁCTICAS QUE SE ESTÁN APLICANDO EN EL TRABAJO REMOTO EN LAS ENTIDADES PÚBLICAS COLOMBIANAS CON EL FIN DE ESTABLECER SU IMPACTO EN LAS DIMENSIONES DE LA SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad se definen como una serie de normas y directrices establecidas por la organización con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información y que buscan además minimizar los posibles riesgos, por lo que relaciona procedimientos e instrucciones técnicas para dar cumplimiento a dicha política. Se resalta que debe ser aprobada por la dirección de la entidad y comunicada a todo el personal.

Como lo menciona Moisés J. Schwartz, Gerente de Instituciones para el Desarrollo del BID, en el reporte de Ciberseguridad, estás políticas son fundamentales para proteger la privacidad y propiedad de los ciudadanos en el entorno digital, más si se tiene en cuenta que los delitos surgidos por falta de seguridad también tienen una afectación económica[44].

Por otro lado, en el mismo reporte Farah Diva Urrutia, secretaria de Seguridad Multidimensional de la OEA, resalta la oportunidad que brinda esta pandemia de COVID-19, para reflexionar sobre el avance que se debe adquirir en el momento para el fortalecimiento de las TIC, la conectividad y la garantizar la ciberseguridad de los estados[45].

En relación con Colombia la OEA, resalta que el gobierno a través del MinTIC ha extendido a nivel nacional el modelo de seguridad y privacidad como apoyo e implementación de estándares y buenas prácticas como protección a los activos de información e infraestructuras tecnológicas tanto para entidades públicas, entes privados y ciudadanía.

En este punto es importante aclarar que Colombia desde el año 2011, ya contaba con marco de referencia normativo, legal y de política que define los lineamientos en materia de Seguridad Digital, por lo que en el siguiente numeral se presenta un resumen del transcurso de ésta última década en materia de políticas de seguridad en Colombia.

[44] SCHWARTZ, Moisés J. Reporte de Ciberseguridad BID-OEA. 2020
[45] Ibít., p. 12

4.1.1 Antecedentes legales y de política pública de seguridad digital en Colombia. En 2010 el Gobierno colombiano genero el “Plan Vive Digital Colombia para un período del 2010-2014. El cual tuvo como enfoque principal ser líder mundial en desarrollo de aplicaciones con orientación social. Buscando reducción de pobreza en el país. Este plan tuvo gran éxito y pue ampliado para el período 2014-2018[46].

En 2011, fue generado el primer Conpes No. 3701 sobre Lineamientos de Política para Ciberseguridad y Ciberdefensa que tenía como objetivo principal fortalecer las acciones del gobierno para afrontar las amenazas con la seguridad y defensa en el entorno cibernético[47].

En 2012, el Gobierno Colombiano establece a través de la Ley 1581, mediante la cual se reglamenta los aspectos relacionados con el tratamiento y uso de datos personales[48].

En 2016, se genera otro Conpes del 3854, el cual tiene como objetivo general de política, que las entidades públicas, así como los ciudadanos conocieran e identificaran los riesgos del ámbito digital y se tomen medidas acertadas para la protección, así como prevenir y actuar eficazmente ante los ataques cibernéticos[49].

En este punto es importante resaltar que el gobierno de Colombia a través de los documentos Conpes 3701 de 2011 y 3854 de 2016, facultó en el Ministerio de Defensa la responsabilidad de dar seguridad nacional y defender el ciberespacio. Lo que conlleva a articular todos esfuerzos civiles enfocados a lograr un ciberespacio más confiable y seguro para las entidades públicas, privadas y a los ciudadanos. Adicionalmente uno de los aportes de esta política de relevancia es del rol de coordinador nacional de seguridad digital que es ejercido directamente por el presidente de la República.

El esfuerzo está encabezado por el Grupo de respuesta de Emergencias Cibernéticas de Colombia COLERT, el cual coordina todos los aspectos de ciberseguridad y ciberdefensa como la protección de la Infraestructura crítica del estados y los temas de cooperación, gestión e intercambio nacional e internacional.

---

[46] MINTIC – Plan Estratégico Sectorial. [En línea]. Disponible en: http://rtvc-assets-qa-sistemasenalcolombia.gov.co.s3.amazonaws.com/plan_estrategico_sctorial_2014-_2018.pdf

[47] DNP. Documento Conpes 3701. [En línea]. Disponible en: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

[48] PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Ley 1581. [En línea]. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20del%2017%20de%20tubreoc%20de%202012.pdf

[49] MINTIC. Lo que usted de saber sobre el Conpes. [En línea]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/15410:Lo-que-usted-debe-saber-del-Conpes-de-Seguridad-Digital

El Comando Conjunto Cibernético -CCOC de las fuerzas militares y las unidades cibernéticas del Ejército de la Armada y la Fuerza Aérea Colombiana, proporcionan la seguridad del país a través de estrategias que permiten prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética.

El Centro Cibernético Policial -CCP, está encargado de la ciberseguridad del territorio colombiano ofreciendo información, apoyo y ante los delitos cibernéticos. Para su operación fue creado el CAI – Comando de Atención Inmediata virtual, para recibir todas las denuncias relacionadas con los delitos informáticos y cibercrimen[50].

En 2018, es creada la Nueva Política de Gobierno Digital, la cual busca promover la innovación ciudadana, logrando una mayor participación en la solución de diferentes problemas de índole público. De esta forma el Ministerio de la TICs, lo que buscaba era que los actores involucrados en la política se dieran en medio de una interacción segura[51]. Adicional a esta nueva política el Ministerio de las Tecnologías y las Comunicaciones a través del Plan TIC 2018-2022: presentó la ruta de conectividad y transformación digital para ese período, bajo el lema: "El futuro Digital es de todos", que busca entre otros puntos, masificar la cobertura de conectividad.

En esta política de Gobierno Digital de 2018, también fue elaborado el Manual de Gobierno Digital, por el Ministerio de las TICS, en el cual se determinan los pasos que deben aplicar las entidades públicas para la implementación de la Política de Gobierno, entre las cuales está el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual permite establecer a través de indicadores el nivel de madurez para las entidades públicas en materia de seguridad digital.

El manual es un gran aporte para las entidades públicas, ya que está alineado con las Norma ISO 27001:201311, en relación con las buenas prácticas, así como también con la Ley de Protección de Datos Personales 1581 con la Ley 1712 de 2014 que está enmarcada en la transparencia y derecho de acceso a la información pública nacional.[52]

En 2019, el gobierno colombiano expidió a través de la Ley 1955 el Plan Nacional de Desarrollo 2018-2022, en la cual en el capítulo VII, hace referencia al Pacto por la transformación digital de Colombia, el cual busca el sendero hacia una sociedad digital y hacia la cuarta generación; asimismo en el capítulo I, establece como

---

[50] COLCERT. Ciberseguridad y Ciberdefensa - Política Nacional de Seguridad Digital

[51] MINTIC. Nueva Política de Gobierno Digital. [En línea]. 2019. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/75180:La-nueva-politica-de-Gobierno-Digital-promueve-la-proactividad-y-la-innovacion-ciudadana

[52] FENALCO. DNP expidió Documento Conpes 3995. [En línea]. 2020. Pag. 11. Disponible en: http://www.fenalco.com.co/gesti%C3%B3n-jur%C3%ADdica/dnp-expidi%C3%B3-documento-conpes-sobre-pol%C3%ADtica-nacional-de-confianza-y-seguridad

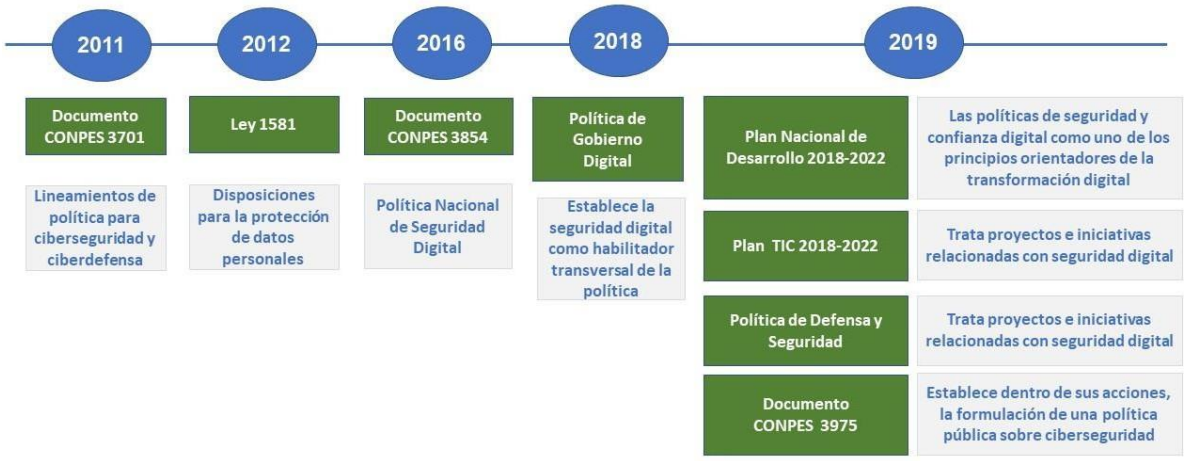
estrategia fortalecer la ciberseguridad y ciberdefensa para la seguridad a nivel de terrestre, marítimo, espacial y ciberespacial como intereses nacionales[53].

Este plan de desarrollo establecerá una hoja de ruta para su implementación a nivel institucional que contará con la contribución de diferentes entes públicos y académicos. Esta actividad iniciará en junio de 2021 y finalizará en diciembre de 2022.

Por otro lado, en el 2019 el Ministerio de Defensa Nacional formulo la Política de Defensa y Seguridad que busca la legalidad, emprendimiento y la equidad de Colombia con el fin de preservar la independencia, soberanía e integridad del Estado.

De esta forma se puede evidenciar como el Gobierno Colombia ha implementado las políticas y estrategias que buscan ofrecer seguridad digital a nivel nacional y defender el ciberespacio, en la figura 3, se presenta a manera de resumen dichas políticas en el transcurso de los últimos años.

Figura 3. Implementación de Políticas y Estrategias del Gobierno Colombiano para entidades públicas



Fuente: DNP - Documento CONPES 3995

Adicionalmente, en noviembre de 2019, a través del Conpes 3795 fue creada la Política Nacional para la Transformación Digital e Inteligencia Artificial, enmarcada entre otros aspectos, a enfrentar los retos de la cuarta generación.

En Colombia el 1 de julio de 2020, el Departamento Nacional de Planeación, expidió un documento Conpes No. 3995 de “Política Nacional de Confianza y Seguridad Digital. Este documento de política pública tiene como finalidad establecer acciones

[53] Ibít., p. 12.

que generen confianza y mejoren la seguridad digital, así como buscar que Colombia en futuro cercano sea competitiva digitalmente.

Esta política aplica no sólo para entidades públicas, sino que también para al sector privado, sectores productos y ciudadanos. La política definió tres grandes ejes en los cuales trabajar, y son[54]:

- Fortalecer capacidades de los ciudadanos del sector público y del privado.
- Actualizar el marco de gobernanza en Seguridad Digital
- Analizar la adopción de modelos, estándares y marcos de trabajo con énfasis en nuevas tecnologías.

Dentro de las medidas que se tomarán en esta nueva política digital que regirá prácticamente a partir del año 2022, ya que para su elaboración se unificarán iniciativas que buscan fortalecer las capacidades en seguridad digital de varios sectores tanto públicos como privados, entre los cuales están el Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio de Defensa Nacional, Departamento de la Presidencia de la República, Ministerio de Educación Nacional, la SIC, y el Servicio Nacional de Aprendizaje (SENA).

Otro punto importante de mencionar es que, en el mes de marzo de 2020, Colombia instauró el documento de adhesión al Convenio de Budapest, ante el Consejo de Europa, que es el estándar mundial en la lucha contra la ciberdelincuencia[55].

Este convenio que busca mejorar la cooperación entre los estados en temas de prevención de delincuencia organizada para Colombia, genera entre otras, las siguientes expectativas:

- Revisar y ajustar la legislación nacional contra la ciberdelincuencia, teniendo en cuenta los estándares internacionales.
- Estandarizar los intercambios de información que faciliten las investigaciones de delitos cibercriminales entre los países miembros del convenio.
- Permitir el acceso a programas académicos, proyectos investigativos, soporte tecnológico y operaciones que tipo bilateral y multilateral.
- Participar en estrategias para ciberdelincuencia en conjunto

[54] CIFUENTES, Aura. Política Nacional Digital [video]. Bogotá, Colombia: YouTube. MinTic. (25 de septiembre de 2020). 35:40 minutos. [consultado 20 de noviembre de 2020]. Disponible en: https://www.youtube.com/watch?v=5bXI6CdH8gQ&t=1025s

[55] CANCILLERÍA DE COLOMBIA. Colombia se adhiere al convenio de Budapest contra la Ciberdelincuencia. [En línea]. 2020. Disponible en: https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia

El Convenio de Budapest del cual ahora es miembro Colombia, adicionalmente cuenta con la participación de 65 países más[56].

Es así como se evidencia que los mayores esfuerzos en materia de Políticas de Ciberseguridad en Colombia se han realizado en estos últimos años, generando lineamientos para fortalecimiento no sólo para las entidades públicas sino también de inclusión a la sociedad y creando confianza digital a nivel nacional.

4.1.2 Políticas Trabajo remoto

En Colombia el teletrabajo está establecido por la Ley 1221 de 2008 y definido como una forma de organización de trabajo, que radica en la descripción de actividades pagadas o por medio de prestación de servicios en los cuales se utiliza tecnologías de la información y comunicación (TIC), como medio de comunicación entre el empleado y la entidad y que no requiere presencia física en un lugar específico[57].

Entre otros beneficios, el Ministerio de las Tics, resalta que puede servir como mejora en la calidad de vida del trabajador, así como se evita el tiempo de desplazamientos a través del transporte y puede generar resultados más productivos.

En este aparte es importante recordar que el escenario laboral y condiciones que gobiernan el teletrabajo a parte de la ley 1221 de 2008, se encuentran especificadas en el Decreto 884 de 2012. Sin embargo, debemos tener en cuenta las nuevas circunstancias generadas por el coronavirus que obligo al trabajo remoto masivo y que todo lo que se implemente en medio de la pandemia en relación con esta modalidad laboral, está avalado y regido por la Circular 0018 del 10 de marzo de 2020[58], tanto para entidades públicas como para organizaciones privadas. No obstante, el 3 de agosto de 2021, también fue formalizado el trabajo remoto bajo la Ley 2121, la cual busca reglamentar la modalidad a través de una política pública que diseñara la implementación y lineamientos para la ejecución del trabajo remoto.

Una política igual de importante e indispensable que ha de tener en cuenta todas las entidades en relación con el acceso remoto, es la política de acceso remoto establecida por la ISO 27001:2013 que busca precisamente proteger ese riesgo a través de controles de seguridad. Igualmente establece condiciones, restricciones, mecanismos y procedimientos para dar permiso al acceso remoto con seguridad.

---

[56] Ibít. Convenio Budapest.

[57] MINTIC. Empresas y teletrabajadores ¿cómo implementar el teletrabajo por estos días?. [En línea]. 2020. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/MinTIC-en-los-Medios/126355:Empresas-y-trabajadores-que-es-y-como-implementar-el-teletrabajo-por-estos-dias

[58] FUNCIÓN PUBLICA. Circular 0018 del 10 de marzo. [En línea]. 2020. Disponible en: https://www.funcionpublica.gov.co/documents/418537/616038/Circular-externa-0018-2020-acciones-contencion-coronavirus.pdf/92ccd0b4-c825-8eeb-a29c-89956d17c80b?t=1583870658660

Los controles que se mencionan sobre teletrabajo y dispositivos móviles en el punto A.6.2.1 de la norma son fundamentales en cualquier organización para determinar la seguridad de la información, entre los cuales están[59],

- Decidir quién puede realizar teletrabajo
- A qué aplicaciones o servicios pueden acceder los teletrabajadores autorizados
- Cuáles controles de acceso se pueden implementar de forma adicional
- Mecanismos de protección en los dispositivos utilizados en el teletrabajo.
- Restricciones de acceso a la información sensible.

4.1.3 Características del Trabajo Remoto

Aun teniendo en cuenta las normas establecidas para el trabajo remoto, se puede decir que va más allá de los establecido en las mismas, dado que la tecnología ha ido evolucionando exponencialmente, lo que hace que para el ámbito laboral no sea la excepción. La tecnología hoy en día permite que un empleado no deba estar físicamente en el espacio del trabajo ni que cumpla horarios largos y las entidades o empresas privadas que se encuentran tecnológicamente al día consideran apropiada esta modalidad, ya que facilitan la comunicación y genera mecanismos de control y seguimientos a las diferentes actividades.

En Colombia, la Ley 1221 de 2008 establece tres tipos de modalidades de teletrabajo, como son: el autónomo, el suplementario y el móvil[60], que se encuentran representados en la figura 4 y en la cual detalla la descripción de cada uno.

[59] ISO 27001. [En línea]. Disponible en: https://normaiso27001.es/a6-organizacion-de-la-seguridad-de-la-informacion/

[60] TELETRABAJO. Definición. [En línea]. Disponible en: https://www.teletrabajo.gov.co/622/w3-article-8228.html

Figura 4. Modalidades de Teletrabajo en Colombia

Fuente: www.teletrabajo.gov.co

4.1.3.1 Consideraciones

El trabajo remoto debe considerar condiciones para que la modalidad sea efectiva para ambas partes, entre las cuales están:

- Las entidades deben suministrar los elementos necesarios para que el trabajador efectúe actividades de manera eficiente, como computador, línea telefónica, silla ergonómica.
- El sitio de trabajado del empleado debe ser revisado por el empleador en conjunto con la ARL
- El trabajador debe ser incluido en los programas que la ARL diseñe para la seguridad y salud, así como permitir su participación en las actividades
- La entidad u organización deben ofrecer al trabajador inducción y capacitaciones.
- El trabajador debe contar con protección de maternidad
- El empleador debe garantizar tanto el mantenimiento de los equipos, como proveer la conexión.

En este contexto característico del trabajo remoto, es importante tener presente los cambios que se generan en esta modalidad a nivel personal, como las nuevas dinámicas de interacción, flexibilidad horaria, adaptación a nuevas tecnológicas, establecer nuevos conceptos de lugar, familia, social. El teletrabajo encierra diferentes matices que pueden transformar la vida de una persona tanto de modo,

lugar, relaciones familiares, hábitos, hasta modo de vestir, modos de incorporarse a la sociedad y la cultura[61].

Ahora si tenemos en cuenta, el trabajo remoto puede tener variación de los tiempos que rigen un día normal al ser humano, entre el trabajo, la familia y el aspecto social y de descanso. En esta nueva modalidad el trabajo elimina los límites entre tiempo libre y tiempo laboral, así como tampoco evidencia el límite entre vida familiar y laboral, vida pública de la privada. Entonces claramente se ve una especie de invasión a los espacios establecidos en una sociedad normal, lo que lleva a cuestionarse que tan válido sea. La Tecnología hoy en día hace posible que esos espacios se expandan y abarquen tanto el espacio como el lugar, permitiendo conexiones desde cualquier lugar y en cualquier momento. Por lo que es importante que el empleado esté presto a reorganizar y crear estrategias para que estas transformaciones sean más adaptables a las realidades espaciotemporales alternativas[62].

4.1.4 Medición del Trabajo remoto en Entidades Públicas

El Ministerio de las TICs, en el años 2019, considero importante realizar una recolección de información que determinará el avance y penetración en la modalidad del trabajo remoto en las entidades públicas, para lo cual contrató el Centro Nacional de Consultoría, actividad que se realizó entre octubre y noviembre del 2019.

Dentro de los resultados arrojados están los relacionados a continuación a manera de resumen:

La involucración del teletrabajo en las entidades va en aumento, por ejemplo, del 13% del 2014 pasó a un 30% en el 2019. De las entidades consultadas el 71% se ubican en etapa de implementación y adopción de esta modalidad, mostrando madurez y el lugar donde teletrabaja el empleado público es la casa de domicilio.[63]

El indicador de aumento en el trabajo remoto va en aumento paulatino en las diferentes entidades. El crecimiento en los últimos 5 años tuvo un aumento de 25 puntos, en comparación con el 2014, es decir que paso del 13% al 38% en el 2019. En ese sentido se resalta que el 71% de las entidades consultadas se encuentran en implementación, lo que muestra cierta madurez en el proceso.

---

[61] ORTIZ, Francisco. El teletrabajo una nueva sociedad laboral en la era de la tecnología. Madrid: McGraw Hill.

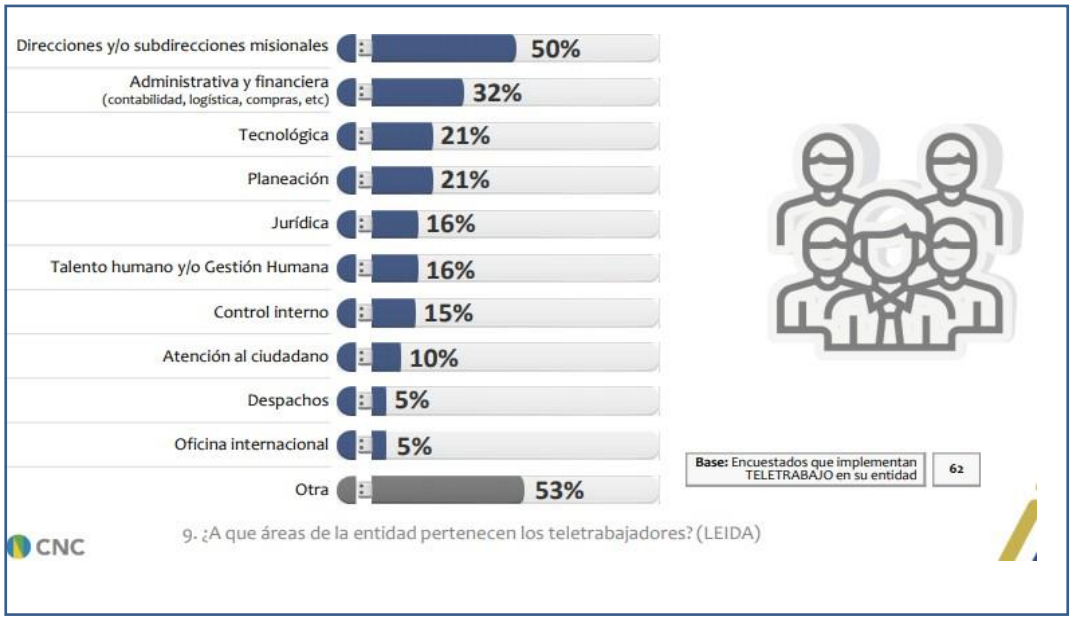
[62] TIETZE, Susanne. MUSSON, Gillian. 2002. When “Work” Meets “Home”: Temporal Flexibility as Lived Experience. Time & Society 11 no. 2/3: 315-334

[63] COMISIÓN NACIONAL DE CONSULTORÍA. Medición del Teletrabajo en Entidades Públicas. Penetración y percepciones. [En línea]. 2019. Disponible en: https://www.teletrabajo.gov.co/622/articles-144782_recurso_1.pdf

En el sector público, se evidencia que la condición de discapacidad ha sido favorecida con un 30%, lo que representa que en este sector es donde hay mayor nivel de inclusión en estas políticas sociales, no obstante, resalta el informe que también hace falta suministro de tecnologías tanto de software como hardware para este grupo de población.

Otro resultado importante que se evidenció es cómo se encuentra focalizado el teletrabajo a nivel interno de cada entidad, en la figura 5, se detalla su distribución teniendo en cuenta las diferentes áreas tanto administrativas, directivas y misionales.

Figura 5. Focalización teletrabajo a nivel interno de las entidades públicas



Fuente: Centro Nacional de Consultoría. 2019.

Otro punto que se tuvo en cuenta como estudio dentro de la encuesta fue la modalidad de trabajo que más está implementada en las entidades públicas y en comparación con el estudio del 2014; en la figura 6, se detalla el resultado.

Figura 6. Porcentajes de modalidad de trabajo en las entidades públicas

Fuente: Centro Nacional de Consultoría. 2019.

Como se evidencia en la figura 6, desde el año 2014 al 2019 ha habido un incremento del 15% adicional, lo que demuestra que cada vez se va a utilizar más esta modalidad.

Una tendencia es la que muestra la figura 7 en relación con que los empleados públicos que realizan el teletrabajo en su mayoría son de perfil profesional.

Figura 7. Perfil de los empleados que realizan teletrabajo en las entidades públicas

Fuente: Centro Nacional de Consultoría. 2019.

Las entidades públicas que tienen implementado el teletrabajo, en cierta forma ratifican que la modalidad no requiere de grandes inversiones tecnológicas, por lo que pide ser difundido como casos de éxito. Bajo este contexto, podemos afirmar que en la actuales circunstancias debido al coronavirus, no es diferente la situación en cuanto a la percepción del teletrabajo en las entidades públicas, dado que los resultados del estudio fueron arrojados sólo cuatro 4 meses antes de declararse la pandemia.

4.1.5 Gestión del Riesgo

Organismos tanto internacionales como de Colombia han aportado marcos, metodologías y modelos que buscan dar protección a los activos de manera organizada y metódica, dando aplicación de esta forma a la gestión del riesgo.

Es por esto, que es importante mencionar el estándar ISO 27001:2013 proporciona la metodología para gestionar la seguridad de la información en las organizaciones, permitiendo evaluar los riesgos.

Otro referente de la gestión del riesgo es el Marco de Ciberseguridad para la protección de infraestructuras críticas, elaborado por el Instituto Nacional de Estándares y Tecnologías (NIST). El marco busca ofrecer un lineamiento de seguridad que pueda ser aplicable en las diferentes compañías que tengan una infraestructura crítica pero que a través de su implementación se pueda priorizar unas actividades que mejoren el rendimiento y beneficio para las organizaciones.[64]

Adicionalmente, cabe resaltar que este marco puede utilizarse como instrumento para abordar de manera integral de gobernanza la ciberseguridad de acuerdo a las necesidades de cada organización. Lo más importante es que realiza una gestión de riesgos de manera flexible, permitiendo evaluar con efectividad los controles establecidos.

4.1.6 Impacto sobre las Políticas y Buenas Prácticas en las dimensiones de la Seguridad de la Información.

Las políticas que han sido creadas para las organizaciones públicas de Colombia de seguridad de la información tienen una relevancia e impacto, dado que serán la guía del comportamiento profesional y personal de los servidores públicos sobre la información a cargo de cada entidad, ya sea generada o procesada, así mismo dichas políticas no sólo permiten que la organización trabaje bajo una guía de

[64] CIBERSEGURIDAD. Marco NIST. Un abordaje integral de la Ciberseguridad.2019. OEA.AWS.

mejores prácticas de seguridad sino que al mismo tiempo se acople y cumpla las obligaciones legales[65].

Dichas políticas y mejores prácticas buscan ser implementadas en las tres grandes dimensiones de la seguridad, como son: Integridad, Confidencialidad y Disponibilidad, perder alguna de estas dimensiones genera un impacto negativo sobre las organizaciones.

La información en toda su extensión tiene un valor incalculable, sea confidencial o no, por lo que requiere de mecanismos efectivos de protección, que no siempre deben estar asociados al encierro ni de los teletrabajadores en una oficina ni de la información [66].

El mayor temor que existe al trabajar de manera remota está el poner en riesgo la información.

La confidencialidad sin lugar a duda, genera un impacto ya sea positivo o negativo, dependiendo del manejo y uso que se le dé a las tecnologías de la información. Hoy en día la información está alcance de los trabajadores por la modalidad del trabajo remoto, generando mayor riesgo a la protección de los datos, bien sea por pérdida de documentación, por ser compartida por drive, por acceso de terceros o simplemente mal uso de los equipos, esto lleva a una vulneración de los datos.

Por consiguiente, es fundamental el compromiso con la Confidencialidad por parte de los empleados, ya que su mal utilización puede causar diversos daños. Lo recomendable es las entidades firmen una serie de contratos y pactos de confidencialidad referidos a lo que el trabajador puede o no puede hacer con la información empresarial. Igualmente debe relacionar unas recomendaciones tanto de protección de datos como de seguridad.

De igual forma la Integridad de la información no debe surtir modificaciones sin que hayan sido autorizadas por el responsable de la misma. Por lo cual su impacto en esta dimensión es igualmente valioso, ya que los datos deben permanecer fiables, completos y sin modificaciones del original.

El problema con la integridad de la información o datos comienza con un recurso humano, quien realiza las modificaciones a los datos originales intencionalmente o por error.

---

[65] MINTIC. Elaboración de la política general de seguridad y privacidad de la información. Guía No. 2. [En línea]. 2016. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

[66] MINTIC. Teletrabajo - Seguridad para trabajo informático a distancia. [En línea]. Disponible: https://www.teletrabajo.gov.co/622/w3-article-4502.html

Conservar la integridad de la información asegura que los datos persistan intactos por todo el ciclo de vida, ya sea en su almacenamiento en el momento de realizar intercambio de realizar copias de seguridad.

La pérdida de la Disponibilidad, indica la probabilidad que afecte la continuidad de la comunicación, capacidad de atención y procesamiento de un área de la empresa. Puede ser propagación de virus, fallas de software o hardware, respaldos insuficientes o mal ejecutado, o por eventos externos como incendios, inundaciones o terremotos.

De igual forma, las buenas prácticas están definidas como un conjunto de acciones eficientes, oportunas, eficaces, flexibles y sostenibles que permitirán la satisfacción de los usuarios ya sea de sus expectativas como necesidades, que aportan a la mejora de los estándares del servicio y que están alineadas con la misión de la organización, además deben ser creadas por los miembros del proceso y apoyadas por la dirección. Asimismo, deben ser documentadas dentro del proceso correspondiente[67]. Dicho esto, las buenas prácticas generan impacto positivo a las dimensiones de la seguridad.

Por su parte, Colombia en los últimos años se ha enfocado en establecer estrategias de ciberseguridad nacional, buscando dar prioridad a la identificación de amenazas y riesgos para la implementación de prácticas que permitan disminuir dichos riesgos. Es por lo que, a través del Ministerio de las Tics, se delegó la elaboración del Modelo Nacional de Gestión de Riesgos de Seguridad Digital[68], el cual está asentado en buenas prácticas para la gestión de riesgos, que no sólo busca la seguridad digital, sino que también contribuya de manera económica y social al país, lo que evidencia también un impacto favorable. Esa dimensión de las políticas en la seguridad de la información permite facilitar y comprender los criterios que sirven para la protección de dicha información.

Es importante mencionar que este Modelo Nacional de Gestión de Riesgo, está enmarcado y alineado con los estándares de seguridad internacionales por lo cual incluye componentes esenciales como son la identificación, evaluación y la forma como se debe tratar el riesgo. Igualmente contiene mecanismos de seguridad, preparación y recuperación a través de protocolos y controles que permiten a la vez realizar la medición de efectividad de este.

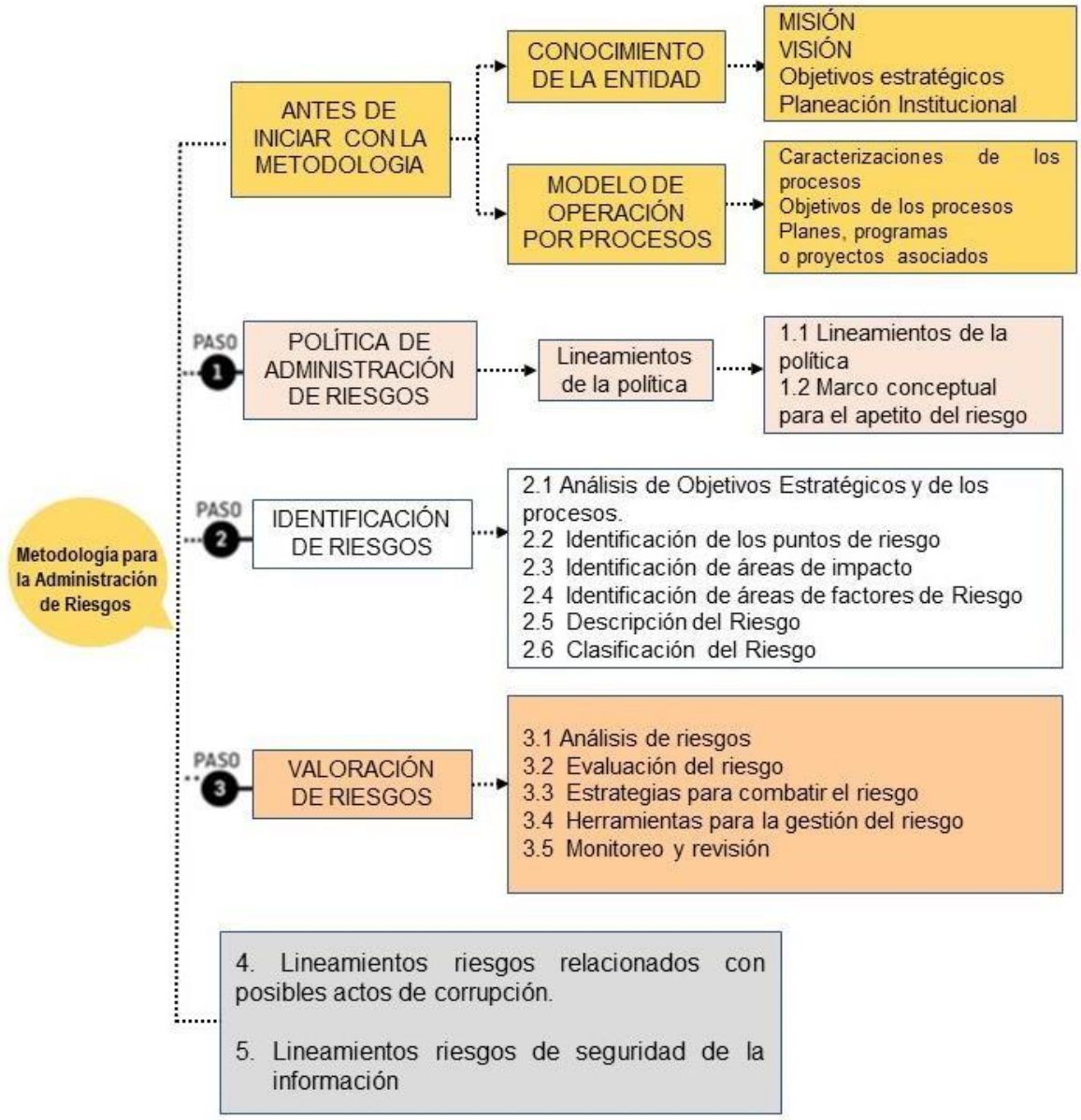
La idea primordial es que el Modelo sea establecido en la mayoría de las entidades públicas de Colombia, así como el sector privado. Teniendo en cuenta esa premisa sugiere aplicar la guía elaborada dentro del mismo modelo de acuerdo al sector que desee su implementación (Anexo 1).

[67] RODRIGUEZ, EDSON. RODRIGUEZ, INGRID. Mejoramiento de las Buenas Prácticas de Seguridad Informática. 2013. Universidad Piloto de Colombia.
[68] MINTIC. Modelo Nacional Gestión de Riesgos de Seguridad Digital. 2018.

En este punto se hace importante mencionar que para realizar una gestión del riesgo acertada y de acuerdo a los lineamientos para las entidades públicas de Colombia, es fundamental tener presente la estructura de la metodología implementada por la Función Pública en el 2018 y actualizada en diciembre de 2020 (figura 8), la cual busca unificar los lineamientos para la administración de todo tipo de riesgos con la finalidad de darle un fortalecimiento al manejo y que se facilite la el tratamiento y gestión de cada uno de los riesgos detectados.[69]

[69] FUNCIÓN PÚBLICA. Guía para la Administración del Riesgo y el Diseño de controles en entidades Públicas. 2018.

Figura 8. Metodología para la implementación del Riesgo en las Entidades Públicas de Colombia



Fuente: Departamento Administrativo de la Función Pública. Guía para la Administración del Riesgo y el Diseño de controles en entidades públicas.

4.2 OBJETIVO 2: ANALIZAR LAS DIFERENCIAS DE TRABAJO REMOTO Y TRABAJO EN SITIO PARA DETERMINAR CUÁLES PUEDEN SER LOS RIESGOS QUE SE RELACIONAN CON LA CIBERSEGURIDAD EN CADA UNA DE LAS MODALIDADES

La ciberseguridad tiene diversos conceptos, por ejemplo, ESET, la precisa como la protección de información digital en sistemas interconectados[70]. Así como ISACA, la define como: "Protección de activos de información, por medio de prevención de amenazas que puedan poner en riesgo la información de los sistemas de información que están interconectados".[71]

Por su parte la ISO 27001:2013, define el activo de información como un conocimiento que tiene valor para las organizaciones y los demás componentes, los define como activos de tecnologías, aplicaciones y servicios del cual se puede hacer uso. En ese orden de ideas se concibe como principal objetivo de la ciberseguridad el proteger la información digital que está interconectada con todos los dispositivos.

- Seguridad de la Información:

En resumen, lo que plantea la seguridad es reducir riesgos hasta niveles aceptables. La información puede representarse de diversas formas: análoga, digital, inclusive a manera de conocimiento de las personas, por lo que requiere, independientemente de su formato es la protección con criterios de nivel de seguridad, y precisamente de esto es lo que trata la seguridad de la información.

Por eso es importante diferenciar Ciberseguridad de Seguridad Informática y una vez analizados dichos conceptos, se puede decir que la seguridad de la información tiene una trascendencia superior, dado que seguridad de la información protege la información de todos los riesgos posibles y la Ciberseguridad se encarga de la información digital y los sistemas con los que se interrelaciona, principalmente los cuales se procesan, almacenan o transmiten.[72]

- Seguridad de las aplicaciones:

Está enfocada a proteger el software y dispositivos de amenazas, ya que a través de ellas podría dar acceso a datos que deben ser protegidos. Por eso es

[70] ESET, «Welive Security,» Miguel Angel Mendoza, 16 06 2015. [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/ .

[71] ISACA (Information Systems Audit and Control Association) Capítulo Monterrey. [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

[72] VALOYES, AMANCIO. La Ciberseguridad en Colombia. Universidad Piloto de Colombia. [En línea]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6370/CIBERSEGURIDAD%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

fundamental tener presente que la seguridad de las aplicaciones inicia antes de su implementación, es decir desde la etapa de diseño.

- Seguridad de Redes:

Busca proteger la red de intrusos ya sean dirigidos o malware oportunistas.

- Seguridad Operativa

Entendida como los permisos otorgados para acceder a una red e indicar a los usuarios los procedimientos de cómo almacenar y compartir datos, es decir incluye decisiones para proteger adecuadamente los recursos de datos.

- Capacitación usuario final

Comprende uno de los factores más importantes de la ciberseguridad y que está directamente relacionado con las personas, ya que de las buenas prácticas que se le socialicen depende el bueno uso de las herramientas y aplicaciones. Capacitar a los usuarios, por ejemplo, en el manejo de archivos adjuntos en los correos electrónicos y que parezca sospechosos son de gran ayuda de prevención.

4.2.1 Tipo de Ciberamenazas

La Ciberseguridad se enfrenta principalmente a tres tipos de Ciberamenazas:

Delitos Cibernéticos: Son afectaciones a los sistemas o aplicaciones a modo de interrupciones que básicamente buscan recompensas financieras.

Ciberataques: Casi siempre están referidos a un secuestro o recopilación de información que en muchas circunstancias terminan siendo realizados fon fines políticos.

Ciberterrorismo: como objetivo principal buscan causar pánico o terror a través de los sistemas electrónicos.

Los métodos más comunes para llevar a cabo las amenazas contra la ciberseguridad, es a través del malware, software malicioso. El malware es un software creado por cibercriminal que busca la interrupción o el daño de un dispositivo de algún usuario genuino. Casi siempre se realiza a través de un correo electrónico solicitando una descarga. Esta acción lo hacen con fines económicos o políticos.

4.2.2 Ciberseguridad en el trabajo remoto

Las tecnologías de la información son un gran aporte a la sociedad. Sin embargo, algunos desarrollos tecnológicos han abierto puertas a conductas delictivas, que atentan contra la privacidad, propiedad de las personas, así como de las organizaciones en formas no usuales y que a través del trabajo remoto se hace más sensible.

Según el informe de Ciberseguridad del BID, las cifras de la ciberdelincuencia se han intensificado por la expansión de la modalidad de trabajo remoto, durante esta época de la pandemia, lo que conlleva a pérdidas económicas a nivel de estado, inclusive se menciona que podría exceder el 1% del producto interno bruto (PIB) en varias naciones y para el caso de la infraestructura crítica esos ataques podrían llegar a sobrepasar hasta el 6% del PIB.[73]

Es por lo que la ciberseguridad busca proteger los computadores, servidores y componentes móviles, electrónicos, redes y datos de los ataques maliciosos, a través de políticas, acciones y herramientas de seguridad que ayuden a proteger dichos activos.

Lo anterior refleja la importancia de proteger la información e infraestructura física y lógica, más teniendo en cuenta que la información es uno de los activos más relevantes de cualquier organización.

Por lo general la información en las entidades públicas de Colombia, está clasificada de diferentes formas, entre las cuales puede haber información confidencial, que son de uso interno únicamente, la pérdida o robo de información de este tipo podría poner en riesgo la privacidad de las personas, reducir la confiabilidad de la entidad o causar daños a la misma.

Para evitar dichas prácticas ciberdelincuenciales, Boston Consulting Group (BCG)[74] recomienda algunos aspectos que a nivel organizacional pueden ayudar a prevenir ataques, sobre todo por la masiva práctica de trabajo remoto, entre los cuales están a manera general:

- Evaluar las Infraestructuras tecnológicas
- Tener dispositivos y aplicaciones seguras
- Integrar la Ciberseguridad Empresarial

[73]. BID-OEA. 2020. Reporte Ciberseguridad

[74] REVISTA DINERO. Boston Consulting Group. Ciberseguridad los riesgos que puede traer el teletrabajo. [En línea]. Disponible en: https://www.dinero.com/management/articulo/los-riesgos-del-teletrabajo-en-ciberseguridad/284349

4.2.3 Ciberseguridad en Sitio

Una de las principales inquietudes en las organizaciones es la Seguridad Informática y no sólo en Colombia sino que es una preocupación a nivel global.

Es un hecho que las organizaciones deben velar entre otros puntos, por la protección de los datos no solo de la entidad, también de sus clientes. Las constantes amenazas o ciberataques siempre han estado sucediendo no solamente en esta época de pandemia ya antes había estadísticas que lo demuestran, por diferentes circunstancias y sobretodo originadas en sitio.

El estudio de Tendencias del Cibercrimen en Colombia, que fue elaborado por la Cámara Colombia de Informática y Telecomunicaciones (CCIT), el Centro para la Ciberseguridad de Colombia de la Policía Nacional y el Tanque de Análisis y Creatividad de las TIC (TicTac), para el período 2019, muestran un incremento de incidentes cibernéticos de más del 50% respecto al año 2018, estos hallazgos hacen parte de sucesos con origen únicamente en sitio y son realizados por empleados o exempleados[75].

Por lo anterior, es que el informe hace énfasis en que las organizaciones deben fortalecer los procedimientos y protocolos de seguridad informática y porque también muchos de los eventos delincuenciales se deben en gran parte a errores humanos, lo que indica que las empresas deben preocuparse no solo por los ciberdelincuentes, también por los empleados.

Los incidentes de ciberseguridad están representando grandes pérdidas millonarias para las empresas, con lo cual queda evidenciado la falta de estrategia integral o gestión de riesgos para la seguridad informática.

4.2.3.1 Riesgos asociados al trabajo en sitio

Los incidentes de vulnerabilidades en las organizaciones relacionadas a la seguridad informática pueden deberse a factores internos como externos. Por lo cual es indispensable detectar las conductas que ponen en riesgo la ciberseguridad, entre las cuales pueden estar las siguientes:

- Uso de dispositivos externos en los equipos de la organización, como por ejemplo las USB, siempre deben ser analizados estos dispositivos o en su defecto formateados para evitar algún virus.
- Acceso a redes sociales en equipos de la organización. Indiscutiblemente esta acción puede generar riesgo por la descarga de archivos
- Acceso al correo de la empresa desde el teléfono móvil con conexión wifi pública, de esta forma se expone los datos de la organización.

[75] CCIT – SAFE – TICTAC – POLICÍA NACIONAL. Informe tendencias Cibercrimen. [En línea]. 2019. Disponible en: https:en//www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

- Olvidar cerrar la sesión o sin bloquear. Cualquiera puede acceder sin autorización.
- Descargar archivos con información institucional desde el correo personal. Todos los archivos deben ser analizados por el antivirus de la organización.
- Subir documentación a la nube sin cifrar. Toda la información de la organización debe estar protegida.
- No realizar backups periódicamente. Debe ser responsabilidad tanto de la organización como del empleado.
- No revisar con detenimiento la habilitación de permisos innecesarios de los empleados
- Hacer envío de correos masivos es un riesgo alto
- Programas maliciosos

4.2.4 Prácticas tecnológicas del trabajo remoto y en sitio

A partir de este contexto, en este capítulo se describe la forma como se viene implementando el trabajo remoto y el trabajo en sitio, de acuerdo con los últimos estudios e investigaciones hechas entorno a las entidades públicas de Colombia.

Por ejemplo, en el documento de Medición de Teletrabajo del Centro Nacional de Consultoría, se permite evidenciar que la principal conexión para comunicación de los empleados que se encuentran en trabajo remoto son redes personales, inalámbricas, de Banda Ancha en su mayoría, sin embargo, también, es bueno aclarar que algunas entidades proveen conectividad móvil.

En cuanto a los dispositivos utilizados por los trabajadores de modalidad remota, cabe resaltar que, aunque es obligación de las entidades proveer dichos equipos, así como la conectividad, en su mayoría los dispositivos pertenecen al funcionario con un 81% smartphone y un 60% computador, por lo cual la cifra de otorgamiento de herramientas disminuyó considerablemente en relación con el 2014 que era del 63% y ahora sólo se otorga el 45%.

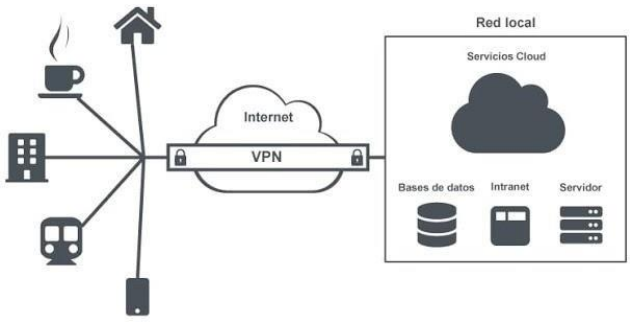
Adicionalmente, algunos equipos de los funcionarios no cuentan con antivirus comerciales, sino que en su mayoría de casos son libres, pero que no cuentan con todas las herramientas necesarias para una debida protección. Otro punto en desventaja, aunque no muy elevado, pero si ocurrente es que en algunos casos los equipos son compartidos por más miembros de la familia.

El tema de contraseñas también es un factor relevante a nivel del empleado ya que en muchas ocasiones tienen la misma clave para diferentes dispositivos.

El tipo de conexión para el trabajo remoto de las entidades públicas que lo implementan es de un 92% por medio de Red Privada Virtual -VPN, similar a la que podemos evidenciar en la figura 9. Por otro lado, el 84% de las entidades lo hacen

con acceso a escritorio remoto y otra gran parte con las dos conexiones simultáneamente.

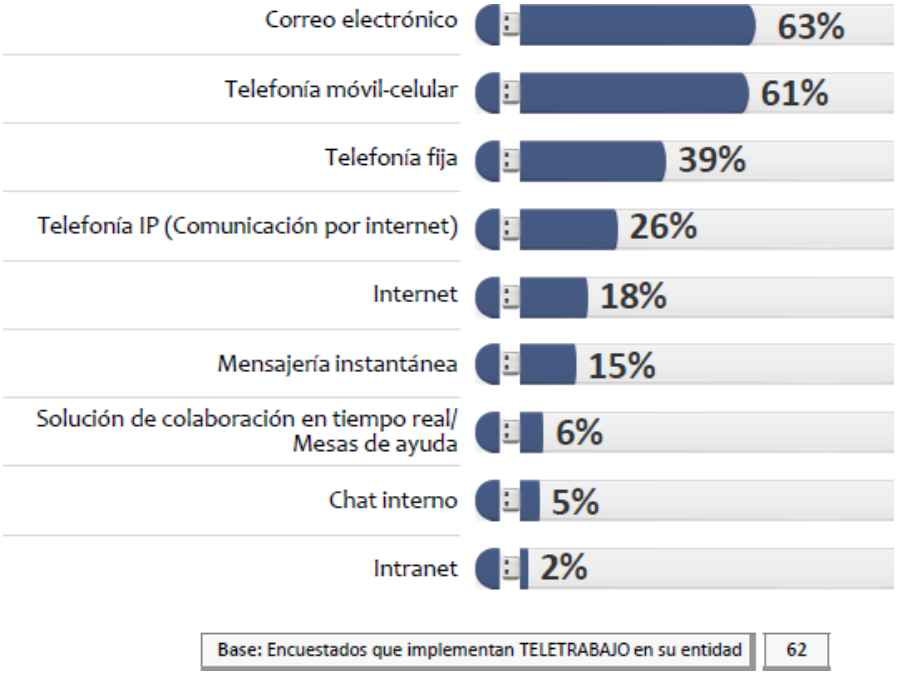
Figura 9. Red Privada Virtual VPN



Fuente: INCIBE

Los principales mecanismos de comunicación entre el trabajador y la entidad que más se han visto reflejados en medio de la pandemia, ha sido correo electrónico y telefonía celular, como se aprecia en la figura 10.

Figura 10. Medios de comunicación utilizados por las entidades públicas de a través del trabajo remoto



Fuente: Centro Nacional de Consultoría. 2019.

Igualmente, en esta época se ha incrementado el uso de la redes de Whatsapp y Telegram como herramientas de mensajería y comunicación; para el

almacenamiento en la nube se realiza a través de One drive y Google drive y para las video conferencias Teams y Hangaust.

Al respecto de la redes de mensajería como herramientas de comunicación en la modalidad de trabajo remoto, en la tabla 3, se evidencian algunas de las vulnerabilidades que determinan lo inconveniente que puede ser su uso en las entidades públicas para la seguridad de la información.

Tabla 3. Vulnerabilidades en el uso de las aplicaciones Telegram y WhatsApp como mensajería

Telegram	Whatsapp
Vulnerabilidad: CCN-CERT IA-23/17 Riesgos de uso de Telegram Referido a riesgos de uso de plataforma	**Vulnerabilidades y fallos de seguridad** Desde el 2019 ha presentado diferentes fallos de seguridad, como el hackeo al móvil a través de llamadas, independiente si se dé respuesta o no. Ha permitido ejecutar códigos malignos de forma remota con sólo recibir gifs o con archivos MP4.
El protocolo de comunicaciones utilizado MTProto – está enfocado en la multiplataforma, multisesión y el transporte de archivos sin tener en cuenta formato o capacidad.	**Las copias de Seguridad No cuentan con cifrado** Los chat que se guardan como copia de seguridad y que quedan en Google drive o Cloud no quedan cifradas.
El cifrado se realiza con Cloud Chat, no muy recomendable ya que obliga a los usuarios a confiar en las medidas de seguridad y de almacenamiento y política de privacidad de Telegram.	**Plataforma dependiente** En el caso de querer utilizar WhatsApp web, no se puede utilizar sin tener encendido el teléfono móvil o si el móvil no tiene internet o si está lejos del computador, es decir depende exclusivamente del celular.
Tiene sincronización de contactos	**No ofrece privacidad total** Los chas quedan almacenados en los servidores de WhatsApp, inclusive los que haya borrado el usuario.
Realiza monitorización de usuarios, según informe del Centro criptológico nacional	**Ubicación Detectada** WhatsApp puede deducir fácilmente la ubicación del usuario, con solo instalar la aplicación en el móvil.
	Solicita que el número de teléfono sea compartido Una vez instalada la aplicación WhatsApp solicita que el número del móvil sea compartido, con lo cual no está de acuerdo la mayoría de los usuarios.

Fuente: elaboración propia

A manera de resumen en la figura 11, se presenta las diferencias entre el teletrabajo y el trabajo en sitio por las actuales circunstancias del COVID-19, de acuerdo al

estudio elaborado por la Federación de aseguradores colombianos – Fasecolda[76], como iniciativa a la emergencia generada por la pandemia y del cual presenta la situación real.

Figura 11. Semejanzas y Diferencias del teletrabajo y trabajo en casa por las actuales circunstancias a Covid-19

Fuente: FASECOLDA

En este contexto también es importante mencionar algunas ventajas del trabajo remoto tanto para el empleado como para las organizaciones, a nivel personal y de producción.

Ventajas trabajo remoto tanto para el empleado como para el empleador

- Mayor productividad lo que equivale mayor ingresos
- Mayor motivación de los empleados
- Reducción costos infraestructura física
- Disminución costo servicios públicos
- Contratación de personal mejor calificado, ya que no requiere de presencia física

[76] FASECOLDA. Guía de buenas prácticas del trabajo remoto para el sector asegurador.

- Mejor distribución de espacio físico para personal de oficina
- Mejor distribución de tiempo ya que se evita los tiempos de desplazamiento
- Reducción de costos para ambas partes

Beneficios Responsabilidad Social

- Inclusión de población vulnerable o en situación de discapacidad
- Reducción del transporte asociado a las jornadas laborales
- Aporte a la calidad de vida de los trabajadores
- Reducción índice de contaminación

Desventajas del trabajo remoto
Según un estudio de la Universidad Simón Bolívar de Barranquilla[77], relaciona que no sólo hay ventajas, sino que también se presentan algunas desventajas en el trabajo remoto como son:

- Dificultad para trabajo en equipo
- Pérdida de jerarquía y se termina trabajando sin mucho lineamiento
- Dificultad de organización individual
- Exceso de jornadas extensas
- No estar totalmente seguro de que el trabajador tenga los protocolos de seguridad

Desventajas del trabajo remoto referidas a la Ciberseguridad

- Exposición a ataques más frecuentes, sofisticados impredecibles y complejos.
- Incrementos en presupuesto e inversiones para la seguridad de la información por parte de la Organización
- Que los empleados no tengan conciencia de los riesgos
- Que no logren identificar amenazas y expongan la información a riesgos.

4.2.5 La vulnerabilidad de la información en el trabajo remoto

La vulnerabilidad está definida por INCIBE[78] como fallos o agujeros que son detectados en aplicaciones, que el malware utiliza para infectar y propagarse. Lo que es aprovechado por atacantes para intrusiones y realizar acciones indebidas.

Esto lo que evidencia es la debilidad en el sistema permitiendo posibilidad para que un atacante pueda trasgredir la confidencialidad, integridad, disponibilidad de la

---

77 UNIVERSIDAD SIMÓN BOLIVAR. Investigadores identificaron las ventajas y desventajas del teletrabajo en Colombia. [En línea]. 2020. Disponible en: https://unisimon.edu.co/blog/investigadores-identificaron-las-ventajas-y-desventajas-del-teletrabajo-en-colombia/1939

78 INCIBE. Las 30 mayores vulnerabilidades explotadas por los ciberatacantes

información. Estas vulnerabilidades son generadas en su mayoría de casos por fallas en el diseño de algún software, sin embargo, puede ser también producto de condiciones de la tecnología para la que fue creado y que no cumple con la seguridad necesaria.

Cuando las vulnerabilidades no se corrigen se da puerta abierta para que atacantes accedan de forma sencilla a las aplicaciones y logren robar información, suspender el servicio o realizar daños a la imagen de la organización.

Las aplicaciones que más son atacadas en la mayoría de las organizaciones son la red de internet explorer, Windows, SQL server, office, java, OpenSSL, entre otras, son las más consideradas como vulnerables[79].

Por otro lado, si tenemos en cuenta la modalidad del trabajo remoto, aunque hay bastante ventajas para las organizaciones, relacionadas con mayor productividad y disminución de costos entre otras, no obstante, también es evidente la transmisión de datos e información confidencial en muchos casos a través de dispositivos sin la seguridad requerida.

Igualmente, dentro de estas amenazas informáticas, se deben contemplar los riesgos que fuera del entorno institucional tiene una alta probabilidad de ocurrencia, como pueden ser las vulnerabilidades y amenazas que casi siempre son aprovechables por ciberdelincuentes, algunas de ellas, se relacionan en la tabla 4.

[79] INCIBE. Las 30 mayores vulnerabilidades explotadas por los ciberatacantes. [En línea]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/30-mayores-vulnerabilidades

Tabla 4. Amenazas y Vulnerabilidades detectadas fuera del entorno institucional

AMENAZAS	VULNERABILIDADES
Engaños basados en Ingeniería Social Actos de manipulación a las personas, con el fin de obtener información privilegiada o acceso a sistemas o robo de activos, suplantación. Puede ser a través de redes, teléfono, personalmente, entre otras técnicas.	**Conexión en redes inseguras** Usar redes wifi-púbicas, genera un alto riesgo, se incrementa la exposición a ataques efectivos y difíciles de detectar, los más comunes son los robos de datos personales e información confidencial.
Ejecución de exploits: Programas con código que buscan explotar vulnerabilidades de software o seguridad.	**Información sin cifrar** El cifrado de información es la conversión de los datos a formato codificado.
Pérdida y daño de dispositivos Puede generar amenaza dado que la información del equipo puede quedar en manos ajenas o si es por daño puede perderse.	**Antivirus obsoletos** Programa con el objeto de detectar y eliminar virus. Por lo que se hace necesario mantenerlos actualizados de lo contrario puede generar vulnerabilidad
No realizar Backups periódicamente No contar con los respectivos respaldos de la información es un riesgo para la organización, dado que pueden presentarse incidentes o amenazas y los datos son vitales para la empresa y sus clientes.	**Contraseñas débiles** Contraseña o clave es la Forma de autenticación para acceso a un sistema, programa o aplicación. Debe cumplir con los parámetros de seguridad para evitar vulnerabilidades.
	Falta de actualización de software Sino se mantienen actualizadas las aplicaciones, pueden generarse vulnerabilidades las cuales pueden ser explotadas a través de ataques. También es importante evitar el software gratuito.

Fuente: elaboración propia

Las entidades públicas, deben abordar con pertinencia los desafíos ligados tanto a la práctica laboral remota como al trabajo en sitio. De lo contrario es probable que la información quede en riesgo, así como su confidencialidad.

Adicionalmente es fundamental que las entidades revisen con atención la tecnología y seguridad que utilizan los empleados remotos, inclusive deben suministrar todos los dispositivos necesarios para la realización de la actividades de manera segura.

4.2.6 Importancia de Proteger la Información

La información es a menudo uno de los activos más importantes que una empresa posee ya que la misma marca la diferencia y proporciona ventajas que llevan a dicha empresa u organización a ser más exitosa

La información se puede clasificar en diferentes categorías con el fin de controlar el acceso a la misma en función de su importancia, su sensibilidad y su vulnerabilidad al robo o al mal uso, basado en esta clasificación las organizaciones deciden asignar más recursos para controlar la información que tiene mayor sensibilidad.

Las organizaciones clasifican la información de diferentes maneras con el fin de gestionar de forma diferente aspectos de su manejo, la información destinada a uso interno que se entiende generalmente puede ser vista por los empleados, contratistas y proveedores de servicios, pero no por el público en general. Este tipo de información suele ser menos restringida, ya que no se gasta mucho tiempo y dinero en la protección, debido a que no supera el valor de la información o el riesgo de su divulgación.

Las entidades pueden tener información confidencial, como puede ser, la planeación de temas misionales, de desarrollo e investigación la planeación estratégica, hasta la estructuración de los procesos.

El propósito de la seguridad de la información es dar protección a los activos más valiosos de cualquier organización, ya sea el software, hardware o los datos, por medio de mecanismos adecuados que protejan la seguridad, lo que representará una mejor desenvolvimiento, confiabilidad y reputación de la organización.

El valor de la información proviene de las características que posee. Cuando una característica de información cambia, el valor de esa información aumenta, por ejemplo, los datos personales de los clientes, procesos de producción, balances financieros e informes de resultados o proyecciones son estrictamente de uso exclusivo ya sea para empresa o para el cliente, el que esta información pueda ser hurtada o modificada sin autorización, lo más probable es que reduzca la competitividad de la organización.

4.3 OBJETIVO 3: ESTABLECER UNA SERIE DE RECOMENDACIONES DE BUENAS PRÁCTICAS DE CIBERSEGURIDAD PARA EL TRABAJO REMOTO EN ENTIDADES PÚBLICAS COLOMBIANAS, CON EL FIN DE CONTRIBUIR EN LA REDUCCIÓN DE BRECHAS DE INSEGURIDAD.

A medida que avanza los efectos generados por la pandemia del Coronavirus (COVID-19), se han incrementado las acciones de las instituciones públicas de Colombia, en torno a garantizar una ciberseguridad más confiable en marco del trabajo remoto que se ha generalizado como medida de desenvolvimiento laboral y a fin de velar por el bienestar de sus empleados.

Sin embargo, queda entre dicho si se han tomado todas las medidas concernientes para un trabajo seguro, que permita reducir las brecas de inseguridad, dado los innumerables ciberataques sufridos en todos los niveles durante el 2020, como lo evidencia el informe del portal de Fortinet el cual menciona que, en América Latina y el Caribe, el registro de intentos de ciberataques superan los 41 billones[80], de los cuales 1.6 mil millones los sufrió Colombia en el último trimestre de 2020[81].

Dentro de las amenazas más frecuentes estaban los correos electrónicos de phishing con adjuntos de archivos HTML que trataban de redirigir las páginas a sitios maliciosos, quedando evidenciado que el trabajo remoto se convirtió en una puerta de acceso por las vulnerabilidades de los enrutadores domésticos, permitiendo a los ciberdelincuentes ejecutar comandos maliciosos, dado que los empleados laboran con menos protección, pero con mayor acceso a la información corporativa.

Otro punto importante que menciona el informe de Fortinet es la sofisticación y a la vez eficiencia con que se están realizando estos ciberataques, ya que muchos de ellos son con tecnología de inteligencia artificial[82].

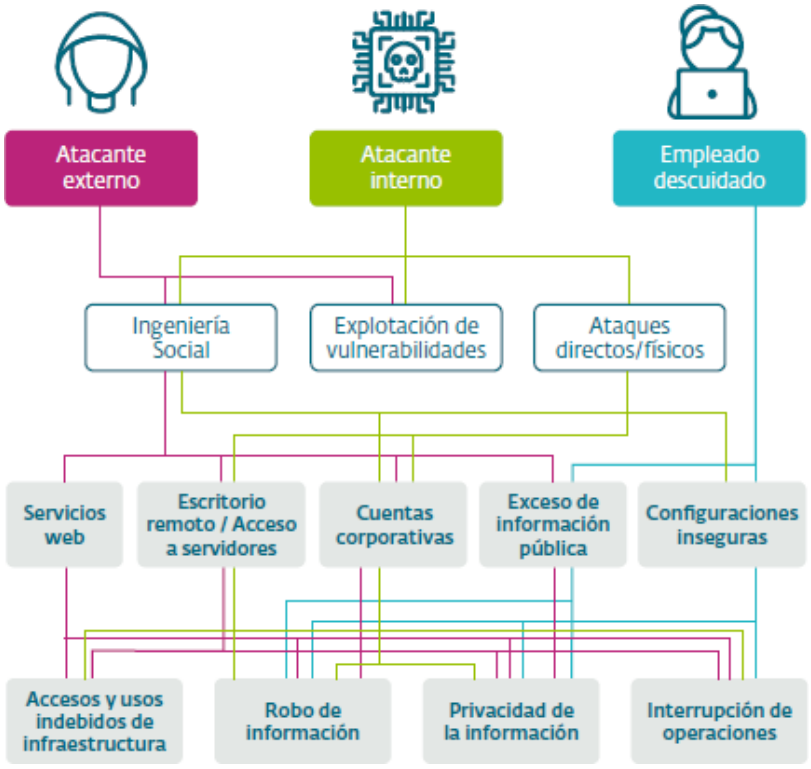
En ese contexto, es importante tener presente los puntos de entrada por los cuales se puede llegar a recibir un ataque, para tomar las medidas más pertinentes. En la figura 12, se presenta un diagrama que fue elaborado por el Laboratorio de Investigación ESET, el cual representa las vías más utilizadas por los atacantes para la ejecución, así como también hace énfasis en las probabilidades que los ataques también puedan surgir dentro de la entidad, no sólo desde fuera.

[80] PORTAL FORTINET. América Latina sufrió más de 41 billones de intentos de ciberataques en 2020. [En línea]. Disponible en: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2021/latin-america-suffered-more-than-41-billion-cyberattack-attempts-in-2020

[81] Ibit., p.2

[82] Ibít.,p.2

Figura 12. Vías más utilizadas para los atacantes de una Organización



Fuente: Laboratorio de Investigación ESET

Lo que se evidencia en la figura 12, es que la ingeniería social y la explotación de vulnerabilidades, son las rutas más aprovechadas por un atacante, luego de lograr el acceso realizan diferentes actos maliciosos. Igualmente es importante resaltar que las vulnerabilidades también se pueden generar por descuido o falta de buenas prácticas de los empleados.

En este contexto, se presentan algunas consideraciones y recomendaciones como buenas prácticas que se pueden implementar para una mejor ciberseguridad dentro de las entidades públicas y así reducir las brechas de inseguridad establecidas como son la ingeniería social, explotación de vulnerabilidades y ataques directos y físicos.

Adicionalmente es importante tener en cuenta que también para mitigar esas brechas de seguridad se debe tener un plan de contingencia que permita erradicar las amenazas y que se repitan.

4.3.1 Implementación política de seguridad

En la modalidad de trabajo remoto se hace indispensable que las entidades públicas no sólo diseñen, sino que implementen políticas de seguridad que permitan abordar con mayor eficiencia y capacidad el procesamiento y conectividad, dada la gran demanda por la masividad generada por la pandemia.

Como punto de partida es indispensable que la política de seguridad tenga clasificada la información a fin de establecer cuál es la información más sensible a proteger, a cuál se puede acceder remotamente o cuál debe tener restricción total. De esta forma es más sencillo determinar cuáles son los riesgos de mayor probabilidad de ocurrencia y establecer los controles más pertinentes.

Asimismo, es indispensable que la organización pueda contar con toda la información del trabajador, su entorno laboral tipos de acceso al sistema, revisar las restricciones que debe tener el equipo y sobre todo un procedimiento para el uso pertinente de los dispositivos electrónicos. Esto con el fin de determinar posibles vulnerabilidades para la entidad.

Lo más indicado es que la institución proporcione los equipos necesarios para el trabajo remoto, sin embargo, hay que tener en cuenta que muchos de sus empleados trabajan con equipo propio. Independientemente de la elección, la organización debe considerar el soporte técnico, para evitar inconvenientes, esto definitivamente ayudara a mitigar cualquier amenaza o riesgo informático.

4.3.2 Fortalecimiento gestión de acceso

Las entidades deben tener como responsabilidad entre otras:

- Contar con una solución o herramienta de gestión de identidad para acceso a las aplicaciones de la institución.
- Realizar seguimientos a la gestión de ciberseguridad
- Tener claro los procedimientos para detectar cuentas huérfanas o en su defecto prevenirlas o eliminarlas[83].
- Revisión minuciosa de privilegios

Entre los anteriores ítems, la revisión de privilegios es muy importante realizarla detalladamente en cada uno de los usuarios, revisar responsabilidades y de esta forma detectar a que recursos se puede acceder y quien no debe tener esos accesos habilitados, esto reflejara una forma de gestión de seguridad tanto en los dispositivos, aplicaciones como en los sistemas operativos.

Cada empleado debe acceder únicamente a las aplicaciones relacionadas con sus tareas y por el tiempo estrictamente necesario para su ejecución como se evidencia en el esquema de la figura 13.

[83] DELOITTE, Consideraciones generales de Ciberseguridad en medio de una pandemia global. 2020

Figura 13. Esquema de privilegios necesarios

Fuente: 3CIENCIAS. Introducción a la seguridad Informática y Vulnerabilidades

4.3.3 Concientizar la probabilidad de nuevas amenazas

Dado que los empleados en su mayoría no estaban a costumbrados a trabajar remotamente, pueden estar con tendencia a cometer errores o realizar acciones no seguras, como compartir las credenciales de acceso o la información privada. Igualmente se ha evidenciado la vulnerabilidad a la ingeniería social, en especial en estas circunstancias de pandemia, por lo que realizar actividades de concientización a los empleados respecto a la seguridad informática puede dar mejores resultados a la seguridad establecida por la organización.[84]

Adicionalmente, esto se puede controlar con mensajes de concientización en relación a los siguientes procesos:

- El correo se debe limitar únicamente a su uso institucional, así como tampoco se debe permitir el uso de cuentas personales para tratar temas laborales. La contraseña debe contemplar los requisitos de asignación de seguridad.

84 ROMERO CASTRO, Martha Irene, *et al*. Introducción a la seguridad Informática y Vulnerabilidades. Ingeniería y Tecnología. Alcoy (Alicante). 3ciencias. Primera Edición 2018.

- El correo institucional no se debe utilizar para envíos de cadenas masivas.
- Desconfiar de los correos electrónicos con archivos adjuntos o hipervínculos con llamadas alusivas a redes sociales, rifas o que no sean de fuentes confiables.
- No dar respuesta a través del correo de solicitudes de información financiera
- Se debe controlar el uso de dispositivos extraíbles ya sean periféricos o como por ejemplo USB.
- El almacenamiento de copia de archivos o de descarga debe ser limitado.

4.3.4 Gestionar las conexiones remotas

Las instituciones deben revisar e identificar los requerimientos para la conexión remota, evitar excepciones que desmejoran la seguridad. Hoy en día se ha incrementado el acceso remoto a través de dispositivos no corporativos, esto podría generar exposición de información confidencial en redes sociales. En los hogares han ingresado muchos dispositivos inteligentes pero que en realidad no tienen una seguridad confiable, sin soporte y sin actualizaciones o como menciona INCIBE en diversas ocasiones los empleados acceden remotamente a las aplicaciones de las instituciones en lugares inusuales como cafeterías, hoteles o salas de internet[85].

- Configuraciones Equipos

Los equipos y dispositivos que requieran de instalaciones, actualización o eliminación de software deben ser configurados únicamente por el personal autorizado para dichas tareas.

- Métodos de acceso remoto

Para el acceso remoto se recomienda realizarlo a través de VPN o escritorio remoto, ya que genera más confiabilidad.

- **VPN**

El acceso remoto a través de VPN, lo que permite es proteger las comunicaciones entre el equipo del empleado y la red interna de la entidad, si se utiliza Internet como medio de acceso.

La VPN (Virtual Private Network) permite el envío de datos de una red privada por medio de una red pública de manera confidencial y segura, ya que se realiza a través de un túnel de comunicación cifrada entre el dispositivo y el lugar de trabajo, evitando que no sea interceptado el tráfico enviado a través de internet.

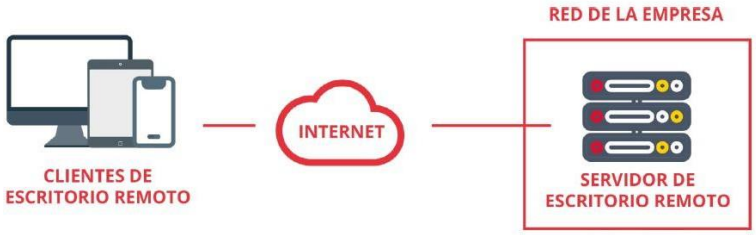
- Escritorio Remoto

[85] INCIBE. Ciberseguridad en el Teletrabajo. Una aproximación para el empresario.

La conexión a través del escritorio remoto es simple, sólo basta tener una aplicación y el teletrabajador lograr controlar el equipo de la oficina remotamente (figura 14), sin embargo, las organizaciones deben verificar que cumpla con medidas suficientes de seguridad, para evitar amenazas y vulnerabilidades dentro de la red de la organización, como las relacionadas a continuación:

- Tener todo el software actualizado
- Evitar utilizar sistemas operativos que ya no posean soporte
- Que las contraseñas sean robustas y estar modificándolas periódicamente
- Elegir acertadamente la red
- Dejar el usuario por defecto para acceso y no ingresar por administrador
- Establecer reglas claras para el firewall

Figura 14. Esquema de acceso remoto



Fuente: INCIBE

Dentro de las recomendaciones más importantes para una mayor seguridad del acceso remoto es utilizar simultáneamente una VPN y el escritorio remoto. Esto hará más eficaz la privacidad y seguridad de la red corporativa.

4.3.5 Virtualización

Una gran alternativa de las instituciones para la modalidad del trabajo remoto es la virtualización de sus entornos. Este enfoque da más seguridad para que la organización tenga mayor control ya sea sobre las aplicaciones o sobre los datos y elimina los riesgos asociados al uso del equipo de propiedad del empleado.

Al estar en un entorno virtualizado se pueden agregar más controles, incluso los archivos estarían dentro de los servidores de la organización y en ningún momento pueden ser transferidos al equipo desde el cual accede el empleado.

Este método no es 100% seguro, pero se lograr incrementar el nivel de protección al limitar al empleado al uso de la información en su dispositivo.

4.3.6 Gestionar Plan de Recuperación

Las entidades públicas deben estar preparadas para posibles ciberataques con excelentes estrategias que den oportuna respuesta a incidentes y solución efectiva. Estas estrategias van a permitir mitigar el impacto, incluso evitar la explotación de vulnerabilidades.

4.3.7 Gestionar Protección Física a los dispositivos

Los dispositivos de las entidades deben estar protegidos de y pérdidas con opciones como, por ejemplo,

- Mantener cifrado completo en el disco
- Cerrar sesión mientras no esté usando el dispositivo, ya sea en el hogar como en sitios públicos, con esto se limita la opción de que acceda a la información.
- Aplicar la política de contraseñas seguras al inicio, establecer tiempo de suspensión en instantes de inactividad y no utilizar contraseñas que quedan pegadas al equipo.

4.3.8 Entorno tecnológico en casa

Para que este entorno sea confiable los empleados deben revisar constantemente las vulnerabilidades, sobre todo cuando se deba conectar los equipos a las red. Se deben tomar medidas con contraseñas seguras cuando se utiliza WIFI y mantener actualizado a las últimas versiones tanto el software como el firmware.

4.3.9 Capacitación

Realizar capacitación sobre Ciberseguridad por parte de la organización a los empleados es fundamental. Esto evita errores humanos que es los ciberdelincuentes intentar tanto explorar. Dicha capacitación no sólo debe estar enfocada a los principales conceptos de seguridad digital, sino que también se debe sensibilizar sobre la importancia de la misma.

5 CONCLUSIONES

Como conclusión del primer objetivo y revisando el compendio de políticas de seguridad existentes en Colombia y sobre todo a nivel institucional, evidencio que representan un excelente medio para operar y dar uso adecuado a los recursos informáticos de manera estructurada y con estándares internacionales.

Como conclusión del segundo objetivo, se tiene que el trabajo remoto evidentemente no sólo es un beneficio para las instituciones en las actuales circunstancias, sino que también beneficia al empleado, por lo que se hace fundamental que ambas partes, no sólo la organización tome conciencia de la seguridad necesaria para realizar esta actividad como se ejecuta normalmente en sitio.

La adopción de mejores prácticas de ciberseguridad para el trabajo remoto va permitir a las instituciones que consoliden una defensa sólida contra posibles ataques y vulnerabilidades informáticas.

El Modelo de Gestión de Riesgo, es un buen aporte de lineamiento para la evaluación del Riesgo dentro de las instituciones.

Las amenazas de ciberseguridad por la alta demanda de acceso remoto en las entidades es una realidad que seguirá incrementándose si no se tienen en cuenta todas las recomendaciones técnicas.

En caso tal que disminuya el acceso remoto o que de alguna forma se vuelva en algún momento a la normalidad, es decir terminen los aislamientos masivos, las entidades tendrán que ajustar todas las excepciones especiales y dejar solo las configuraciones puntuales y realizar una actualización, estableciendo medidas para los procesos rutinarios de la operación y retornar a la seguridad habitual, bajo la premisa de cero confianza.

El conocimiento adquirido a través de este estudio es un gran aporte para un mejor desempeño profesional y tecnológicamente más eficaz y seguro.

6 RECOMENDACIONES

Socializar las políticas de seguridad aplicadas al acceso remoto a todos los empleados de las entidades públicas, puede ser que no todos las conozcan.

Las entidades deben efectuar una revisión a los dispositivos utilizados por los empleados que no son de propiedad de la institución.

Incentivar y crear mecanismos para que los empleados de las entidades adopten buenas prácticas tecnológicas y de seguridad en su entorno de acceso remoto, esto permitirá reducir las brechas de seguridad.

Se recomienda a las entidades que establezcan si los empleados, realmente necesitan acceder a la red organizacional o si únicamente es necesario acceso a correo electrónico y servicios que estén en la nube, así como definir si deben mantener el mismo nivel de acceso a la información cuando se está laborando en sitio a cuando está desempeñando sus labores de manera remota.

Los equipos de los empleados deben contener la misma política de un computador de la organización, desde las aplicaciones firewalls, antimalware, entre otras. En estas eventualidades como la que se vive actualmente por la pandemia del Covid-19, los proveedores pueden ofrecer más licencias en caso de requerirse para los equipos de los empleados, es decir es necesario que se le otorgue al empleado licencias de las mismas condiciones de la entidad.

Las instituciones deben realizar seguimiento a las situaciones anormales o accesos sospechosos y ejecutar planes de seguridad, así como poner énfasis especial a los manejos de usuarios con acceso privilegiado.

El monitoreo debe estar enfocado sobre todo en uso de información confidencial.

Es recomendable que las instituciones realicen oportunamente copias de la información disponible en la nube, así como de la información histórica.

Lo ideal para garantizar un acceso autenticado es que se utilice una herramienta de aplicaciones o token que genere códigos únicos.

Los protocolos de comunicación tanto para los empleados como para los responsables de TI, deben ser claros y concisos si llegase a presentarse un problema inusual. Asimismo, se debe considerar aplicaciones seguras de toma de control remoto.

BIBLIOGRAFÍA

ÁLVAREZ MARAÑÓN, Gonzalo. Seguridad informática para empresas y particulares. Madrid etc, Spain: McGraw-Hill España. G. (2004). p. 20 – 41. Recuperado de https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/50050?page=1

ASSUL, Miguel. Blog. Los grandes retos de trabajar con equipos remotos y cómo superarlos. [En línea]. 2018. Disponible en: https://www.workana.com/blog/emprendimiento/7-grandes-retos-de-trabajar-con-equipos-remotos-y-como-superarlos/

BID – OEA. Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. 2020.

BORDA PÉREZ, M. (2013). El proceso de investigación: visión general de su desarrollo. (Pag 14-16) Barranquilla, Colombia: Universidad del Norte. Recuperado de https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/69882

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Evaluación, Retos y Amenazas a la Ciberseguridad. [En línea]. 2021. Disponible en: https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf

CENTRO CIBERNÉTICO POLICIAL. Balance cibercrimen. Bogotá. [En línea]. 2020. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-semana_45.pdf

CIBERSEGURIDAD – MARCO NIST. Un abordaje integral de la ciberseguridad. OEA. 2019.

COLOMBIA. FUNCIÓN PÚBLICA. Decreto 491 Emergencia Sanitaria (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 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. Bogotá. 2020.

COLOMBIA. FUNCIÓN PÚBLICA. Decreto 491 Emergencia Sanitaria (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 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. Bogotá. 2020.

COLOMBIA. OEA. Ley 273. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – Denominado "De la Protección de la Información de y de los Datos" y se preservan integralmente los sistemas que utilicen las Tecnologías de la Información y las Comunicaciones, entre otras disposiciones". 2009.

COLOMBIA. MINTIC. Decreto 884 de 2012. Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones. [En línea]. Disponible en: https://www.mintic.gov.co/portal/inicio/3638:Decreto-884-de-2012

COLOMBIA. PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Ley 1928 de 2018, Por medio de la cual se aprueba el «Convenio sobre la Ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest. Bogotá, D.C 2018.

CONSEJO NACIONAL POLÍTICA ECONÓMICA Y SOCIAL. CONPES 3854 Departamento Nacional de Planeación. 2020. Política Nacional de Seguridad Digital.

CIFUENTES, Aura. Política Nacional Digital [video]. Bogotá, Colombia: YouTube. MinTic. (25 de septiembre de 2020). 35:40 minutos. [consultado 20 de noviembre de 2020]. Disponible en: https://www.youtube.com/watch?v=5bXI6CdH8gQ&t=1025s

DEPARTAMENTO NACIONAL DE PLANEACIÓN – DNP. Documento Conpes 3701. [En línea]. 2018. Disponible en: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

DEPARTAMENTO NACIONAL DE PLANEACIÓN. Protección de datos. [En línea]. 2019. Disponible en: https://www.dnp.gov.co/programa-nacional-del-servicio-al-ciudadano/Paginas/Proteccion-de-datos-personales.aspx

DELOITTE, Consideraciones generales de Ciberseguridad en medio de una pandemia global. Bogotá, D.C. 2020.

DI MARTINO, Vittorio. 2004. El teletrabajo en América Latina y el Caribe. Ginebra. Fuente: www.idrc.ca (Consultado el: 01-02-2010).

ESCRIVÁ GASCÓ, Gonzalo. (2013). Seguridad informática. Macmillan Iberia, S.A.

ESET, «WeliveSecurity,» Miguel Angel Mendoza.. [En línea]. 16-06- 2015. Disponible en: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/ .

FASECOLDA. Guía de buenas prácticas del trabajo remoto para el sector asegurador. Bogotá, D.C., 2020.

FENALCO. DNP expidió Documento Conpes 3995 de 2020 de "Política Nacional de Confianza y Seguridad Digital". [En línea]. 2020. Disponible en: http://www.fenalco.com.co/gesti%C3%B3n-jur%C3%ADdica/dnp-expidi%C3%B3-documento-conpes-sobre-pol%C3%ADtica-nacional-de-confianza-y-seguridad

FREIRE LÓPEZ, Kirk Bryan. Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad. Repositorio Digital. Universidad Católica de Santiago de Guayaquil. Repositorio Digital. [En línea]. 2017. Disponible en: http://repositorio.ucsg.edu.ec/handle/3317/9203

FUNCIÓN PÚBLICA. Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Bogotá, D.C. 2018.

GAMBOA SUÁREZ, José Luis. Importancia de la Seguridad Informática y Ciberseguridad en el mundo actual. Repositorio Institucional Universidad Piloto de Colombia. [En línea]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/8668

IBM. La Política de Seguridad. [en línea]. Disponible en: https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives

IPS TECHNOLOGY. Importancia dl teletrabajo seguro. [En línea]. Disponible en: https://ipsleon.com/acceso-remoto-y-vpn-la-importancia-del-teletrabajo-seguro/

ISACA (Information Systems Audit and Control Association) Capítulo Monterrey. [En línea]. 2015. Disponible en: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

MARSH . MICROSOFT. Estado del Riesgo Cibernético en Latinoamérica en Tiempos de COVID-19. Octubre. 2020. [En línea]. Octubre 2020. Disponible en: https://coronavirus.marsh.com/mx/es/insights/research-and-briefings/report-cyber-risk-in-latin-america-in-times-of-covid19.html

McCLURE, S., Scambray, J., & KURTZ, G. (2010). Hackers 6: secretos y soluciones de seguridad en redes. [En línea]. (Vol. 10) (pp 43-77). México DF: McGraw-Hill

Interamericana. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/37303?page=72

MEDICIÓN DEL TELETRABAJO EN ENTIDADES PÚBLICAS. Penetración y percepciones. [En línea]. 2019. Disponible en: https://www.teletrabajo.gov.co/622/articles-144782_recurso_1.pdf

MCCLURE, S., SCAMBRAY J., y KURTZ, G. (2010). Hackers 6: secretos y soluciones de seguridad en redes. [En línea]. (Vol. 10) (pp 7-42). México DF: McGraw-Hill Interamericana. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/37303?page=36

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Marco de Referencia que alinea la gestión tecnológica de las entidades públicas. [En línea]. Bogotá. Disponible en: https://www.mintic.gov.co/portal/inicio/Ministerio/Viceministerio-de-Transformacion-Digital/7729:El-Marco-de-Referencia-que-alinea-la-gestion-tecnologica-de-las-entidades-publicas

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Nodos: Ciberseguridad. [En línea]. Disponible en: https://www.mintic.gov.co/portal/inicio/Micrositios/I+D+I/Nodos/6120:Ciberseguridad

MINTIC. Modelo Nacional Gestión de Riesgos de Seguridad Digital. Bogotá, D.C. 2018.

MINTIC. Manual de Gobierno Digital. Implementación de la Política de Gobierno Digital Decreto 1078 de 2015 libro 2, parte 2, título 9. Cap. 1. [En línea]. Disponible: http://estrategia.gobiernoenlinea.gov.co/623/articles-7929_recurso_1.pdf

MORENO, L. M. (2019). Los nuevos retos en materia de ciberseguridad para Colombia. [En línea]. Disponible en: http://hdl.handle.net/10654/20664.

MORNING CONSULT. IBM SECCURITY. IBM Consumer Survey: Security Side: Effects Of the Pandemic. [En línea]. Junio 2021. Disponible en: https://filecache.mediaroom.com/mr5mr_ibmnews/191177/Pandemic%20Security%20Side%20Effects%20Global%20Survey_IBM%20Analysis.pdf

NOTICIAS DEL SEL SECTOR. Importancia de la seguridad digital. [En línea]. Disponible en: https://acis.org.co/portal/content/Noticiasdelsector/la-importancia-de-la-seguridad-digital-en-tiempos-de-covid-19

OBSERVATORIO DE INNOVACIÓN EDUCATIVA. La pandemia como un catalizador de una nueva cultura laboral. Paola Villafuerte. [En línea]. México. 2020 Disponible en: https://observatorio.tec.mx/edu-news/trabajo-remoto-postcovid19

OEA. Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina. [En línea]. 2019. Disponible en: https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

OPS. Organización Panamericana de Salud. Enfermedad por el Coronavirus. Covid-19. [En línea]. Disponible en: https://www.paho.org/es/tag/enfermedad-por-coronavirus-covid-19?topic=All&d%5Bmin%5D=&d%5Bmax%5D=&page=25

ORTIZ, Francisco. El teletrabajo una nueva sociedad laboral en la era de la tecnología. Madrid: McGraw Hill. España. 1995.

PORTAFOLIO. Empresas admiten que empleados laboran más en casa. [En línea]. 2020. Disponible en: https://www.portafolio.co/negocios/empresas/que-tan-preparadas-estaban-las-empresas-colombianas-para-el-trabajo-remoto-541592

PORTAFOLIO. Delitos informáticos, la otra pandemia en tiempos del coronavirus. [En línea]. 2020. Disponible en: https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642

PORTAL FORTINET. América Latina sufrió más de 41 billones de intentos de ciberataques en 2020. [En línea]. Disponible en: Https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2021/latin-america-suffered-more-than-41-billion-cyberattack-attempts-in-2020

PORTAL KIENYKE. https://www.kienyke.com/tecnologia/colombia-vivio-el-ano-con-mas-intentos-de-ciberataques

REVISTA DINERO. WEF alerta sobre aumento dramático de riesgos en ciberseguridad tras la pandemia. Bogotá. [En línea]. 2020. Disponible en: https://www.dinero.com/internacional/articulo/aumento-dramatico-de-riesgos-en-ciberseguridad-tras-la-pandemia/286804

RODRIGUEZ, Edson. RODRIGUEZ, Ingrid. Mejoramiento de las Buenas Prácticas de Seguridad Informática. 2013. Universidad Piloto de Colombia. Bogotá, D.C.

ROMERO CASTRO, Martha Irene, et al. Introducción a la seguridad Informática y Vulnerabilidades. Ingeniería y Tecnología. Alcoy (Alicante). 3ciencias. Primera Edición 2018.

SOLANO, Victor. Grandes Genios, Consultor en reputación. [En línea]. Disponible en: http://www.grandesgenios.co/digital-transforma-socorro

TECNOLOGÍA PARA LOS NEGOCIOS. El teletrabajo una alternativa para las empresas en tiempo de coronavirus. Cámara Valencia. España. [En línea]. Disponible en: https://ticnegocios.camaravalencia.com/servicios/tendencias/el-teletrabajo-una-alternativa-para-las-empresas-en-tiempos-de-coronavirus/

TELETRABAJO. Definición. [En línea]. Disponible en: https://www.teletrabajo.gov.co/622/w3-article-8228.html

TELEFÓNICA. Importancia de la Ciberseguridad. Blog de Políticas Públicas. [En línea]. Disponible en: https://www.telefonica.com/es/web/public-policy/blog/articulo/-/blogs/la-importancia-de-la-ciberseguridad

TIETZE, Susanne. MUSSON, Gillian. 2002. When “Work” Meets “Home”: Temporal Flexibility as Lived Experience. Time & Society 11 no. 2/3: 315-334

UNIVERSIDAD ESTATAL A DISTANCIA. Programa de Teletrabajo. Costa Rica. [En línea]. Disponible en: https://www.uned.ac.cr/viplan/teletrabajo/que-es-teletrabajo/historia

UNIVERSIDAD SIMÓN BOLIVAR. Investigadores identificaron las ventajas y desventajas del teletrabajo en Colombia. [En línea]. 2020. Disponible en: https://unisimon.edu.co/blog/investigadores-identificaron-las-ventajas-y-desventajas-del-teletrabajo-en-colombia/1939

VALOYES, Amancio. La Ciberseguridad en Colombia. Universidad Piloto de Colombia. [En línea]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6370/CIBERSEGURIDAD%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

ANEXOS

Anexo 1. Guía para la administración del Riesgo y el diseño de controles en Entidades Públicas de Colombia

Anexo 2. Plantilla RAE

Estructura del documento para la estructura del Resumen Analítica Especializado -RAE

Fecha de Realización:	26/09/2021
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Gestión de Sistemas
Título:	Importancia de las buenas prácticas en Ciberseguridad en el trabajo remoto de entidades públicas de Colombia en época de Pandemia
Autor(es):	Ortiz Osorio Myriam
Palabras Claves:	Amenaza, Buenas Prácticas, Ciberseguridad, Confidencialidad, Política, Trabajo remoto.
Descripción:	El documento refleja la importancia de implementar y mantener buenas prácticas como necesidad de abordar las brechas de seguridad generadas por el trabajo remoto generado de manera masiva por la pandemia en las instituciones públicas de Colombia.

Referencias Bibliográficas:

BID – OEA. Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. 2020.

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Evaluación, Retos y Amenazas a la Ciberseguridad. [En línea]. 2021. Disponible en: https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf

CIBERSEGURIDAD – MARCO NIST. Un abordaje integral de la ciberseguridad. OEA. 2019.

DELOITTE, Consideraciones generales de Ciberseguridad en medio de una pandemia global. 2020

DEPARTAMENTO NACIONAL DE PLANEACIÓN – DNP. Documento Conpes 3701. [En línea]: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

MINTIC. Manual de Gobierno Digital. Implementación de la Política de Gobierno Digital Decreto 1078 de 2015 libro 2, parte 2, título 9. Cap. 1. [En línea]. Disponible: http://estrategia.gobiernoenlinea.gov.co/623/articles-7929_recurso_1.pdf

Contenido del documento:

	4.2.5 La vulnerabilidad de la información en el trabajo remoto..... 4.2.6 Importancia de Proteger la Información ..... OBJETIVO 3: ESTABLECER UNA SERIE DE RECOMENDACIONES DE BUENAS PRÁCTICAS DE CIBERSEGURIDAD PARA EL TRABAJO REMOTO EN ENTIDADES PÚBLICAS COLOMBIANAS, CON EL FIN DE CONTRIBUIR EN LA REDUCCIÓN DE BRECHAS DE INSEGURIDAD..... 4.3.1 Implementación política de seguridad..... 4.3.2 Fortalecimiento gestión de acceso..... 4.3.3 Concientizar la probabilidad de nuevas amenazas..... 4.3.4 Gestionar las conexiones remotas ..... 4.3.5 Virtualización ..... 4.3.6 Gestionar Plan de Recuperación ..... 4.3.7 Gestionar Protección Física a los dispositivos ..... 4.3.8 Entorno tecnológico en casa ..... 4.3.9 Capacitación ..... 5 CONCLUSIONES..... 6 RECOMENDACIONES ..... BIBLIOGRAFÍA ..... ANEXOS .....
Marco Metodológico:	Consulta masiva de estudios, estadísticas, informes de referentes tanto académicos como de investigación y consultorías.
Conceptos adquiridos:	Después del desarrollo del trabajo de grado se reforzaron algunos conceptos de ciberseguridad, así como también se adquirieron entre otros, el de **Exploit**, punto débil en un sistema informático, que puede usarse para atacar este sistema. **Honeypot**, técnica que tiene como objetivo distraer a los piratas informáticos con un objetivo falso (una computadora o datos) y hacer que lo persigan en lugar del real. **IDS (Sistema de detección de intrusiones):** Herramienta de seguridad que intenta detectar la presencia de intrusos o la ocurrencia de violaciones de seguridad para notificar a los administradores, permitir un registro más detallado o enfocado o incluso desencadenar una respuesta como desconectar una sesión o bloquear una IP.
Conclusiones:	Como conclusión del primer objetivo y revisando el compendio de políticas de seguridad existentes en Colombia y sobre todo a nivel institucional, evidencio que representan un excelente medio para operar y dar uso adecuado a los recursos informáticos de manera estructurada y con estándares internacionales. Como conclusión del segundo objetivo, se tiene que el trabajo remoto evidentemente no sólo es un beneficio para las instituciones en las actuales circunstancias, sino que también

	beneficia al empleado, por lo que se hace fundamental que ambas partes, no sólo la organización tome conciencia de la seguridad necesaria para realizar esta actividad como se ejecuta normalmente en sitio. La adopción de mejores prácticas de ciberseguridad para el trabajo remoto va a permitir a las instituciones que consoliden una defensa sólida contra posibles ataques y vulnerabilidades informáticas. El Modelo de Gestión de Riesgo, es un buen aporte de lineamiento para la evaluación del Riesgo dentro de las instituciones. Las amenazas de ciberseguridad por la alta demanda de acceso remoto en las entidades es una realidad que seguirá incrementándose si no se tienen en cuenta todas las recomendaciones técnicas. El conocimiento adquirido a través de este estudio es un gran aporte para un mejor desempeño profesional y tecnológicamente más eficaz y seguro.