BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN PARA EL TELETRABAJO EN COLOMBIA

BEST PRACTICES IN INFORMATION SECURITY FOR TELEWORKING IN COLOMBIA

Carmen Rosa Sánchez Castillo
Miguel Angel Mateus Gutiérrez
Miller Camilo Gavilán Ordoñez
Yenny Isabel Serrato Rodríguez

RESUMEN

A lo largo de los años, las tecnologías de la información han presentado diferentes cambios que son de gran ayuda para las personas y las empresas, estas permiten que los procedimientos, para pagos, envió de información o identificación se realicen de forma ágil, facilitando la interacción entre las personas y los dispositivos; debido a esto surgen las siguientes preguntas, ¿Qué tan seguras son las nuevas tecnologías? ¿Cómo proteger la información ante los delitos informáticos? ¿Como salvaguardar los datos de la compañía con estas nuevas tecnologías?

Esta investigación pretende dar a conocer la importancia de proteger la información en la modalidad de trabajo que al día de hoy se está volviendo más común "El Teletrabajo", cabe aclarar, que actualmente Colombia no cuenta con las suficientes recomendaciones o buenas prácticas para implementar controles que ayuden a mitigar, reducir, minimizar y evitar los riesgos en esta modalidad de trabajo, por lo anterior, se desarrollará un listado de recomendaciones para aprovechar las tácticas o formas de asegurar los datos en los sistemas de información sin importar desde donde se acceden.

Palabras clave: Teletrabajo**,** trabajo en casa, trabajo remoto, seguridad de la información.

ABSTRACT

Over the years, information technologies have presented different changes that are of immense help to people and companies, they allow procedures for payments, sending information or identification to be carried out in an agile way, facilitating the interaction between people and devices; Due to this, the following questions arise, how safe are the innovative technologies? How to protect information against computer crimes? How to save company data with these modern technologies?

This research aims to publicize the importance of protecting information in the work modality that today is becoming more common "Telecommuting", it should be clarified, that currently Colombia does not have enough recommendations or good practices to implement controls that help minimize, reduce, minimize and avoid risks in this work modality, therefore, a list of recommendations will be developed to take advantage of tactics or ways to secure data in information systems regardless of where it is accessed.

Key words: Telecommuting, work at home, remote work, information security.

I. INTRODUCCIÓN

Hoy en día la información es considerada como el factor más importante para las personas y las organizaciones, sin embargo, existen muchas personas que no conocen la importancia de ella; para dar un mejor contexto de la importancia de esto, se relaciona un ejemplo de la vida real:

"¡Cuidado! Delincuentes están usando códigos QR para estafar a sus víctimas" (El Espectador, 2022), esta noticia es de enero del presente año, y su objetivo como tal, es alertar al lector del actuar de la delincuencia, esto para ayudar a proteger la información de los ciudadanos y de las organizaciones. Según el título, hoy en día el uso de los códigos QR son muy útiles ya sea para ver el menú de comidas en un restaurante o para realizar pagos en lugares comerciales, muy útil ¡verdad!; si se le mencionara a una persona que al escanear un código QR que estuviera alterado por un delincuente, pudiera perder información de sus cuentas bancarias, de sus fotos, de las conversaciones en las redes sociales y hasta generar daños en los dispositivos, no los usaría ¡verdad!, ya que dichos datos son personales y pueden contener muchos archivos que en manos equivocadas pudiesen generar daños significativos no solo a nivel económico sino también a nivel personal.

"El teletrabajo, moda que llegó para quedarse. Todas las noticias derivadas del coronavirus fueron malas, excepto el impulso al teletrabajo" (La República, 2022), muchas organizaciones se vieron fuertemente golpeadas por la pandemia, sin embargo, otras utilizaron las herramientas tecnológicas con las que contaban para dar continuidad a sus empresas, no obstante, en muchos casos no tuvieron en cuenta factores importantes como: la seguridad de su información. Con base en el enunciado anterior, se plantea el articulo buenas prácticas en seguridad de la información para el teletrabajo en Colombia, con el fin de ayudar a las organizaciones y a las personas en el manejo correcto de la seguridad.

Este artículo, busca realizar una investigación detallada de los diferentes modelos de trabajo a distancia en el país, y con ayuda de estándares internacionales de seguridad de la información y la normativa colombiana, desarrollar buenas prácticas para el correcto uso de los recursos tecnológicos de las organizaciones, cuidando el activo más importante para las compañías y personas (la información).

Es importante resaltar que los usuarios son de mucha importancia para la seguridad de la información, debido a que son el blanco más común para los atacantes, por esta razón, se realizará una encuesta con el fin de determinar el conocimiento de las personas con respecto a las normativas colombianas en el teletrabajo y el uso de buenas prácticas para la seguridad; con el fin de analizar los resultados y establecer medidas que pueden ayudar a las organizaciones y las personas a conocer los factores fundamentales de la seguridad de la información, para ponerlas en práctica en el campo laboral y en la vida diaria.

Hoy por hoy es más común escuchar en las personas que su forma de trabajar ha cambiado, y que ahora pueden realizar sus funciones laborales desde casa. Anteriormente, las organizaciones exigían a los empleados una asistencia netamente presencial, pero con los cambios que se han presentado en estos últimos años, las compañías se han restructurado para continuar con sus operaciones y de esta forma dar continuidad y evitar pérdidas monetarias.

Para abordar el tema del teletrabajo, los riesgos que existen bajo esta modalidad y como proteger información en las organizaciones, se plantean como objetivos específicos: Describir las modalidades de trabajo, las normas que los rigen y las condiciones de cada uno; identificar los estándares y normas para la seguridad de la información aplicables al teletrabajo y proponer buenas prácticas de seguridad de la información aplicables al teletrabajo en Colombia.

II. METODOLOGÍA

En el desarrollo de la investigación se van a mencionar varios temas de interés referente a las modalidades de trabajo a distancia, el énfasis del documento consiste en la información que actualmente está registrada dentro de leyes y/o normas en Colombia, después de esto, se realizará análisis y se dará una explicación más detallada para la facilidad del lector.

Luego, se procederá a realizar la descripción del problema que se quiere abordar y se explicaran los detalles en relación con los riesgos en la información dentro de la investigación, esto para llegar al punto de recomendar una adecuada gestión en la seguridad de la información para la modalidad del teletrabajo.

Para lo cual se realizarán con los siguientes pasos:

1. Diferenciar los métodos de trabajo a distancia en Colombia, basados en las leyes que los rigen, diferenciar las características de cada uno y de esta manera definir un punto de partida dentro del documento:

A continuación, se nombran las leyes que rigen el trabajo a distancia.

- Ley 1221 de 2008
- Ley 2088 de 2021
- Ley 2121 de 2021

2. Recopilar normas, métodos y/o documentos de buenas prácticas, estipulados por los organismos de control correspondientes en Colombia, con información importante para la seguridad de la información en el teletrabajo y de este modo visualizar el panorama de cómo se encuentra regulada esta modalidad de trabajo en seguridad de la información.

3. Se aplicarán mecanismos para la generación de estadísticas, con una metodología cuantitativa, por medio de un formulario web compartido en las redes sociales s, de esta manera reunir el concepto que tienen las personas del teletrabajo y el conocimiento de cómo proteger la información tanto personal como de las empresas, en este modelo de trabajo.
4. Realizar el análisis respectivo de las estadísticas realizadas, para visualizar que tan preparados o informados están los trabajadores que practican el Teletrabajo, con este análisis plasmar los posibles riesgos de seguridad de la información asociados a esta modalidad de trabajo.
5. Formular las recomendaciones adecuadas para la seguridad de la información en los riesgos identificados, de esta manera generar conciencia en los trabajadores y las organizaciones. y.
6. Se llevará a cabo la construcción de imágenes, tablas y/o anexos que sean de utilidad en la investigación.

III. DISCUSIÓN

1. Modalidades de trabajo

La forma de trabajar en Colombia los últimos dos años ha tenido un cambio drástico, ya que en el 2019 a mediados del mes de diciembre se reportó un nuevo virus proveniente de Asia, llamado COVID-19, haciendo que la enfermedad alcanzará los 5 continentes, generando un alto nivel de contagio en las personas, haciendo que la Organización Mundial de la Salud determinará la enfermedad como una emergencia sanitaria a nivel mundial.

Esto obligó a las personas y a las organizaciones a adoptar distintas formas de trabajo para darle continuidad a sus negocios, como consecuencia, surge la pregunta: “¿Cuáles son las formas

de trabajo a distancia que están reguladas por el gobierno colombiano?", en la búsqueda de leyes en Colombia que se pueden aplicar para el trabajo a distancia; se encuentran las siguientes:

1. Según la Ley 1221 del 2008 "por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones."[1] se encuentra una definición orientada a la modalidad Teletrabajo "Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación (TIC) para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo." (Congreso de Colombia, 2008).

Es decir, que el empleador y el trabajador firman un acuerdo de trabajo según las actividades a desempeñar, teniendo en cuenta, el uso de las TIC como contacto entre las partes y la ubicación para el desarrollo de las funciones del trabajador (este lugar es a disposición del trabajador, el empleador no tiene la facultad de definir el sitio en el cual el empleado deba trabajar).

2. En el año 2021, dentro de la emergencia sanitaria, el gobierno colombiano formaliza la Ley 2088[2] la cual implanta una nueva modalidad para trabajar a distancia nombrada Trabajo en Casa, cuya definición es la siguiente:

"Se entiende como trabajo en casa, la habilitación al servidor público o trabajador del sector privado para desempeñar transitoriamente sus funciones o actividades laborales por fuera del sitio donde habitualmente las realiza, sin modificar la naturaleza del contrato o relación laboral, o legal y reglamentaria respectiva, ni tampoco desmejorar las condiciones del contrato laboral, cuando se

[1] Ley 1221 - http://www.desarrolloeconomico.gov.co/sites/default/files/marco-legal/Ley-1221-2008.pdf
[2] Ley 2088 del 2021 "Por la cual se regula el trabajo en casa y se dictan otras disposiciones" https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=162970

presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus funciones en su lugar de trabajo, privilegiando el uso de las tecnologías de la información y las comunicaciones.

Este no se limita al trabajo que puede ser realizado mediante tecnologías de la información y las comunicaciones, medios informáticos o análogos, sino que se extiende a cualquier tipo de trabajo o labor que no requiera la presencia física del trabajador o funcionario en las instalaciones de la empresa o entidad." (Congreso de Colombia, 2021)

En esta definición, es claro que bajo esta modalidad de trabajo no hay cambio en la naturaleza del contrato o la relación laboral entre el empleador y el trabajador, solo se llevará a cabo cuando se presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus funciones en su lugar de trabajo; también indica que es transitoria (Que se realiza bajo un periodo de tiempo acordado) y depende de las actividades que deba desempeñar el empleado (Solo si no se requiere la presencia física del funcionario).

3. Por último, el Congreso colombiano introduce una nueva modalidad de trabajo llamada Trabajo Remoto, la cual está regida por la Ley 2121[3] del 3 de agosto del 2021, esta modalidad tiene un significado diferente a las anteriores.

"Es una forma de ejecución del contrato de trabajo en la cual toda la relación laboral, desde su inicio hasta su terminación, se debe realizar de manera remota mediante la utilización de tecnologías de la información y las telecomunicaciones u otro medio o mecanismo, donde el empleador y trabajador, no interactúan físicamente a lo largo de la vinculación contractual. En todo

[3] Ley 2121 "Por medio de la cual se crea el régimen de trabajo remoto y se establecen normas para promoverlo, regularlo y se dictan otras disposiciones"
https://dapre.presidencia.gov.co/normativa/normativa/LEY%202121%20DEL%203%20DE%20AGOSTO%20DE%202021.pdf

caso, esta forma de ejecución no comparte los elementos constitutivos y regulados para el teletrabajo y/o trabajo en casa y las normas que lo modifiquen.” (Congreso de Colombia, 2021)

La definición indica específicamente que la relación entre las partes se acuerda desde el momento de realizar la firma del contrato, este debe indicar que de inicio a fin el empleado ejercerá las funciones del trabajo desde un lugar remoto a las oficinas de la organización, dando a entender que la relación entre colaborador y empleador será únicamente por medios tecnológicos y no por relación física alguna.

Según a lo anterior, se detalla en las características de cada modalidad y sus diferencias, ver la siguiente tabla:

ITEM	TELETRABAJO	TRABAJO EN CASA	TRABAJO REMOTO
NORMA	Ley 1221 de 2008 y Decreto 884 de 2012	Ley 2088 de 2021	Ley 2121 de 2021
DEFINICION	Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación (TIC) para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.	Se entiende como trabajo en casa la habilitación al servidor público o trabajador del sector privado para desempeñar transitoriamente sus funciones o actividades laborales por fuera del sitio donde habitualmente las realiza, sin modificar la naturaleza del contrato o relación laboral, o legal y reglamentaria respectiva, ni tampoco desmejorar las condiciones del contrato laboral, cuando se presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus funciones en su lugar de trabajo, privilegiando el uso de las tecnologías de la información y las comunicaciones.	Es una forma de ejecución del contrato de trabajo en la cual toda la relación laboral, desde su inicio hasta su terminación, se debe realizar de manera remota mediante la utilización de tecnologías de la información y las telecomunicaciones u otro medio o mecanismo, donde el empleador y trabajador, no interactúan físicamente a lo largo de la vinculación contractual.
CONTRATACION	Debe constar por escrito. Se deben identificar las condiciones mínimas. Si el contrato se suscribe bajo la modalidad de teletrabajo, no aplica la reversibilidad al trabajo presencial.	No se requiere pacto o la suscripción de otro contrato. Debe haber una comunicación por parte del empleador indicando el tiempo que durará esta modalidad. El empleador mantiene la facultad unilateral de exigir al trabajador volver a prestar sus servicios presencialmente.	Debe constar por escrito y se celebra mediante firma electrónica o digital. (El costo del uso de la tecnología para la firma debe asumirlo el empleador). Solo prevé la presencialidad para: 1. Atender asuntos que involucren salud ocupacional. 2.Verificar los estándares y requisitos que deben cumplir las herramientas y los equipos de trabajo para la realización de la labor. 3. Para instalar o actualizar programas o herramientas manualmente en los equipos de trabajo. 4. Para adelantar procesos disciplinarios.
JORNADA	Deberán pagarse las horas adicionales cuando se generen labores fuera de la jornada máxima legal. Se debe tener en cuenta el derecho al descanso y a la desconexión laboral. Se deben respetar los tiempos familiares durante la jornada y la finalización de esta.	Aplican las jornadas previstas en el Código Sustantivo del Trabajo. Se debe respetar el derecho al descanso y a la desconexión laboral. Se deben respetar los tiempos familiares durante la jornada y a la finalización de esta.	Aplican las jornadas previstas en el Código Sustantivo del Trabajo. No obstante, las partes puede acordar la distribución de la jornada pactar y su distribución en la semana sin que implique un cumplimiento estricto de horario al día. Si la persona acredita tener a su cargo el cuidado de menores 14 años, personas con discapacidad o adultas mayores en 1er grado de consanguinidad que convivan con el trabajador y que requieran asistencia especifica, tendrán derecho a horarios compatibles con las tareas de cuidado a su cargo y/o a interrumpir la jornada, con una autorización previa al empleador que permita la interrupción. Prevé el derecho al descanso y a la desconexión laboral. Se deben respetar los tiempos familiares durante la jornada y a la finalización de esta.
SEGURIDAD SOCIAL	Su afiliación es exactamente igual a la de cualquier trabajador. Se debe notificar a la ARL.	Su afiliación es exactamente igual a la de cualquier trabajador. Se debe notificar a la ARL.	Se debe informar a la ARL a través del formulario que esta designe. El Gobierno deberá diseñar un formulario único de afiliación al SGSS, que no requiere firma manuscrita.
MINISTERIO DEL TRABAJO	Requiere notificación al Ministerio del Trabajo.	No Requiere notificación al Ministerio del Trabajo.	No requiere notificación al Ministerio del Trabajo.
RIT	Requiere reglamentación en el RIT.	No requiere reglamentación en el RIT.	No requiere reglamentación en el RIT.
AUXILIOS ECONOMICOS	El empleador debe otorgar un subsidio para el pago del internet y la energía.	El empleador debe otorgar el subsidio de transporte, como auxilio de conectividad a quienes devenguen menos de 2 smmlv.	El empleador debe otorgar un subsidio para el pago del internet y la energía.

Tabla 1. Diferencias en las modalidades de trabajo en Colombia.

Por lo anterior, con referencia a las leyes del gobierno colombiano, las organizaciones están en la obligación de formalizar estos métodos de trabajo a distancia, al no realizarlo pueden incurrir

en faltas graves que conlleven a multas o sanciones por parte de las entidades de control; generando daños reputacionales y pérdida de clientes.

2. Seguridad de la información en las modalidades de trabajo

Con la información de los párrafos anteriores, se determina que Colombia cuenta con tres (3) leyes que regulan las formas de trabajo para los empleados que ejercen labores fuera de las instalaciones propias de cada organización; estas modalidades utilizan los medios tecnológicos para ejercer cualquier tipo de actividad en la generación de valor para las empresas, debido a esto surge la pregunta: ¿Cómo se controla la seguridad de la información en estas modalidades de trabajo?

Para el Teletrabajo la ley 1221 anexa el Decreto 0884 de 2012 el cual, en el Articulo 3. "Contrato o vinculación de Teletrabajo" relaciona que el empleador está en la obligación de indicar "Las medidas de seguridad informática que debe conocer y cumplir el teletrabajador.", también en el Articulo 5. "Uso adecuado de equipos y programas informáticos" menciona lo siguiente: "El empleador debe informar al teletrabajador sobre las restricciones de uso de equipos y programas informáticos, la legislación vigente en materia de protección de datos personales, propiedad intelectual, seguridad de la información y en general las sanciones que puede acarrear por su incumplimiento." (Ministerio del Trabajo, 2012)

En el caso del Trabajo en Casa, la regulación entregada por la ley 2088 para seguridad de la información es más corta y menos detallada con el tema de seguridad, Articulo 8. "Elementos de Trabajo" menciona lo siguiente: "El empleador definirá los criterios y responsabilidades en cuanto al acceso y cuidado de los equipos, así como respecto a la custodia y reserva de la información de conformidad con la normativa vigente sobre la materia.

En todo caso, el empleador es el primer responsable de suministrar los equipos necesarios para el desarrollo de las actividades, cumplimiento de funciones y prestación del servicio bajo la habilitación de trabajo en casa.” (Congreso de Colombia, 2021)

Por último, en la ley 2121 del 03 agosto de 2021 para el Trabajo Remoto menciona en el Articulo 10. “Herramientas y equipos de trabajo”, el empleador deberá constatar lo siguiente: “Las medidas de seguridad informática que debe conocer y cumplir el trabajador remoto”, adicional, en el Articulo 3. Definiciones, hace alusión a un mecanismo de autenticación OTP (One Time Password) “el cual consiste en un código temporal que le llega a la persona a través de mensaje de texto SMS o correo electrónico certificado, para que, de manera segura, pueda realizar acciones virtuales, en donde se certificará la identidad de la persona, ya sea vía internet o mediante la aplicación para teléfonos móviles (APP)” (Congreso de Colombia, 2021), sin embargo, el empleador tiene la posibilidad de considerar si es necesario para la seguridad de sus acciones remotas en su organización.

Según a todo lo anterior, se concluye que el empleador es el mayor responsable de la seguridad de la información para la entidad, y está en su deber velar por el cumplimiento de las políticas y normas de seguridad, esto sin importar la modalidad de trabajo en la que se encuentren los trabajadores.

3. Problemática del teletrabajo en la seguridad de la información

El Teletrabajo es una de las modalidades que se está adoptando en Colombia desde la regulación entregada por el gobierno colombiano en el 2008, y con el transcurso de los años se va adaptando cada vez más en las organizaciones con ayuda de las tecnologías de información.

Como complemento, cabe mencionar que muchas de las personas y entidades que utilizan esta modalidad de trabajo indican que es muy útil y no desmejora el rendimiento en la ejecución de actividades dentro de las organizaciones, por el contrario, ha sido un beneficio obtener un contrato, que facilite el cumplimiento de las funciones a realizar por medio del Teletrabajo.

Hay que tener en cuenta que, al realizar actividades fuera de un ambiente de oficina, las cosas cambian y se deben plantear nuevos escenarios; por lo que se pueden presentar situaciones adversas para las entidades y las personas en general, ya que al materializarse un incidente de tal índole puede causar consecuencias como: pérdida de dinero, daño de instalaciones, afectación en la reputación, daños emocionales y/o muertes.

Por causa de la importancia en la seguridad en la información, surge una incógnita:

¿Qué tan informadas y preparadas están las organizaciones que utilizan el Teletrabajo, en temas de seguridad de la información?

En la norma NTC:ISO/IEC 27001[4] de 2013 en el Anexo A.6.2 Dispositivos móviles y teletrabajo, indica que las entidades que se quieran certificar en dicha normativa deben establecer una política de seguridad para el uso de herramientas y/o tecnologías en esa modalidad de trabajo; también expresa claramente, que se debe contar con medidas de seguridad para gestionar los riesgos por el uso de dispositivos móviles y el uso de la información procesada o almacenada por el método de trabajo indicado.

[4]Norma 27001, "es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa" (Dimitrios, 2020)

Según Icontec[5], la norma 27001 va orientada a la evaluación que se debe realizar a las organizaciones por parte de un auditor, ya sea interno o externo, con el fin de medir la postura ante la seguridad de la información; es decir que, si una empresa quiere mejorar a nivel de seguridad en el teletrabajo, deberá tener en cuenta lo que exige esta norma para una posible certificación.

¡Pero, solo con esas cortas líneas que indica la norma es suficiente!

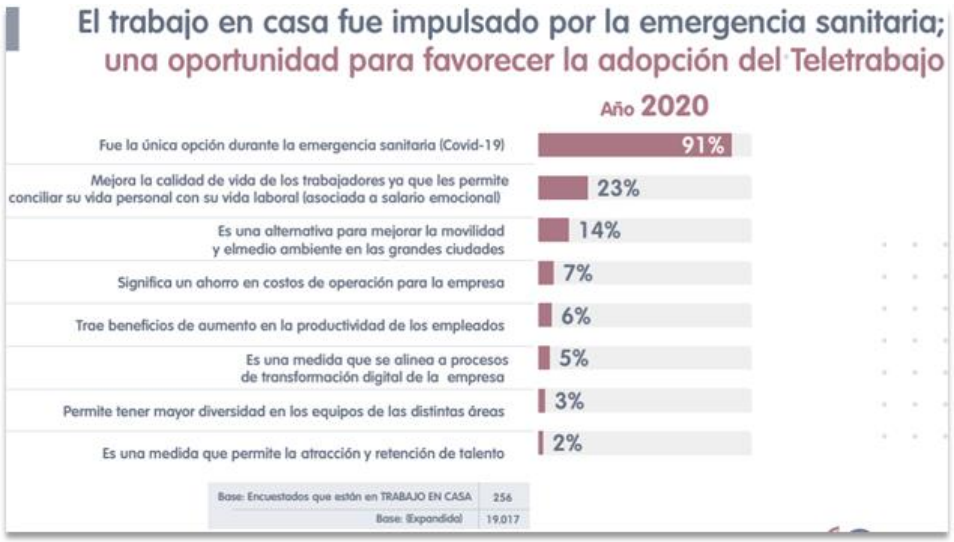
En otros estándares como la NIST, la NERC o las demás ISO, es limitado encontrar información detallada que se centre en la seguridad para el Teletrabajo; el estándar más cercano que toma en cuenta esta modalidad de trabajo es la GTC/ISO/IEC 27002, que es una extensión de la 27001 en la cual explica un poco más al detalle el tema de las políticas que se deben tener para cumplir con ese control de la norma.

Con lo anterior, se puede determinar que la información que actualmente existe para la seguridad de la información en el teletrabajo es mínima, esto implica que el mensaje sea poco claro e incompleto, es decir, que la información actual no es suficiente para proteger los sistemas y/o datos que se generan en el teletrabajo.

4. Estadísticas del teletrabajo en Colombia

A mediados del 2020, el gobierno colombiano realizó una encuesta a los ciudadanos y organizaciones para dimensionar el incremento del teletrabajo, los resultados de dichas encuestas arrojaron estadísticas que fueron útiles para verificar como se adaptó esta modalidad de trabajo en el país; a continuación, se puede observar como el teletrabajo se fue ajustando en el transcurso de la pandemia y cuál fue el porcentaje de aceptación según los ítems de mejora:

[5] Organización para la normalización en Colombia, https://www.icontec.org/quienes-somos/



Grafica 1: Adopción del teletrabajo por el COVID-19. (Gobierno de Colombia, 2020)

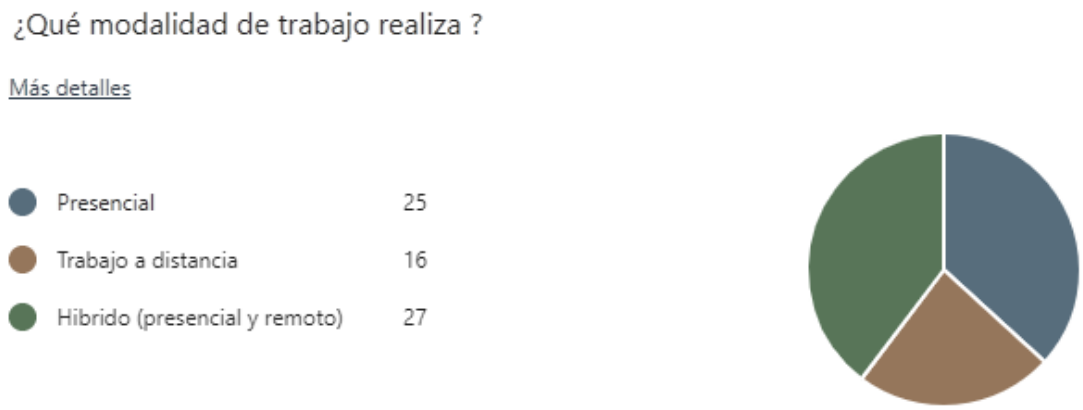
De acuerdo a la Imagen 1, se observa que debido a la emergencia sanitaria, el 91 % de las entidades optó por un trabajo desde la casa, dando oportunidad de crecimiento al teletrabajo; en la encuesta, se menciona como este tipo de metodologías de trabajo impulsa a tener una mejor calidad de vida a los trabajadores, también, relaciona los beneficios en el ahorro en costos de producción y el aumento de la productividad en los empleados; estos, son muchos de los beneficios que trae consigo el teletrabajo, y las organizaciones son conscientes de esto.

Grafica 2: Incremento del teletrabajo. (Gobierno de Colombia, 2020)

En la gráfica de la imagen 2 se observa un incremento significativo del teletrabajo tomando como referencia el año 2012 hasta el 2020 con intervalos de dos años, esto muestra que de acuerdo con las estadísticas el teletrabajo puede tener un incremento cada vez mayor en el transcurso de los

años siguientes, debido que muchas organizaciones encontraron muchos beneficios al utilizar esta modalidad de trabajo, por esta razón es de vital importancia emplear buenas prácticas para proteger la información.

Por otra parte, y con respecto al presente artículo, se realizó una encuesta dirigida a varias personas de diferentes carreras universitarias y actividades laborales, con el fin de determinar el conocimiento que tienen sobre teletrabajo y la importancia que le prestan a la seguridad de la información bajo esta modalidad de trabajo.

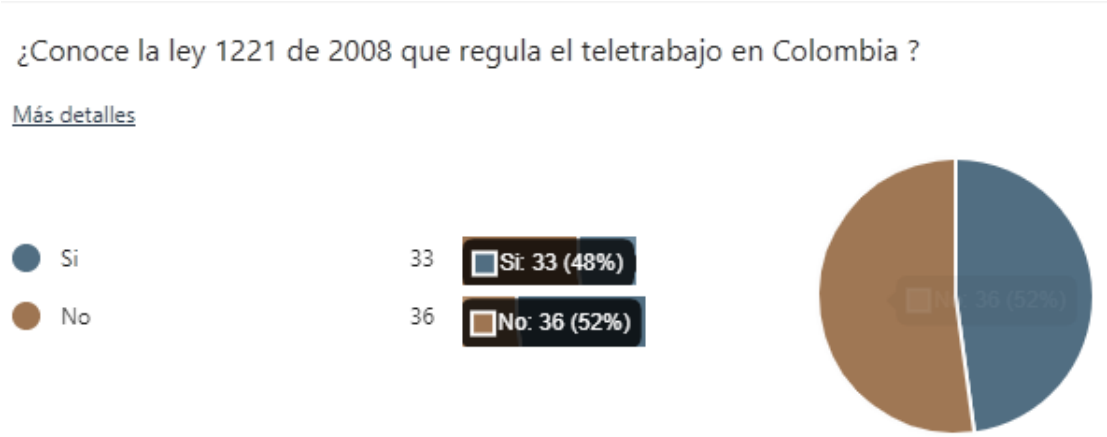


Grafica 3: Modalidad de trabajo.

Una de las primeras preguntas, fue identificar el tipo de modalidad de trabajo que se encuentran realizando actualmente, en la imagen 3 se evidencia que a pesar que las restricciones de la emergencia sanitaria en Colombia ya fueron retiradas, muchas empresas aún utilizan modalidades a distancia, debido a que, encontraron beneficios en el uso del trabajo remoto o hibrido, uno de estos, es la contratación, dado que ya no se limitan en contratar personal en la ciudad donde se encuentran ubicados, por el contrario, ampliaron su mercado laboral, de esta forma pueden ubicar recurso humano idóneo para los cargos en diferentes zonas del país; por otro lado, desde el punto de vista del trabajador, un factor importante es que el empleado al trabajar desde

casa no tiene que movilizarse, por esta razón no debe lidiar con el tráfico, por lo que estará más relajado para realizar sus actividades y puede disfrutar más tiempo con sus seres queridos.

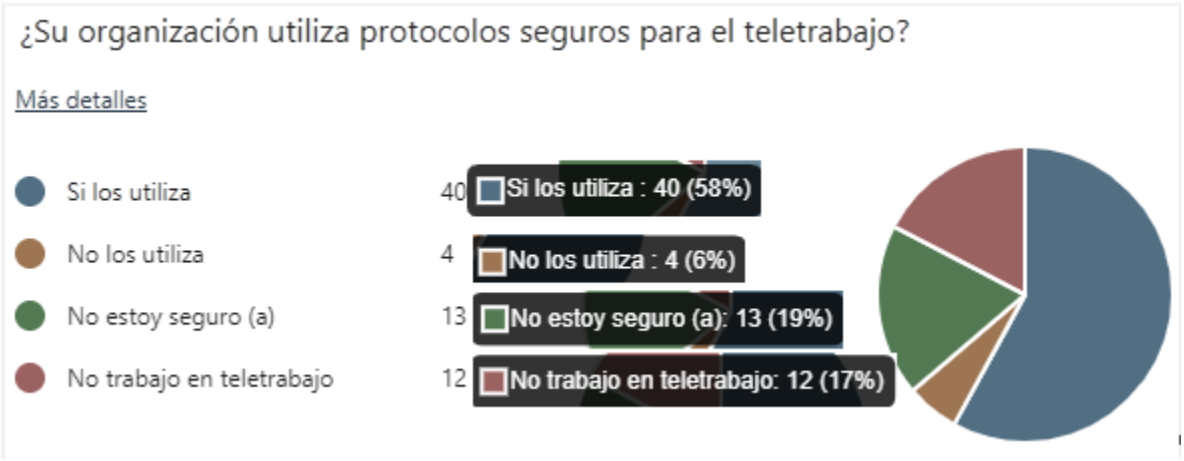
En la siguiente pregunta de la encuesta se cuestionó si los encuestados conocían la ley que regula el teletrabajo y el resultado fue que el 53% de los interrogados, no conocen la existencia de la ley.



Grafica 4: Conocimiento de la Ley 1221 de 2008.

Lo cual constata que muchos utilizan o utilizaron está modalidad de empleo, pero desconocen cómo se regula y en que cosiste, en vista de esto, este punto es primordial puesto que el conocimiento de estos puntos puede ayudar a las personas a garantizar que sus derechos laborales están siendo respetados.

Desde el punto de vista de la seguridad de la información, durante la encuesta se incluyó una pregunta asociada a las organizaciones, donde se indagaba si estas utilizan protocolos seguros para el teletrabajo, cuya respuesta de acuerdo con la imagen 5 demuestra que la gran mayoría si los utiliza, no obstante, existe un 19% que desconoce estos protocolos, y por otro lado un 6% de los interrogados indica que no se utilizan dichos controles.



Grafica 5: Protocolos Seguros

Con esta información se concluye que aún existen entidades que no prestan la atención adecuada al tema de la seguridad de la información, dejándola en segundo plano, no invirtiendo tiempo ni recursos en capacitación a sus colaboradores; es necesario, recalcar que las jornadas de inducción de las buenas prácticas ayudan a reducir los incidentes de seguridad y contribuyen a crear cultura de seguridad dentro de la organización.

.

5. Riesgos de seguridad de la información en el teletrabajo

El teletrabajo es cada vez más común, sin embargo, muchas empresas desconocen los riesgos de seguridad de la información que existen bajo esta modalidad, teniendo en cuenta, que la comunicación con se realiza a través de herramientas tecnológicas como el correo electrónico, chats, videoconferencias, y la conexión de los empleados a la organización es realizada a través de la redes poco confiables, además, en algunos casos, deben utilizar dispositivos personales sin ningún protocolo de seguridad para desempeñar sus labores; todos estos factores pueden ocasionar incidentes de seguridad que al concretarse, ocasiona pérdidas de información, monetarias, daños reputacionales y problemas legales.

Sumado a lo anterior, los colaboradores pueden cometer errores ocasionando eventos de seguridad. Un ejemplo de esto, es el uso indebido del equipo asignado por la organización para desempeñar su cargo, ya que además de realizar sus actividades laborales también lo usan para temas personales: ingreso a sus correos personales, redes sociales, realizar compras por internet entre otros; todos estos componentes pueden ser la puerta de entrada a una incidencia, ya que pueden presentar ataques dirigidos a los usuarios al momento de ingresar a sitios ajenos a la compañía, así las cosas, el computador corporativo es afectado de forma indirecta por posible ransomware[6], phishing[7] o troyanos[8],

Existen otros riesgos en el teletrabajo que pueden afectar a las organizaciones cuando no se tienen los controles adecuados, por ejemplo, la pérdida o robo de información; al no tener un control adecuado la exposición aumenta, puesto que, utilizando dispositivos como discos duros externos, USB o copiando y pegando información desde el equipo corporativo al computador con el cual el usuario trabaja por escritorio remoto, se puede sustraer información sin dejar rastro de lo sucedido.

Todos los ejemplos antes mencionados son muy comunes, algunos son causados por desconocimiento de los empleados, es importante, implementar protocolos seguros en el teletrabajo y reforzar el conocimiento de los colaboradores, fomentando el buen uso de los recursos tecnológicos y la importancia de la seguridad de la información, en su entorno laboral como personal, de esta manera, crear entornos seguros para quienes trabajan desde lugares externos a la organización.

[6] El ransomware es un tipo de programa maligno que luego de comprometer un equipo secuestra la información. (Eset, 2021)
[7] Phishing, técnica de ciberdelincuencia que utiliza el fraude, el engaño y el timo para manipular a sus víctimas y hacer que revelen información personal confidencial. (Ivan Belcic, 2021)
[8] Un troyano oculta software malicioso dentro de un archivo que parece normal. (Norton, 2022)

EVENTO	RIESGOS
Acceso al dispositivo	Personas ajenas a la organización pueden acceder al equipo o dispositivo del empleado y conocer información confidencial.
Robo o perdida del equipo o dispositivo	Teniendo en cuenta la facilidad de trabajo en cualquier sitio, el empleado puede ser objeto de robo o perder el dispositivo, poniendo en riesgo la información de la organización.
Uso de dispositivos USB para sustraer información	Robo de información confidencial de la organización debido a falta de control en la copia de los datos
Equipos con sistemas operativos desactualizados	El uso de equipos informáticos sin las ultimas actualizaciones de seguridad pueden ser objeto de ataques cibernéticos.
Instalación de software no autorizados o de origen no oficial	El uso de software descargado de sitios no autorizados es un factor de riesgo debido a la posible inyección de Código malicioso en el software de o programas para espiar y robar información.
Hacer clic en enlaces desconocidos	El desconocimiento en los riesgos al acceder a enlaces desconocidos puede ocasionar perdida de información producto de malware o ransomware.
Mal uso del equipo de computo	El uso del ordenador en actividades tales como ingreso a páginas de juegos, películas, redes sociales entre otras puede exponer el equipo a riesgos en el teletrabajo.

Tabla 2: Posibles riesgos en el teletrabajo

IV. RESULTADOS

Teniendo claridad sobre qué es el teletrabajo y sus normativas, se genera una serie de pautas para la implementación de recomendaciones en seguridad de la información, con apoyo de lo establecido por el Ministerio de Tecnologías de la información y las Comunicaciones (MinTic).

1. Empresas

Es responsabilidad de las empresas brindar herramientas y guías que ayuden a proteger la información, tanto interna como externa del negocio, para lo cual se recomienda implementar

algunas medidas como la autentificación Multifactor[9], lo cual permite que toda persona ingrese a los aplicativos o información de la organización de manera más segura, imposibilitando el guardado de las credenciales de manera automática.

Es importante el uso e implementación de herramientas como: VPN y EDR, esto permite que la empresa tenga canales de comunicación seguros y centralizados, para usar la información sin arriesgar su disponibilidad y confidencialidad.

Para guardar la información, se deben usar carpetas compartidas y servidores empresariales, generando copias de respaldo, de manera recurrente; De cada uno de los empleados depende la implementación y buen uso de las herramientas que brindan las organizaciones, por consiguiente, evitar incidentes de seguridad.

ACCIÓN	¿QUE SE DEBE HACER?
Autentificación multifactor	Configurar más de un método de autentificación para ingresar a los dispositivos y aplicativos, por ejemplo; Contraseñas, SMS, correo, huella dactilar, reconocimiento facial o de voz.
VPN (Virtual Private Network)	Establecer conexiones privadas para el uso de la red corporativa desde un lugar externo a la organización, de tal manera que, la información se transmita cifrada y sea inaccesible para terceros.
SSL (Secure Sockets Layer)	Garantizar que las aplicaciones expuestas a internet cuenten con los certificados de seguridad.
Implemente validaciones de seguridad mínimas para ingresar por SSL VPN, para dispositivos BYOD (Bring Your Own Device)	Realizar la asignación de usuarios y contraseñas a cada uno de los usuarios, acorde con las necesidades de sus cargos, para el ingreso a redes corporativas por medio de la VPN.
Habilitar algún servicio de cara a internet	Instalar un WAF o firewall que permita detectar las amenazas y controlar el tráfico de red expuesto a internet
Sistema operativo con los últimos parches, software y antivirus.	Tener un inventario de los sistemas operativos, antivirus y parches en cada equipo, con fechas de actualización, tener el consolidado de las actualizaciones vigentes. .
Política de privacidad de la información	Esta política se debe dar a conocer a todos los empleados de la compañía, con el fin de establecer un compromiso sobre el uso de la información.

[9] La autenticación Multifactor (MFA) agrega una capa de protección al proceso de inicio de sesión. Cuando se obtiene acceso a una cuenta o aplicación, los usuarios deben pasar por una verificación de identidad adicional; por ejemplo, tienen que escanear su huella digital o especificar un código que reciben en su teléfono. (Microsoft, 2022)

OneDrive o Drive corporativo a través de la infraestructura del servidor de archivos implementada.	La empresa debe contar con servidores y/o almacenamiento en la nube, de tal manera que cuente con un espacio seguro para guardar la información y las copias de respaldo.
Impedir que se guarde de forma automática las credenciales	Por medio de configuraciones y de capacitación a los empleados, impedir que se guarde de manera automática las claves y usuarios para ingresar a los aplicativos y/o equipos de la empresa.
Políticas de cifrado en equipos, servidores y herramientas transaccionales	Implementar el cifrado en los equipos y servidores. Administrar los usuarios desde el directorio activo para cada equipo y aplicativo.
Implementar la segmentación (mínimo privilegio)	Configurar segmentos de red dentro de la organización, para restringir el acceso a determinados recursos tecnológicos.
Herramientas EDR (Endpoint Detection and Response)	Implementar un antivirus que cuente con esta tecnología, lo cual permita monitorear y detectar amenazas para la protección de los sistemas.
Prohibir el uso de dispositivos rooteados o a los que se ha realizado jailbreak.	Implementar dentro de las normas, políticas y capacitaciones el no uso de dispositivos alterados tecnológicamente.
Configurar localización, bloqueo de pantalla, borrado remoto de datos y seguimiento de las aplicaciones ejecutadas	Generar configuraciones en todos los equipos de tal manera que permitan ver la localización, realizar borrado de archivos en caso de requerirse y monitorear el histórico de ingresos a las aplicaciones.
Plan de capacitación y formación del correcto uso de los medios tecnológicos y políticas de seguridad	Tener un cronograma continuo de capacitaciones actualizadas que permita tener informado y actualizado, a todo el personal del buen uso de los equipos y políticas de seguridad de la compañía.

Tabla 3: Acciones de mejora para las organizaciones

2. Móviles

Al igual que todas las herramientas que se utilizan para el trabajo, se debe tener precauciones al momento de usar los dispositivos móviles, por lo cual, es recomendable no conectarse a redes wifi-desconocidas o redes abiertas, ya que este tipo de acciones permite el acceso a la información que se tiene en estos dispositivos; también se recomienda no enviar documentos por este medio, en caso de necesitarlo, se deben enviar cifrados.

Al instalar aplicaciones, estas deben ser de lugares autorizados y que no requieran el permiso a acceder a la información que se tiene en el dispositivo; por último, no conectarse a puertos USB desconocidos para no establecer relaciones de confianza con puertos no autorizados, (MinTic, 2022)

ACCIÓN	¿QUE SE DEBE HACER?
Envió de mensajes	Utilizar políticas de cifrado de información cuando se requiera enviar información sensible.
Implementar cifrado y autentificación	Configurar un método de cifrado y un proceso de autentificación para ingresar a los equipos o aplicativos, por ejemplo: Contraseñas, huella dactilar, reconocimiento facial o de voz.
No conectarse a puertos USB	Bloquear la conexión a puertos USB para no crear relaciones de confianza con equipos no autorizados.
Hotspots Wi-Fi	Tener datos disponibles Evitar conectarse a redes abiertas.
Instalación de aplicaciones	Generar configuraciones de administrador para instalar aplicaciones en los dispositivos empresariales, esto, con el fin de que no se instale software no autorizadas ni de sitios no oficiales.
Backup y Sistema Operativo	Realizar copias de seguridad periódicas, las cuales se almacenan en sitios autorizados y mantener los sistemas operativos actualizados.

Tabla 4: Acciones de mejora para el uso de celulares

3. Personas

Como personas y empleados responsables, se debe garantizar la seguridad en la información que está a disposición y/o que este en uso según las actividades realizadas por cada uno, por lo cual el Ministerio de Tecnologías de la Información y las Comunicaciones genera una serie de recomendaciones que se pueden poner en práctica, por ejemplo: Realizar el cambio de clave de wifi, no utilizar redes abiertas para que la información no esté a disposición de personas ajenas, priorizar el uso de internet para las actividades organizacionales dentro de los horarios laborales, cerrar la sesión de los equipos cada vez que se levante del lugar de trabajo o cuando no estén en uso los equipos, no enviar información sin cifrar o por correos no corporativos, al generar la instalación de programas, no hacerlo desde sitios poco confiables, de preferencia solo realizarlo a través de las autorizadas o solicitarlo directamente a la empresa.

Además, se recomienda un lugar adecuado óptimo para trabajar que impida la pérdida de información, ya sea por daño de los equipos, robo de información o suplantación de identidad, cumpliendo con las normas establecidas por la organización.

ACCIÓN	¿QUE SE DEBE HACER?
Doble o triple factor de autenticación en transacciones financieras.	Se debe configurar un sistema de autentificación para ingresar a los aplicativos financieros, por ejemplo: Contraseña, token físico, SMS, llamada, huella dactilar o reconocimiento facial.
Cambio de claves de wifi	A través del ingreso a aplicativos de administración del Router realizar periódicamente el cambio de contraseña del wifi.
No usar redes abiertas	No realizar actividades con redes abiertas en sitios públicos.
Copias de seguridad	Realizar periódicamente copias de seguridad de la información en sitios autorizados, como discos físicos o en la nube de cuentas confiables.
No utilizar medios como whatsapp, dropbox, wetransfer, correos de dominio gratuito para envió de información corporativa.	Siempre enviar los archivos a través de correos empresariales, carpetas compartidas en la nube de la empresa o los medios autorizados por la entidad.
Cerrar siempre la sesión	Activar el bloqueo de pantalla o cierra de sesión de aplicativos después de 20 segundos de inactividad, esto permitirá que si la persona no cierra la sección esta se bloquee automáticamente y requiera autentificación para ingresar nuevamente.
Instale y mantenga actualizado el software, antivirus y el sistema operativo con los últimos parches	Tener un inventario de los sistemas operativos, antivirus y parches en cada equipo, esto con fechas de actualización, de esta manera tener el consolidado de las actualizaciones y así realizarlas en todos los equipos.
Instalación de programas.	Cuando requiera instalar programas o aplicaciones no lo realice de sitios desconocidos estas pueden traer malware, realícelo desde fuentes confiables.
Uso de aplicaciones de escritorio remoto no autorizadas por la organización	Se debe preguntar a las entidades que escritorios remotos se pueden utilizar, que sean seguros y no permitan abrir puertas traseras generando incidentes de seguridad.
Garantizar la seguridad de los datos	Es impórtate garantizar la seguridad de la información cumpliendo con las normas establecidas por la empresa, la ley de protección de datos y las buenas prácticas de seguridad para protección de esta.

Tabla 5: Acciones de mejora para las personas

4. Recomendaciones adicionales para la seguridad de la información en el teletrabajo

a. Se debe cambiar la contraseña del wifi periódicamente, que sea mínimo de 10 caracteres utilizando caracteres especiales, números, mayúsculas, minúsculas y, procurar que esta sea lo más aleatoriamente posible.

b. Configurar el modem de forma que solo acepte dispositivos identificados previamente por la dirección MAC, ocultar la red WIFI para que no sea visible a personas externas, cambiar la dirección IP por defecto del modem.

c. Si se tiene indisponibilidad del servicio de internet, abstenerse de utilizar redes públicas, si es de carácter urgente abstenerse de realizar actividades con información sensible; de

acuerdo con el tiempo de la indisponibilidad utilizar otra red de confianza o desplazarse a la empresa.

d. A pesar de que se tenga conocimiento en la instalación o actualización de programas, mejor solicite la instalación de forma directa con el área de soporte de la empresa.
e. Abstenerse de utilizar el correo personal para temas laborares, si es de fuerza mayor solicitar la autorización del empleador.
f. Si se utiliza el computador personal para trabajar, crear un usuario independiente para temas laborales y garantizar que este no cuente con permisos de administrador.
g. Tener un lugar asignado para trabajar de preferencia que cuente con escritorio, silla y buena ventilación, que solo sea utilizado por una persona y no consumir alimentos en este lugar de trabajo.
h. No compartir usuarios o contraseñas entre compañeros de trabajo.
i. Si cuenta con celular corporativo usarlo solo para labores de trabajo y no prestarlo a otras personas ajenas a la empresa.
j. No utilizar los correos corporativos para el uso de suscripciones o para él envió de publicaciones, como por ejemplo cadenas y/o promociones.
k. Activar los antivirus en los dispositivos físicos como computadores, tabletas, celulares, etc.
l. No utilizar dispositivos USB encontrados y/o regalados, en los cuales, es incierto su origen y la información que contiene.
m. No dar clic o abrir correos electrónicos de dudosa procedencia, es decir, no se conoce de donde viene el correo y no se esperaba recibir correos con ese asunto.
n. Al recibir mensajería por algún tipo de aplicación de dudosa procedencia, no dar clic o abrir archivos adjuntos, preferiblemente comunicarse con el área de seguridad de la información de la entidad.

o. Al utilizar contraseñas como factor de autenticación al ingresar a un aplicativo o alguna cuenta, no utilizar datos como: fechas de cumpleaños, números de identificación, direcciones y/o nombres propios.
p. No hacer uso de papelería para almacenar datos de usuarios y/o contraseñas, preferiblemente utilizar programas seguros para el almacenamiento de estos datos.
q. Verificar que los dispositivos que se van a movilizar fuera de las instalaciones de la organización cuenten con un cifrado seguro, esto para prevención ante un robo de los dispositivos.
r. Al navegar en internet, hay que asegurar que las páginas web utilicen protocolos seguros como https.
s. Evitar el uso de dispositivos en lugares cercanos a fuentes de agua o con riesgo de humedad, se puede generar un daño al equipo.
t. Al movilizar elementos tecnológicos, velar por la seguridad de estos, guardándolos con la protección adecuada.
u. Al ingresar a paginas web, verificar que las URLs correspondan al sitio oficial.
v. Asistir a capacitaciones orientadas a la seguridad de la información.

V. CONCLUSIONES

En el desarrollo del documento se evidenció que el teletrabajo tiene varias falencias a nivel de normativas y de apoyo para la seguridad de la información en las organizaciones, sobre todo en las personas, por tal motivo, se plasmaron varias recomendaciones para mejorar los niveles de seguridad en dicho aspecto.

Según los resultados obtenidos en la investigación realizada, se observa que a pesar de que el uso del teletrabajo es más común en este momento a diferencia de años anteriores, aún existen

diferentes riesgos de seguridad asociados al desconocimiento de las personas y las organizaciones, por lo cual se considera necesario reforzar la importancia de este tema , debido a que, al no tomar las medidas pertinentes podría desencadenar a incidentes de seguridad, que podrían poner en riesgo la información de la organización.

En referencia a las recomendaciones para la seguridad de la información, se realizaron tres (3) tablas con ayuda de la información entregada por el Ministerio de las Tecnologías de la Información y las Comunicaciones, basados en estas, se documentó cómo implementarlas mediante consejos, herramientas y mecanismos para la protección de los datos, puntualmente por cada una de las categorías, de esta manera tener un punto de vista más claro de como aplicarlas.

Al explicar al detalle, qué realizar para cada una de las recomendaciones entregadas por MinTic, se concluye que aún hay formas de aconsejar a los empleados y a las personas con respecto a las tácticas de seguridad de la información; como profesionales en el campo de la seguridad de los datos, se elabora un listado de recomendaciones adicionales, con el fin de ayudar a los teletrabajadores a proteger su información, sin importar el lugar desde donde estén ejecutando sus actividades por medio de esta metodología de trabajo.

Las organizaciones al tratar de adopta una nueva modalidad de trabajo, deben tener en cuenta la importancia de documentarse sobre las leyes que rigen estas formas de trabajar, los riesgos de seguridad de la información que estas implican y las diferentes técnicas de protección para los datos, y asimismo poder contar con mecanismos de defensa en la infraestructura tecnológica, en los procedimientos organizacionales y en los empleados.

VI. AUTORES

Carmen Rosa Sánchez C., Nació en Tunja (Boyacá), Colombia. Candidata a Especialista en seguridad de la información de la Fundación Universitaria Los Libertadores e Ingeniero en sistemas de la Corporación Universitaria Remington. Email: crsanchezc@libertadores.edu.co .Cuenta con experiencia en la implementación de proyectos de telecomunicaciones; actualmente se desempeña como ingeniera Reporting Senior para una empresa privada.

Miguel Ángel Mateus G. Nació en Bogotá, Colombia. Candidato a Especialista en seguridad de la información de la Fundación Universitaria Los Libertadores e Ingeniero de Sistemas de la Universidad Cooperativa de Colombia. Email: mamateusg@libertadores.edu.co .Es certificado como: Auditor interno en ISO 27001:2013. Adicional, posee conocimientos en: gestión de identidades, gestión de servicios TI, ciberseguridad, administración de herramientas Microsoft para la seguridad en nube y endpoint. Se ha desempeñado como: analista de seguridad informática para organizaciones privadas y como Consultor Senior de Ciberseguridad para entidades del estado.

Miller Camilo Gavilán O. Nació en Bogotá, Colombia, Candidato a Especialista en seguridad de la información de la Fundación Universitaria Los Libertadores e Ingeniero de sistemas egresado de la Corporación Universitaria Remington. Email: mcgavilano@libertadores.edu.co Certificado como: ITIL, Microsoft y AWS, ha desempeñado el cargo de ingeniero de Infraestructura y plataforma.

Yenny Isabel Serrato R., Nació en Bogotá, Colombia. Especialista en Seguridad de la Información de la universidad Sergio Arboleda e Ingeniero en Telemática de la Universidad Distrital Francisco José de Caldas. Email: yiserrator@libertadores.edu.co Es certificada como:

CHE, Auditor Líder e Interno ISO 27001:2013, Auditor interno ISO 22301:2019, ITIL, COBIT, SCRUM Foundations, entre otros. Adicional, posee conocimientos en informática forense, ciberseguridad, auditoría interna y manejo de proyectos. Se ha desempeñado como Oficial de Seguridad de la información para empresas multinacionales, consultor para empresas públicas y privadas, liderando equipos de trabajo multidisciplinarios, además docente universitario en varias universidades.

VIII. AGRADECIMIENTOS

Ya en esta instancia habiendo concluido no queda más que agradecer a aquellos que hicieron parte de este interesante proyecto, mismos que fueron de fundamental ayuda para el desarrollo de este.

Doy gracias a Dios, por su gran respaldo y bendición en el transcurso de mi vida, a mis seres queridos, quienes han sido esa columna que impulsa mis metas sin importar los tropiezos y las victorias, a mis compañeros y a mis instructores, por el apoyo incondicional que me brindaron en el desarrollo de esta investigación y en la formación como especialista en seguridad de la información, muchas gracias. Miguel Angel Mateus.

IX. REFERENTES TEÓRICOS

Congreso de Colombia. (2008). *www.desarrolloeconomico.gov.co.* Obtenido de http://www.desarrolloeconomico.gov.co/sites/default/files/marco-legal/Ley-1221-2008.pdf

Congreso de Colombia. (03 de Agosto de 2021). *dapre.presidencia.gov.co.* Obtenido de https://dapre.presidencia.gov.co/normativa/normativa/LEY%202121%20DEL%203%20DE%20AGOSTO%20DE%202021.pdf

Congreso de Colombia. (12 de Mayo de 2021). *www.funcionpublica.gov.co.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=162970

Dimitrios, J. (2020). *Platzi*. Obtenido de https://platzi.com/blog/que-es-norma-iso-27001/?utm_source=google&utm_medium=paid&utm_campaign=17446514363&utm_adgroup=&utm_content=&gclid=Cj0KCQjwwJuVBhCAARIsAOPwGARd6r9YQ-un7uEPrTvY_wNCyb7A28L0ccmox7fQwoTTu4ma1O3ktHwaArELEALw_wcB&gclsrc=aw.ds

El Espectador. (21 de 01 de 2022). *www.elespectador.com*. Obtenido de https://www.elespectador.com/tecnologia/cuidado-delincuentes-estan-usando-codigos-qr-para-estafar-a-sus-victimas/

Eset. (21 de 05 de 2021). *welivesecurity.* Obtenido de https://www.welivesecurity.com/la-es/2021/05/21/que-es-ransomware/

Gobierno de Colombia. (16 de Diciembre de 2020). *QUINTO ESTUDIO DE PERCEPCIÓN Y PENETRACIÓN EN EMPRESAS COLOMBIANAS.* Obtenido de MinTic - Teletrabajo: https://mintic.gov.co/portal/715/articles-179742_recurso_1.pdf

Ivan Belcic. (20 de Septiembre de 2021). *Avast.* Obtenido de https://www.avast.com/es-es/c-phishing

La República. (18 de 04 de 2022). *www.larepublica.co*. Obtenido de https://www.larepublica.co/opinion/editorial/el-teletrabajo-moda-que-llego-para-quedarse-3343128

Microsoft. (26 de 05 de 2022). *Protege el acceso a los recursos con la autenticación multifactor.* Obtenido de https://www.microsoft.com/es-co/security/business/identity-access-management/mfa-multi-factor-authentication

Ministerio del Trabajo. (30 de Abril de 2012). *www.mintrabajo.gov.co.* Obtenido de https://www.mintrabajo.gov.co/documents/20147/36491/decreto_0884_de_2012.pdf/317004d2-cb38-5088-b719-5ed047bec077

MinTic. (Abril de 2022). *www.teletrabajo.gov.co.* Obtenido de https://www.teletrabajo.gov.co/622/w3-article-126328.html

Norton. (26 de 05 de 2022). *Software malicioso.* Obtenido de https://co.norton.com/internetsecurity-malware-what-is-a-trojan.html