UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN TELECOMUNICACIONES
MENCIÓN: GESTIÓN DE LAS TELECOMUNICACIONES

Resolución: RPC-SE-01 - No.016-2020

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
El teletrabajo como una nueva forma de relación laboral en el Ecuador
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor/a:
Manuel de Jesús Rivas Coronel
Tutor/a:
Ph. D. Fidel David Parra Balza – Mg. Wilmer Fabián Albarracín Guarochico

Quito – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, Ph. D. Fidel David Parra Balza con C.I: 1757469950 en mi calidad de Tutor del proyecto de investigación titulado: El teletrabajo como una nueva forma de relación laboral en el Ecuador.

Elaborado por: Manuel Rivas Coronel, de C.I: 0103538690, estudiante de la Maestría: en Telecomunicaciones, mención: Tecnologías de la Información y la Comunicación (TIC) de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., 19 de Marzo de 2022

_____

Firma

Agradecimiento

A Dios, por sus bendiciones, por la vida
a mi esposa Patricia Janeth,
a mis hijos Mishell Estefanía, Angelo Joseph y Jessie Arleth,
a mis Padres, a mi familia a mis amigos,
por su tiempo, por su paciencia, por su incondicional apoyo.

A la Universidad Israel, por darnos esta oportunidad de aprender,
a mis tutores, por su guía y ayuda,
a mis profesores que impartieron su conocimiento,
a mis revisores por sus aportes y observaciones,
A todos quienes de una u otra forma colaboraron para la culminación de esta tesis

Manuel Rivas Coronel
Marzo - 2022

Contenido

Índice de tablas

Índice de Figuras

INFORMACIÓN GENERAL

Contextualización del Tema

El inicio del estudio parte en la necesidad de determinar la situación del teletrabajo en el Ecuador, que tomo su mayor repunte a partir de la pandemia del Covid – 19, tomando desprevenidos a los ecuatorianos en sus sistemas de comunicación, además en la capacidad para enviar y recibir información (Pérez, 2020). Pero eso no lo es todo, porque el incremento del tráfico en la red entre los empleados y las empresas, deja un punto sin considerar como lo es el resguardo seguro de la información confidencial, así como el almacenamiento de datos, contraseñas de acceso y otras entradas expuestas a los ciberataques. De ahí que se realizará un análisis de los métodos de telecomunicación que se han utilizado, con el fin de establecer las dificultades que han tenido los trabajadores en el cumplimiento de los objetivos empresariales, considerando además la normativa jurídica expedida hasta el momento.

El trabajo a distancia o comúnmente llamado teletrabajo, se lo considera así porque no se lo desarrolla dentro de la misma oficina o lugar de la empresa contratadora, sino que se ejecuta fuera del lugar habitual con los equipos tecnológicos necesarios y el servicio de internet, es decir, con todo el apoyo de la Tecnología de Información y Comunicación (TIC) (Joric, 2020). Mediante esta metodología, el empleado realiza sus actividades sin necesidad de salir de su casa, considerando que de ninguna manera perderá sus derechos laborales adquiridos, con toda la igualdad de condiciones que los empleados que asisten presencialmente a laborar.

Debido al entorno laboral y económico existente en el Ecuador y en el mundo por la pandemia del COVID 19, el teletrabajo es hoy en día una práctica laboral que se ha elegido como una manera preventiva para el cuidado de la vida del empleado (OIT, 2020), mismos que a pesar de que desempeñan su labor desde su propio hogar, no están exentos del cumplimento de los objetivos de la empresa, aportando a la rentabilidad, lo que ha permitido conservar su empleo y con ello, reducir la incidencia del desempleo (López, 2020).

Como se dijo anteriormente, Ecuador ha seguido la modalidad del teletrabajo no solamente en el ámbito privado, sino que las instituciones públicas también se acogieron a este modelo laboral (Barragán, 2021) que lo han valorado por que no afecta a sus intereses, continuando con sus actividades normalmente y acoplándolo a sistema presencial obligatorio, como en el caso de las industrias de transformación que requieren mano de obra (Narváez, 2020). Pero, nunca se consideró al inicio del contrato de trabajo, como una alternativa laboral, tampoco estaban listos los sistemas informáticos,

redes, routers, computadores, programas y seguridad de los datos, sorprendiendo al empleador y al trabajador que vieron en esta modalidad, como una alternativa para continuar trabajando, sin considerar la problemática de seguridad que podía conllevar.

Tradicionalmente Ecuador no ha sido un usuario del teletrabajo, más bien todos los ejecutivos y trabajadores siempre han asistido a su sitio de trabajo, desplazándose a través de sus calles, para cumplir sus funciones. Todas las empresas tenían su manera de controlar la asistencia, los tiempos de trabajo, los días laborados y las vacaciones. Para los empleadores era fundamental la presencia en el lugar de oficina, por la facilidad de supervisión y la conexión con su personal, la información estaba dentro de su mismo sistema de redes y almacenamiento, la papelería se archivaba en sus bodegas, es decir, no existía un mayor riesgo de que personas externas puedan usurpar documentos o informes confidenciales, basándose en la confianza que tenían en sus empleados y en la presión del desempeño. (Campaña *et al.*, 2020).

La modalidad de teletrabajo habitualmente en el Ecuador estaba reservada para los grupos vulnerables como adultos mayores, inmunodeficientes, digitadores, servicios contables y otros que realmente no requerían presencia o que eran contratos a honorarios (Ortiz *et al.*, 2020), a sabiendas que dichas personas debían contar con un computador, internet e impresora, para ejercer sus tareas, lo que significa una inversión por parte del trabajador (López, 2020, pág. 8).

Por lo antes expuesto, se puede afirmar que Ecuador no estaba listo para el teletrabajo, tanto en su legislación, como en su sistema de hardware, software y comunicación (Parra, 2020). Los trabajadores no esperaban esta modalidad para cumplir con sus labores, por lo que no disponían de computadores extras en sus casas y si lo tenían, fue para que sus hijos reciban sus clases, tampoco estaban capacitados en sistemas informáticos, métodos de comunicación avanzados y la telecomunicación fue algo que se acomodó en la marcha.

Problema de Investigación

Sin duda alguna, el Covid 19 ha afectado el desempeño de las actividades económicas en el Ecuador y el mundo, obligando al crecimiento de las telecomunicaciones a través de medios tecnológicos, ya que el trabajador se ha visto en la necesidad de prestar sus servicios desde su propio hogar o un sitio específico que no es su habitual oficina o sitio de trabajo, sin su presencia física.

El confinamiento, obligado por el temor de contagio de una enfermedad mortal, motivó al crecimiento del teletrabajo que ya no era solo una elección, sino que fue obligatorio, pero inicia como un experimento porque nadie estaba preparado desde el punto de vista de las herramientas

informáticas, así como de las telecomunicaciones, planteándose varios desafíos como son los de la ciberseguridad, la exposición de la información que puede ser confidencial y la misma privacidad.

Por el lado de la ciberseguridad, si bien no hay estadísticas que lo demuestren, una gran parte de la población ecuatoriana trabaja con software pirata, sin mayor conocimiento de las herramientas de telecomunicación y falta de habilidades digitales, lo que puede acarrear fácilmente a problemas de ciberseguridad de la información, ya que las computadoras personales no tienen configuraciones de seguridad, tampoco tienen políticas de conexión remota, antivirus, un sistema especializado de almacenamiento de datos, un *Virtual Private Network* (VPN) o Red Privada Virtual, autentificación, autorización e incluso desconocen de las copias de seguridad.

Debido a que hoy en día, las personas que están teletrabajando no se miran cara a cara, hay mucho riesgo de autentificación, no hay un monitoreo ni control del acceso, tampoco se ha fomentado la creación de contraseñas seguras, estos problemas pueden incrementar el ataque de phishing, la instalación de malware que se adhieren a los correos.

Es necesario exponer que el trabajador, no ha recibido ningún apoyo para la telecomunicación, por el contrario, ha tenido la reducción de los ingresos, porque para trabajar desde su domicilio deberá consumir más servicios básicos como es de la luz eléctrica, el agua potable, pagar un mayor ancho de banda para el internet e incluso contratar un antivirus para la protección de sus datos, aparte de ello, está la capacitación en programas de navegación, de comunicación y seguridad, sin dejar de lado el gasto para adaptar su espacio o sitio de trabajo para el mejor desempeño de su labor.

Por lo antes expuesto se plantea la siguiente interrogante:

¿Cuáles son los principales problemas de telecomunicaciones que están generando inseguridad al teletrabajo como nueva forma de relación laboral en el Ecuador?

Objetivo General

Analizar el teletrabajo como nueva forma de relación laboral, a través del estudio de los métodos de telecomunicación utilizados, que establezca su sostenibilidad en el tiempo.

Objetivos Específicos

- Contextualizar los fundamentos teóricos desde el punto de vista técnico y legal del teletrabajo en el Ecuador.
- Diagnosticar el criterio de los teletrabajadores en la ciudad de Quito, con relación a los métodos de telecomunicaciones utilizados.

- Diseñar estrategias de telecomunicación que permitan enfrentar los problemas encontrados para el teletrabajo.
- Validar a través de expertos, las estrategias propuestas

Vinculación con la Sociedad y Beneficiarios Directos:

Cabe destacar que la investigación se justifica su estudio en la necesidad que tienen las empresas en mantener su información confidencial a buen resguardo, ante posibles ataques o filtración de información confidencial, por lo que necesitan de mantener un alto conocimiento de ciberseguridad, misma que se deberá compartir a todos sus empleados que trabajan en la modalidad de teletrabajo, dando así seguridad a las telecomunicaciones y un respaldo a esta nueva modalidad de empleo.

Además, es necesario que la ciberseguridad se difunda en todo el país, con estrategias comunicacionales y recomendaciones, basadas en la vivencia actual del sistema de teletrabajo, que es improvisado y tiene muy bajos estándares de seguridad, para beneficio especialmente de las medianas empresas que no disponen de recursos para una auditoría de sistemas y comunicación.

Es necesario poner en relieve los desafíos de las telecomunicaciones en el Ecuador, así como las amenazas y el reto que se presenta, para el conocimiento de todas las empresas e instituciones públicas y privadas, así como la colectividad, para poner en alerta los problemas detectados y la forma como se podría afrontarlos, dando un primer inicio a este estilo de informe que beneficia a todo el país.

Finalmente, se espera diseñar estrategias de telecomunicación que logren un efectivo cumplimiento del trabajo con el aprovechamiento de las Tecnologías de Información y Comunicación para cumplir con los objetivos planteados, optimizando recursos económicos en el hogar acogiéndonos a la amplia capacitación que entregan las redes sociales, como son YouTube, Facebook, etc., también páginas especializadas en capacitaciones muchas de ellas gratuitos en internet para de ésta manera mejorar la comprensión de los temas que involucran la utilización del internet, los programas, las comunicaciones y permitir el cumplimiento óptimo de las actividades.

Finalmente hay que mencionar que el teletrabajo es una opción que ofrece numerosos beneficios tanto a las pequeñas y medianas empresas como para los trabajadores, sobre todo en momentos delicados como los que estamos viviendo, siendo los principales beneficiarios y a quienes va principalmente dirigido.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización General del Estado del Arte

El presente estudio se basará en bibliografía, artículos científicos y demás publicaciones existentes en las plataformas bibliográficas publicadas en la web de autores que han abordado el problema de las telecomunicaciones y la ciberseguridad, tales como De León, Altamirano, Gallusser y Osio, pero también de Instituciones públicas y privadas como el Instituto Nacional de Ciberseguridad de España, la Secretaría de Comunicaciones y Transporte de México y la Organización Internacional del Trabajo (OIT).

Como se ha dicho, el enfoque de las telecomunicaciones está dirigido hacia la ciberseguridad en el teletrabajo, siendo estas dos variables las que serán abordadas en el marco teórico y para el desarrollo de la propuesta, considerando la realidad del Ecuador y la forma cómo han implementado esta modalidad de trabajo en las empresas privadas de la ciudad de Quito.

Por ser un tema muy importante que involucra la realidad nacional que enfrentan los trabajadores para evitar el contagio del Covid 19, la investigación será muy influyente en las pequeñas y medianas empresas privadas, ya que, por no contar con grandes recursos para implementar sistemas informáticos de alta seguridad, deben implementar estrategias que el mercado ofrece o aprovechar las herramientas que tienen, de esta manera se evitará el ataque o usurpación de su información, en el desarrollo del paso o almacenamiento de sus datos.

Para el desarrollo se utilizarán recursos tecnológicos como el Wifi, Bluetooth, Dispositivo móvil (celular inteligente), Antivirus y VPN (Red Privada Virtual). Todos estos serán utilizados para, de forma integral, establecer las entradas potenciales de ataque a la ciberseguridad de una empresa, desde un periférico con el que trabaja un empleado a modo de teletrabajo.

Para el desarrollo de la investigación, es necesario establecer el estado del arte, es decir, cómo se encuentran actualmente las investigaciones similares donde se hayan abordado las variables: telecomunicación, ciberseguridad y teletrabajo. Así se encontró el trabajo del autor Gallusser (2018) titulado “Creciente avance del teletrabajo como modalidad laboral” donde la autora primeramente busca el fundamento legal del teletrabajo en la Unión Europea, encontrando diferentes sistemas digitales de comunicación que se han instalado en los países miembros de dicho grupo, estableciendo así una serie de principios para la Tecnología de Información y Comunicación que debe ser utilizados por las empresas y las personas que teletrabajan con estrategias de cambios en su mentalidad y el fundamento de conceptos para conocer cada uno de los sistemas con los que trabajan, así se realiza una

encuesta estadística para enfocar el problema, estableciendo porcentajes de las herramientas utilizadas en la comunicación y con ello, lograr bases de su propuesta. Es así que este estudio aportará con su metodología para alcanzar resultados similares y fortalecer la propuesta de la investigación en curso.

Otro trabajo importante es el de (Lubiza Osorio, 2020). publicado bajo el título de "El Teletrabajo: Una opción en la era digital" buscando relacionar el teletrabajo con la telecomunicación, ya que estos dos aspectos no han sido abordados a profundidad por la falta de necesidad, así el estudio realiza varias visitas de campo en domicilios de teletrabajadores analizando sus problemas jurídicos y tecnológicos, así como las aptitudes para el afrontamiento, logrando así definir los problemas relevantes y proponiendo respuestas a los mismos, en conclusión, genera estrategias para que reduzca las posibilidades de un ciberataque, dato que será muy importante para el estudio en curso.

Seguidamente se analiza el informe de la (Secretaría de Comunicación y Transporte , 2020). de México que publican la "Guía de ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo" con la finalidad de apoyar a las empresas mexicanas y a sus trabajadores en la capacitación sobre ciberseguridad, misma que está siendo vulnerada con ataques provenientes de países extranjeros, así se identifican los principales problemas de seguridad, por dónde llegan, las formas de ataques y se propone sistemas de navegación segura, teleconferencias y Redes Privadas Virtuales (VPN) con herramientas seguras en la nube y recursos bien utilizados. Es así como esta Guía será utilizada también como modelo de la propuesta, por su semejanza a la realidad que vive el país, aportando con información técnica y especializada en telecomunicaciones frente al ciberataque hacia un teletrabajador.

Otra publicación importante es la del (Instituto Nacional de Ciberseguridad de España , 2020) que presenta una "Ciberseguridad en el teletrabajo. Una guía de aproximación para el empresario" con el objetivo de establecerse como una herramienta para evitar los ciberataques en las organizaciones. Lo hacen primeramente identificando los accesos remotos en las empresas a través de un trabajo de campo en algunas empresas modelo, estableciendo la infraestructura de escritorio virtual y el almacenamiento en la nube, posteriormente presenta soluciones con herramientas colaborativas, así como recomendaciones de seguridad en el uso de las diferentes aplicaciones que utilizan los trabajadores para videollamadas, generando finalmente estrategias para asegurar las terminales de trabajo, dispositivos móviles más las copias de seguridad. Con este estudio muy completo, se podrá realizar una mejor propuesta, enriquecida con la información y la forma como han abordado el tema, ya

que se realiza a empresarios de pequeñas y medianas empresas, con fines de dar una mayor seguridad al teletrabajo.

Finalmente está la publicación realizada por (De León Gómez, 2021) titulado “Mejores Prácticas de Seguridad en el Teletrabajo: una revisión” cuyo objetivo es establecer buenas prácticas de seguridad en el teletrabajo, con reglas que den paso a un funcionamiento confiable de todas las conexiones remotas, debido a que por la pandemia del Covid 19 la información que antes se almacenaba solamente en la empresa, ahora circula a través de internet, con información sensible e inseguridad tanto en el punto de entrada y como en el destino. El autor utilizó un sistema de revisión metódica de procesos de información con lo que logró establecer la principal problemática de ciberseguridad, con lo que estableció un modelo de buenas prácticas con énfasis en las PYMES. Es así como este trabajo tiene una temática similar con la presente investigación, por lo que servirá de modelo en su base teórica y propuestal, mejorando así la seguridad de la información y comunicación en las empresas

1.2. Proceso Investigativo Metodológico

1.2.1. Enfoque de Investigación

La investigación tendrá un enfoque cuantitativo y cualitativo. Cualitativo porque se pretende extraer de los teletrabajadores los problemas que ha traído el teletrabajo, la inseguridad de los datos que mantienen en sus computadores y el posible ataque de la ciberdelincuencia. Bajo esta premisa, según Hernández *et al.* (2017) exponen que esta metodología se apoya en la utilización de varias técnicas e instrumentos como la encuesta y entrevista, cuyo objetivo principal es el de recabar información directa de los involucrados en el estudio, en este caso, con los teletrabajadores que prestan sus servicios a las empresas privadas y se lo hará mediante la recolección de sus experiencias, así como lo que opinan del entorno laboral.

Otro método utilizado es inductivo-deductivo el que se basa en razonamientos contrapuestos bajo una relación de dependencia mutua. Es así que, mediante la formulación inductiva se estudia un problema planteado con un estudio basado inicialmente en lo particular, para llegar hacia algo más general. En este caso, se parte de un problema como lo es el teletrabajo para llegar hasta la ciberseguridad, y su parte, la metodología inductiva busca estudiar el problema desde un punto más general, desde donde se ramifica y extiende hacia un lugar en particular (Villabella, 2020). Con este método se partirá del estudio del teletrabajo hasta llegar a lo más concreto que es la comunicación y el ciberataque a los sistemas que trabajan bajo este modelo. Así también analizar el problema que tienen

los teletrabajadores al momento de enviar información y establecer estrategias de telecomunicación que permitan enfrentar los problemas encontrados para el teletrabajo.

1.2.2. Tipo de Investigación

El tipo de investigación será la forma en la que el investigador estudiará y con ello podrá contestar la pregunta planteada en el problema científico (Arias, 2016). Considerando esta conceptualización, el presente estudio optará por un diseño mixto que estará compuesto por una combinación entre los resultados cualitativos y los cuantitativo que son requeridos para el estudio.

También será descriptiva, porque se narrará un hecho importante para la humanidad que ha influenciado en el problema y que dio pie al repunte del teletrabajo como es el Covid 19, además del criterio que tienen los trabajadores respecto a las telecomunicaciones, la seguridad, la ciberdelincuencia y la comunicación, entre otros problemas existentes dentro de su relación de trabajo, exponiendo los resultados que describen el problema, como un reflejo de sus opiniones y vivencias propias que les da el mantener un trabajo a distancia, más el temor de ser objeto de la ciberdelincuencia y la apropiación de su información (Hernández *et al.,* 2017).

1.2.3. Población y Muestra

La población de estudio de la investigación está conformada por la Población Económicamente Activa (PEA) de la ciudad de Quito, que representa el 48,9% del total de sus habitantes (2’690.150), es decir 1’315.483. La muestra se calcula en base a la fórmula para poblaciones finitas que se presenta a continuación:

$$n = \frac{Z^2 Npq}{e^2(N-1) + Z^2 pq}$$

Fuente: Weiers (2016)

Reemplazando sería:

$$n = \frac{1{,}964^2 x 1'315.483 x 0{,}5 x 0{,}5}{0{,}1^2(1'315.483 - 1) + 1{,}964^2 x 0{,}5 x 0{,}5} = 68$$

Dónde:

n = el tamaño de la muestra.

N = tamaño de la población.

p = probabilidad de éxito.

q = probabilidad de fracaso.

Z = Valor obtenido mediante niveles de confianza.

e = Límite aceptable de error muestral

Aplicada la fórmula se estableció una muestra de 68 quiteños para encuestar.

1.2.4. Métodos, Técnicas e Instrumentos

Las técnicas o instrumentos de recogidas de datos representan los medios que se emplean para recopilar y almacenar la información necesaria para responder los objetivos planteados en una investigación científica. Las técnicas e instrumentos que se utilizaron para el desarrollo de la presente investigación son los siguientes:

Tabla 1

Fichas Técnicas para recopilar datos

Fichas técnicas	Instrumentos
Cuantitativas (Encuesta).	Cuestionario
Cualitativa (Conversacionales	Entrevista

1.2.5. Resultados de la Encuesta

Una vez realizada la encuesta a la población de estudio, utilizando mediante el Microsoft Forms, se presenta a continuación los resultados.

Pregunta 1 ¿En qué sector vive?

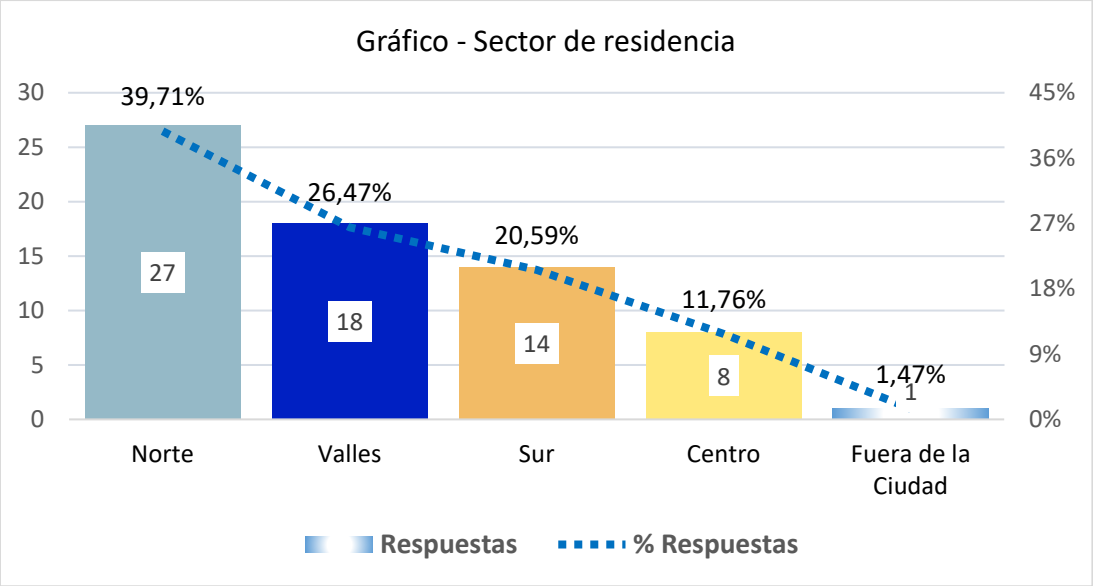
Tabla 2

Encuesta - En que sector vive?

Sector	Respuestas	%
Centro	8	11.76%
Fuera de la Ciudad	1	1.47%
Norte	27	39.71%
Sur	14	20.59%
Valles	18	26.47%
Total	**68**	**100.00%**

Figura 1

Sector donde vive



Análisis

La respuesta a esta pregunta deja ver una distribución casi equitativa entre el sector sur y los valles de Quito, mientras otra parte más grande de los encuestados viven al norte de la capital, una minoría habitan en el centro y fuera de la ciudad. Es de considerar que la tendencia habitacional se ha trasladado mayormente al norte, por la comodidad de transporte público y las construcciones de nuevas carreteras, así como centros comerciales y de ahorro, adicional porque es un polo de desarrollo y posee mejor infraestructura.

Pregunta 2 ¿En qué área de su empresa trabaja?

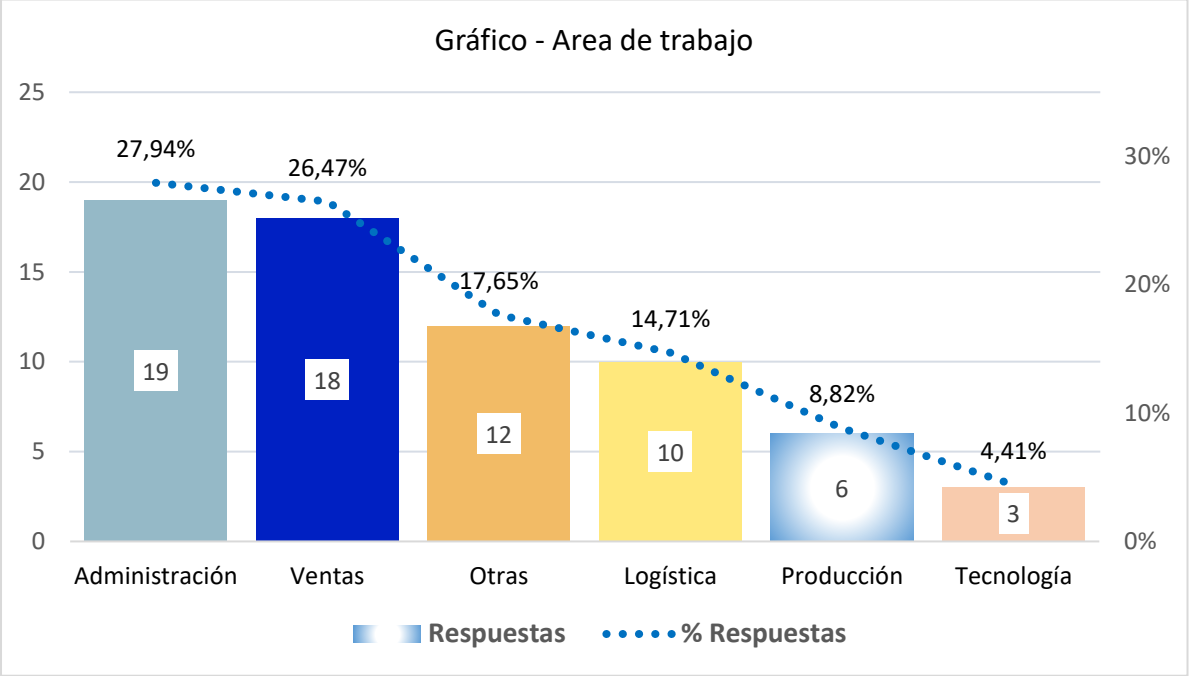
Tabla 3

Encuesta – en que área de su empresa trabaja

Área Trabajo	Respuestas	%
Administración	19	27,94%
Ventas	18	26,47%
Otras	12	17,65%
Logística	10	14,71%
Producción	6	8,82%
Tecnología	3	4,41%
Total	**68**	**100,00%**

Figura 2

Área de trabajo del encuestado



Análisis

El teletrabajo principalmente ha sido motivado para los trabajadores administrativos, que pueden desempeñar sus funciones desde su casa, por lo que el personal de producción, mantenimiento y limpieza, hacen su trabajo de manera presencial, por la necesidad de utilizar maquinaria o realizar labores que requieren de su esfuerzo físico manual. Bajo esa perspectiva, las personas que han respondido esta encuesta en su mayoría están representados por las personas administrativas, comerciales, de logística y otras (asesores externos, consultores, auditores).

Solo una minoría correspondiente al 8,8% de personas que labora en la producción y 4,4% tecnológica en tecnología, están presentes en la encuesta. Hay que considerar que aún el personal de producción y tecnología, parcialmente pueden desempeñar sus funciones a modo de teletrabajo, compartiendo reportes, dando instrucciones y resolviendo problemas.

Pregunta 3 ¿Antes estuvo o en la actualidad está en teletrabajo? (si su respuesta es sí, pase a la siguiente pregunta, de lo contrario, muchas gracias)

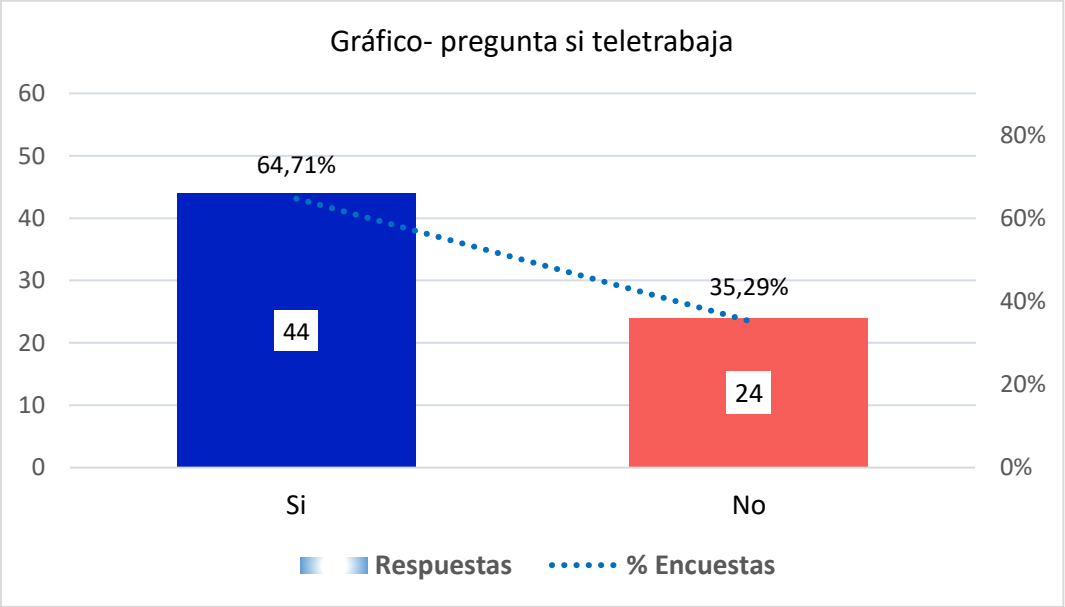
Tabla 4

Encuesta - Estuvo o está actualmente en Teletrabajo

Teletrabajo	Respuestas	%
Si	44	64.71%
No	24	35.29%
Total	**68**	**100.00%**

Figura 3

Estuvo o está actualmente en Teletrabajo



Análisis

De los encuestados, la mayoría han pasado por el teletrabajo, han iniciado en él o continúan teletrabajando, esto ocurre desde marzo del 2020 y se han cumplido dos años desde el inicio de la pandemia del Covid 19 que impulsó esta manera de contratación, con sus respectivos beneficios y desventajas. Si bien un 35,29% afirma que no está teletrabajando, esto ocurre porque un grupo de encuestados pertenece a la dirección empresarial, lo que obligaba a dichas personas a estar al frente de sus empresas, para el control de la producción, ventas y logística misma.

Pregunta 4 ¿Qué nivel de confidencialidad tiene la información con la que usted trabaja?

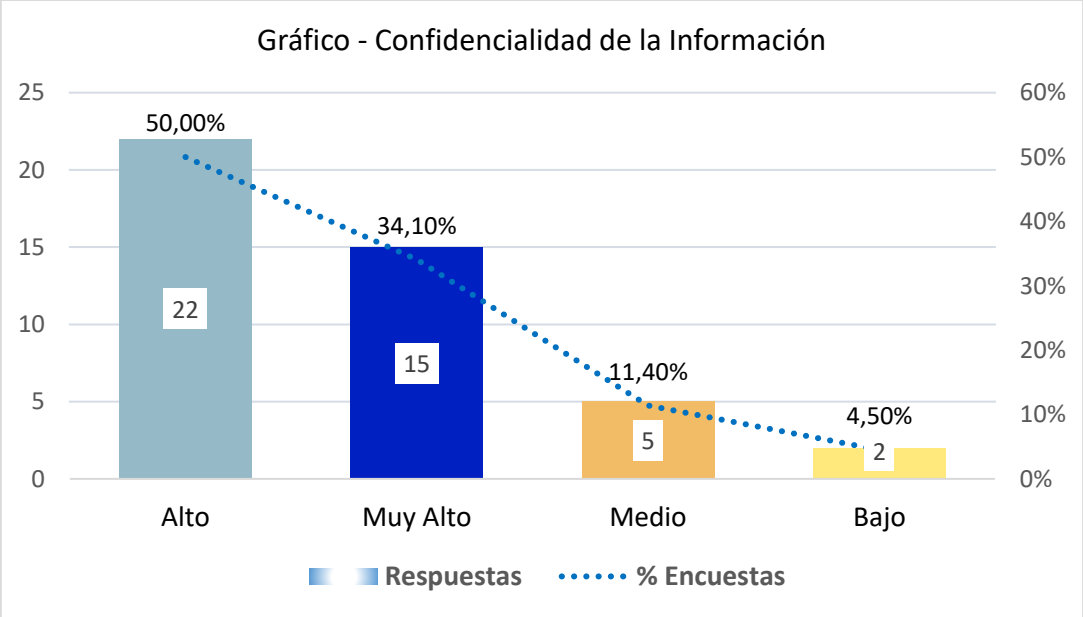
Tabla 5

Encuesta - Confidencialidad de la información

Confidencialidad	Respuestas	%
Alto	22	50,00%
Muy Alto	15	34,09%
Medio	5	11,36%
Bajo	2	4,55%
Total	**44**	**100,00%**

Figura 4

Confidencialidad de la información



Análisis

Como se puede analizar en el Figura 4, la mayoría de los encuestados trabaja con información confidencial entre muy alta, alta y media, más bien una mayoría de tan solo el 4,55% piensa que su trabajo no emite informes que puedan afectar la confidencialidad de la empresa donde laboran. Esto pone en realce la necesidad de mantener segura la base de datos y los envíos de información desde la persona que se encuentra teletrabajando, hacia su empresa o personal directivo, considerando que las empresas grandes y las corporaciones a los datos los denominan y dan el trato de activo de la empresa.

Pregunta 5 ¿Qué medio o medios electrónicos utiliza para recibe o envía su trabajo? (puede marcar más de uno)

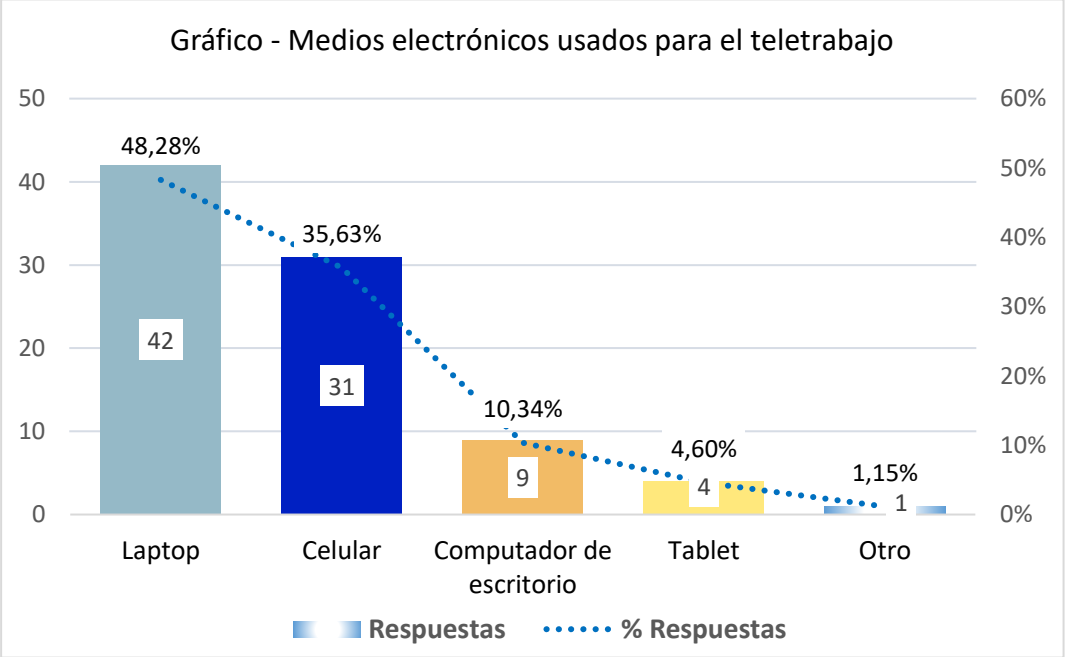
Tabla 6

Encuesta – que medios electrónicos utilizados en el trabajo

Equipos	Respuestas	%
Laptop	42	48,28%
Celular	31	35,63%
Computador de Escritorio	9	10,34%
Tablet	4	4,60%
Otro	1	1,15%
Total	**87**	**100,00%**

Figura 5

Medios electrónicos para realizar el teletrabajo



Análisis

En esta pregunta se resalta que la mayoría de los encuestados, utilizan medios tecnológicos móviles como la laptop y el celular para recibir o enviar información desde su lugar de trabajo y su empresa empleadora, esto representa un riesgo mayor de la información, porque en caso de pérdida de los aparatos móviles, existiría un alto riesgo de que la información caiga en manos equivocadas, por lo

que será necesario que tengan sus equipos con contraseñas robustas, así como los reportes más especializados e incluso salir de sus email o disponer de una política de desconexión digital cada que terminan sus tareas del teletrabajo.

Pregunta 6 ¿Cuáles de los siguientes programas son los que más utiliza? (puede marcar más de uno)

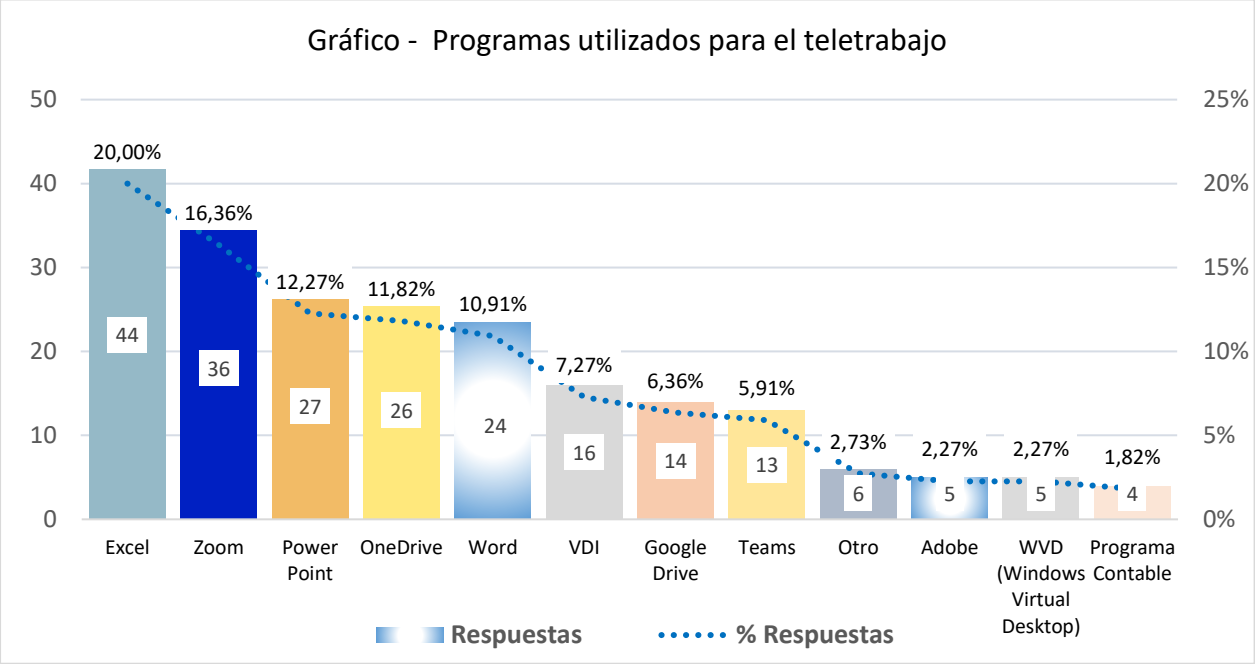
Tabla 7

Encuesta - programas que utiliza en el teletrabajo

Programas	Respuestas	%
Excel	44	20,00%
Zoom	36	16,36%
PowerPoint	27	12,27%
OneDrive	26	11,82%
Word	24	10,91%
VDI	16	7,27%
Google Drive	14	6,36%
Teams	13	5,91%
Otro	6	2,73%
Adobe	5	2,27%
Windows Virtual Desktop	5	2,27%
Programa Contable	4	1,82%
Total		**100,00%**

Figura 6

Programas usados en el teletrabajo



Análisis

Los encuestados han confirmado que, en su mayoría, utilizan programas como: Excel, Zoom, Power Point, OneDrive y Word, en ese orden. La utilización de otros programas especializados ya está en función del tipo de negocio y actividad comercial, un procesador de palabras y una hoja electrónica son básicos, pero por el teletrabajo, se utiliza mucho Excel, Zoom y Power Point para presentar informes y reportes, almacenando sus datos en un sitio seguro como lo es el OneDrive.

Pregunta 7 ¿Tiene usted licencias de los programas que utiliza?

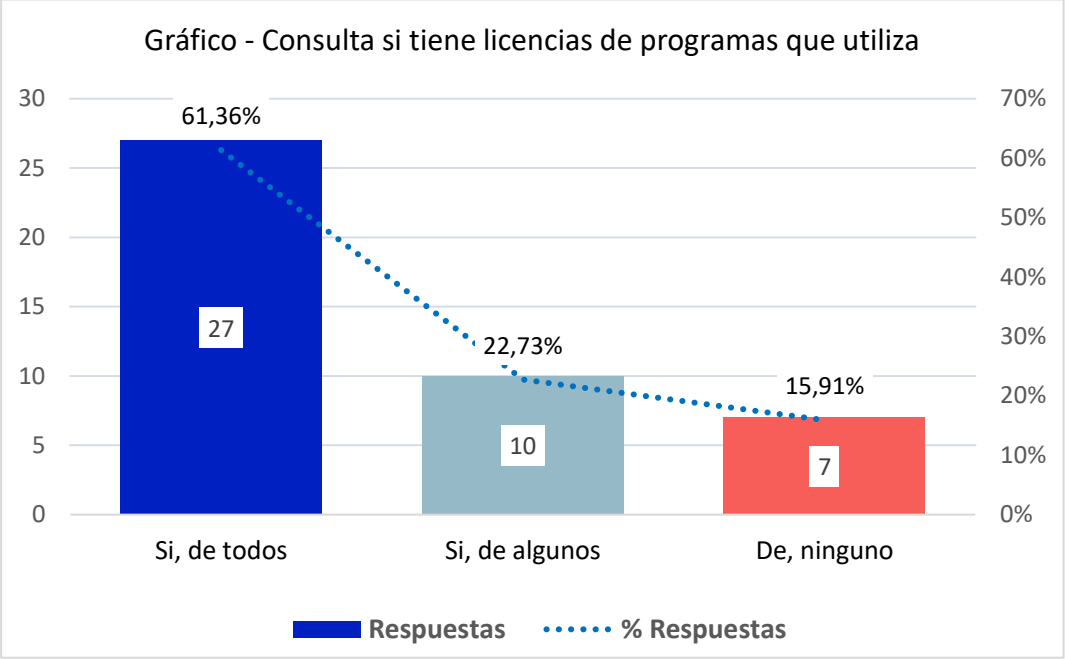
Tabla 8

Encuesta - Posee licencia de los programas que utiliza

Licencias	Respuestas	%
Si, de todos	27	61,36%
Si, de algunos	10	22,73%
De, Ninguno	7	15,91%
Totales	**44**	**100,00%**

Figura 7

Licencias de los programas que usa



Análisis

Mantener programas que no tienen licencia en un equipo informático, viene constituyéndose casi una tradición en los hogares ecuatorianos. Un reporte de Diario el Comercio (2015) daba cuenta que el 68% de los equipos en el país, tiene uno o más software sin licencia, es decir, pirata. Ante las respuestas a esta pregunta, se puede analizar que las personas de teletrabajo se han interesado en tener en sus equipos programas bajo licencia, ya que un programa pirata representa un peligro en el computador, porque no tiene opciones de actualización y deja la puerta abierta a la intrusión y el ciberataque.

Pregunta 8 ¿Califique usted el espacio con que dispone para el desarrollo del teletrabajo?

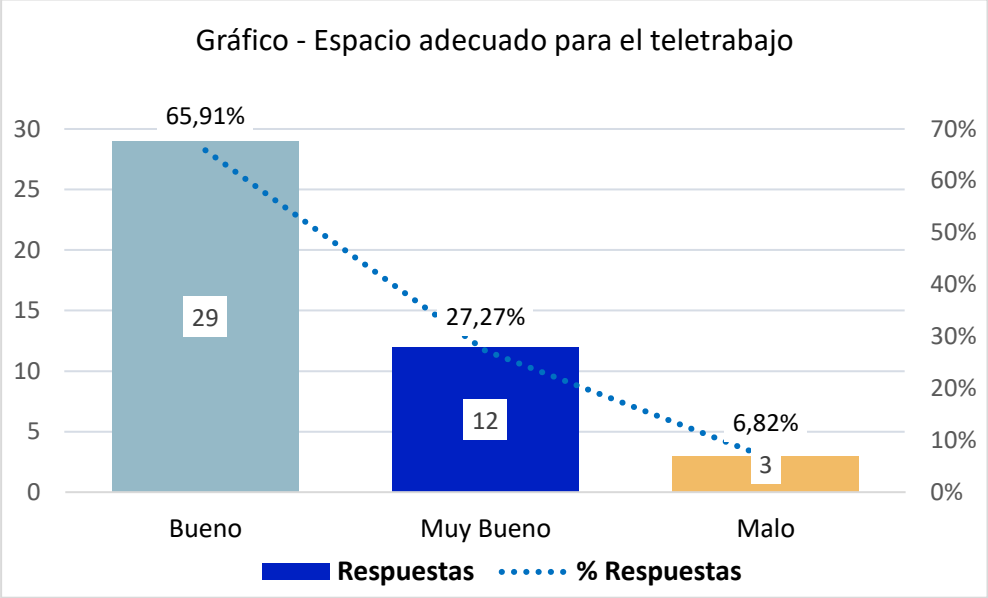
Tabla 9

Encuesta - Dispone de espacio adecuado para el teletrabajo

Espacio para teletrabajo	Respuestas	%
Muy bueno	12	27,27%
Bueno	29	65,91%
Malo	3	6,82%
Totales	**44**	**100,00%**

Figura 8

Espacio adecuado para el teletrabajo



Análisis

Para un buen desarrollo del trabajo, siempre es necesario mantener un espacio suficiente, libre de ruido excesivo, con ventilación, luz y sobre todo que tenga acceso a los servicios básicos de sanidad. De acuerdo con las respuestas recibidas, solo el 27,27% tienen un lugar muy bueno, es decir, cumple con todas las necesidades para cumplir el trabajo, han logrado adaptarlo completamente en sus hogares y están satisfechos con ello. Por otro lado, una mayoría tiene un sitio bueno, es decir, no es el que esperan, pero por efectos de presupuesto y por qué este tipo de trabajo nunca estuvo previsto, aún no se acomodan perfectamente, mientras que una minoría definitivamente está inconforme con su lugar de trabajo, siendo ellos el 6,82% del total de encuestados.

Pregunta 9 ¿En qué concepto se ha incrementado sus gastos como consecuencia del teletrabajo? (puede marcar más de uno).

Tabla 10

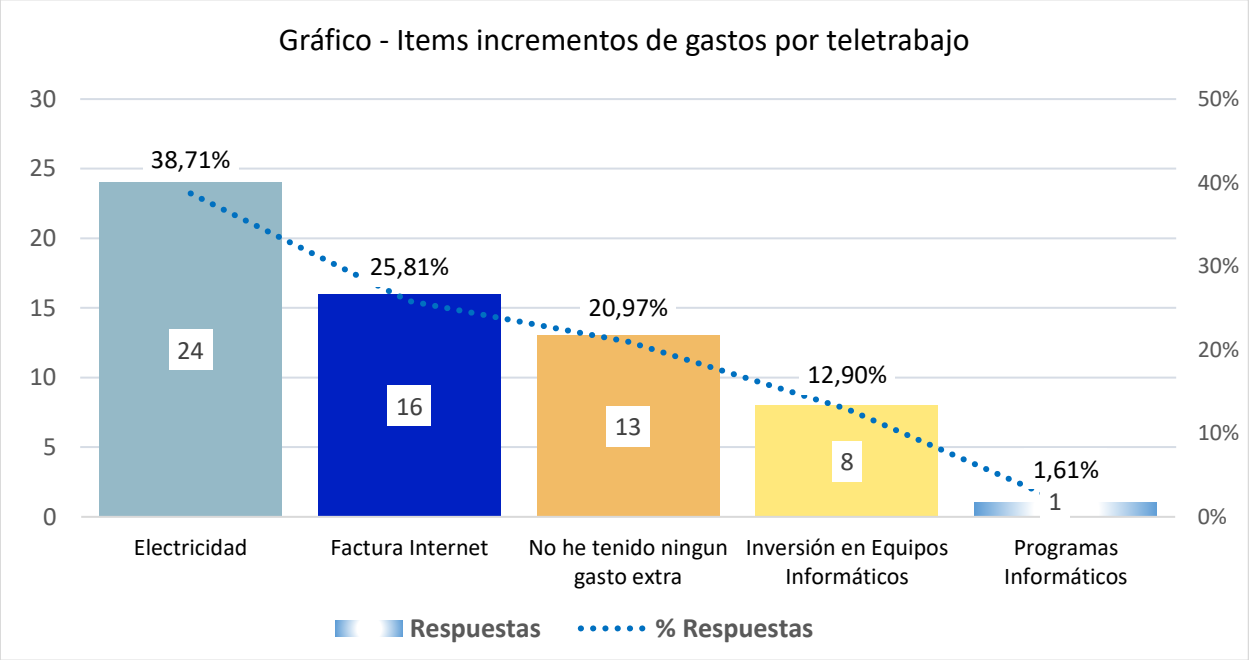
Encuesta - Incremento de gastos por teletrabajo

Ítem	Respuestas	%
Electricidad	24	38,71%
Factura Internet	16	25,81%
No he tenido ningún gasto extra	13	20,97%

Inversión en Equipos Informáticos	8	12,90%
Programas informáticos	1	1,61%
Total	**62**	**100,00%**

Figura 9

Gastos incrementados durante el teletrabajo



Análisis

Todos los aparatos electrónicos como computadores de escritorio, laptops, tablets, celulares, ups, entre otros, utilizan energía eléctrica para su funcionamiento, sin ella, se descargarían y dejarían de funcionar. En el caso del teletrabajo, las personas se han visto en la necesidad de tener o utilizar sus aparatos electrónicos que tienen en casa, obligando al incremento del consumo eléctrico, es por eso que las respuestas a esta pregunta confirman lo dicho, con una tendencia hacia la electricidad como el mayor gasto incrementado, seguido por el internet, que debe ser mejorado para una buena transmisión de datos. Algunas personas incluso han tenido que invertir en tecnología y programas informáticos, pero son una minoría.

Pregunta 10 ¿Qué nivel de capacitación ha recibido usted de parte de su empresa para el envío y recepción de información de manera segura?

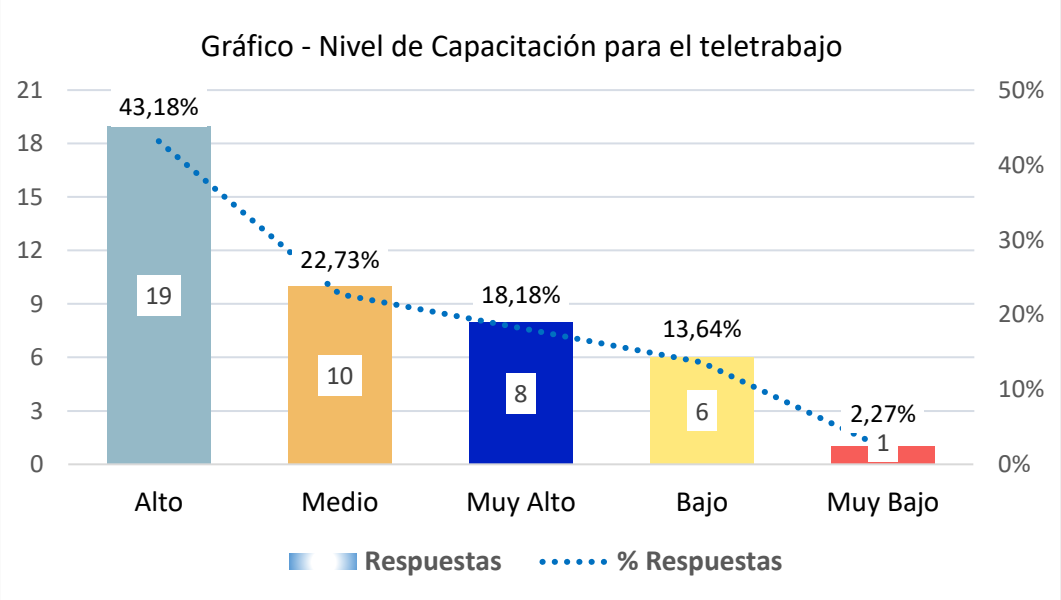
Tabla 11

Encuesta - Nivel de capacitación recibida

Capacitación Recibida	Respuestas	%
Alto	19	43,18%
Medio	10	22,73%
Muy Alto	8	18,18%
Bajo	6	13,64%
Muy Bajo	1	2,27%
Total	**44**	**100,00%**

Figura 10

Nivel de capacitación



Análisis

Las empresas, sabiendo que su personal manejará información confidencial desde un lugar que no es el entorno seguro de su localidad, han tenido que capacitar a sus trabajadores y ejecutivos, de tal manera que exista un alto nivel de seguridad y confidencialidad de los datos. Lo dicho lo corrobora esta pregunta donde prácticamente todos los encuestados han recibido capacitación desde un nivel medio,

alto y muy alto, por lo que se analiza el interés que tienen las instituciones por velar por la seguridad de sus datos.

Pregunta 11 ¿Su antivirus instalado tiene cobertura para la protección de tráfico en línea?

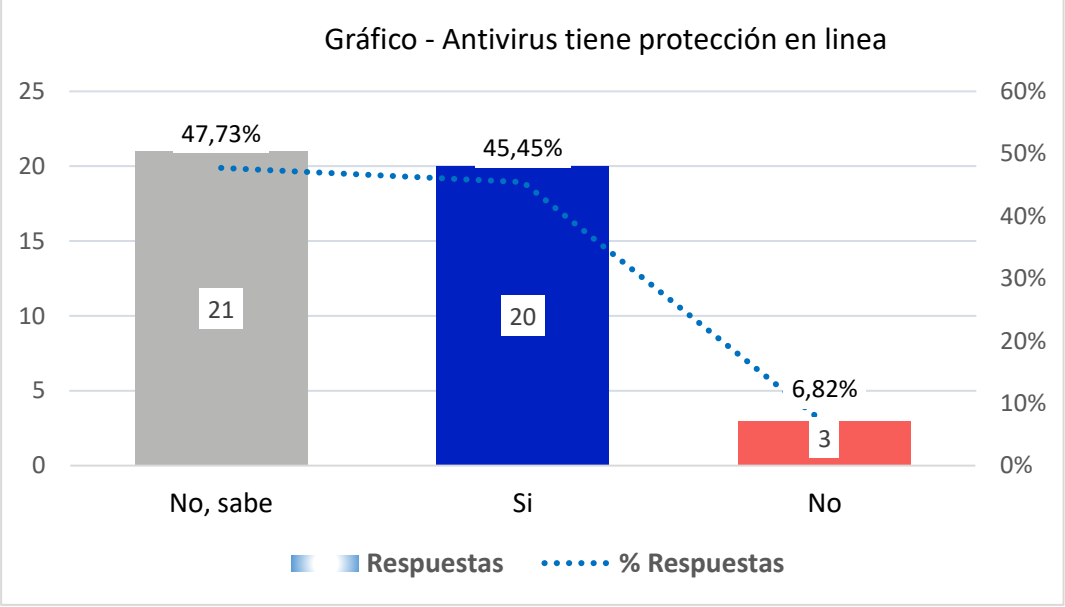
Tabla 12

Encuesta - Antivirus especializado para la protección de tráfico en línea

Antivirus	Respuestas	%
No sabe.	21	47,73%
Si	20	45,45%
No	3	6,82%
Total	**44**	**100,00%**

Figura 11

Antivirus especializado para la protección de tráfico en línea



Análisis

La utilización correcta y bien lograda de un antivirus no es muy frecuente dentro de la comunidad ecuatoriana (Mosquera Chere, 2021), pese a que constituye una necesidad para la seguridad de los datos y la protección del sistema operativo de un computador o medio que se sustente bajo un sistema operativo, es por eso que la respuesta a la pregunta estaba prevista, donde una gran parte de los encuestados desconoce o no sabe nada respecto a la protección del tráfico de datos que proporciona un antivirus. Pese a ello, parte de la capacitación recibida por las personas que utilizan computadores en

teletrabajo, consiste en mantener actualizado su antivirus y conocer cómo configurarlo para una mayor protección del acceso al sistema y los programas informáticos.

Pregunta 12 ¿Qué problemas técnicos ha tenido para su conexión a internet?

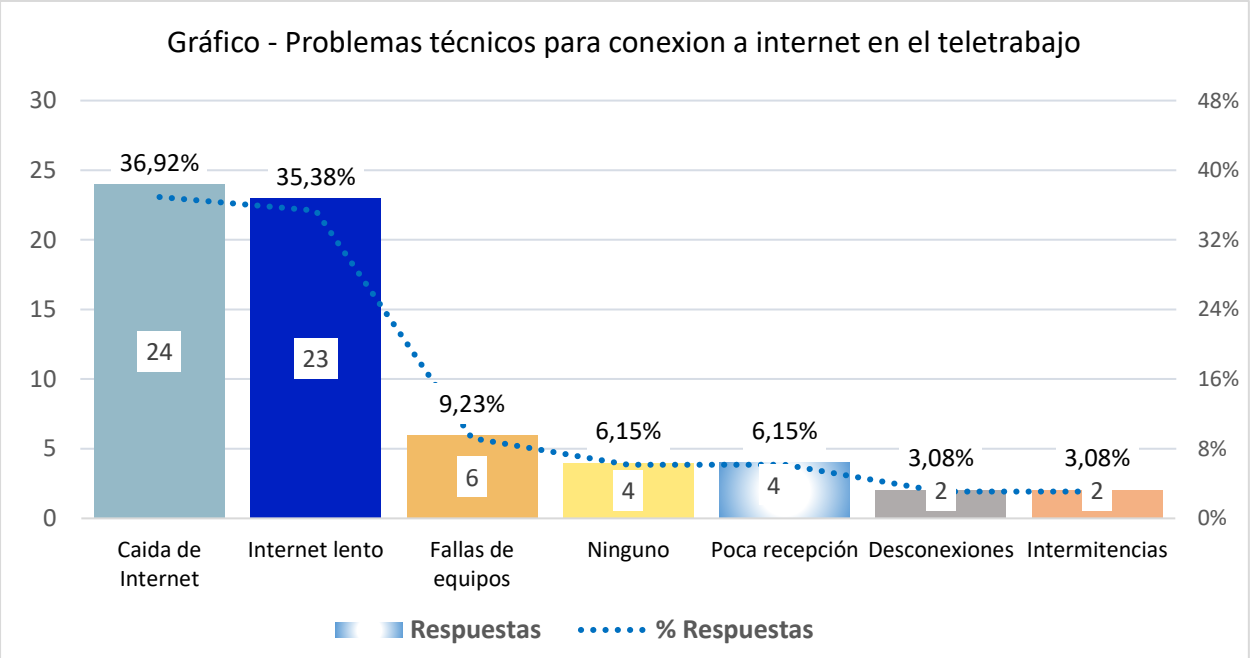
Tabla 13

Encuesta - Problemas técnicos para conexión a internet

Ítems	Respuestas	%
Caída de Internet	24	36,92%
Internet lento	23	35,38%
Fallas de Equipos	6	9,23%
Ninguno	4	6,15%
Poca recepción	4	6,15%
Desconexiones	2	3,08%
Intermitencias	2	3,08%
Total		**100,00%**

Figura 12

Problemas técnicos para conexión a internet



Análisis

Otro de los grandes inconvenientes en la utilización de computadores, tablets, celulares inteligentes y cualquier dispositivo electrónico que se sustenta en un sistema operativo, es la conexión e interconexión a través del internet. Para que todo funcione perfectamente, es necesario tener un sistema con cableado acorde a la velocidad del internet, además un computador con capacidad para aprovechar el ancho de banda y equipos de recepción que den los resultados de velocidad esperados, además, se requieren conocimientos básicos ante fallas e intermitencias, juntamente con un buen servicio técnico del proveedor. Ante todo, lo dicho, se observa que la caída del internet y su lentitud, son los mayores problemas, que deberán ser resueltos por el proveedor y si este no reacciona a tiempo, lo mejor es buscar uno nuevo.

Pregunta 13 Califique el nivel de complejidad que tienen los programas que usted utiliza

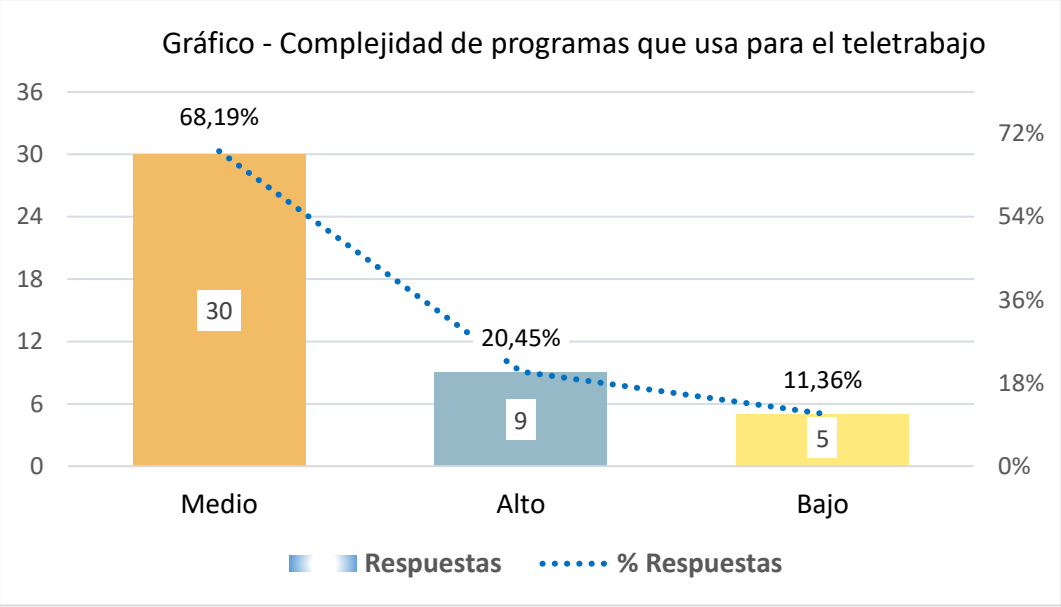
Tabla 14

Encuesta - Complejidad de los programas que se utilizan

Complejidad	Respuestas	%
Medio	30	68,2%
Alto	9	20,5%
Bajo	5	11,4%
Total	**44**	**100,0%**

Figura 13

Complejidad de los programas que se utilizan



Análisis

Antes de la pandemia, los ejecutivos y trabajadores de las empresas utilizaban los programas más básicos de Microsoft Office, lo que no sucede hoy en día, que tienen que saber utilizan otros tipos de programas para la comunicación persona a persona y con equipos de trabajo, por ello, la respuesta a esta pregunta es de esperarse, donde el conocimiento sobre los programas que se utiliza en teletrabajo es medio, con el 68,19%, solo un grupo que quizá antes ya utilizaba estos medios de comunicación, creen que sus programas no son complejos. De todas maneras, la capacitación va a influir en su conocimiento y por ende el desarrollo eficiente de su trabajo con el soporte de los programas que utilizan.

Pregunta 14 ¿En qué medida ha tenido ciberataques a su cuenta o la de su empresa?

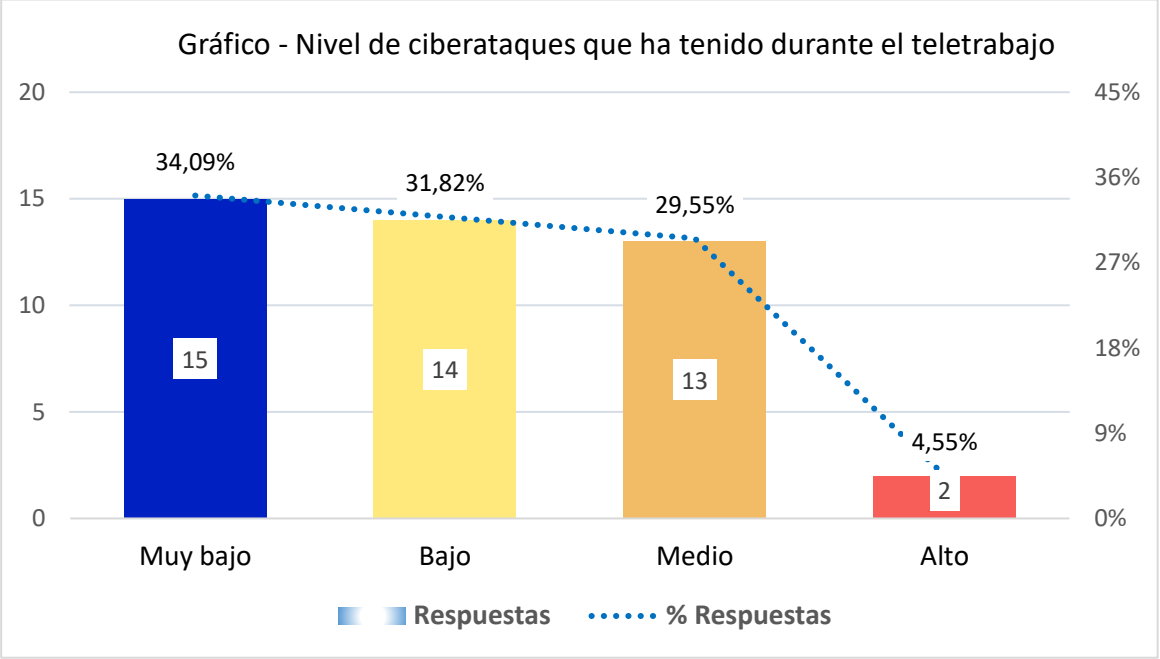
Tabla 15

Encuesta - Nivel de ciberataques

Ciberataque	Respuestas	%
Muy Bajo	15	34,09%
Bajo	14	31,82%
Medio	13	29,55%
Alto	2	4,55%
Total	**44**	**100,00%**

Figura 14

Nivel de ciberataques



Análisis

A inicios del año 2021, la empresa *CheckPoint Research* daba cuenta que, a nivel mundial, el ciberataque contra los sistemas informáticos había incrementado en un 56%, con especial énfasis a las instituciones públicas (Revista Ekos, 2021), esto ocurrió a la empresa CNT en Ecuador, pero esto no quita que este porcentaje también tenga su ocurrencia a las empresas privadas, por lo que se constata que el 4,5% han sido atacadas o se sospecha que implantaron un virus en su sistema, provocando daños que trajeron pérdidas, además el 29,5% podría haber sufrido un ataque. Esto deja una probabilidad de 3 de cada 10 empresas ha sufrido la embestida de la ciberdelincuencia en el Ecuador.

Pregunta 15 ¿Qué problema ha tenido con sus equipos durante el teletrabajo?

Tabla 16

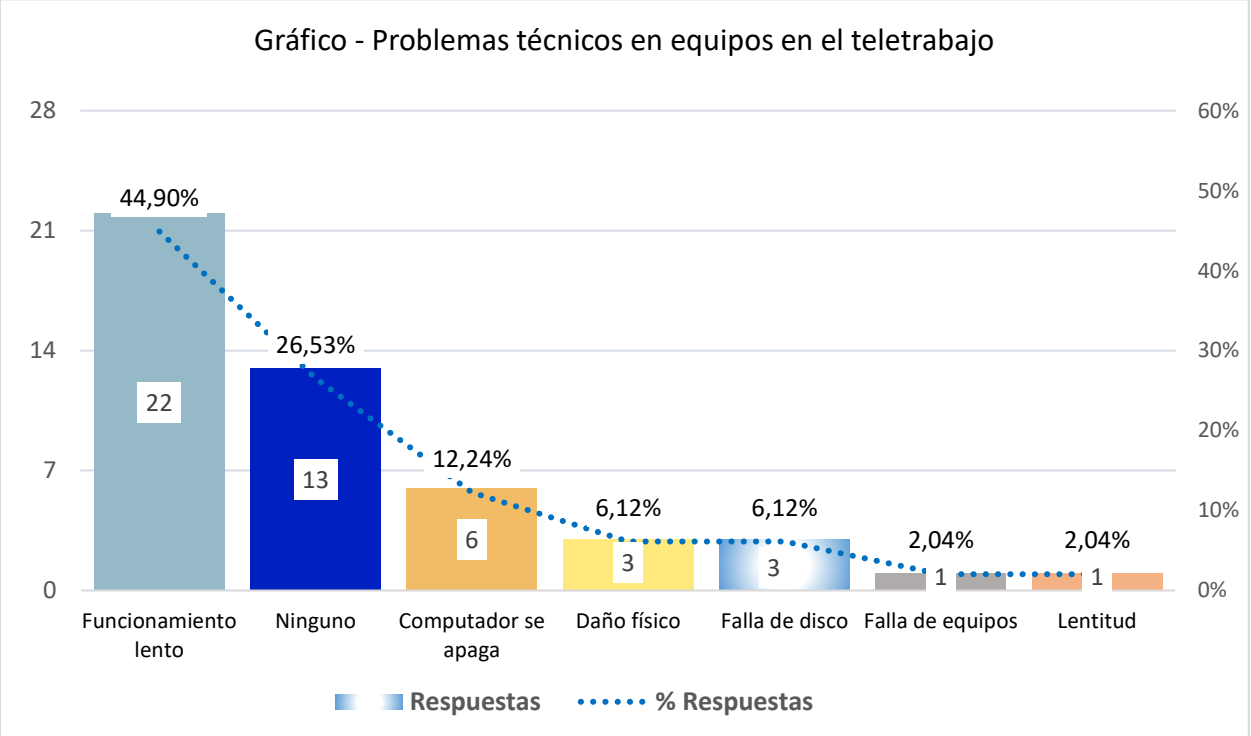
Encuesta - Problemas con equipos en el teletrabajo

Problemas Equipos	Respuestas	%
Funcionamiento Lento	22	44,9%
Ninguno	13	26,5%
Computador se apaga	6	12,2%
Daño físico	3	6,1%

Falla de disco	3	6,1%
Falla de Equipos	1	2,0%
Lentitud	1	2,0%
Total	**49**	**100,0%**

Figura 15

Problemas con equipos en el teletrabajo



Análisis

El advenimiento de la pandemia del Covid 19 fue algo muy inesperado, las personas en sus hogares no disponían de un computador o si lo tenían, era un computador muy modesto que era utilizado para juegos, escribir cartas sencillas o simplemente era un adorno, es por eso que, al iniciar el teletrabajo en uso de estos equipos, era lógico que cause problemas, así se puede justificar las respuestas, donde una gran pare de los encuestados han tenido problemas de lentitud de sus equipos, daños físicos, del sistema operativo y en general, solo el 26,5% parece no tener ningún problema.

Pregunta 16 ¿En qué tipo de dispositivo realiza su copia de seguridad?

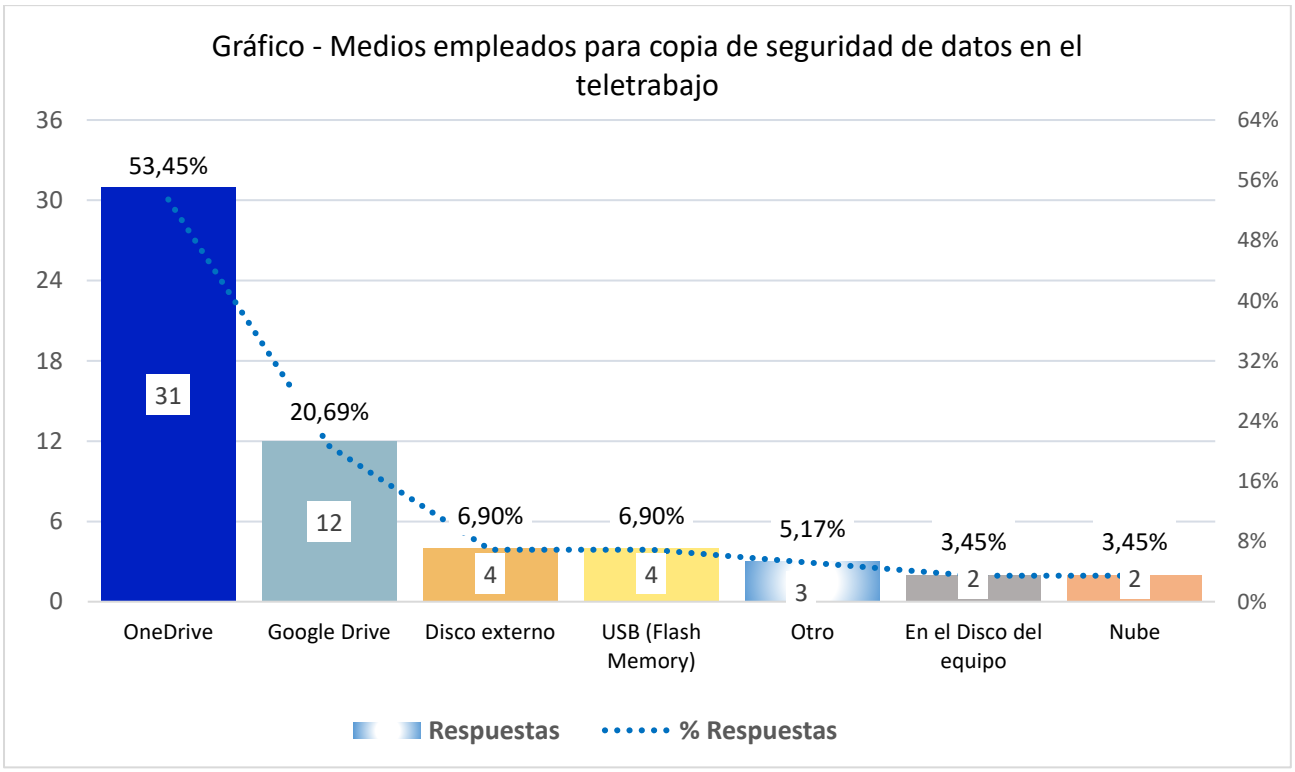
Tabla 17

Encuesta - Copias de seguridad de su información

Copia Seguridad	Respuesta	%
OneDrive	31	53,45%
Google Drive	12	20,69%
Disco Externo	4	6,90%
USB (Flash Memory)	4	6,90%
Otro	3	5,17%
En el disco del equipo	2	3,45%
Nube	2	3,45%
Total	**58**	**100,00%**

Figura 16

Copias de seguridad de su información



Análisis

El paso al teletrabajo impulsado desde inicio de la pandemia en el año 2020 motivó la utilización de periféricos como la memoria USB, los discos externos, las bases de datos internacionales como OneDrive, entre otros, por lo que es importante conocer cuál es el dispositivo de mayor utilización. En base a las respuestas de esta pregunta se analiza que el sitio OnDrive de Microsoft es el que mayor concurrencia tiene, ya que se almacena con mucha facilidad, está protegido bajo la contraseña del usuario y tiene una gratuidad hasta de 5 Gigabytes de almacenamiento por usuario, le sigue Google Drive y los discos duros externos. Es de prever que poco se utilice una memoria USB por su facilidad de pérdida o también la memoria del computador, por la fragilidad de acceso de los ciber piratas.

Pregunta 17 ¿Piensa que el teletrabajo debe continuar?

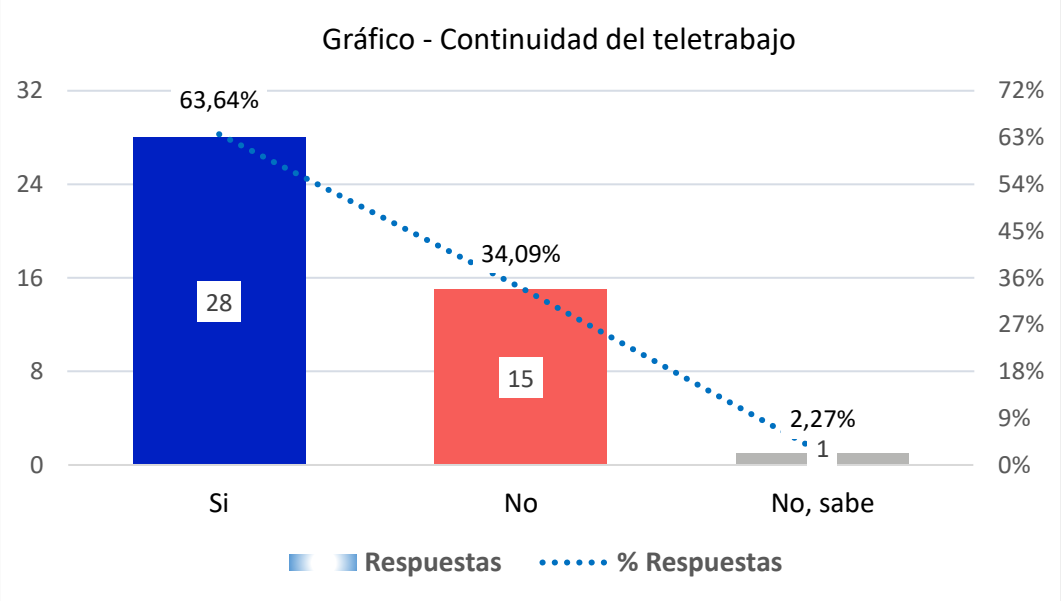
Tabla 18

Encuesta - Continuidad del teletrabajo

Continuar Teletrabajo	Respuestas	%
Si	28	63,64%
No	15	34,09%
No sabe	1	2,27%
Total	**44**	**100,00%**

Figura 17

Continuidad del teletrabajo



Análisis

Una pregunta final y muy clave para medir la satisfacción de los encuestados frente al teletrabajo es esta, donde se requiere saber si el teletrabajo debe o no continuar, así tenemos una respuesta contundente de sí, con el 63,64% de aceptación, lo que sugiere que los encuestados en su mayoría, están satisfechos con el teletrabajo, a pesar de que no todos están cómodos con las adecuaciones o tienen problemas informáticos, lo que ahora viene es la necesidad de protección contra los ciberataques.

CAPÍTULO II: PROPUESTA

2.1 Fundamentos Teóricos Aplicados

2.1.1 El Teletrabajo

Base Conceptual del Teletrabajo

El teletrabajo, de manera general, sería conceptualizado como un trabajar a distancia, de manera virtual, sin la presencia personal en las instalaciones de la empresa o el sitio de trabajo designado por un empleador para el desempeño de las funciones asignadas dentro de un sistema de procesos. El trabajo dentro de esta modalidad puede ser bajo una jornada completa o a media jornada, donde será indispensable la utilización de tecnología de información y comunicación (TIC), acompañada del conocimiento de programas informáticos, de telecomunicación y presentación, así mismo los de navegación. Los trabajadores que se han acogido esta modalidad de trabajo, es porque pueden ajustarse al mismo sin que afecte el desempeño de la organización, tienen espacio efectivo dentro de su domicilio y cuentan con un computador o similares para la transferencia de la información (Selma, 2016).

A nivel mundial, el teletrabajo se ha establecido dentro de las organizaciones por su forma dinámica y flexible para desarrollarse, partiendo desde una primera ventaja que es que el trabajador no tendrá que desplazarse largas distancias hasta llegar a su sitio habitual de trabajo puesto que no es necesaria su presencia en la empresa del empleador. Así, el teletrabajo es un método laboral donde la persona que se acoge a él, recibe una remuneración similar a aquel que se lo realiza presencial siendo su herramienta indispensable para el cumplimiento las TIC (Narváez, 2020).

En definitiva, se utiliza al teletrabajo como una de las modalidades de la relación laboral donde el empleado o trabajador se desempeña desde su hogar o el lugar que así lo ha dispuesto, diferente al de la sede del empleador, pudiendo ser muy lejano o a distancia considerable como de país a país o de ciudad a ciudad, enviando su trabajo a través del internet con la utilización de un medio mecanizado como lo es una computadora de escritorio, laptop, celular o cualquier otro dispositivo tecnológico avanzado. Esta forma de trabajo no le deslinda la responsabilidad del cumplimiento de objetivos, además de mantener un acercamiento y contacto con las autoridades de la organización, así como con sus compañeros de trabajo (OIT, 2020).

Para poder estar claro en el lenguaje que se utilizará en la presente investigación, será necesario exponer algunas definiciones sobre lo que es el teletrabajo, desde varias ópticas y ajustado a la realidad actual. Así se pueden mencionar los siguientes:

La OIT u Organización Internacional del Trabajo conceptualiza al teletrabajo como “una opción que tiene el empleado, para realizar su labor fuera de las dependencias del empleador u oficina central. Bajo esta premisa, las funciones a ejecutar serán en un lugar diferente a las que realiza el grupo organizacional (empleado-empleador) donde será necesario la utilización de aparatos de comunicar y todo el respaldo de las TIC” (OIT, 2020, pág. 14).

Igualmente, la organización internacional reseña que el teletrabajo como modalidad laboral debe cumplir con los requisitos mínimos siguientes: que el cumplimiento o desarrollo de las actividades laborales se deben realizar fuera de la sede laboral que se tenía para la producción y, el empleo de las nuevas tecnologías para poder ejecutar las actividades laborales y de esta forma poder mantener la comunicación con los superiores y/o compañeros de trabajo. En ese marco, a diferencia de los criterios doctrinarios, se establece una definición con elementos sólidos y explícitos de lo que se debe tener en cuenta para comprender lo que se transmite o conceptualiza por teletrabajo, siendo estas de forma resumida: la distancia de la sede laboral y el empleo de las tecnologías de la información (OIT, 2020).

Por su parte, dentro de la legislación ecuatoriana, se incluyó al teletrabajo dentro de la Ley Orgánica de Apoyo Humanitario, entrando en vigor en el año 2020 y formulando un concepto del teletrabajo como:

> Una metodología de organización laboral o prestación de servicios, que se basa en la realización de actividades gratificadas bajo un salario o remuneración, utilizando como soporte las tecnologías de la información y la comunicación para la comunicación entre el empleado y el empleador, sea esta una persona o una organización legalmente constituida, sin necesidad de la presencia física del empleado en un lugar determinado de trabajo. (Asamblea Nacional, 2020, pág. 14)

Es así como al teletrabajo se le ha considerado como un modelo para el desempeño laboral que puede abarcar todas las modalidades del desempeño profesional, con un alto grado de flexibilización en su aplicación, ya que las personas que quieren laborar bajo este formato, pueden hacerlo en jornadas completas mensuales, a medio tiempo e incluso por horas, pero siempre será acompañado de herramientas informáticas y telecomunicaciones.

Considerando todos los conceptos expuestos anteriormente, se puede deducir que, hoy en día, y luego de dos años de pandemia, se puede definir con mayor claridad la metodología del teletrabajo con todos sus elementos o características integrales ya que ahora es mucho más conocido y practicado, transformándose en un término muy utilizado dentro de la sociedad ecuatoriana. Sin embargo, las

palabras más seguras para poder definir al teletrabajo como la forma de realizar un trabajo convencional y pasarlo a un virtual, lejano de la sede central del empleador, bajo la utilización de varios instrumentos de trabajo y el apoyo de la telecomunicación (Narváez, 2020).

En un concepto mejor formulado que reúne todos los elementos antes mencionados, Ripani (2020) puntualiza sobre el teletrabajo, que este constituye una actividad laboral retribuida en donde el trabajador, mediante un acuerdo bilateral con el empleador, conviene la realización de las actividades empresariales fuera de la sede de la compañía, sosteniendo la comunicación apoyada de las tecnologías de la información.

2.1.2 Características del Teletrabajo y sus Modalidades

La OIT como organismo que regula a nivel internacional los derechos y obligaciones de los trabajadores, al igual que los deberes de las personas u organizaciones que fungen como empleadores, ha establecido tres particularidades indispensables del teletrabajo que deben cumplirse de manera obligatoria como requisitos para decir que una persona está bajo la modalidad de teletrabajo. Estas particularidades son las siguientes:

1.- La Locación

El servicio prestado por un empleado o trabajador que se distingue bajo la modalidad de teletrabajo debe realizarse en un lugar distinto del área común de trabajo, es decir, distante al sitio o sede del empleador. Este es un requisito común o característica principal del teletrabajo muy diferente a una relación profesional convencional, descentralizando el sitio o lugar de trabajo donde habitualmente se desarrolla la actividad productiva (Palacios, 2017).

2.- Uso de la Tecnologías de la Información y Comunicación TIC

La utilización de herramientas tecnológicas o de la nueva generación para la comunicación es fundamentalmente esencial para el cumplimiento de la relación laboral bajo el modelo de teletrabajo ya que de ellas va a depender el cumplimiento de las labores, así como el éxito de esta figura. Las TIC, serán la bandera que diferencie dentro de otras modalidades de relación laboral que da la oportunidad al empleado o trabajador de prestar sus servicios legales desde cualquier sitio donde esté ubicado, pero con la condicionante que se encuentre conectado a internet y a su vez, a una red informática empresarial a la cual tenga acceso para el envío y recepción de información, con el uso de las programas o software ofimáticos (Vargas, 2020).

3.- Organización y Forma de Realización del Trabajo

La evolución de las TIC ha dado un vuelco a las oportunidades laborales, prescindiendo de la presencia física del trabajador dentro de una dependencia u oficinas, para desempeñarse de forma exitosa en una actividad propuesta en función a su capacidad profesional. De ahí que la utilización de la tecnología ha permitido a las empresas públicas y privadas aprovechar de esta nueva modalidad de trabajo para insertar nuevos trabajadores sin necesidad de ampliar sus oficinas reduciendo el desempleo y la posibilidad de mejorar la economía de un país (Correa, 2021).

2.1.3 Antecedente Histórico

La palabra teletrabajo proviene de dos vocablos existentes dentro del lenguaje cotidiano, el primero es la voz griega "tele" cuyo significado es "lejos", en conjunto con el vocablo "trabajo" que es un verbo cuyo significado es realizar una actividad o servicio para recibir una remuneración o pago. Juntos crean la nueva y moderna terminología "teletrabajo" como la capacidad de brindar un servicio o actividad laboral a distancia (Rodríguez *et al.*, 2020).

El teletrabajo no es una actividad que nace en la presente década, ya que sus inicios se registran en los Estados Unidos de Norteamérica a inicios de la década de los 70, como resultado del aumento de la explotación petrolera y por ser dicho país un fuerte consumidor del hidrocarburo, las empresas acostumbraban a movilizar sus trabajadores bajo su propio costo, desde sus domicilios hasta los lugares de trabajo. En un momento en donde el precio de la gasolina incrementó, el traslado de trabajadores resultaba altamente costoso e incluía en los precios, las organizaciones se vieron obligadas a tomar otras alternativas para reducir este costo, abordando por primera vez la idea del teletrabajo (Joric, 2020).

Por otro lado, el físico Jack Nilles durante su tiempo de investigación en los Estados Unidos al ver las multitudes de trabajadores movilizándose bajo dificultosas condiciones a sus lugares de trabajo, emprendió nuevas alternativas que permitan optimizar el consumo de gasolina y bajar el costo hacia el trabajador para su movilización, tuvo la brillante idea de llevar el trabajo al trabajador naciendo así el término *telecommuting*, que en español significa tele desplazamiento, reemplazando de esta manera el uso del transporte público o privado que generaba el consumo de gasolina y contaminaba el ambiente, además del fuerte y estrés que provocaba transportarse o movilizarse en las grandes ciudades de este país (Ripani, 2020).

En aquella época, el desarrollo tecnológico no estaba lo suficientemente avanzado como para que el trabajo llegara a ser una realidad masiva, sin embargo, las décadas venideras hasta la actualidad han sido observadoras cercanas del avance tecnológico y la bajada de los costos informáticos, la

velocidad de las redes de comunicación y la difusión comercial de Internet, mismas que pusieron a disposición de millones de personas los recursos necesarios para emprender el teletrabajo hoy en día (Rugel & Romero, 2020).

Tipos de Teletrabajo

Se han abordado ya los antecedentes, expuesto definiciones, así como las principales características del teletrabajo, ahora se propone conocer cuáles son las variedades en la modalidad de esta forma laboral para comprender de mejor manera una de las variables de estudio.

Las principales formas de teletrabajo son las siguientes:

Tabla 19

Categorías del teletrabajo

Categoría de teletrabajo	Descripción
Escritorio multiusuario	Esta modalidad de trabajo se da cuando una persona trabaja la mayor parte del tiempo fuera de la sede del empleador, por lo que no existe la necesidad de proveerle de una oficina o lugar específico de trabajo dentro de sus instalaciones
Escritorio multiusuario con reserva	Este es semejante que el antes descrito, con la diferencia en que el trabajador, realiza una reserva previa para ocupar un sitio de trabajo dentro de las instalaciones de la empresa o empleador
Telecentros	Son centros especializados que alquilan sus instalaciones a quienes necesitan realizar teletrabajo, tienen las herramientas necesarias para el envío y recepción de datos, así también impresoras, escáner y demás tecnología, con la desventaja de la inseguridad de los datos, que son públicos dentro de esa red.
Oficinas colaborativas	Son pequeños lugares que comparten empleados de otras empresas con otros trabajadores, de manera temporal y sin fines de lucro, más se lo hace para colaborar con sus pares.

Fuente: Ortiz (2020).

Contrato de Teletrabajo

El teletrabajo como figura contractual remunerada está totalmente legalizada en el Ecuador y ajustada a los mismos parámetros lícitos de un contrato de trabajo convencional, donde se establecen todos los requisitos necesarios en relación a su dependencia frente al empleador y la remuneración que se dará por su ejecución, con ello, el teletrabajador se encontrará con las mismas ventajas y obligaciones que tiene un trabajador presencial, por tanto con todos sus derechos laborales invulnerables conforme a lo establecido en la ley competente (Vallejo, 2020).

En ese sentido, una de las características del teletrabajo es que es una modalidad lícita y remunerada, que se da de manera personal bajo una dependencia laboral, y regulada por el Código del Trabajo para trabajadores privados o la Ley Orgánica de Servicio Público para trabajadores del Estado. Es necesario aclarar que para que un trabajador que trabaja bajo esta modalidad debe cumplir con las características de legalidad, de forma sana y sin mala fe, con la que se basará la relación laboral (Palacios, 2017).

2.2 Uso de la Tecnologías de la Información y Comunicación TIC

El uso y empleo de las nuevas tecnologías de la información son un pilar esencial en la modalidad de teletrabajo pues de ellas depende la efectividad de esta figura. Las TIC, dentro del teletrabajo lo distingue de las otras modalidades laborales permitiendo este último, prestar los servicios pertinentes desde cualquier lugar siempre y cuando exista la conectividad y la afluencia de redes informáticas empresarial o al internet mediante el uso de las herramientas ofimáticas (Vargas, 2020).

En palabras de Sanguineti (2021) las TIC son la unión de varias tecnologías que facilitan la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones, a través de la utilidad de la voz, imágenes y datos comprendido en marcas de naturaleza acústica, óptica o electromagnética.

En resumen, este cúmulo de tecnología y comunicación representan las herramientas necesarias que darán lugar a la creación, transformación, recuperación, transmisión y almacenamiento de la información. De esta manera, se emplea esta figura como instrumento de trabajo que permite navegar en la web, consultar en bases de datos para obtener información, relacionarse con otros individuos de un mismo grupo de trabajo, entre otros (Parra, 2020).

2.2.1 Desafíos de las Telecomunicaciones en la Pandemia

En la actualidad y cuando la pandemia del Covid – 19 ha mermado su impacto en la salud de los habitantes, tanto el sector público como el privado, ponen todos sus esfuerzos por reducir los

obstáculos que significa el teletrabajo. En este aspecto, las empresas de telecomunicaciones han mantenido un rol fundamental en el reto de la conectividad.

Algunas empresas han mantenido iniciativas favorables hacia la tele educación proporcionando el servicio sin costo en los sectores rurales, también fomentando la alianza público – privada con el Ministerio de Educación con conexiones estables de internet, por otro lado, han creado planes para los hogares en mejora del teletrabajo, donde no solo se conectan los estudiantes, sino también uno o dos de los padres de familia (Sunkel & Trucco, 2020), todo esto considerando que solo el 45,5% de la población del Ecuador tenía internet en sus hogares (PRIMICIAS, 2020).

En general, en América Latina, tanto reguladores como operadores tomaron medidas frente a un posible colapso de las redes de telecomunicaciones ya que, gracias al teletrabajo, se incrementó el tráfico. Un caso probado es el de España donde se afirmaba que se había incrementado un 40% en la demanda (Pautasio, 2020) en estas economías maduras, tomando decisiones para contener posibles daños. Así el Covid – 19 puso a las telecomunicaciones en el lugar más protagónico de una película calificada como distópica, con un nivel muy parecido a lo que es la electricidad, el agua potable o el gas de uso doméstico.

Así es como se establece que la telecomunicación debe procurar el acceso a la banda ancha en todo el país, con miras a una reducción de la brecha digital que garantice la conexión de un mayor número de personas, pero también con un precio accesible, para que todos puedan tener este servicio en sus hogares, en escuelas, colegios, con el afán educativo, social y no solamente comercial.

En Ecuador, el confinamiento obligatorio obligó a las redes de interconexión a incrementar su capacidad, pasando esta prueba de resistencia con muy buena calificación, debido a que los proveedores tuvieron la cabida para abarcar este nuevo contexto de mercado, pero la tarea de la telecomunicación no queda ahí, las personas que están en teletrabajo o utilizan las redes para acceder a las ventas, deben evolucionar digitalmente para ser más rápidos y flexibles, considerando que están en un terreno totalmente diferente a su anterior modo de trabajo y que tendrán un alto nivel de competitividad. Por ello, es necesario que se simplifiquen, tanto en su estructura como en sus procesos y sistemas, en otras palabras, debe existir una modificación cultural frente a este nuevo reto, ofreciendo su experiencia transmitida en la red y cuidándose de no caer en los ciberataques (Vargas Borbúa *et al.,* 2017).

2.2.2 Amenazas a la Ciberseguridad en Teletrabajo

En el transcurso de la pandemia del Covid - 19 todas las personas que están a modo de teletrabajo reciben y envían información de manera constante de diversos tipos de fuentes, sean estas internas o externas, en su mayoría, mantienen un estado de alerta bajo, puesto que no manejan información confidencial o que podría afectar significativamente a su empleador, considerando a los ciberataques muy improbables (OIT, 2020).

Se estima que una gran mayoría de los ciber trabajadores desconocen como los cibercriminales trabajan, no están enterados de que a través de las campañas de phishing relacionadas con temas importantes del momento como pueden ser el COVID-19, el mundial de futbol, se agregan archivos o enlaces fraudulentos, que buscan el engaño o la apropiación de información que se podría catalogar como confidencial. Este tipo de invasiones pueden propagarse con mucha velocidad en el internet y, por tanto, en las redes empresariales, con la apropiación indebida de la identidad. Por esta razón, es importante que las organizaciones permanezcan atentas a mensajes fraudulentos relacionados con esta pandemia (Corrado *et al.,* 2020).

Ante esta problemática, autores como Corrado *et al.,* (2020) hacen recomendaciones para evitar el ataque de la ciber delincuencia como:

- **a)** Mantenerse atento ante la entrada a la bandeja de correo principal de email provenientes de personas o empresas desconocidas con archivos adjuntos o hipervínculo que tengan temas de su interés e incluso que digan ser fuente de información primaria sobre la pandemia, también de personas que piden ayuda, enlaces a otros sitios web, inversiones, préstamos a bajos intereses y montos altos, loterías, herencias o pornografía.
- **b)** Siempre buscar utilizar e ingresar a sitios confiables y legítimos, sean públicos o privados, recibir información sobre la pandemia de sitios autorizados o que provengan del Ministerio de Salud Pública, en su página original.
- **c)** Nunca revelar datos personales o claves de acceso al banco, no ingresar desde otros lugares a la página web del banco, tampoco exponer información estrictamente personal en Facebook, Twitter, Instagram u otro medio clasificado como redes sociales.

En la actualidad, los accesos remotos son ilimitados, tanto las redes sociales como los juegos u aplicaciones de diversión ajenos a los que se consideran como seguros, generan una alta tentación de ingreso y utilización, exponiendo la información personal ante cualquier ataque de la ciberdelincuencia. Esta situación, en el caso del teletrabajo, pone en riesgo las plataformas empresariales, especialmente

de las pequeñas y medianas empresas que no tienen altos presupuestos para una protección apropiada y que pueden ser víctimas, sin si quiera darse cuenta de dónde vino el ataque (Ventanales, 2021).

Por su lado, los nuevos dispositivos móviles y las aplicaciones (App) también corren con responsabilidad el no mantener funciones de seguridad fuertes, ya que es más fácil encontrar su debilidad que su resistencia ante ataques externos, sumando así los riesgos que han sido advertidos por las propias empresas de seguridad, por el Estado e incluso por las propias aplicaciones que inducen a utilizar programas especiales llamados "antivirus" que neutralicen ataques o intenten un acceso remoto a los dispositivos, buscando hacer daño incluso desinteresado plantando un virus o dañando la configuración de los sistemas operativos. Es de considerar que la ausencia de mantenimiento o el escaso soporte técnico de ciberseguridad por parte del proveedor, también suma a la debilidad de los sistemas, posibilitando el acceso a desconocidos con malos propósitos (Arias Buenaño *et al.*, 2016).

Por lo antes dicho, es una necesidad evidente que las organizaciones empresariales logren identificar y establecer los requerimientos básicos y complementarios de una conexión remota, capacitando a todos los usuarios sobre el riesgo de ciberataques y virus, así como la apropiación de información personal y confidencial, evitando que se cruce el umbral de seguridad que afecta a la economía o finanzas de una Empresa. De igual manera, es importante establecer los sitios restringidos a la par de evitar aceptar información de fuentes no seguras, generando excepciones desde los mismos ordenadores que suban el nivel de seguridad y control de la seguridad de la información (Amutio Gómez *et al.*, 2012).

2.2.3 Principales Retos

La presencia de la pandemia ha obligado a muchas empresas, sean públicas como privadas, a rediseñar sus sistemas de trabajo, dentro de ellas, la implementación del teletrabajo que ha puesto en duda el trabajo presencial ya que, de una manera óptima o básica, las organizaciones se han adaptado y miran con buenos ojos este tipo de relación laboral, incluso empresas como FUJITSU han anunciado que disminuirán su espacio de oficinas y apoyando a sus trabajadores en la implementación de sus oficinas desde casa.

Con una quinta parte de los empleados teletrabajando en estos momentos, la crisis del coronavirus nos ha enseñado una lección en lo que al trabajo remoto se refiere, y muchos expertos creen que nuestra forma de trabajar podrá cambiar para siempre. Empresas como la FUJITSU, ha anunciado que reducirá el espacio de sus instalaciones administrativas en un 50% y ofrecerá a sus empleados condiciones de trabajo flexibles de forma indefinida (Ibarra Cisneros *et al.,* 2019).

2.3 Descripción de la propuesta

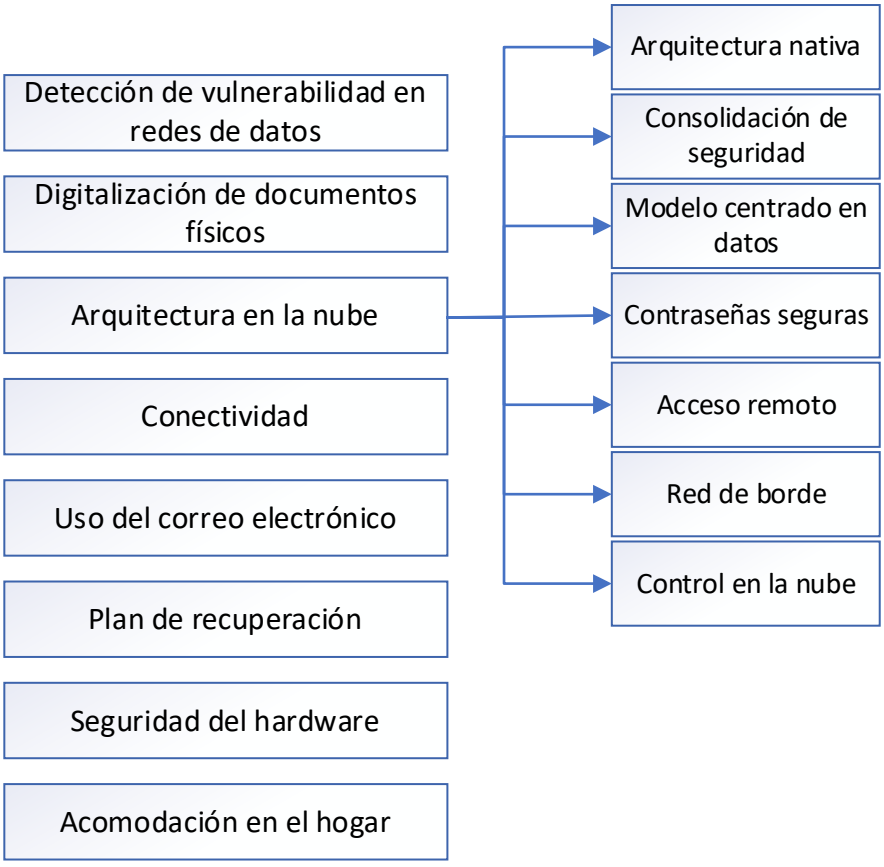
A continuación, se expone la propuesta de investigación, considerando la percepción que tienen los teletrabajadores extraída de la encuesta, así como la necesidad de salvaguardar los datos que se encuentran en los computadores o lugares de almacenamiento, del ataque de la ciberdelincuencia.

2.3.1 Estructura general

De manera general, la estructura del proyecto se centrará en la protección de datos frente a los ciberataques y el phishing al que están expuestas las personas que trabajan con la modalidad de teletrabajo, considerando, de acuerdo con las encuestas, que son personas que han sido capacitadas para evitar poner en riesgo la información delicada de las empresas donde laboran, es así que a continuación se presenta un esquema de la propuesta:

Figura 18

Esquema de la propuesta



2.4 Explicación del aporte

Los ciberataques y los virus que se camuflan en la publicidad no deseada, son los problemas más recurrentes en el teletrabajo, por lo que se presenta la necesidad de proponer alternativas básicas para

los ejecutivos y trabajadores que realizan este tipo de actividad, a fin de salvaguardar la información de sus empleadores, así como evitar tener un conflicto legal por la pérdida de información confidencial, es por eso que se presentan estrategias de telecomunicación que permitan enfrentar ataques a los sistemas y usurpación de información.

Para una mejor implementación de la propuesta, será necesaria la asesoría de expertos informáticos para llegar a los pormenores informáticos, instalaciones de redes, medición de velocidad de transmisión de datos y demás actividades que el ingeniero de informática puede mejorar o proteger.

Detección de Vulnerabilidad en Redes de Datos

La detección de vulnerabilidades será aquella etapa inicial donde se podrá reconocer, clasificar y caracterizar los lugares más vulnerables o inseguros, no solamente en los computadores, laptops, teléfonos y Tablet sino en la infraestructura de red cableada e inalámbrica, enrutadores, los paquetes informáticos instalados y el sistema operativo.

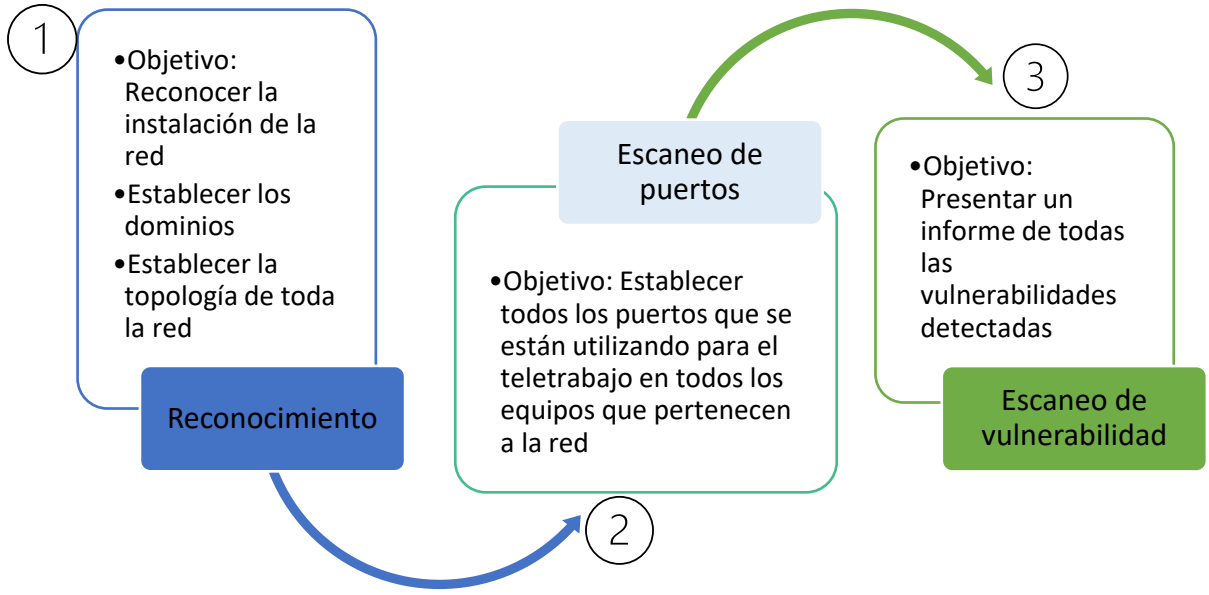
Con la ayuda de un experto informático, la detección inicia bajo tres premisas:

a) Evaluación interna de los programas informáticos instalados en los aparatos con los que se teletrabaja, sean estos: computadores, tablets, laptops o celulares inteligentes, verificando la vulnerabilidad de cada uno.
b) Evaluación externa para establecer la vulnerabilidad a la exposición pública de la infraestructura tecnológica (IT) que tiene la empresa
c) Evaluación de la vulnerabilidad de la red.

Con el apoyo informático, la detección tendrá tres objetivos:

Figura 19

Detección de vulnerabilidades



Digitalización de documentos

La práctica diaria en oficinas administrativas, de marketing y publicidad, de talento humano, informática, entre otras, se hacía con la utilización de papelería, sean estas facturas, reportes, informes, memos, solicitudes, órdenes y demás, pero hoy en día, las personas que laboran en teletrabajo, deben hacerlo desde sus domicilios o cualquier otro sitio que no es su oficina habitual dentro de la empresa, por lo que los documentos recibidos o generados, se almacenan en el lugar del teletrabajo, no pudiendo llegar a todas las personas del equipo o quedando fuera del alcance de quienes también lo requieren en algún momento determinado.

Es por ello la necesidad de digitalizar todos los documentos que pasan por manos del teletrabajador, para que puedan estar al alcance de todo el equipo que compete dentro de la empresa. Esta digitalización deberá venir acompañada del escaneo de todos los documentos históricos dentro de un ciclo de tiempo, así podrán estar al servicio en el momento que se quiera, desde cualquier parte del país o del mundo por medio del internet.

La única desventaja de la digitalización podría ser que requiere mucho espacio de almacenamiento, puede ser pesada y estar expuesta al ataque de la ciber delincuencia. Por el lado de sus ventajas, tiene la gran propiedad de mantener toda la información de muchos años en un solo lugar,

sin ocupar espacio físico ni estar expuesto a las inclemencias del clima, además de evitar el deteriorar el original y sus características visuales de alta calidad.

Un método efectivo para digitalizar documentos físicos es con la utilización del Google Drive, que es una aplicación (App) que se encuentra en los teléfonos inteligentes, muy sencilla y rápida de utilizar y para su utilización se deben seguir los siguientes pasos:

1. Localizar y abrir la aplicación Google Drive

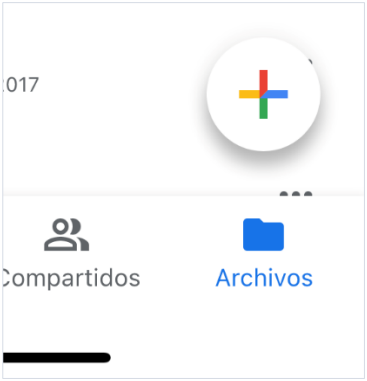
Figura 20

Abrir Google Drive

2. Abierta la aplicación, en la esquina inferior derecha se encuentra el ícono con el signo + como se mira a continuación

Figura 21

Opción botón más "+"



3. A continuación, escoger la opción "escanear" en dispositivos Android y foto en IOS que se encuentra dentro del Menú "crear nuevo".

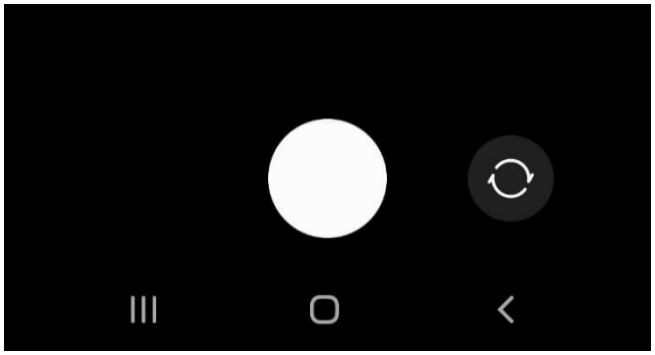
Figura 22

Seleccionar opción Escanear / Foto

4. A continuación, tomar una foto del del documento que requiere escanear

Figura 23

captura del documento



5. Para mejorar el área de escaneado, se puede utilizar la herramienta recortar con la que se comprimirá al sitio específico de guardado
6. Presione “guardar” con el nombre que se dará al archivo, así como el lugar donde se almacenará
7. Si existe la necesidad de escanear una y otra vez, se deberá presionar en la opción del ícono + como se estableció de inicio
8. Todos los archivos estarán dentro del Google Drive que cuenta con almacenamiento gratuito hasta de 15 Gigabytes compartidos con correo y fotos de la cuenta Google o se puede contratar todo el espacio que se necesite

Arquitectura en la nube

Lo que se almacena desde un dispositivo electrónico informático puede estar de manera local o en la nube, es decir, en el ciberespacio al cual se accede solamente con la utilización del internet. Frente a este almacenamiento existe el peligro de ataque por parte de la ciberdelincuencia organizada, considerando que solo las grandes empresas tienen sus propios centros de datos, así como un personal que sabe cómo defender su información de la acometida delincuencial con altos niveles de seguridad, dejando como reto a las pequeñas y medianas empresas el afrontar el problema, pese al alto costo que esto puede significar.

El migrar la información a la nube, ya no es novedad, se lo ha venido haciendo años atrás, con un incremento del 2018 al 2022 del 81% como así lo informa Gartner (Rodríguez M. , 2021) gracias a los servicios disponibles inmediatos, bajos precios y rápida transmisión de datos. Esto está obligando a generar un sistema de buenas prácticas como el propuesto por Cloud Security Alliance (CSA) que están proponiendo los principales aspectos para la seguridad en la nube.

Una de las principales ventajas que ha traído el almacenamiento en la nube a raíz de la pandemia del Covid - 19 es que las empresas mantienen centralizada la información en un solo sitio, donde el proveedor asegurará la integridad, conectividad, privacidad, confidencialidad y disponibilidad de los datos durante las 24 horas del día, los 365 días al año. En ocasiones, algunas organizaciones pueden dudar de esta forma de almacenamiento porque sus servidores no se encuentran en el país donde se solicita sus servicios, por lo que las leyes y jurisdicciones podrían ser diferentes en donde se hallan físicamente, en lo que se refiere a la privacidad y protección de datos.

Pero el crecimiento de esta tecnología, el almacenamiento de información y el auge de la ciberdelincuencia, fuerza a tomar medidas ante los ciberataques y por ente, alternativas sobre el uso de redes físicas y móviles con nuevos modelos de seguridad que se basa en la consolidación de múltiples tecnologías de seguridad, enfocados en el *User Experience* (Ex) o experiencia del usuario con tendencia hacia la reducción de precios.

Para establecer una arquitectura coherente y segura, las empresas en conjunto con sus teletrabajadores y la asesoría del personal encargado de los sistemas informáticos, deberá converger toda su tecnología de seguridad y de conectividad de red en una única plataforma proporcionada a través de la nube, para ello será necesario considerar lo siguiente:

Arquitectura Nativa

Escoger una plataforma de arquitectura como la de *Secure Access Service Edge* (SASE) misma que permite una convergencia de todas las redes y su seguridad hacia un servicio de nube que facilitará el trabajo con una alta velocidad, sistema amigable y disponible los 365 días del año. Esta opción permite cambiar todas las operaciones de servicios hacia un administrador de servicios de seguridad que utiliza un entorno apoyado en microservicios nativos de la nube

Consolidación de la Seguridad

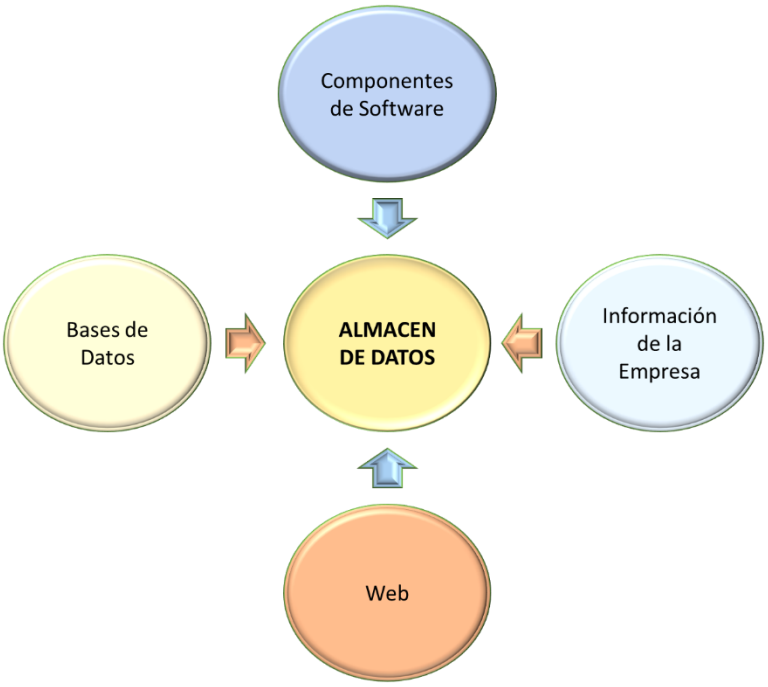
Los empresarios y sus teletrabajadores deben considerar la posibilidad de combinar, tanto la tecnología que se utiliza en la seguridad de la web y la que se usa en la nube, de esta manera se simplificaría la configuración, así como las operaciones, con resultados en la reducción de los costos. Y no solo eso, será posible incluso aumentar la productividad, garantizar una seguridad integral de los datos y mejorar la eficiencia.

Modelo Centrado en Datos

Si los datos están centralizados, será posible la implementación de controles aún más sensibles que detecten y puedan prevenir con mayor facilidad el ciberataque delincuencial, así también establecer los movimientos desde y hacia la web y la nube, incluso entre empresas asociadas y el talento humano que trabaja de asesor externo o consultores.

Figura 24

Modelo Centrado de datos



Para una arquitectura centrada en datos está desarrollada bajo dos componentes:

1. Un repositorio de datos que sirve de almacén permanente de toda la información de la empresa.
2. Una colección de componentes que se manejan de manera independientes operando desde un almacén de datos centralizado donde se realizan varias funciones operativas como el cálculo y envío sin ningún tipo de retraso de los resultados (DhTrust, 2021).

La comunicación para todos los usuarios de los datos se la realiza únicamente por intermedio del almacén de datos y serán estos datos la única manera que tienen para comunicarse entre clientes internos.

Contraseñas seguras

Los ciberataques se han consolidado como las mayores amenazas en la web con un panorama poco alentador. El establecimiento del phishing es frecuente por lo que es necesario establecer una alta barrera de seguridad en las contraseñas que evite el acceso a la inspección de los datos de las empresas.

Previamente es importante recomendar que siempre se utilice conexiones VPN (Red Privada Virtual) que genera accesos seguros a la red interna del teletrabajo con la oficina central y los demás clientes internos, recordando que se debe utilizar el internet contratado por el teletrabajador. Además, evitar las conexiones en redes Wi-Fi desconocidas, públicas o externas como las que provee un restaurante, cafetería o lugares de acceso colectivo, incluso de aquellos de trabajo colaborativo (coworking). Finalmente, asegurarse que el router del lugar del teletrabajo, esté configurado bajo el estándar WPA2, que es el que protege de los accesos y requiere de contraseña.

De ahí que toda contraseña tiene que ser robusta y para ello se presentan las siguientes recomendaciones:

Figura 25

Recomendaciones para contraseñas robustas y seguras

Es de recomendar que se utilicen portales seguros para crear contraseñas como:

- https://www.lastpass.com/es/password-generator
- https://www.dashlane.com/es/features/password-generator
- https://www.roboform.com/es/password-generator
- https://www.avast.com/es-ww/random-password-generator
- https://www.pandasecurity.com/es/homeusers/passwords-generator/

Acceso remoto

Si la conexión VPN es heredada, es decir se la realiza a través de una central principal, suelen ser muy ineficientes, además que cuestan mucho más y con alta dificultad de mantenimiento por lo que será necesario adoptar un enfoque de confianza cero para una conexión segura de todos los usuarios y el arranque de los programas utilizados sin distinción del lugar en donde se encuentren los clientes internos.

Configuración de VPN CheckPoint en un Equipo Cliente

La Instalación y configuración del Software EndPoint Security VPN, checkpoint, nos permitirá crear un túnel virtual de acceso seguro desde el equipo del usuario final a un servidor o servidores de la empresa, y podremos acceder a programas e información sensible de manera segura, con autenticación de doble factor y encriptación de información, cabe indicar que es un software con licencia y que

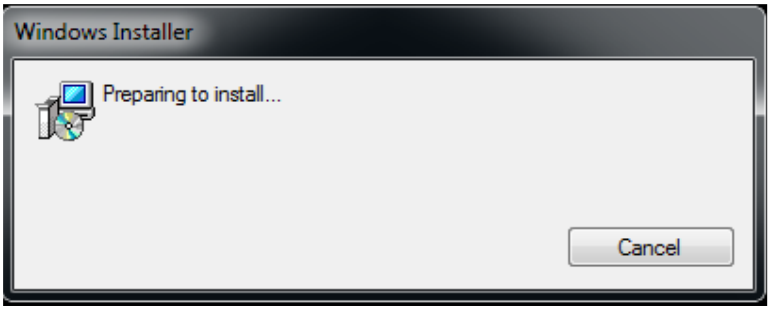
necesita la intervención de áreas IT, sin embargo para efectos prácticos y de información se adjunta el proceso de instalación del aplicativo.

Proceso de instalación de VPN

1. Ejecutar el archivo *CheckPoint VPN* e80.62, clic Run. Aparecerá una ventana que indicará que estará preparando la instalación.

Figura 26

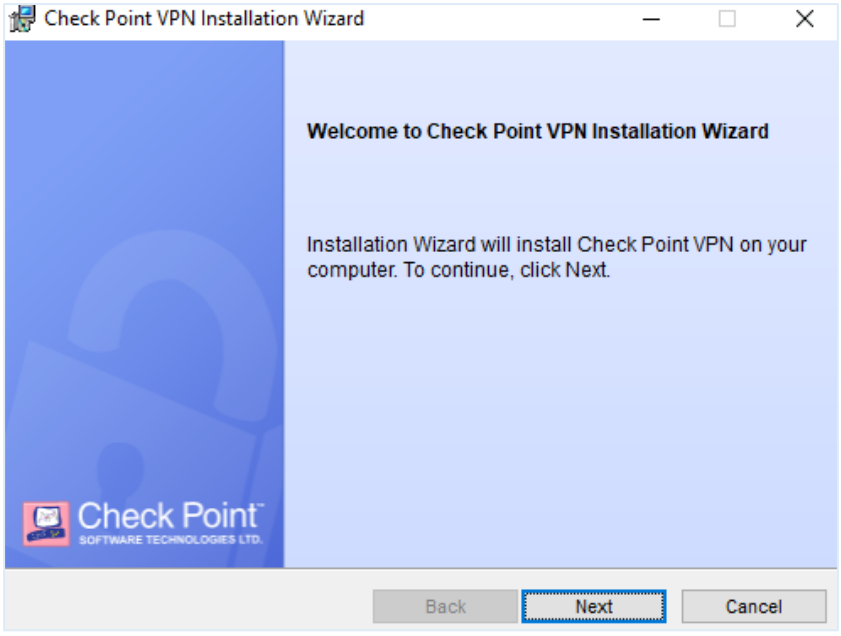
Instalador de CheckPoint (VPN)



2. Desplegara la siguiente ventana de inicio de la instalación, dar clic en Next.

Figura 27

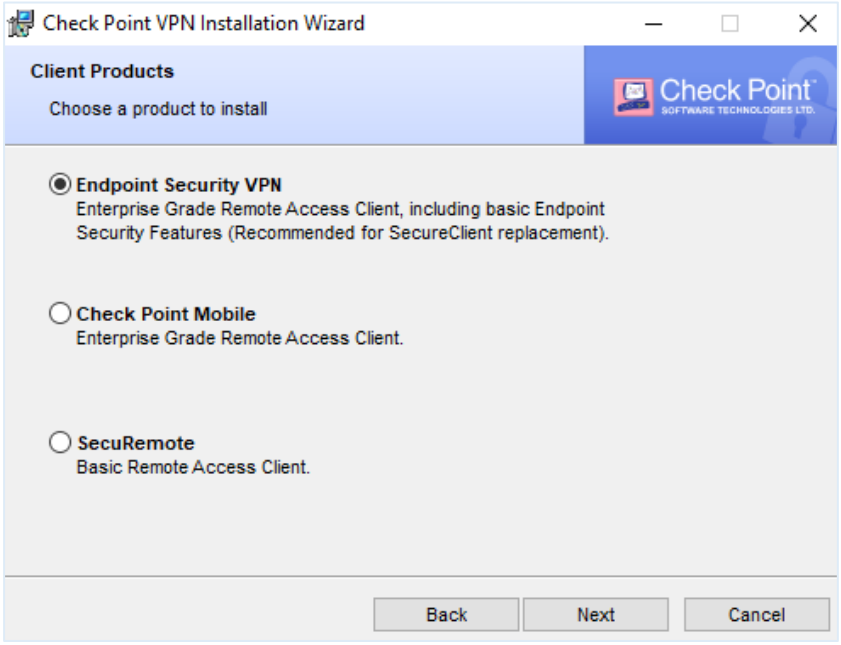
Ventana Inicio de instalación CheckPoint



3. Se debe seleccionar el modo *Endpoint Security VPN*, y dar clic en *Next.*

Figura 28

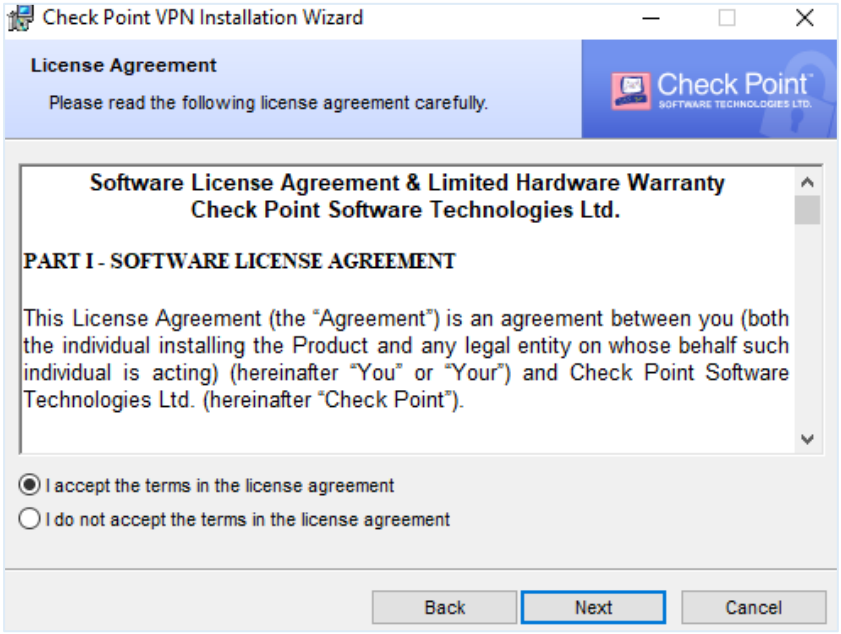
Seleccionar el producto a Instalar



4. Aceptar los acuerdos de la licencia, clic en Next.

Figura 29

Aceptar lo términos de la licencia

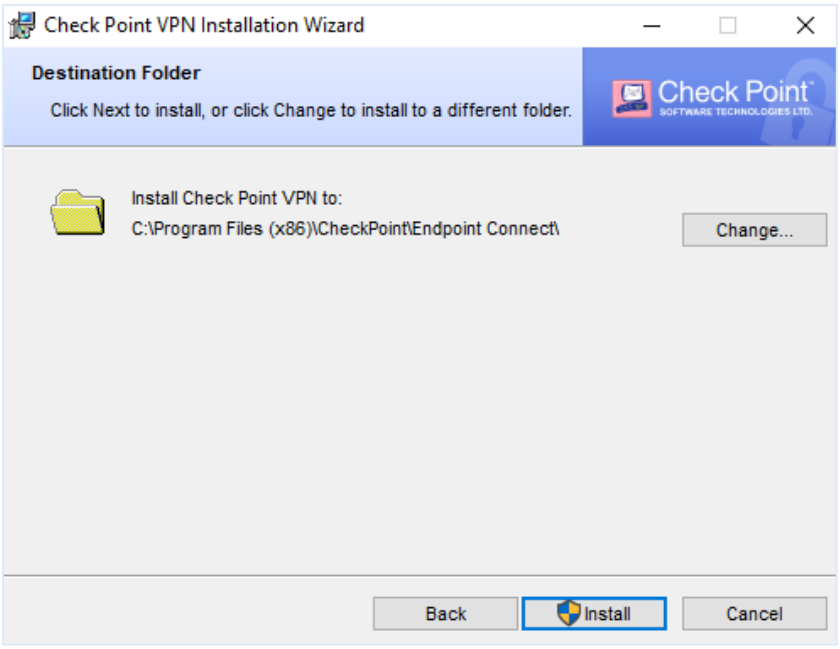


5. Para mayor seguridad en el acceso remoto se recomienda lo siguiente: Aceptar el directorio por default para la instalación del software. *Clic en Install*. En caso de querer

instalar en otra carpeta el software, dar clic en *change* para buscar el destino, posteriormente Clic en *Install.*

Figura 30

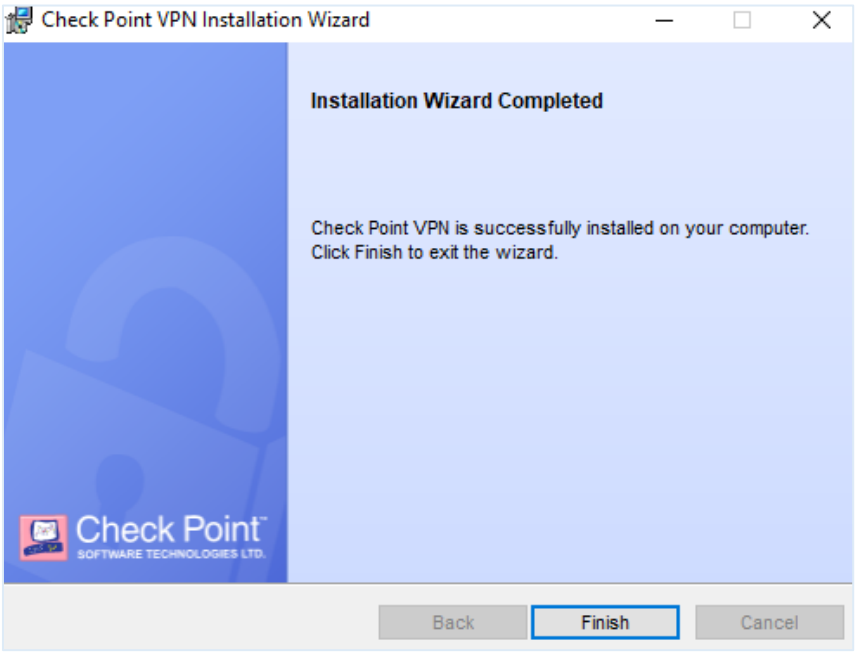
Destino de carpeta de instalación



6. Esperar a que acabe el proceso de instalación, Cuando indique que la instalación fue completada exitosamente, dar clic en *Finish*.

Figura 31

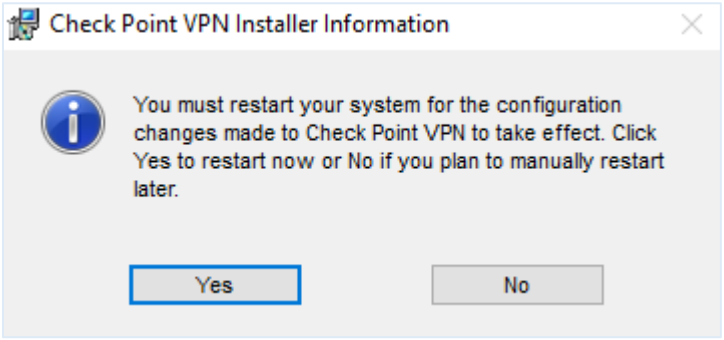
Mensaje de instalación completada



7. Mostrará una ventana que indica que deben reiniciar su máquina, por lo cual procedemos a dar clic en Yes. Al reiniciarse terminará de configurar y nos permitirá acceder a las configuraciones de accesos.

Figura 32

Reiniciar equipo para cambios



Esta herramienta de acceso remoto nos permite desde el teletrabajo, acceder a los programas sensibles de la empresa, con las siguientes ventajas:

1. Seguridad de punto final: Mantiene el antivirus actualizado, así como una correcta configuración del firewall. No se debe descuidar la actualización de todo el software y que los datos enviados y recibidos no se queden guardados en el caché.
2. Red privada virtual (VPN): red segura con autentificación de doble factor y encriptada.
3. IPsec VPN: Este punto debe ser controlado por el experto informático y consiste en establecer una VPN a través de Internet pública con la utilización de un modelo estándar e Ipsec.
4. VPN SSL: De igual manera, con apoyo del personal informático, se debe usar protocolo *Secure Sockets Layer*, que es un modelo tecnológico que permite la autenticación y encriptación total de cada navegador web, considerando que se está navegando en un sistema muy inseguro como lo es el Internet.
5. Administración de acceso privilegiado: Estas herramientas serán seleccionadas por el personal informático y serán las que aseguren, supervisen y administren el acceso a los datos empresariales desde cuentas seleccionadas.
6. Uso compartido de escritorio: Permite que otros usuarios dispongas de datos específicos y seleccionados de un computador que no es propio y que está en otra ubicación diferente a la propia (Ciberseguridad, 2022).

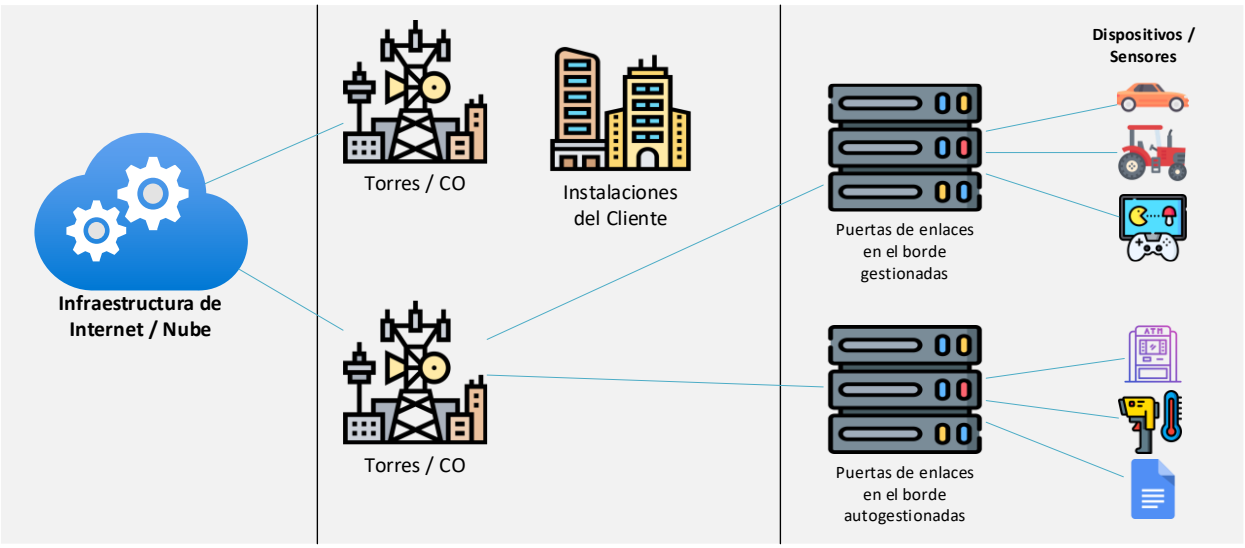
Red de Borde

En la actualidad, el auge de las telecomunicaciones ha permitido tener varios proveedores de internet y el almacenamiento en la nube tiene costos muy económicos, por lo que la recomendación en este tema, es mantener una arquitectura SASE (*Secure Access Service Edge)* con la asesoría de su profesional informático, para lograr un alto rendimiento y capacidad en el servicio de la red, sin dejar de lado la seguridad.

Será necesario tener una auditoría de la red existente que dé cuenta de la infraestructura que ofrece el actual proveedor y comprobar que está preparado para enfrentar ciber ataques o intentos de violar la seguridad de la red, con la propiedad de soportar un tráfico pesado en la nube o "*cloud heavy*". Si la auditoría detecta que se está utilizando soluciones de red de área amplia, será necesario conectarse con un software especializado de borde de red (*ver figura siguiente*) para tener un mejor rendimiento y eficacia.

Figura 33

Modelo de Arquitectura Red de borde



Nota: *Los operadores de red serán los protagonistas en la creación de nuevos ingresos por servicios a partir del borde de la red*

Con el modelo de borde de red se realiza el procesamiento de datos de dispositivos en tiempo real, ejemplo con el internet de las cosas, para que el usuario puede disponer de ellos con mayor rapidez usando el internet. Esto también permite reducir la latencia general de la red y de internet, permitiendo mejorar el tiempo de respuestas en el teletrabajo, las aplicaciones de acceso remoto y de misión crítica.

Control en la Nube

Mientras el asesor informático o el departamento de informática de la empresa consolida el sistema de seguridad de conformidad con la arquitectura SASE, será también muy importante alinear las herramientas administrativas y de gestión que reduzcan la complejidad e incrementen la eficiencia, implementando consolas e interfases de uso para las diferentes personas que entran en la red, que estén de verdad integradas, al igual que los clientes de punto final, simplificando todo, eliminando el caos interno.

Figura 34

Control en la Nube

La Seguridad y el control en la nube presenta varios desafíos importantes como son; las políticas y las tecnologías que existen y se van a usar, requiriendo el apoyo de personal especializado en este tema considerando el uso de controles, y las metodologías para proteger los datos, los accesos y la infraestructura de una empresa.

Conectividad y Acceso a la Red

Para la conectividad se debe iniciar con requisitos básicos como son:

1. Seguir los protocoles de seguridad de la información, es decir contraseñas robustas, equipos en buen estado, de preferencia una red privada, programas con licencias.
2. Disciplina para ser constante en la conectividad con todos los clientes internos y externos, sin dedicarse a otras labores.
3. Establecer horarios bien definidos de trabajo y transformarlos en rutina formal.
4. Una buena conectividad depende también de un buen computador o periférico semejante.
5. Contratación de banda ancha para mayor velocidad en la conexión en internet.
6. Mantener un trabajo colaborativo con clientes internos, es decir, fomentar una buena comunicación a través de los diferentes medios de comunicación como son los chats, las video llamadas, llamadas personales u otros medios como el correo electrónico.
7. Para una comunicación efectiva, es mejor tener un espacio totalmente dedicado para el trabajo, de tal manera que no haya interrupciones de ninguna especie.
8. Opcional sería el de tener un teléfono inteligente más su computador.

Cabe resaltar que toda empresa o empleador, deben subir su nivel de capacitación y autoformación, para enfrentar los riesgos que se hallan vinculados estrechamente con la ciberseguridad en el teletrabajo.

Para establecer el acceso a la red, primeramente, será necesario determinar cuántos y qué empleados necesitan acceso a la red interna o a los servicios de correo electrónico que se mantiene en la nube, así se podrán crear perfiles con los permisos competentes y niveles de acceso a datos públicos o confidenciales y dependiendo si es un empleado presencial o teletrabajador. En el caso de que se requiera acceso a la red interna se recomienda:

Tabla 20

Recomendaciones para el acceso a la red

Item	Recomendación
1	Se de acceso solamente cuando el computador utilizado, sea un activo de la empresa, con las configuraciones respectivas de seguridad
2	Siempre utilizar un VPN para la conexión de teletrabajadores a la red interna, evitando así la exposición al tráfico provenientes del exterior que está normalmente en una red pública.
3	Mantener un estricto control de dispositivos periféricos como los USB o discos externos, bloqueándolos para que no tengan programas de arranque automatizado y revisando si tienen virus troyanos o semejantes
4	Es necesario que se contraten programas especializados en antimalware, firewalls para mayor seguridad de servidores y computadores de todos los empleados. Hoy en día existen licencias múltiples que respaldan a todos los usuarios de la red
5	El administrador de la red debe poner límites en las descargas, almacenamiento, así como en la copia de datos, evitando una fuga o brecha que ocasione una pérdida de datos por usurpación o ciberataque, con la apropiación indebida de datos confidenciales o secretos.
6	Establecer una autentificación multifactorial, es decir, tener varias barreras de acceso antes de llegar a los datos. Este punto ya se lo había tratado con anterioridad. De ser necesario, debe utilizarse un sistema basado en aplicaciones e incluso puede ser un token de hardware (ver gráfico 24) para la creación de códigos únicos para el acceso

Figura 35

Modelo token de hardware

Adicional a las recomendaciones antes expuestas, será necesario que el administrador de la red, genere accesos incluso a los chats, llamadas y video conferencias que se crean para la comunicación interna, estableciendo así una mayor seguridad entre los propios usuarios que sabrán a ciencia cierta que están conversando con un compañero de trabajo y no con un suplantador de identidad.

Hay que estar siempre pendiente de la ciberdelincuencia que está por aprovechar cualquier oportunidad que le da un sistema inseguro que utiliza el teletrabajo como modo de acceso remoto, infectando las redes con actos malintencionados, enviando mensajes internos con información falsa, pasando mensajes catalogados como urgentes y que tienen virus, solicitando fondos entre otros modos de hacer daño. Por eso es necesario mantener claves de acceso en todos los sistemas como un modo de aprobación y validación de acceso.

Uso de Correo Electrónico

En base a lo que ha venido trabajando y explicando el teletrabajo nos presenta muchos desafíos que se deben abordar de manera exhaustiva y el uso del correo electrónico debe ser tratado con mucho detenimiento y cuidado, cada empresa debe establecer políticas, normas y procedimientos relacionados con el manejo y buen uso que se debe dar al correo electrónico empresarial o corporativo, asegurando que todo el personal de la institución / empresa, conozca las responsabilidades y obligaciones del uso de ésta herramienta previniendo el mal uso accidental o intencional de la información y minimizar el impacto de amenazas reales tales como la saturación del sistema, los accesos no autorizados, daños por virus, conducta ilegal, acoso o fraude. La política puede poner límites a los tipos de archivos que los empleados son capaces de abrir, descargar o intercambiar con otros, también debe explicar qué hacer si un empleado recibe un correo electrónico ofensivo, para protegerse contra la responsabilidad legal para el efecto se sugiere lo siguiente:

a) Mantener una política con normas y procedimientos para uso del correo electrónico.

b) El usuario es responsable del uso exclusivo para asuntos relacionados con sus labores.
c) La información transmitida mediante el correo electrónico tiene la misma responsabilidad que cualquier envío tradicional de información y requiere se cumpla con las normas dispuestas por la empresa.
d) Asegurarse que los mensajes no incluyan comentarios abusivos, obscenos, difamatorios, ni material alguno que pueda poner en situación conflictiva a la empresa y a su personal.
e) Eliminar mensajes que se reciban de fuentes desconocidas, por el riesgo de ataques y contagio de virus.
f) La cuenta de correo electrónico es personal e intransferible. El usuario se compromete a hacer un uso responsable de la cuenta.
g) Para comunicación con usuarios externos, asegúrese de incluir una denegación de responsabilidad apropiada en cada mensaje de correo electrónico.
h) El usuario es responsable de realizar respaldos periódicos de sus mensajes, carpetas de correo y agenda de direcciones electrónicas.
i) Establecer una política de eliminación de correos de los servidores para evitar sobrecargas en las bases de datos, política de retención de correos por 90 días, por ejemplo.

Plan de Recuperación, Soporte y Gestión en Crisis

La necesidad urgente de conexión que trajo el teletrabajo permitió que se descuide la ciberseguridad, así como el descontrol en la administración de los sistemas informáticos y dispositivos electrónicos. Pero una vez superada esta crisis inicial, es necesario brindar apoyo y soporte al teletrabajador para garantizar el buen funcionamiento de todo el sistema, así como el resguardo de la información. Estos trabajadores deben mantener un protocolo muy claro para su comunicación con sus clientes internos, así también con su administrador del sistema para solventar cualquier problema inusual que ocurra o se sospeche que hay algún intruso que está alterando la información.

Ante esto, el administrador del sistema o a su vez el asesor externo informático, debe tener implementado y socializado un DRP (*Disaster Recovery Plan*), donde se describan las acciones y los procedimientos que deben ejecutarse durante y después de un desastre, así como las procedimientos para reestablecer y tener disponibles los servicios informáticos, los equipos de comunicaciones y las aplicaciones. Para permitir la continuidad del negocio con el mínimo impacto posible, instalar en los

computadores programas seguros de acceso o control remoto para una reacción inmediata. Dentro del soporte debe estar considerada la comunicación a través de mensajes grupales exponiendo, en resumen, lo que se está trabajando para la seguridad, los problemas detectados y las experiencias vividas.

Todos los empleados de la empresa deben estar conscientes que el teletrabajo es muy diferente al que se desarrolla dentro de la empresa, por tanto, la respuesta de un teletrabajador puede ser un poco más lenta, acorde con el tipo de comunicación con la que se quiere llegar.

En momentos de crisis, es necesario que exista un protocolo de gestión, con procedimientos claros que partan desde las jefaturas y que den cuenta a todos los trabajadores y especialmente a los que trabajan de manera remota, sobre las medidas a tomar en el caso de un ataque delincuencial al sistema. A partir de un problema detectado, se deben programar reuniones grupales obligatorias, informes de la situación por parte del administrador del sistema, colaboración de los diferentes directores de equipos y reportes finales de las soluciones implementadas.

Seguridad del Hardware

Los equipos informáticos empleados para el teletrabajo, en especial los asignados por la empresa deben tener seguridad en su hardware, para la protección en caso de caer en manos incorrectas, para esto los departamentos de tecnología podrán usar algunas de las siguientes opciones disponibles.

Colocar claves de seguridad en el BIOS, para de esta manera prevenir cambios de las configuraciones de arranque de los equipos.

Activar sistemas de protección de datos de los equipos como pueden ser el BitLocker, que cifra el disco y solo se puede desactivar colocando la clave de cifrado.

Para empresas más grandes que manejan presupuesto de seguridad en la Información se sugiere trabajar con Intune de Microsoft, que permiten gestionar dispositivos mediante software dedicando directamente al control sobre el hardware, tanto en computadoras, tablets y teléfonos inteligentes: permitiendo crear políticas de seguridad muy variadas, tales como no permitir capturas de pantalla en los dispositivos, requerir el uso de contraseñas para trabajar con el dispositivo, y muchas otras configuraciones destinadas a proteger los datos y evitar el acceso a personas no autorizadas.

Acomodación en el hogar

El teletrabajo llego para quedarse y un buen espacio destinado en el hogar será fundamental, para el óptimo desempeño de las actividades por lo que de acuerdo con las mejores prácticas se pueden recomendar las siguientes:

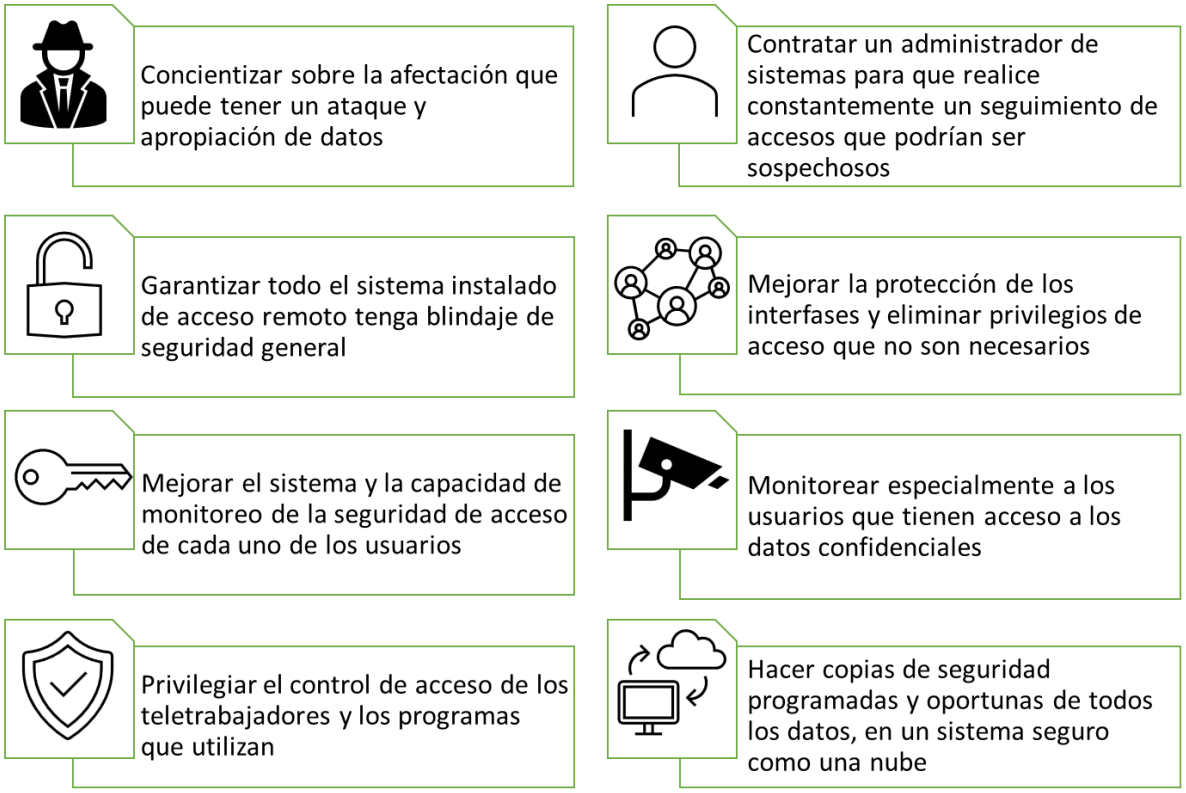
a) Mantén tu horario laboral, similar como si estuvieses en la oficina.
b) Define horarios para el almuerzo, el café, el descanso etc.
c) Implementa un espacio con buena iluminación para trabajar.
d) No trabajes desde la cama o acostado en el sillón. Esto puede provocarte dolores de columna y cuello e incluso alguna lesión.
e) Mantén el orden del entorno que te rodea. Un espacio ordenado y limpio nos permite laborar más animosamente.
f) Evita el multitasking, enfócate en una tarea a la vez.
g) Utiliza responsablemente la tecnología, organiza horarios para contestar los emails, los mensajes, dentro de lo posible que sea en horarios laborales.
h) Usa un escritorio, las conexiones tanto de red como eléctricas deben ser desde las tomas de la pared, no uses cables extensores, pueden ser causales de accidentes.
i) Evita realizar tus tareas en espacios donde no tengas privacidad, te distraerás fácilmente.
j) Cuida tus equipos electrónicos, da una limpieza diaria con un paño semihúmedo, limpia el teclado y la pantalla. Evita comer cerca de ellos puedes derramar líquidos y dañarlos.
k) En caso de averías de tus equipos electrónicos o fallos en los programas notifica a tu departamento técnico o mesa de ayuda.
l) No trates de arreglar los equipos, pide apoyo técnico.
m) Elimina archivos temporales del equipo con frecuencia te ayudarán en el rendimiento.
n) Mantén organizada tu información de manera que sea fácil acceder rápidamente.
o) No compartas el equipo de trabajo con tus familiares, pueden ser causal de llamados de atención.

2.4.1 Consideraciones de Ciberseguridad Aplicados al Teletrabajo

Para las empresas que actualmente mantienen un sistema organizado de teletrabajo, es necesario que tomen en cuenta las siguientes recomendaciones de ciberseguridad en sus redes:

Figura 36

Recomendaciones de ciberseguridad



2.4.2 Estrategias y/o Técnicas

Para la elaboración del producto propuesto, se revisaron cuidadosamente los informes sobre ciberseguridad y ciberdelincuencia, para que de esta manera estar al día con la información que ya se ha publicado al respecto y ofrecer herramientas actualizadas que serán de mucha ayuda para las empresas, en especial las pequeñas y medianas que actualmente no mantienen un alto nivel de seguridad y reparación sobre la utilización de redes informáticas.

Adicionalmente se dialogó con empresarios que tienen teletrabajadores, extrayendo información sobre su modelo de teletrabajo, así como el manejo de sus redes, la seguridad de sus datos, la capacitación de su talento humano, entre otros temas, mismo que sirvió para dar un mejor enfoque a la propuesta.

Una técnica muy importante fue la del trabajo de campo, visitando las empresas, acudiendo a los administradores de redes y así también acompañando en su trabajo a las personas que laboran de manera externa en las organizaciones y tomando nota de cómo se desempeñan durante sus labores, pidiendo información sobre los envíos de datos, archivo de información, respaldo, antivirus y manejo de

las redes o los paquetes informáticos, así se tuvo la alimentación suficiente para dar una propuesta acorde a las necesidades.

2.5 Validación de la Propuesta

Para la validación de la propuesta se solicitó el apoyo de especialistas en las áreas competentes como de comunicación e informática, considerando un perfil acorde a los siguientes criterios: formación académica relacionada con el tema investigativo, experiencia académica y/o laboral orientada a la gestión administrativa y motivación para participar.

Para la validación informática se solicitó el apoyo de la Ingeniera Mónica Ronquillo, profesional con amplia trayectoria en el manejo de redes y sistemas de información y comunicación, radicado en el Ecuador y con una amplia carpeta curricular.

Para el apoyo del área de comunicación, se tuvo el respaldo del Ingeniero Milton Salazar quien actualmente trabaja en el Municipio de Quito, con amplia trayectoria exitosa en las empresa públicas y privadas del país.

En los dos casos, se solicitó la revisión de la propuesta, dejando muy buenos comentarios y exponiendo su aprobación en la totalidad del contenido, con sugerencias menores que fueron acogidas para la presentación del presente trabajo de fin de master.

Los objetivos que persigue la validación son los siguientes:

- Validar el método utilizado en el desarrollo de la propuesta.
- Revisar, comentar, acotar y aprobar la propuesta bajo su punto de vista profesional y experiencia en el medio.
- Sugerir cambios o redefinir en el caso de ser necesario, en alguno o algunos de los puntos tratados en la propuesta, considerando su propia experiencia.
- Exponer si la propuesta es aplicable como un modelo de gestión de la ciberseguridad para las pequeñas y medianas empresas

En el Anexo 2, se encuentra el modelo de evaluación propuesto a los expertos y que sirvió para medir la aceptabilidad de la propuesta. Adicionalmente, en el anexo 3 se encuentra la tabla de valoración de criterios cualitativos que se utilizó como un segundo formato para validar la propuesta, acorde con la importancia y representatividad.

Tabla 21

Descripción de perfil de Validador

Nombres y Apellidos	Años de experiencia	Titulación Académica	Cargo
Milton Mesías Salazar Tamayo	12	MAGISTER EN GERENCIA DE PROYECTOS EDUCATIVOS Y SOCIALES	Jefe de Proyectos tecnológicos Municipio de Quito
Martha Mónica Ronquillo Cuellar	22	MAESTRIA EN ADMINISTRACION DE TECNOLOGIAS DE INFORMACION	Jefe de Proyectos y Tecnología METROVIA - Guayaquil

2.6 Matriz de Articulación de la Propuesta

A continuación, se expone la Matriz de articulación de la propuesta

Tabla 22

Matriz Articulación de la Propuesta

PROBLEMA	PREGUNTAS	OBJETIVOS	IDEA A DEFENDER / PRODUCTO A DESARROLLAR
Poco conocimiento de la forma como se lleva la telecomunicación de los trabajadores que se acogieron el teletrabajo en la ciudad de Quito	¿Cómo se ha logrado una comunicación entre el trabajador y el empleador?	Establecer los acuerdos alcanzados por el trabajador y el empleador para el cumplimiento del trabajo	Los medios de telecomunicación con que cuenta el trabajador que se ha acogido al teletrabajo, no le permiten proteger los datos que maneja y proteger contra un ciberataque.
	¿Qué métodos de telecomunicación son los más utilizados en el teletrabajo?	Indicar los medios de telecomunicación que ha tenido que utilizar el trabajador que se ha acogido al teletrabajo	

¿Por qué no se han cumplido las metas u objetivos planteados por los empleadores?	Saber los motivos por los que el trabajador, no ha logrado cumplir las metas que le han sido planteadas para el cumplimiento de su trabajo
¿Se respeta su derecho a la desconexión digital?	Establecer si el trabajador mantiene un horario de trabajo, después del cual, se desconecta totalmente de su trabajo

CONCLUSIONES

A pesar de la pandemia del Covid-19, los estudios sobre el teletrabajo y la ciberdelincuencia han fructificado y multiplicado, ya que se pudo encontrar en las diferentes plataformas de almacenamiento de estudios y artículos, así como en bibliotecas en el ciberespacio, una gran cantidad de información que pudo sustentar este trabajo de investigación, ya sea desde el punto técnico así como el legal, aplaudiendo el amparo jurídico que tiene el teletrabajo en el Ecuador y las múltiples publicaciones sobre la ciberseguridad.

Los teletrabajadores de la ciudad de Quito y que fueron considerados en la encuesta, fueron sorprendidos con esta nueva forma de trabajo y muchos se encontraron en incertidumbre los primeros meses de trabajo, pero de a poco, fueron acostumbrándose a su nueva forma de laborar, desarrollando nuevas aptitudes y métodos de envío de su trabajo a su empleador.

Se logró diseñar estrategias de telecomunicación aptas para usuarios, desde un nivel básico hasta medio, con un lenguaje propicio y amigable, de tal manera que se pueda entender y aplicar en las empresas. Dichas estrategias servirán para enfrentar los problemas de ciberseguridad y acceso de datos, explicando a los lectores como crear una contraseña segura, así como tomar medidas preventivas ante la sospecha de ciberataques.

El trabajo realizado ha sido sometido a validadores expertos en las materias, con amplia experiencia en sus carreras, mismos que han validado positivamente el contenido, dando sus recomendaciones previas, que fueron acogidas e implementadas antes de la presentación de este estudio, así tiene un carácter de aceptación muy alto, de tal manera que podrá ser leído para el enriquecimiento de la comunidad educativa del país.

RECOMENDACIONES

Revisadas las plataformas de almacenamiento de información científica, se constató que hay publicaciones ricas en información sobre ciberseguridad y teletrabajo, pero aún falta llegar a los lectores que desconocen sobre los temas, con palabras más fáciles de interpretar, es decir, con un lenguaje más amigable para un lector que necesita apoyo sobre sus datos, pudiendo incluso ser más visuales y gráficos, haciendo más amigable la comunicación y por ende, apoyando a quienes aún no conocen profundamente sobre redes y seguridad.

Los teletrabajadores se han acoplado a la nueva realidad laboral, pero aún mantienen un alto nivel de desconocimiento sobre seguridad de datos, utilización de antivirus y demás programas de apoyo para la transferencia segura de información, por lo que sería muy recomendable que las empresas donde laboran, les brinde mayor capacitación sobre estos temas, para el propio beneficio de la conservación segura de sus datos, evitando cualquier tipo de usurpación. Pero la capacitación debe ser constante, con actualizaciones sobre nuevos modelos de acceso y usurpación de información, para mantenerse actualizados y pendientes ante cualquier ataque de la ciberdelincuencia.

Se ha presentado un trabajo sustentado e investigado en las principales plataformas de búsqueda, logrando abordar los problemas más recurrentes que surgen en el día a día de los teletrabajadores, ahora lo importante es que las pequeñas y medianas empresas a la cual va principalmente dirigido la tomen para su implementación y capacitación de sus teletrabajadores, ya que esa es la principal motivación del estudio, y no quede solo como una letra muerta.

La propuesta ha sido validada, pero quedan algunos temas por profundizar, por lo que se recomienda a los lectores, tomar aquellos temas que no se han tratado y preparar un nevo estudio que mejore las estrategias propuestas y se actualice con lo nuevo que cada día nace en el mundo de la informática y la comunicación.

BIBLIOGRAFÍA

Altamirano, M., & López, T. (2020). *El Teletrabajo como un contrato de trabajo amparado por el Derecho Laboral.* Guayaquil: Universidad Católica de Santiago de Guayaquil.

Amutio Gómez, M. A., Candau, J. M., & Porras, M. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Ministerio de Hacienda y Administraciones Públicas. doi:630-12-171-8

Arias Buenaño, G., Merizalde Almeida, N., & Noriega García, N. (2016). *Análisis y solución de las vulnerabilidades de la seguridad informática y seguridad de la información de un medio de comunicación audio - visual.* UPS.

Arias, F. G. (2016). *El proyecto de investigación. Guía para su elaboración.* Caracas: Editorial Episteme.

Asamblea Nacional. (2020). *Ley Orgánica de Apoyo Humanitario.* Quito: Registro Oficial Suplemento 229 .

Barragán, A. (27 de marzo de 2021). *El Teletrabajo en España*. Obtenido de https://www.pymerang.com/administracion-de-empresas/recursos-humanos/funciones-de-recursos-humanos/satisfaccion-y-comunicacion/375-el-teletrabajo-en-espana

Cabanellas, G. (2016). *Diccionario Jurídico Elemental.* Buenos Aires: Heliasta.

Campaña, M., Melendes, E., Flores, J., & Acosta, R. (2020). La Intervención del Trabajador Social en la Junta Cantonal de Protección de Derechos. *Revista científica Dominio de las ciencias*, 739 - 809.

Canal, N. (2006). Técnicas de muestreo. Sesgos más frecuentes. *Revista Eden*, 121-132.

Ciberseguridad. (11 de marzo de 2022). *Acceso remoto seguro*. Obtenido de https://ciberseguridad.com/guias/acceso-remoto-seguro/

Corrado, N., & Soulages, V. (2020). *Consideraciones generales de ciberseguridad en medio de eventos extraordinarios.* Deloitte.

Correa, T. (2021). Crisis mundial de Covid-19 y teletrabajo: la nueva normalidad para las relaciones laborales. *Vol.9*(No.1).

DhTrust. (noviembre de 2021). *Arquitectura centrada en datos*. Obtenido de https://dhtrust.org/instrucciones/arquitectura-centrada-en-datos/

Diario El Comercio. (09 de julio de 2015). *El 68% del software que se vende en el país es pirata.* Obtenido de https://www.elcomercio.com/actualidad/seguridad/software-pirateria-ecuador-seguridad-delito.html

Gallusser, P. (2018). Creciente avance del teletrabajo como modalidad laboral. *La Trama de la Comunicación, vol. 10*, 1 - 15.

Hernández, R., Fernández, C., & Baptista, M. d. (2017). *Metodología de la Investigación.* Máxico D.F: Interamericana Editores S.A.

Ibarra Cisneros, M. A., & González Torres, L. A. (2019). La flexibilidad laboral como estrategia de competitividad y sus efectos sobre la economía, la empresa y el mercado de trabajo. *Contadaduría y Administración, 231*, 33 - 52.

Joric, C. (15 de Diciembre de 2020). *El teletrabajo nació de otra crisis.* Recuperado el 19 de Junio de 2021, de La Vanguardia: https://www.lavanguardia.com/historiayvida/historia-contemporanea/20200521/481297391719/teletrabajo-covid19-crisis-petroleo-sociedad-consumo.html

López, E. (2020). Flexibilidad, protección del empleo y seguridad social durante la pandemia global del Covid-19. *Instituto Universitario de Investigación en Estudios Latinoamericanos – Universidad de Alcalá, 1*(1), 2 - 74.

Lubiza Osorio, H. (2020). El Teletrabajo: Una opción en la era digital. *Observatorio Laboral Revista Venezolana, 3*(5), 93 - 109. doi:1856-9099

Mosquera Chere, S. O. (20 de enero de 2021). *La vinculación entre la inteligencia artificial y la seguridad cibernética en el Ecuador.* Obtenido de https://polodelconocimiento.com/ojs/index.php/es/article/view/2430/html

Narváez, A. (2020). *El teletrabajo y la prevención de riesgos laborales en el sector.* Cuenca: Universidad De Cuenca .

OIT. (2020). *El teletrabajo durante la pandemia de COVID-19 y después de ella. Guía práctica.* Ginebra: Organización Internacional de Trabajo.

Ortiz, S., Ortiz, A., Paredes, J., & Córdova, M. (2020). Teletrabajo: un análisis normativo en la legislación ecuatoriana. *Vol. 24*(Nº 106).

Palacios, M. (2017). *El teletrabajo: hacia una regulación garantista en el Ecuador.* Quito: Universidad Andina Simón Bolívar .

Parra, P. (2020). *El teletrabajo una transformación del entorno laboral y una oportunidad de cambio frente a la prospectiva Organizacional.* Bogotá: Universidad Nacional Abierta y a Distancia UNAD.

Pautasio, L. (26 de marzo de 2020). *Covid-19 impulsa a reguladores a garantizar el acceso y equiparar las telecomunicaciones con servicios públicos*. Obtenido de https://www.telesemana.com/blog/2020/03/25/covid-19-impulsa-a-reguladores-a-garantizar-el-acceso-y-equiparar-las-telecomunicaciones-con-servicios-publicos/

Pérez, E. (22 de septiembre de 2020). *Aprobada la Ley del Teletrabajo: dudas y respuestas sobre la nueva regulación del trabajo a distancia*. Obtenido de https://www.xataka.com/legislacion-y-derechos/aprobada-ley-teletrabajo-dudas-respuestas-nueva-regulacion-trabajo-a-distancia

PRIMICIAS. (29 de agosto de 2020). *Solo el 45,5% de hogares en Ecuador tiene acceso a Internet, según el INEC*. Obtenido de https://www.primicias.ec/noticias/tecnologia/ecuador-hogares-acceso-internet-inec/

Revista Ekos. (28 de julio de 2021). *Ataques informáticos a empresas públicas crecen 56% en el mundo.* Obtenido de https://www.ekosnegocios.com/articulo/ataques-informaticos-a-empresas-publicas-crecen-56-en-el-mundo

Ripani, L. (24 de Marzo de 2020). *Coronavirus: un experimento de teletrabajo a escala mundial.* Recuperado el 19 de Junio de 2021, de Factor Trabajo: https://blogs.iadb.org/trabajo/es/coronavirus-un-experimento-de-teletrabajo-a-escala-mundial/

Rodríguez, D., & Pardo, M. (2020). *El teletrabajo en tiempos de covid-19.* Bogotá: Universidad Católica de Colombia.

Rodríguez, M. (14 de junio de 2021). *Gartner predice que el mercado de servicios en la nube pública alcanzará los 397.400 millones de dólares en 2022*. Obtenido de https://www.cloudmasters.es/gartner-predice-que-el-mercado-de-servicios-en-la-nube-publica-alcanzara-los-397-400-millones-de-dolares-en-2022/

Ros Guasch, J. A. (2016). *Análisis de roles de trabajo en equipo: un enfoque centrado en comportamientos.* Universitat Autónoma de Barcelona.

Rugel, J., & Romero, R. (2020). *Las percepciones de los trabajadores frente al teletrabajo durante la pandemia Covid-19, caso de estudio realizado a los residentes de una urbanización del Cantón Daule.* Guayaquil: Universidad Católica de Santiago de Guayaquil.

Sanguineti, W. (2021). El teletrabajo como fenómeno social y como noción jurídica. *Vol.2*(No. 4).

Sanguineti, W. (2021). *Teletrabajo y globalización: en busca de respuestas al desafío de la transnacionalización del empleo.* Salamanca: Universidad de Salamanca.

Secretaría de Comunicación y Transporte . (2020). *Guía de ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo.* Estados Unidos Mexicanos.

Selma, J. (2016). *El Teletrabajo, ¿una solución?* Alicante: Facultad de Ciencias Sociales y Jurídicas de Elche.

Sunkel, G., & Trucco, D. (2020). *Las tecnologías digitales frente a los desafíos de una educación inclusiva en América Latina.* CEPAL.

Tamariz, M. d. (2019). *El teletrabajo como alternativa de flexibilidad e inclusión laboral y su institucionalización jurídica social en el Ecuador.* Cuenca: Universidad de Cuenca.

Vallejo, G. (2020). *Análisis de la implementación del teletrabajo en el sector privado en Ecuador. Casos prácticos.* Quito: Universidad Andina Simón Bolívar .

Vargas Borbúa, Recalde Herrera, L., & Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO - Revista Latinoamericana de Estudios de Seguridad, 1*(20), 31 - 45. doi:dx.doi.org/10.17141/urvio.20.2017.2571

Vargas, J. (2020). El teletrabajo: nueva modalidad laboral y una opción digital para las empresas y la sociedad. *Vol.1*(No.1).

Ventanales, A. (30 de diciembre de 2021). *El teletrabajo y la virtualización del mundo*. Obtenido de https://www.casagrande.edu.ec/project/el-teletrabajo-y-la-virtualizacion-del-mundo/

Villabella, C. M. (2020). *Los métodos en la investigación jurídica. Algunas precisiones.* México: Universidad Nacional Autónoma de México.

Weiers, R. (2016). *Introducción a la estadística para los negocios.* México: Thomson.

ANEXOS

ANEXO 1

FORMATO DE ENCUESTA

La presente encuesta tiene la finalidad establecer el criterio que tienen los teletrabajadores en la ciudad de Quito, con relación a los métodos de telecomunicaciones utilizados y sus resultados servirán como aporte para el desarrollo del trabajo de la Maestría en Telecomunicaciones, mención: Gestión de las Telecomunicaciones de la Universidad Israel. En este cuestionario habrá confidencialidad, por favor conteste con toda veracidad, ya que sus respuestas son muy importantes para establecer estrategias de telecomunicación que permitan enfrentar los problemas del ciberataque.

1. ¿En qué sector vive?

Norte		Centro		Sur		Valles		Fuera de Quito	

2. ¿En qué área de su empresa trabaja?

Administración		Ventas		Producción		Mantenimiento		Otro	

3. ¿Antes estuvo o en la actualidad está en teletrabajo? (si su respuesta es sí, pase a la siguiente pregunta, de lo contrario, muchas gracias)

Sí		No	

4. ¿Qué nivel de confidencialidad tiene la información con la que usted trabaja?

Muy alto		Alto		Medio		Bajo		Muy bajo	

5. ¿Qué medio o medios electrónicos utiliza para recibe o envía su trabajo? (puede marcar más de uno)

Computador de escritorio		Celular		Tablet		Laptop		Otro	

6. ¿Cuáles de los siguientes programas son los que más utiliza? (puede marcar más de uno)

Word		Excel		Power Point		Adobe		Visio	
Contable		Outlook		Google Maps		SPSS		Otro	

7. ¿Tiene usted licencias de los programas que utiliza?

Sí, de todos		Sí, de algunos		De ninguno	

8. ¿Califique usted el espacio con que dispone para el desarrollo del teletrabajo?

Muy bueno		Bueno		Malo		Muy malo		Deficiente	

9. ¿En qué concepto se ha incrementado sus gastos como consecuencia del teletrabajo? (puede marcar más de uno.

Electricidad		Internet		Equipos informáticos		Programas informáticos		No he tenido gastos extras	

10. ¿Qué nivel de capacitación ha recibido usted de parte de su empresa para el envío y recepción de información de manera segura?

Muy alto		Alto		Medio		Bajo		Muy bajo		Ninguno	

11. ¿Su antivirus instalado tiene cobertura para la protección de tráfico en línea?

Sí		No		No sabe	

12. ¿Qué problemas técnicos ha tenido para su conexión a internet?

Caída del internet		Internet lento		Falla equipos		Poca recepción		Ninguno	

13. Califique el nivel de complejidad que tienen los programas que usted utiliza

Muy alto		Alto		Medio		Bajo		Muy bajo		Ninguno	

14. ¿En qué medida ha tenido ciberataques a su cuenta o la de su empresa?

Muy alto		Alto		Medio		Bajo		Muy bajo		Ninguno	

15. ¿En qué tipo de dispositivo realiza su copia de seguridad de la información?

Disco externo		USB		OneDrive		Drive		Otro	

16. ¿Piensa que el teletrabajo debe continuar?

Sí		No		No sabe	

Link de la encuesta en Microsoft Forms:

https://forms.office.com/r/sAQnnZsL35

ANEXO 2

Criterios de Aceptación

Preguntas para el instrumento de validación

Tabla 23

Anexo 2

Criterios	Descripción
Impacto	Representa el alcance que tendrá el modelo de gestión y su representatividad en la generación de valor público.
Aplicabilidad	La capacidad de implementación del modelo considerando que los contenidos de la propuesta sean aplicables
Conceptualización	Los componentes de la propuesta tienen como base conceptos y teorías propias de la gestión por resultados de manera sistémica y articulada.
Actualidad	Los contenidos de la propuesta consideran los procedimientos actuales y los cambios científicos y tecnológicos que se producen en la nueva gestión pública.
Calidad Técnica	Miden los atributos cualitativos del contenido de la propuesta.
Factibilidad	Nivel de utilización del modelo propuesto por parte de la Entidad.
Pertinencia	Los contenidos de la propuesta son conducentes, concernientes y convenientes para solucionar el problema planteado.

ANEXO 3

Evaluación según Importancia y Representatividad

Tabla 24

Anexo 3

CRITERIOS	EVALUACION SEGUN IMPORTANCIA Y REPRESENTATIVIDAD				
	En Total Desacuerdo	En Desacuerdo	Ni de Acuerdo Ni en Desacuerdo	De Acuerdo	Totalmente Acuerdo
Impacto					X
Aplicabilidad					X
Conceptualización					X
Actualidad					X
Calidad Técnica					X
Factibilidad					X
Pertinencia					X