Importancia de la seguridad informática para proveer teletrabajo seguro en Costa Rica.

Victor Ureña Araya[1]. Universidad Latinoamericana de Ciencia y Tecnología, Costa Rica.

Resumen

A partir de la pandemia por COVID-19 que ha afectado a la sociedad a nivel mundial, se desencadenó a nivel empresarial la necesidad de implementar la modalidad de teletrabajo para que la actividad financiera y productiva continuara desarrollando. Es por lo que la implementación de la tecnología y el uso de esta han aumentado a nivel general en el país, siendo un factor que amenaza la seguridad informática de las empresas que no cuentan con las herramientas de protección cibernéticas adecuada. Por lo anterior, el alcance de esta investigación es recomendar las mejores prácticas de seguridad informática a empresas que buscan diversificar y aplicar métodos de teletrabajo seguro, partiendo de la cuestionante sobre ¿Cuáles son las mejores prácticas de seguridad informática para implementar teletrabajo seguro en Costa Rica? La presente investigación se realizó desde un paradigma positivista y un enfoque cuantitativo, beneficiando directamente a las 51 empresas entrevistadas, ya que con cada una de ellas se recopilará información para observar las metodologías aplicadas en el país, siendo estas de suma importancia para el manejo de la información a nivel tecnológico, así como para brindarle una respuesta más segura a sus diligencias. Entre los principales hallazgos de este estudio se comprobar que existen muchas empresas que aún no están capacitadas en términos de seguridad informática, así mismo se identifica que a nivel general la mayor parte de las empresas no llevan un control de ciberseguridad de sus trabajadores lo que ha incrementado la cantidad de ciberataques.

Palabras clave

Ciberseguridad: Es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional.

Teletrabajo: Es una modalidad de trabajo mediante la cual se les permite a los empleados realizar sus tareas y asignaciones fuera de las instalaciones físicas de la empresa.

VPN: Es una tecnología de red que permite conectar uno o más ordenadores en una red privada virtual, a través de una red pública como Internet.

Ataques Cibernéticos: Es una acción delictiva y malintencionada que se realiza para acceder a información privada a través de las redes computacionales.

[1] **Victor Ureña Araya** es Ingeniero Informático, estudiante de la Maestría en Gerencia de Proyectos de la ULACIT, cuenta con cerca de 6 años de experiencia en el área de redes y telecomunicaciones, desarrollando más de 10 proyectos de diseño y optimización de redes. Ha logrado mantener la ciberseguridad a más de 500 usuarios de empresas a nivel nacional. Actualmente, tiene bajo su responsabilidad 15 equipos de ciberseguridad con certificaciones internacionales de herramientas y fabricantes como Fortinet, Symantec, GFI e Infoblox. Email: victor14ua@gmail.com

Abstract

From the COVID-19 pandemic that has affected society worldwide, the need to implement teleworking was triggered the business level so that financial and productive activity could continue to develop. That is why the implementation of technology and its use has increased at a general level in the country, being a factor that threatens the computer security of companies that do not have the appropriate cyber protection tools. This is why, that the scope of this research is to recommend the best computer security practices to companies that seek to diversify and apply secure teleworking methods, starting from the question about What are the best computer security practices to implement secure teleworking in Costa Rica? This research was carried out from a positivist paradigm and a quantitative approach, with 51 companies interviewed, since with each one of them information will be collected to observe the methodologies applied in the country, these being of utmost importance for the management of information at a technological level, as well as to provide you with a more secure response to your inquiries. Among the main findings of this study, it was possible to verify that there are many companies that are not yet trained in terms of computer security, it was also possible to identify that at a general level most of the companies do not carry out a cybersecurity control of their workers. which has increased the number of cyber attacks.

Keywords

Cybersecurity: It is the area related to computing and telematics that focuses on the protection of computing infrastructure.

Teleworking: It is a work modality by which employees can carry out their tasks and assignments outside the physical facilities of the company.

VPN: It is a network technology that allows one or more computers to be connected in a virtual private network, through a public network such as the Internet.

Cyber Attacks: It is a criminal and malicious action that is carried out to access private information through computer networks.

Introducción

En la actualidad se ha producido un gran desarrollo e incremento en cuanto a la creación y al uso de los dispositivos que ahora poseen o requieren conectarse a internet (IoT), para Barrio (2018) el internet de las cosas tiene como finalidad “brindar una infraestructura que supere la barrera entre los objetos en el mundo físico y su representación en los sistemas de información” (p.19). Como sociedad hemos presenciado la evolución de las diferentes áreas de trabajo como las conocemos educación, medicina, finanzas, ventas, entre muchas otras que se encuentran reinventándose día a día.

Es así como a partir de la evolución industrial, la apertura y el acceso al internet con la posibilidad de tener grandes anchos de banda se ha vuelto accesible para las diferentes empresas implementar modalidades de teletrabajo para sus trabajadores.

El teletrabajo no es un concepto nuevo, ya que surge de los años 70, luego de que el científico Jack Nilles, escrutara opciones para sobrellevar la crisis petrolera que sufría Estados Unidos, haciendo referencia al uso de las tecnologías de la información y comunicación (UNED, 2019). En la actualidad, después de más de 40 años podemos observar que esta modalidad es cada vez más utilizada en las diferentes empresas, siendo el 2020 el año de mayor incremento en la aplicación del teletrabajo a partir de la pandemia por COVID-19 a nivel mundial.

A pesar de que la modalidad de teletrabajo sea llamativa para algunas personas, existen elementos que deben de ser tomados en cuenta para poder aplicarla correctamente. En primer lugar, las empresas deben de contar con el capital económico para darles a sus trabajadores los implementos necesarios para laborar desde sus casas, así como también deben de mantener todos los dispositivos tecnológicos protegidos y en incesante mantenimiento para evitar que los atacantes cibernéticos puedan obtener su información confidencial.

Así como se ha podido estimar, la evolución y el avance a nivel tecnológico de igual manera se han visto en aumento los ataques, fraudes y robo de información a través de las redes. Durante el período de pandemia del presente año en Costa Rica se han presentado más de 51 millones de intentos de ciberataques, información corroborada por el gerente de Fortinet, Joaquín Martínez (La prensa Latina, 2020). A partir de esta información se vuelve necesario que las diferentes empresas protejan la información que manejan y que inviertan en prácticas de seguridad informática de calidad.

Es importante plantear diferentes preguntas acerca del cómo las empresas se han protegido y enfrentado a los ciberataques durante la implementación de la modalidad de teletrabajo, como las siguientes: ¿Se han implementado prácticas de seguridad de la forma correcta? ¿Conocen del riesgo que conlleva no utilizar prácticas de seguridad?, ¿Utilizan los métodos más seguros?, ¿Han capacitado al personal en ciberseguridad para esta modalidad de trabajo?

A partir de las preguntas anteriores es necesario generar un proyecto que indague el estado actual del país en cuanto a estas y que además le suministre a diferentes empresas conocimientos acerca de prácticas informáticas seguras. Entendiendo que cada vez son más las empresas que utilizan el teletrabajo como la modalidad predominante tal y como lo menciona la página presidencial oficial (2020) afirmando que “14.668 personas funcionarias de 56 instituciones se encuentran laborando bajo la modalidad de teletrabajo” (párr.1). Es preciso brindarles recomendaciones desde el manejo por parte del usuario, así como herramientas y protocolos que ofrezcan estándares de seguridad para disminuir el riesgo ante posibles amenazas cibernéticas.

Pregunta de Investigación

¿Cuáles son las mejores prácticas de seguridad informática para implementar Teletrabajo seguro en Costa Rica?

Objetivo general de la Investigación

Recomendar las mejores prácticas de seguridad informática a empresas que buscan diversificar y aplicar métodos de teletrabajo.

Objetivos específicos de la investigación

1. Demostrar las diferentes prácticas de seguridad informática utilizadas en Costa Rica en la modalidad de teletrabajo.
2. Evaluar las ventajas y desventajas del uso de la seguridad informática en la modalidad de teletrabajo a nivel nacional e internacional.
3. Explicar los protocolos de seguridad informática más utilizados a nivel nacional e internacional en la modalidad de teletrabajo.
4. Crear un documento acerca de protocolos de red, métodos y herramientas para implementar un teletrabajo seguro.

Forma de alcanzar dichos objetivos

El trabajo de investigación se desarrollará únicamente con información fidedigna, y cumplirá con los criterios de calidad de fiabilidad y validez interna. Se tomará en cuenta la opinión de expertos en la temática, como lo es el gerente de Fortinet, el Señor Joaquín Martínez quién facilitará información valiosa para fundamentar los resultados del estudio. La investigación se realizará a partir de un paradigma positivista y un enfoque cuantitativo, el cual permitirá el procesamiento de datos a nivel estadístico. Para la fundamentación teórica se hará una búsqueda exhaustiva de información en diferentes bases de datos como lo es la plataforma EBSCO. Es preciso mencionar que para la recolección de datos se utilizará como instrumento la encuesta, la cual será resuelta por una muestra representativa de la población (diferentes empresas que se encuentren en modalidad de teletrabajo).

Marco teórico

Teletrabajo

Parada Visual (2020) conceptualiza el teletrabajo como "una forma flexible de organización del trabajo, que consiste en llevar a cabo la actividad profesional para la empresa a distancia, es decir, sin que el trabajador esté físicamente en su centro de trabajo durante una parte importante de su horario laboral" (párr.1).

Así mismo, es necesario entender que según el Ministerio de Salud (2020) en el Artículo 6, Decreto Ejecutivo N°. 39734-S se establecen tres tipos o modalidades para realizar teletrabajo:

- **Móvil:** Es cuando el funcionario trabaja desde diferentes puntos y viaja habitualmente según la naturaleza de sus funciones.
- **Domicilio:** Es el que se realiza desde el domicilio del funcionario.
- **Telecentro:** Es el lugar destinado por la Institución para que sus trabajadores puedan desarrollar las actividades que previamente fueron definidas como teletrabajables. (párr.1)

Prácticas de seguridad informática

Según el CSIRT-CV (2018) a partir de las amenazas tecnológicas a nivel mundial actualmente es imposible poder considerar que un equipo posea un 100% de seguridad, y plantean algunas pautas para considerar un equipo como confiable:

> … "Un equipo confiable es aquel que ha sido plataformado y securizado por personal cualificado (implica antivirus, actualizaciones automáticas, bastionado, etc.…), instalando el sistema operativo desde una fuente confiable y sobre el cual el usuario no dispone de permisos de administración". (p.7)

A partir de lo anterior se denota la importancia que cobra el poder brindarles a diferentes empresas información que les permita utilizar prácticas seguras para protegerse ante posibles ciberataques. Es por esto que el CSIRT-CV (2018) incluye una propuesta priorizada de medidas de seguridad a aplicar (p.7):

- Instalación del sistema operativo desde una fuente fiable.
- Sistema operativo y aplicaciones actualizadas.
- Software antivirus.
- Cuentas de usuario sin permisos para instalar software.
- Control de acceso robusto.
- Configuraciones seguras en aplicaciones (navegación web, correo electrónico, etc.).

- Software antirootkits.
- Control de software original.
- Cifrado del disco. (p.7)

El CSIRT-CV (2018) afirma que es de gran importancia al menos contar con un equipo protegido frente a los posibles peligros o amenazas que se pueden encontrar en la red, enlistando los principales consejos para mantener un equipo protegido (p.12):

- Disponer de un antivirus
- Utilizar un equipo actualizado.
- Utilizar contraseñas robustas.

Así mismo, se debe de mantener una configuración con un cifrado en la conexión Wifi que se esté utilizando, así como estar pendientes de cambiar las credenciales de inicio de sesión y la contraseña del router. Es de suma importancia bloquear los dispositivos cuando no se encuentren cerca de los mismos, así como utilizar los servicios corporativos para los correos y todo lo que sea referente al trabajo (Grustniy, 2020).

Es por lo anterior que se presentan dos soluciones factibles a utilizar; la solución basada en la nube para teletrabajar de forma segura la cual consiste en la utilización del acceso remoto a la nube, accediendo desde cualquier lugar y con medidas de seguridad como el doble factor de autenticación y la trazabilidad total de las conexiones realizadas por usuarios remotos y la solución basada en los sistemas locales para teletrabajar de forma segura que consiste en desplegar equipos en los que se use internet como medio de acceso seguro a los servicios corporativos requiriendo de múltiples mecanismos de seguridad (LISA Institute, 2020).

A continuación, se presenta una lista de 11 consejos de protección ante amenazas cibernéticas para teletrabajar de forma segura, planteadas por LISA Institute (2020):

1. Evitar navegar por páginas sin https, Deep Web o la Dark Web.
2. Evitar realizar pagos online y, si lo haces, ten en cuenta los consejos de prevención del phishing y los consejos de seguridad bancaria online.
3. Evitar o limitar el acceso de equipos conectados entre sí o con la misma red, para evitar los riesgos de los wearables y el IoT.
4. Tener instaladas las últimas actualizaciones del sistema operativo.
5. Tener activados servicios de monitorización con alertas definidas.
6. Revisar los registros y auditorías de las conexiones remotas.
7. Restringir el montar unidades mapeadas del organismo en equipos remotos inseguros.
8. Evitar las opciones de “Split-Tunneling” en equipos inseguros o que no cumplan todas las medidas de seguridad.
9. Revisar o tener más vigiladas unidades para intercambiar información.

10. Asegurar si los antivirus escanean los dispositivos USB conectados a los equipos remotos o si se bloquea el acceso de USB en dichos equipos.
11. Tener actualizado el listado de personas que pueden acceder remotamente a los equipos de la organización con la dirección IP de acceso y medio de conexión. (párr.15)

Ventajas del uso de la seguridad informática

Según el INCIBE (Instituto Nacional de Ciberseguridad) (2018) existen diferentes ventajas con respecto al uso de prácticas de ciberseguridad, las cuales se señalan a continuación:

- Mejora la confianza de clientes y proveedores.
- Mejora de la imagen corporativa, tanto a nivel interno, como externo.
- Evita pérdidas de servicio (y por lo tanto, económicas y de imagen), derivadas de una caída o mal funcionamiento de los sistemas de información.
- Optimiza la ejecución de procesos.
- Disminuye la cantidad de incidentes de seguridad.
- Gestiona riesgos.
- Cumplen la normativa para evitar sanciones administrativas.
- Asegura la integridad y privacidad de la información de un sistema informático y sus usuarios. (párr.5)

Es importante resaltar que a nivel internacional el e-Governance Academy, a partir de la *Figura 1* nos muestra una calificación acerca de los países con mayor ventaja en el manejo de la ciberseguridad, a partir de parámetros como el nivel de preparación de prevención de ataques, la implementación de políticas y educación y profesionales en el área, entre otros.

Rank	Country	National Cyber Security Index	Digital Development Level	Difference
1.	Greece	96.10	65.44	30.66
2.	Czech Republic	92.21	69.37	22.84
3.	Estonia	90.91	79.27	11.64
4.	Lithuania	88.31	70.95	17.36
5.	Spain	88.31	73.24	15.07

Figura 1

International Cibersegurity Ranking

Fuente: e-Governance Academy, 2020.

En primer lugar, se encuentra Grecia con un 96.10% según la medición anteriormente mencionada. En segundo lugar, está República Checa con un 92,21% y en tercer lugar se encuentra Estonia con un 90.91 %. Al contrario de los últimos datos, Costa Rica se encuentra muy lejos de cumplir a cabalidad los parámetros establecidos por el NCSI, encontrándose en el puesto 48 del ranking, con un porcentaje de 53,25% (e-Governance Academy, 2020).

Desventajas del uso de la seguridad informática

La ciberseguridad en términos generales ha sido una herramienta beneficiosa para todas las personas que utilizan dispositivos electrónicos y guardan su información personal y laboral en ellos. Sin embargo, existen algunas desventajas sobre el uso de estas prácticas, las cuales Julio (2016) menciona a continuación (párr.5):

- La seguridad absoluta es imposible y la seguridad informática es un conjunto de técnicas encaminadas a obtener altos niveles en los sistemas informáticos.
- En los equipos de cómputo más desactualizados un antivirus realmente efectivo puede ser muy pesado, puede hacerlos más lentos y ocupar mucho espacio en la memoria.
- Los requisitos para la creación de contraseñas son cada vez más complejos, la mayoría de los sitios web requieren inicio de sesión, y el cambio de contraseñas con frecuencia se ha vuelto obligatorio en muchos lugares de trabajo, recordarlas en ocasiones es muy difícil.

Otra desventaja es la necesidad que existe de capacitar al personal de las empresas en el manejo adecuado de las herramientas tecnológicas, ya que en ocasiones estas empresas no cuentan con capital y los dispositivos para implementar la ciberseguridad en el teletrabajo.

Protocolos de seguridad informática

Janssen (2019) nos ayuda a entender en que consisten los protocolos de seguridad basados en VPN. Una VPN “cifra tus datos antes de enviarlos a los servidores de la VPN. El sistema que es el responsable de este cifrado se conoce usualmente como protocolo de cifrado o protocolo VPN” (párr.2).

Entre los protocolos VPN más populares se encuentran los siguientes recopilados por Janssen (2019):

- **OpenVPN:** entre los protocolos destaca por atribuir un fuerte cifrado ofreciendo alta seguridad, actualmente es compatible con gran cantidad de softwares en el mercado y sistemas operativos, por su procesamiento es necesario aplicarlo con software adicionales.
- **PPTP:** Se encuentra entre los protocolos mas antiguos de VPN y su primera compatibilidad con Windows genero un gran auge en su uso, pero se ha logrado encontrar fallos de

seguridad a la falta de un cifrado de alto nivel, por su parte es más rápido y fácil de usar pero su falta de cifrado es un gran blanco para hackers.

- **L2TP/IPSec:** el protocolo de túnel capa 2 que al igual que el PPTP no posee una encriptación por lo que se debe complementar con IPSEC protocolo de encriptación agregado, por motivos de utilizar estos 2 protocolos es mas lento a nivel de comunicación en la actualidad, posee una gran compatibilidad con muchos sistemas operativos, a pesar de sus métodos de encriptación se ha encontrado vulnerabilidades por su antigüedad.
- **IKEv2:** aumenta la seguridad del L2TP aplicando métodos de claves adicionales los cuales deben ser ingresado por los administradores de red las claves o contraseñas que se apliquen repercutirán en el aumento o carencia de la encriptación del VPN, no pose gran compatibilidad como los demás protocolos.
- **Wireguard:** es el protocolo mas nuevo el cual aun se encuentra en desarrollo, en las pruebas de benchmarks realizadas es el protocolo más rápido del mercado, solo se recomienda en ambientes de experimentales ya que todavía no se encuentra completo por lo que no es compatible con la mayoría de los software y sistemas operativos. (párr.10)

Por último, es de gran importancia comprender que el trabajo está acompañado de muchos riesgos a nivel tecnológico por el uso de los diferentes dispositivos electrónicos, es por lo que se considera una amenaza no tener prácticas de ciberseguridad a la hora de teletrabajar. El aumento de teletrabajo ha producido una gran oleada de ciberataques y nace de ahí la necesidad de tomar medidas de seguridad que garanticen un teletrabajo seguro tanto para las empresas como para sus trabajadores (LISA Institute,2020).

Metodología de la investigación

La presente investigación se realiza bajo un enfoque cuantitativo ya que este utiliza la recolección de datos numéricos para lograr comprobar la hipótesis de investigación planteada. (Hernández, Fernández, Baptista, 2016). Es preciso mencionar que a partir de este método se podrán recolectar datos de una mayor cantidad de participantes, lo cual dará un mayor panorama de la realidad actual en cuanto al uso de prácticas de ciberseguridad en la modalidad de teletrabajo.

El tipo de investigación será descriptivo, ya que según Hernández, Fernández y Baptista (2014) los estudios de alcance descriptivos pretenden describir fenómenos y especificar las características de estos, entendiendo que “pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, su objetivo no es indicar como se relacionan estas” (p.92). De esta manera se entiende que la presente investigación no busca relacionar variables, sino de una forma más clara, describir la única variable presente en la misma, y describir su comportamiento en un determinado momento del tiempo.

Para la recolección de la información se utilizará una muestra representativa de 50 personas de empresas que hoy en día utilizan la modalidad de teletrabajo y a la vez diferentes prácticas de seguridad para su implementación. Es por esto, que se utilizará una muestra probabilística, para que la población general (las diferentes empresas), cuente con la misma posibilidad de ser elegida. El tipo de muestreo será por racimos ya que este permitirá poder elegir en primer lugar al azar por muestreo simple, diferentes provincias, y a partir de esto, elegir al azar diferentes empresas de estas (Hernández, et al, 2016).

En cuanto al instrumento de recolección de datos a utilizar se encuentra el cuestionario, ya que es el más idóneo para la obtención de datos a nivel numérico y poder organizar los datos bajo el método cuantitativo. El cuestionario según Chasteauneuf (2009) citado por Hernández, et al (2016) consiste en "un conjunto de preguntas respecto de una o más variables a medir" (p.217) es por lo que, para la presente investigación se realiza un cuestionario virtual anónimo de 15 preguntas a través de la plataforma Google Forms para un mayor alcance de la población. Es preciso resaltar el anonimato de las empresas que responderán el cuestionario, ya que ninguna de estas puede exponer la forma en que se protegen a nivel de redes por la delicadeza de la información.

A partir del planteamiento del problema de investigación y de los objetivos se planteó la siguiente hipótesis: Las empresas que se encuentran en modalidad de teletrabajo por la pandemia de COVID-19 y la rapidez con la que tuvieron que aplicar el mismo, no cuentan con las herramientas necesarias como el conocimiento o soporte en ciberseguridad para proteger su información de posibles ataques cibernéticos.

Análisis de resultados

Como instrumento para la recolección de datos se utilizó la encuesta, ya que esta favoreció a que el proceso de estos fuera más viable para las empresas. En total 51 usuarios de diferentes empresas, que pertenecen al área técnica o de jefatura, completaron la encuesta, acordando que los datos ingresados serían anónimos por motivos de seguridad.

Es de gran importancia poder interpretar los datos que se presentan a continuación por medio de gráficas. De los 51 usuarios pertenecientes a diversas empresas de la GAM, a partir de la *figura 2* se conoce que un 88.2 % se encuentran en modalidad de teletrabajo, mientras que un 11.8% continúan en modalidad presencial.

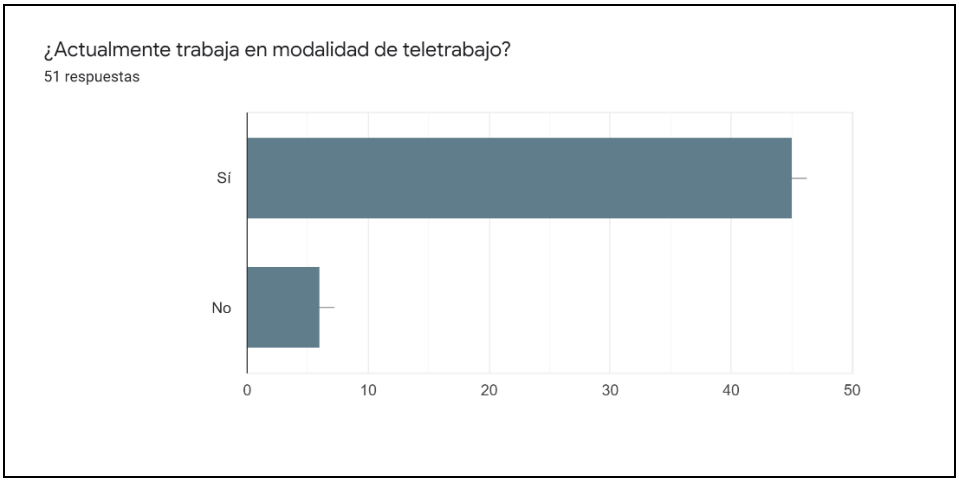

Figura 2. Modalidad de teletrabajo

Fuente: Elaboración propia, 2020.

Así mismo, a partir de la *Figura 3*, la muestra señaló que 28 empresas cuentan con más de un 75% de la población total de cada una de las empresas realizando teletrabajo.

Figura 3. Porcentaje de usuarios en teletrabajo.

Fuente: Elaboración propia, 2020.

Por otra parte, a partir de la *Figura 4*, se observa que la población meta señaló que un 41,2% de la totalidad de empresas fue capacitada en temas de ciberseguridad para la modalidad de teletrabajo, mientras que un 58.8% no obtuvo ningún tipo de capacitación al respecto.

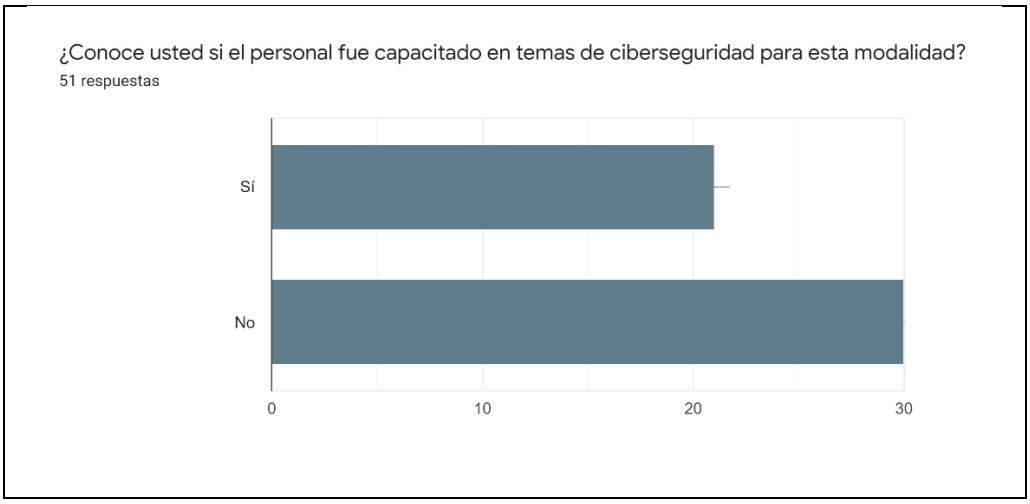

Figura 4. Capacitación en temas de ciberseguridad**.**

Fuente: Elaboración propia, 2020.

A partir de la *Figura 5*, se puede observar que el 84.3% de la población utilizan VPN para ingresar a los datos institucionales, mientras que un 15,7% no utilizan el mismo.

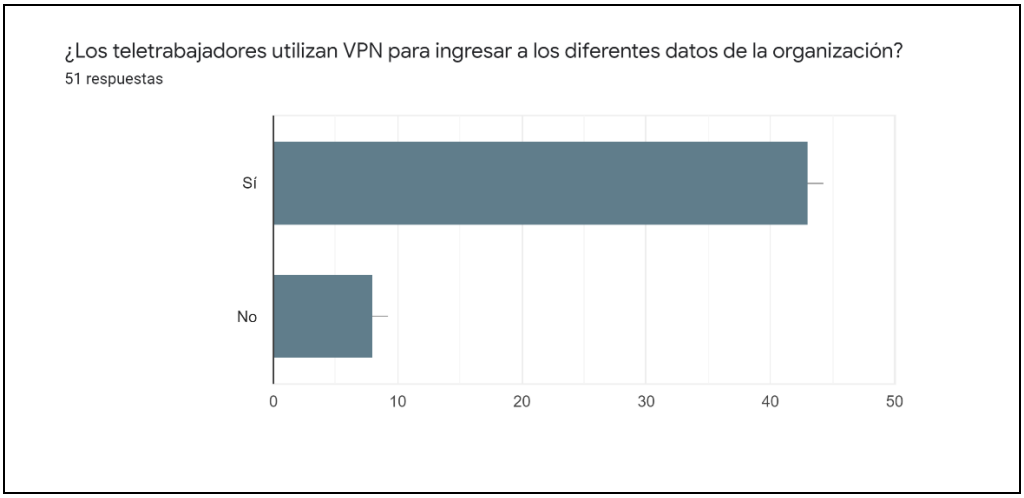

Figura 5. Utilización del VPN.

Fuente: Elaboración propia, 2020.

Con respecto al gráfico anterior, la *figura 6* nos señala que dentro de las empresas que sí utilizan VPN, predomina la utilización del IPSec, así como la del Open VPN (SSL). Es preciso mencionar que el protocolo menos utilizado por las empresas es el L2TP.

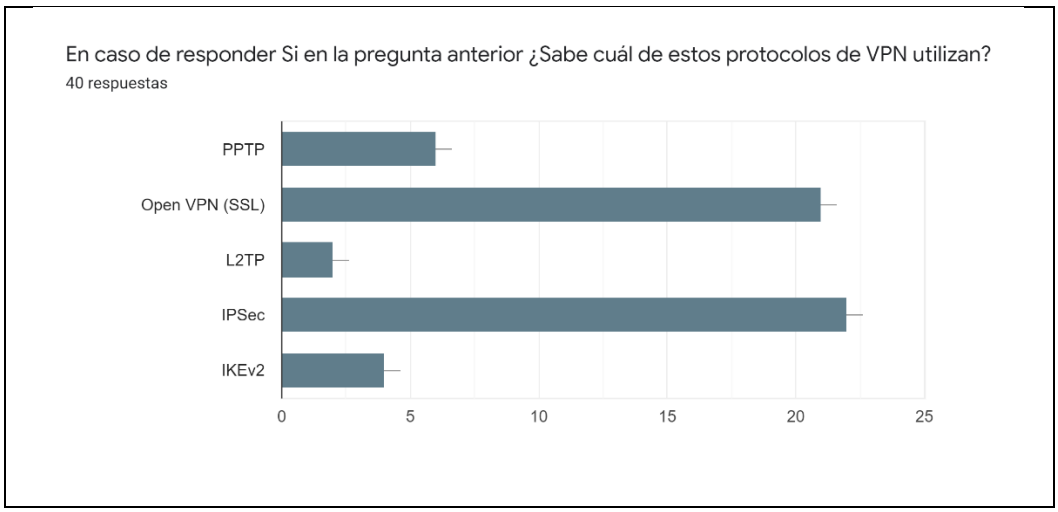

Figura 6. Protocolos de VPN más utilizados.

Fuente: Elaboración propia, 2020.

Es preciso mencionar que a partir de la *Figura 7*, se puede visualizar que un 62,7 % de la población meta utiliza máquinas institucionales para teletrabajar mientras que un 9,8% utiliza máquinas personales.

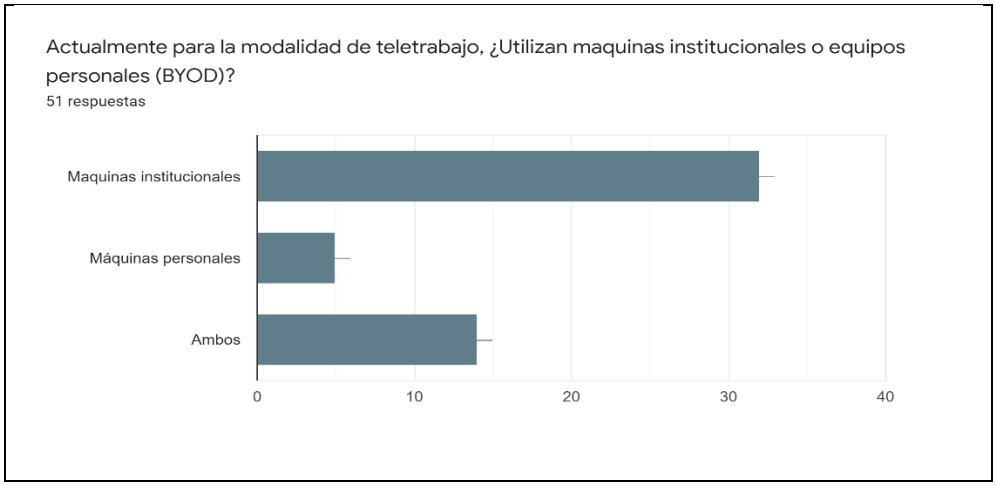

Figura 7. Dispositivos electrónicos utilizados en el teletrabajo.

Fuente: Elaboración propia, 2020.

A partir de la *Figura 8* se puede visualizar que las herramientas de protección cibernética más utilizadas son en primer lugar el antivirus con un 86.3 %, seguidamente en segundo lugar el VPN con un 72,5% y en tercer lugar el control de filtrado web con un 52,9%.

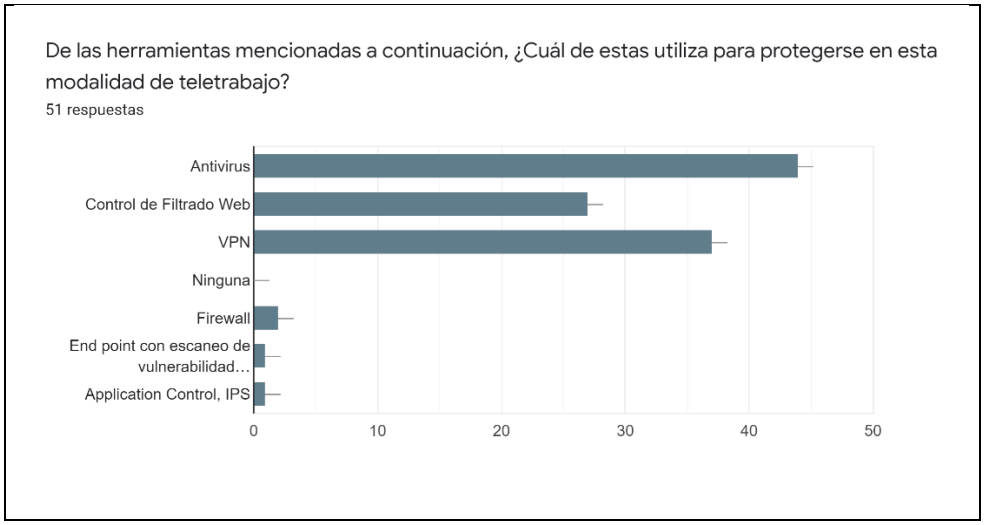

Figura 8. Herramientas de protección cibernética.

Fuente: Elaboración propia, 2020.

A partir de la *Figura 9* se puede visualizar como 44 empresas utilizan el acceso remoto para realizar teletrabajo mientras que únicamente 7 empresas no hacen uso de este.

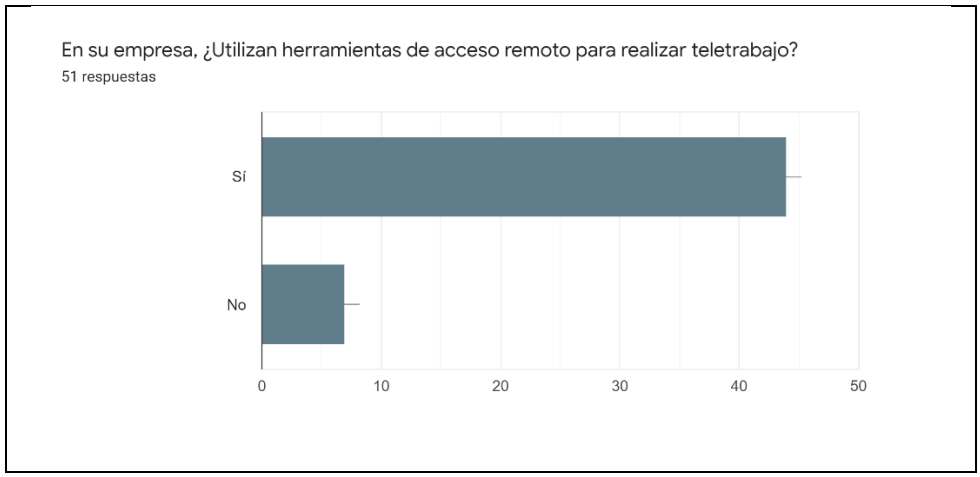

Figura 9. Utilización de acceso remoto.

Fuente: Elaboración propia, 2020.

Por otra parte, como se presenta en la *Figura 10*, un 90% de las empresas están interesadas en conocer más prácticas de ciberseguridad.

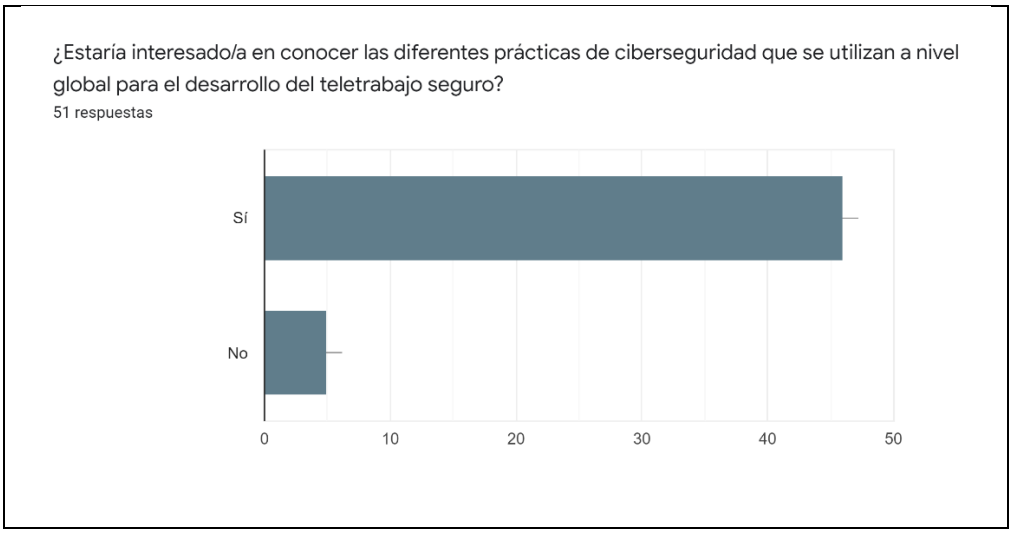

Figura 10. Interés en conocer prácticas de ciberseguridad.

Fuente: Elaboración propia, 2020.

Por último, La *Figura 11*, nos indica que un 66% de las empresas poseen controles o registros de seguridad de los usuarios que se encuentran en modalidad de teletrabajo mientras que un 34% del total de empresas no poseen los mismos.

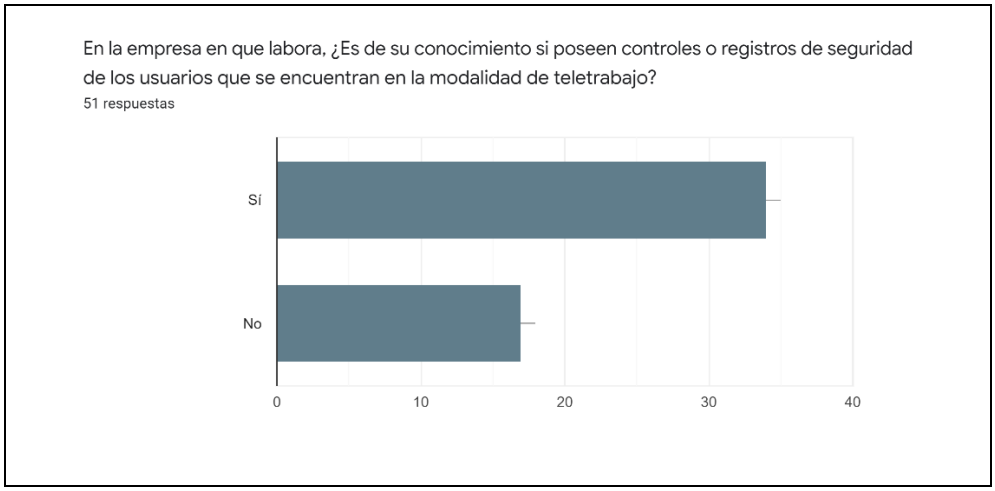

Figura 11. Control de seguridad de los usuarios en teletrabajo.

Fuente: Elaboración propia, 2020.

Discusión

A partir de la recopilación de datos por medio de una encuesta aplicada a 51 empresas diferentes y de la búsqueda de referencias bibliográficas e información fundamental acerca de la ciberseguridad, se puede responder a la hipótesis planteada argumentando que a pesar de que las empresas que se encuentran en teletrabajo por la pandemia de COVID-19 tuvieran que utilizar esta modalidad de manera tan repentina, casi un 50% de estas si cuentan con las herramientas necesarias para proteger su información de posibles ataques cibernéticos.

Es preciso señalar la modalidad de trabajo predominante en el total de empresas entrevistadas, ya que, según la encuesta, un 88,2% de las empresas se encuentran aplicando la modalidad de teletrabajo. Así mismo es importante indicar que un total de 28 empresas mencionaron tener un 75% o más de sus empleados laborando bajo esta modalidad. Por lo que se puede entender que a partir de la pandemia por COVID-19, ha aumentado la modalidad de teletrabajo y por ende la cantidad de ciber ataques (LISA Institute, 2020)

A partir de la encuesta, se encontró que el 12% de las empresas no poseen personal en informática lo cual denota la necesidad de que en las empresas haya profesionales capacitados en estas áreas para reducir el riesgo al que pueden estar expuestos los sistemas informáticos. También, es importante señalar que el departamento más proliferante entre las empresas es el de soporte (encargado de la ayuda a los usuarios y mantenimiento informático) con un 82 % de empresas que cuentan con el mismo, sin embargo, este departamento no cuenta con el conocimiento o el expertis para verificar la fiabilidad, el control y la confidencialidad de los datos, como si lo tienen los departamentos de seguridad, que según la encuesta solo un 50% de las empresas cuentan con el mismo. Esta información es realmente preocupante ya que, a nivel nacional es de conocimiento que los ciber ataques siguen en aumento y esto podría causar grandes inconvenientes en las diferentes empresas como bien lo mencionó el gerente de Fortinet, Joaquín Martínez (La prensa Latina, 2020).

Con respecto a los datos anteriores en los que se indica que un 50% de las empresas cuentan con un departamento de seguridad, es preciso retomar que aún así existen flaquencias en el conocimiento sobre ciberseguridad que poseen los teletrabajadores, ya que por medio de la encuesta se comprobó que un 58.9% de la empresas no ha realizado capacitaciones formales acerca de métodos de ciberseguridad aplicados al teletrabajo, así también como mencionan que el 52% de las empresas nunca han recibido charlas de ciberseguridad en términos generales dándonos un panorama preocupante en términos de falta de capacitación en el tema, tomando en cuenta que al utilizar eficazmente las prácticas de ciberseguridad y al tener conocimiento en el área se pueden reducir riesgos y asegurar la integridad y privacidad de la información de los sistemas informáticos y de sus los teletrabajadores (INCIBE, 2018).

A partir de la información técnica recopilada con respecto a los diferentes métodos de protección aplicados se observa que el 84.3% de las empresas implementan VPN para realizar teletrabajo, lo que quiere decir que los teletrabajadores tienen una conexión desde sus casas hasta los servidores de sus empresas ya que el VPN cifra los datos antes de enviarlos a los servidores (Janssen, 2019).

Es importante entender que el VPN contiene diferentes protocolos, los cuales pueden brindar mayor o menor seguridad en la encriptación de los datos. En relación estos protocolos de seguridad se encuentran como predominantes los protocolos IPSec y SSL, estando ambos en los mayores estándares a nivel mundial en ciberseguridad por su nivel de encriptación, sin embargo, todavía se encuentra algunas empresas, formando estas un 20.5%, que todavía utilizan protocolos desactualizados como lo son el L2TP y el PPTP teniendo un latente riego en términos de seguridad por sus problemas de encriptación (Janssen, 2019).

Con respecto al uso de dispositivos personales e institucionales, la encuesta señala que un 38% de las empresas permiten el uso de máquinas personales para realizar teletrabajo, esto confiando en el estado de estas máquinas y los protocolos o herramientas de ciberseguridad que los usuarios implementen en sus dispositivos. Aunado a lo anterior, la encuesta señala que existe un 66% de empresas que tienen controles de ciberseguridad para sus teletrabajadores, mientras que a la vez señala que hay un 34% de empresas que no poseen controles de los niveles de ciberseguridad de sus trabajadores. Entre las herramientas de protección más utilizadas se encuentran el antivirus con un 86,3% y el filtrado Web con un 52,9%, entendiendo que estas deben de ser las herramientas priorizadas al momento de elegir controles de seguridad (CSIRT-CV, 2018).

Es preciso señalar que, a partir del total de empresas encuestadas, 44 de éstas utilizan el acceso remoto para realizar teletrabajo mientras que únicamente 7 de estas no lo utilizan. Para poder implementar una solución de acceso remoto en los dispositivos electrónicos, se requiere de la aplicación de soluciones que se desplieguen de sistemas locales, los cuales necesitan de personal e infraestructura adecuadas para su implementación. Lo anterior representa un inconveniente en cuanto al desarrollo de prácticas seguras en las empresas debido que no todas poseen lo necesario para cumplir con los estándares mínimos de seguridad o incluso personal que le pueda brindar seguimiento a posibles riesgos (lo que posiblemente puede estar afectando al porcentaje de empresas que no lo utilizan). Es por esto que aún existen empresas sin prácticas de seguridad y cada vez es un reto más grande para las empresas poder implementarlas y evitar vulnerabilidades por malware**s**, botnet**s,** ransomware**s,** suplantaciones de identidad, entre otras (LISA Institute, 2020, párr.6).

Por último, un 90 % de las empresas encuestadas se encuentran interesadas en conocer más prácticas de ciberseguridad para la posible implementación de estas en un futuro próximo. Por lo que resulta realmente necesaria la creación de un manual con recomendaciones de ciberseguridad para las empresas, por el cual responde este informe escrito.

Conclusiones y recomendaciones

A partir de esta investigación se pueden concluir diferentes puntos los cuales se mencionarán a continuación:

- Se concluye que las diferentes prácticas de seguridad informática más utilizadas en Costa Rica en la modalidad de teletrabajo son la utilización de VPN, el uso de antivirus

y el filtrado web, siendo estas de utilidad, sin embargo, no cuentan con todas las herramientas para asegurar la información y la integridad de las empresas. Es por esta razón, que se deben de aplicar las mejores prácticas de ciberseguridad, así como varias de estas al mismo tiempo para aumentar la eficacia de protección de los datos y de los usuarios en modalidad de teletrabajo.

- Se comprueba que existen muchas ventajas en cuanto a la utilización de seguridad informática durante la modalidad de teletrabajo tanto a nivel nacional como internacional, ya que esto les permite a las empresas reducir el riesgo ante ciber ataques, puede mejorar la confianza de sus clientes, optimiza el planteamiento y la ejecución de procesos a nivel remoto y asegura la privacidad de los sistemas y de los usuarios.
- Se concluye a partir de la recopilación de la información y de la aplicación de las encuestas que los protocolos de seguridad informática más utilizados a nivel nacional e internacional son el IPSec, y el Open VPN (SSL) ya que estos cuentan con mayor encriptación de los datos, así como con mayor compatibilidad con diferentes sistemas operativos lo que hace más viable el acceso con clientes y proveedores.
- Es necesario que desde las empresas surjan capacitaciones en temas de ciberseguridad en general y principalmente para los usuarios que se encuentren en la modalidad de teletrabajo ya que según los resultados de la encuesta se pudo evidenciar el gran vacío en términos de conocimiento sobre seguridad informática.
- Es de gran importancia, que las empresas cuenten con personal especializado en informática y en ciberseguridad ya que es una necesidad a nivel social, solventar la falta de información y de personal que pueda minimizar el riesgo de exposición de los datos.

Dentro de las recomendaciones que se pueden realizar a las diferentes empresas se encuentra la importancia de no utilizar los protocolos de VPN de L2TP y PPTP ya que estos cuentan con un gran nivel de vulnerabilidad y exponen los datos que viajan a través de estos.

Por otra parte, es preciso recomendar que las empresas implementen cada vez más controles de seguridad de los usuarios que se encuentren en modalidad de teletrabajo y utilicen dispositivos personales, ya que esto les permitirá mantener una mejor gestión de los datos, reducir los riesgos de ataques por infección de softwares maliciosos, o robo de información confidencial de los usuarios o a nivel empresarial.

En cuanto a la creación de un manual de protección de ciberseguridad en la modalidad de teletrabajo, es preciso recomendar algunas temáticas que deben de ser incluidas en el mismo, las cuales se presentan a continuación:

- Prácticas de seguridad informática.
- Ventajas del uso de la seguridad informática.
- Mejores Protocolos de seguridad VPN a nivel nacional e internacional.
- Herramientas Protección de ciberseguridad.

Referencias Bibliográficas

Banco Interamericano de Desarrollo. (2020). *CIBERSEGURIDAD RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE*. publications.iadb.org. Recuperado de: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Barrio, M. (2020). *INTERNET DE LAS COSAS*. www.editorialreus.es. Recuperado de: https://www.editorialreus.es/static/pdf/primeraspaginas_9788429020380_internetdelascosas.pdf

CSIRT-CV. (2018). *Guía de seguridad en el teletrabajo*. concienciat.gva.es, Recuperado de: https://concienciat.gva.es/wp-content/uploads/2018/03/infor_guia_de_seguridad_en_el_teletrabajo.pdf

Grustniy, L. (2020). *10 consejos de seguridad para el teletrabajo*. kaspersky.es, Recuperado de: https://www.kaspersky.es/blog/remote-work-security/22229/

e-Governance Academy. (2020). *National Cybersecurity Index.* Recuperado de https://ncsi.ega.ee/ncsi-index/?order=rank

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación.* (6a. ed.). México D.F.: McGraw-Hill

Holloway, C. (2020). *El estado de la seguridad IT en 2020: Las superficies de ataque se amplían y las personas nunca fueron tan importantes para la defensa*. itmastersmag.com. Recuperado de: https://itmastersmag.com/informes-whitepapers/el-estado-de-la-seguridad-it-en-2020-las-superficies-de-ataque-se-amplian-y-las-personas-nunca-fueron-tan-importantes-para-la-defensa/

INCIBE. (2018). *La ciberseguridad es cosa de todos, establece buenas prácticas*. INCIBE, Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/ciberseguridad-cosa-todos-establece-buenas-practicas

Janssen, D. (2019). *Comparación de protocolos VPN*. vpnoverview, Recuperado de: https://vpnoverview.com/es/informacion-vpn/protocolos-vpn/

Julio, I. (2016). *La seguridad informática, características, ventajas y desventajas*. Conocimiento Digital, Recuperado de: https://grupo4herramientasinformatica.blogspot.com/2016/03/la-seguridad-informatica.html

LISA Institute. (2020). *Medidas de seguridad para teletrabajar de forma segura*. www.lisainstitute.com. Recuperado de: https://www.lisainstitute.com/blogs/blog/medidas-de-seguridad-para-teletrabajar-de-forma-segura

Ministerio de Salud. (2020). *Tipos de teletrabajo*. Ministerio de Salud Costa Rica, Recuperado de: https://www.ministeriodesalud.go.cr/index.php/teletrabajo/tipos-teletrabajo

Parada Visual. (2020). *Teletrabajo: modalidades, regulación, ventajas y desventajas*. Paradavisual, Recuperado de: https://www.paradavisual.com/el-teletrabajo-modalidades-regulacion-ventajas-y-desventajas/

Prensa Latina (2020). *Costa Rica Recibió Más De 51 Millones De Intentos De Ciberataques*. El país.cr. Recuperado de: https://www.elpais.cr/2020/08/14/costa-rica-recibio-mas-de-51-millones-de-intentos-de-ciberataques/

Presidencia. (2020). *CASI 15 MIL FUNCIONARIOS SE ACOGIERON AL TELETRABAJO POR COVID-19*. presidencia.go.cr. Recuperado de: https://www.presidencia.go.cr/comunicados/2020/03/casi-15-mil-funcionarios-se-acogieron-al-teletrabajo-por-covid-19/

UNED. (2019). *Programa de Teletrabajo*. www.uned.ac.cr. Recuperado de: https://www.uned.ac.cr/viplan/teletrabajo/que-es-teletrabajo/historia

Anexos

Anexo 1

Enlace:
https://docs.google.com/forms/d/e/1FAIpQLSfLemr59h5UWzxPQqA1ieDSokx3lAoTG8c2NXH4xwy5qNyQIw/viewform

Encuesta:

1. Actualmente trabaja en modalidad de teletrabajo:

a. Si

b. No

2. Qué porcentaje de usuarios de la organización se encuentra en teletrabajo:

a. 0-25%

b. 25-50%

c. 50%-75%

d. 75%-100%

3. ¿Conoce usted si el personal fue capacitado en temas de ciberseguridad para esta modalidad?

a. Si

b. No

4. ¿Los teletrabajadores utilizan VPN para ingresar a los diferentes datos de la organización?

a. Sí

b. No

5. En caso de responder Si en la pregunta anterior ¿Sabe cuál de estos protocolos de VPN utilizan?

a. PPTP

b. Open VPN (SSL)

c. L2TP

d. IPSec

e. IKEv2

6. Actualmente para la modalidad de teletrabajo, ¿Utilizan máquinas institucionales o equipos personales (BYOD)?

a. Máquinas institucionales

b. Máquinas personales

7. De las herramientas mencionadas a continuación, ¿Cuál de estas utiliza para protegerse en esta modalidad de teletrabajo?

a. Antivirus

b. Control de Filtrado Web

c. VPN

8. ¿Cree usted que la modalidad de teletrabajo aumenta las probabilidades de riesgo de su

seguridad informática?

a. Sí

b. No

9. En su empresa, ¿Utilizan herramientas de acceso remoto para realizar teletrabajo?

a. Si

b. No

10. De las siguientes subdivisiones departamentales de la informática ¿Con cuales cuenta su empresa actualmente?

a. Departamento de soporte

b. Departamento de redes

c. Departamento de seguridad

e. Departamento de infraestructura

11. Seleccione la cantidad de personal de informática con el que cuentan en su empresa.

a. 0 - 1

b. 2 - 5

c. 6 - 9

d. 10 - 15

e. 15 – más

12. ¿Estaría interesado/a en conocer las diferentes prácticas de ciberseguridad que se utilizan a nivel global para el desarrollo del teletrabajo seguro?

a. Sí

b. No

13. En la empresa en que labora, ¿Es de su conocimiento si poseen controles o registros de seguridad de los usuarios que se encuentran en la modalidad de teletrabajo?

a. Sí

b. No

14. En la empresa en que labora, ¿Han impartido capacitaciones acerca de ciberseguridad o charlas acerca de las mejores prácticas de seguridad y cómo implementarlas?

a. Sí

b. No

15. De la siguiente escala, ¿Qué tan confiado/a se siente al ingresar, compartir y manejar los datos de forma remota en teletrabajo?

a. Desconfiado

b. Poco confiado

c. Indiferente

d. Confiado

e. Muy confiado