ANÁLISIS DE CIBERSEGURIDAD SOBRE LAS VULNERABILIDADES QUE SE PUEDEN PRESENTAR CON EL TELETRABAJO.

CYBERSECURITY ANALYSIS OF THE VULNERABILITIES THAT MAY ARISE WITH TELEWORKING.

Nombres y Apellidos

Andrés Danilo Arévalo Morales

Camilo Andrés Buitrago Ropero

Especialista en seguridad informática

Director

Hector Manuel Herrera

RESUMEN

La modalidad de trabajo en casa o teletrabajo es una tendencia que creció exponencialmente desde el inicio de la pandemia del COVID 19, lo cual deriva en uno de los tantos retos que tiene la ciberseguridad ante diversos riesgos y amenazas latentes. Cada día los ciberdelincuentes se idean

nuevas formas de ataque para afectar un sistema o simplemente robar información, es por ello que se quiere identificar las diferentes amenazas y vulnerabilidades que existen y pueden ser un riesgo para un empleado que trabaja desde casa y derivar en un impacto considerable para las organizaciones.

Palabras clave: Información, seguridad, informática, VPN, autenticación, internet, vulnerabilidad, amenaza, ciberdelincuentes, teletrabajo

ABSTRACT

The modality of working at home or telecommuting is a trend that has grown exponentially since the beginning of the COVID 19 pandemic, which results in one of the many challenges that cybersecurity has in the face of various risks and latent threats. Every day cybercriminals devise new forms of attack to affect a system or simply steal information, which is why they want to identify the different threats and vulnerabilities that exist and can be a risk for an employee who works from home and lead to an impact significant for organizations.

Keywords: information, security, computing, VPN, authentication, internet, vulnerability, threat, cybercriminal, telecommuting

INTRODUCCIÓN

Desde la propagación del virus COVID año 2019 la humanidad se ha ajustado a nuevos hábitos entre ellos la manera en que trabajamos, desde el inicio de la pandemia las corporaciones tomaron diversas medidas entre ellas que sus empleados trabajen desde casa, esto originó en un ahorro de infraestructura para las empresas lo cual beneficia en términos de utilidades.

Pero cabe resaltar si las empresas se han preguntado ¿los empleados son conscientes de la importancia de la ciberseguridad mientras trabajan en modo de teletrabajo? Es allí donde se quiere

explorar si un empleado que trabaja desde su casa tiene el conocimiento de los riesgos y amenazas a las cuales está expuesta la información y los activos de la compañía, adicional a esto saber si conocen las diferentes prácticas de la seguridad informática y si estas se están aplicando.

Este artículo quiere además de exponer las vulnerabilidades a las que se expone un empleado en casa, quiere brindar una serie de recomendaciones para la protección de los datos frente a múltiples amenazas y ataques.

La seguridad digital en los nuestros hogares es un problema mayor impacto y que las autoridades regulatorias de las comunicaciones y las TIC en Colombia, están dejando a un costado por su relevante importancia ya que no han contemplado o manifestado a la opinión pública las vulnerabilidades que puede tener hoy en día nuestra información personal, profesional, familiar y laboral. Por lo tanto, para estos organismos de control el seguimiento y la regularidad jurídica a lo que nos vemos vulnerados no ha generado metástasis en sus estadísticas, pero vemos con preocupación el incremento de las nuevas modalidades de trabajo, educación y transacciones que día a día realizamos desde nuestros escritorios.

Como resultado de la investigación se plantea una propuesta para el desarrollo de una guia el cual ayude a fomentar conocimientos y culturizar al trabajador con la ciberseguridad, con el fin tener el buen uso de las herramientas tecnológicas que se tienen en el ambiente de teletrabajo y así crear un espacio más seguro y confiable frente a los delitos informáticos que hoy en día se ven más expuestos por los ciberdelincuentes.

Descripción del planteamiento de trabajo.

Teniendo el conocimiento de este problema que nos aqueja a todos los cibernautas planteamos una ejecución del plan de trabajo que consiste en fomentar y crear la concientización que debemos tomar en los riesgos de seguridad, a los cuales estamos expuestos haciendo uso de los equipos de cómputo corporativos fuera de la red empresarial y exponiendo información sensible y confidencial que manipulamos donde afecta directamente e indirectamente la integridad de la información de la compañía.

Pregunta investigación

¿Por medio de la propuesta de una guía de buenas prácticas de ciberseguridad enfocada para el teletrabajo, se podrá disminuir los riesgos y vulnerabilidades que existen en el ciberespacio?

Objetivo general.

- Analizar las posibles vulnerabilidades en los sistemas informáticos están expuestos los teletrabajadores y proponer una guía con buenas prácticas sobre ciberseguridad.

Objetivos específicos

- Identificar riesgos, amenazas y los ataques informáticos más comunes a los cuales un empleado está expuesto en la modalidad de teletrabajo.
- Analizar el nivel de conocimiento sobre seguridad y exponer diversas destrezas para mitigar, reportar y evitar ataques informáticos como el Phishing y robo de contraseñas.
- Construir una guía de buenas prácticas para la seguridad en el teletrabajo basada en la norma ISO 270001:2013

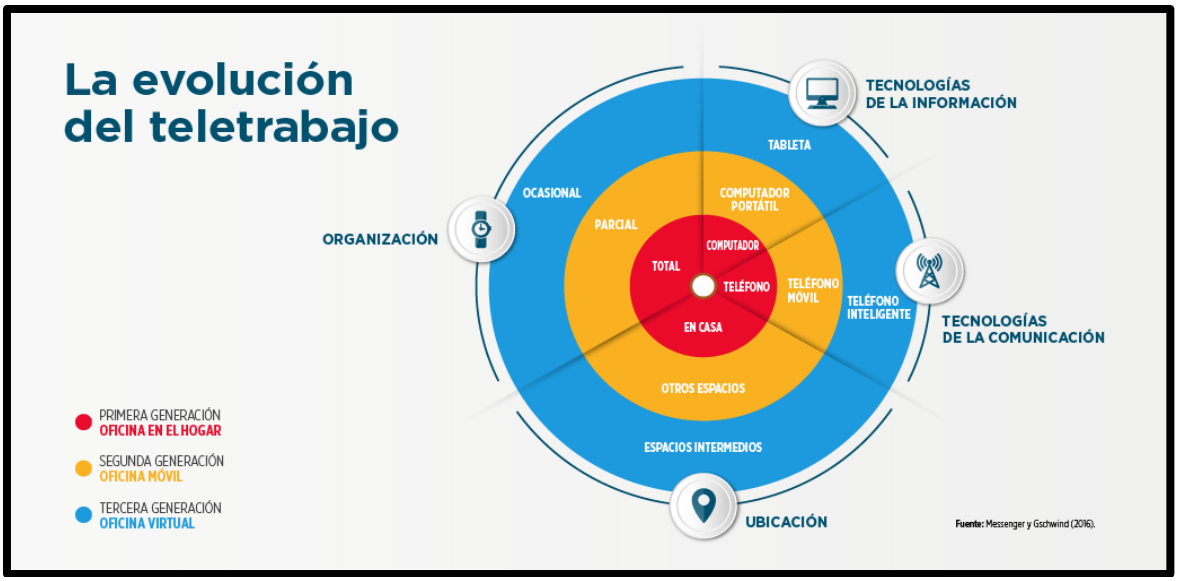
Alcance

Se propone en este artículo plantear una guía de buenas prácticas para el teletrabajo basados en el cumplimiento de la norma ISO 270001:2013 (A 6.2.1, A 6.2.2 y A 7.2.2) Política de dispositivos móviles, teletrabajo y Sensibilización, educación y formación en Seguridad de la Información con el fin de preservar la confidencialidad, la integridad y la disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos, esto nos permitirá tener una culturización efectiva con los teletrabajadores sobre la importancia del activo más importante de las empresas que es
la información.

Contexto

Se aborda una preocupación sobre la importancia de la seguridad de la información en el ámbito de los empleados que están laborando en la modalidad de teletrabajo y determinar qué tan preparados están sobre la seguridad y si conocen las prácticas para salvaguardar la información y los activos de las organizaciones.

Ilustración 1 La evolución del teletrabajo



Autor 1 https://blogs.iadb.org/, s.f.)

REFERENTES TEÓRICOS

¿En qué nos preocupamos para llegar a la solución del problema?

El tener acceso remoto a la información y a los servicios de las empresas con el menor índice de riesgo posible, es hoy en día el mayor reto de seguridad al que se enfrentan las compañías. Para ello, la solución más eficaz y comúnmente adoptada es la implementación de redes privadas virtuales (VPN, Virtual Private Network), pero no solo basta con la implementación de este modelo de conexión, si pensamos que cada vez hay mayor incidencia de ciberataques sofisticados

y por tanto sus tasas de éxito son mayores.

La mayor incidencia de riesgos se da en pequeñas y medianas empresas, que por lo general no cuentan con personal especializado en ciberseguridad, ni con la culturización de los trabajadores comprendiendo el impacto al que se encuentran expuestos en el ciberespacio, llegando a representar casi el 43% de los ciberataques por la falta de controles e implementación de políticas de seguridad.

Esto no solo representa un riesgo de pérdida de información, sino con también daños económicos y de reputación institucional, tras la transformación digital acelerada por la pandemia y por la falta de implementación de controles de seguridad de la información y el poco bagaje de conocimiento para el desarrollo de técnicas de ciberdefensa y validando el nivel de vulnerabilidad y criticidad en el que nuestro país está expuesto a los ciberataques, según un informe soportado por la firma *Fortinet* Colombia tuvo 11.200 millones de ataques en el último año siendo así uno de los países de américa latina que más recibe ataques, adicional el 60% de las pequeñas compañías desaparecen dentro de los 6 meses siguientes a sufrir un ciberataque, por tal motivo vemos necesario la propuesta de una guía de ciberseguridad para conocer las amenazas y los riesgos a los que se enfrenta la empresa es fundamental establecer un esfuerzo que debe ser conjunto, empresa-empleado (CIBERSEGURIDAD, s.f.), (INFOBAE, 2022).

Es de suma importancia para cualquier persona tener conocimiento sobre la ciberseguridad, es importante que no solo los ingenieros o trabajadores en tecnología comprendan los diferentes conceptos sobre seguridad, amenazas, riesgos o medidas de seguridad informática, sino que también las personas del común u otras profesiones entiendan la importancia de tener a salvo los activos digitales si no que tengan claro los diferentes conceptos que pueden evitar ataques.

Amenazas:

Es un peligro latente sobre un medio tecnológico, ya sea físico o intangible que está en riesgo de un ataque.

Riesgo:

Se puede entender como la probabilidad de que algo ocurra y tenga un impacto negativo

Teletrabajo:

"Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación -TIC- para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio especifico de trabajo" (Articulo2, 2008)

Ciberdelincuente:

Es un tipo de criminal o delincuente el cual busca vulnerabilidades en la red, en dispositivos digitales con el fin de causar daño, ya sea el robo de información, daño a infraestructura tecnológica.

Gestor de contraseñas:

Es una herramienta de software que permite al usuario salvaguardar y permitir fácil acceso a sus contraseñas sin riesgo de perderlas o que lleguen a conocimiento de terceros, estas aplicaciones pueden ser gratis o de pago.

Phising:

Partiendo de que es un delito informático esta técnica es una de las más populares que se emplean por parte de los ciberdelincuentes, la cual consiste en engañar a su víctima para que comparta información confidencial, tales como números de tarjetas, contraseñas. la táctica más común en el Phishing es por medio de un correo electrónico o mensaje de texto donde se suplanta la identidad ya sea de una persona o de una compañía, allí la técnica es por medio de la intimidación es lograr que la víctima comparta información ya sea por urgencia o miedo a perder sus cuentas o accesos a alguna plataforma. (Malwarebytes, s.f.)

Backup:

Copia de seguridad que se realiza a archivos o aplicaciones contenidas en un ordenador o un medio de almacenamiento, con el fin de recuperar la información en caso de pérdida accidentales, daño

o falta a la integridad de la misma. (Ciberseguridad, 2018)

VPN “Virtual Private Network” (Red privada virtual)

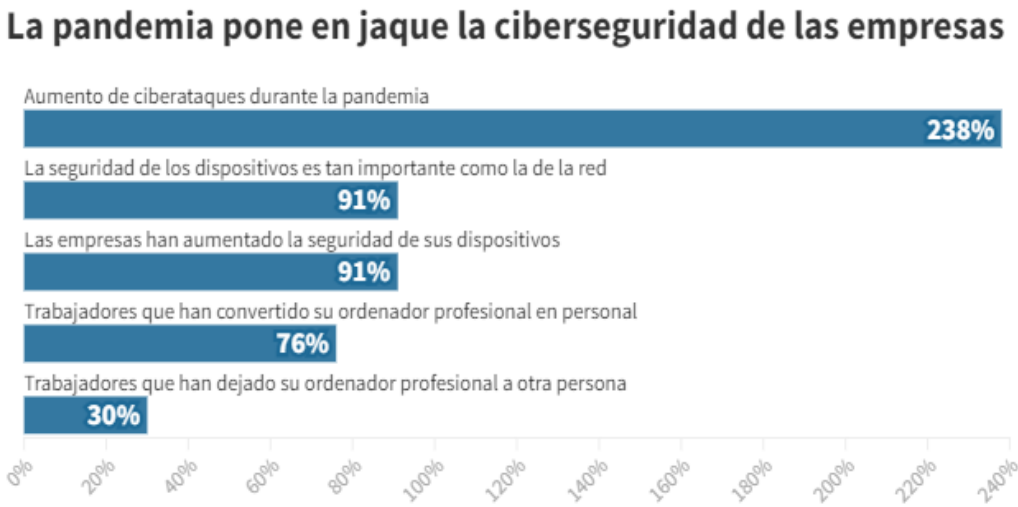
Es una red la cual permite utilizar una conexión pública segura y protegida. La VPN cifra el tráfico en internet disfrazando la identidad del usuario, esto para dificultar a los ciberdelincuentes puedan interceptar la conexión y vulnerar un sistema. (Kapersky, s.f.)

Antecedentes

La pandemia impuso en todo el mundo un aumento del teletrabajo, lo que incidió positivamente sobre la comodidad y la conciliación de muchos trabajadores, pero negativamente sobre su ciberseguridad.

Un informe (Blurred Lines & Blindspots) elaborado por HP, pone cifras a esta realidad. Según su investigación, el volumen de ciberataques al sector financiero, por poner un ejemplo, ha aumentado un 238% durante los meses más críticos de la pandemia (de febrero a abril de 2020). Las mayores víctimas de estos ataques han sido los trabajadores en remoto, más vulnerables ante este tipo de ofensivas, ya que los ciberdelincuentes no tenían por qué atacar a la red informática de la empresa, sino a los dispositivos de sus empleados. De hecho, el informe también revela que los dispositivos conectados a internet recibieron 1,5 ataques por minuto en todo el mundo en 2020. (Brands, 2022).

Ilustración 2 Volumen de Ciberataques al sector financiero



Autor 2 Infome realizado por Hewlett Packard

La historia del teletrabajo.

Lo que anteriormente se conocía como *Telecommuting* que fue usado para superar una crisis económica, gracias a los avances de la tecnología tanto las personas como las compañías han podido acceder a los grandes beneficios del teletrabajo (Brands, 2022)

El teletrabajo ha sido un gran avance para las compañías y empleados que pueden ejercer funciones y operaciones ahorrando por ejemplo costos de infraestructura, comodidad para los trabajadores. adicionalmente una solución para superar crisis para las empresas y personas que no cuentan con empleo que vieron en el teletrabajo una manera de ofrecer sus servicios (COMUNICACIONES, s.f.).

METODOLOGÍA

Para tener un análisis completo se determina el uso de la metodología de investigación con enfoques cualitativo y descriptivo el cual recolectó cuatro (4) etapas y se constituyen de la siguiente manera, ver ilustración 3.

Ilustración 3 Diagrama de metodología

Autor 3 Andrés Danilo Arévalo y Camilo Andrés Buitrago

- **Identificar vulnerabilidades en el teletrabajo**

Durante esta etapa se realiza un análisis para identificar las diversas vulnerabilidades y amenazas a las que un teletrabajador está expuesto y pondría en riesgo la seguridad de la infraestructura tecnológica de la compañía.

- **Evaluación de conocimientos en ciberseguridad.**

En esta etapa se realiza una encuesta con múltiples cuestionamientos para comprender qué opciones de mejora se pueden implementar y qué conocimiento tienen los empleados en temas de ciberseguridad.

- **Análisis de resultados**

En esta etapa se determina el análisis del resultado obtenido por las encuestas y se determina las conclusiones.

- **Propuesta de guía para la solución del problema.**

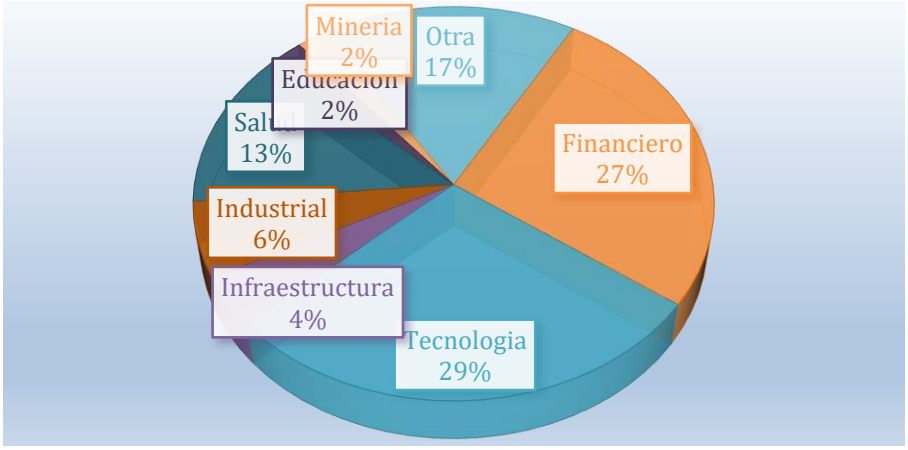
Al realizar la investigación y el análisis de la problemática se tiene un conocimiento más natural y cotidiano de la realidad de los trabajadores que están inmersos en este tipo de modalidad laboral y que pueden estar expuestas a los ciberdelincuentes en doble vía, usuario y empresa. siendo así óptimo la creación de una guía que busca identificar los factores clave para generar una solución a la problemática y llevar a culturizar al trabajador.

ANÁLISIS Y RESULTADOS

En esta fase se hará un enfoque a los aspectos más críticos que se dieron como resultado de la encuesta y que deben ser tomados como puntos a reforzar mediante la propuesta de la guía de buenas prácticas.

Como resultado de la encuesta realizada a 46 personas que trabajan activamente en la modalidad de teletrabajo, las personas a quienes se les realizó la encuesta hacen parte de diferentes sectores empresariales como el financiero, agrícola, tecnológico, industrial entre otros, la siguiente gráfica muestra los porcentajes de participación de los sectores en la encuesta realizada, donde se observa que los sectores con más presencia fueron el tecnológico con un 29% y el financiero con el 27%.

Grafica 1 Sector empresarial encuestado



Autor 4 Andrés Danilo Arévalo y Camilo Andrés Buitrago

La grafica anterior brinda una perspectiva que nos da una idea de la expansión y de la

transformación que ha tenido la manera en que trabajamos después de la pandemia, donde el teletrabajo está siendo usado con gran auge en los diferentes sectores empresariales.

La encuesta entregó datos que confirman que una parte desconoce de qué se trata el concepto de ciberseguridad lo cual es preocupante para la parte de la seguridad de la información y la gran oportunidad que tienen los ciberdelincuentes de aprovechar el desconocimiento de ciertos conceptos de seguridad. En la encuesta realizada se realizó la pregunta *¿Tiene conocimiento o ha escuchado el concepto de ciberseguridad?* donde las personas contestaron de la siguiente manera:

Grafica 2 ¿Tiene conocimiento o ha escuchado el concepto de ciberseguridad?

Autor 5 Andrés Danilo Arévalo y Camilo Andrés Buitrago

Se comprende que hay que tener conciencia de que no hay garantías de que todas las personas que hayan contestado *si* tengan claro lo que abarca dicho concepto, pero lo más llamativo es que un 6% sugiere que tal vez conoce el concepto y un 2% confirma que no tiene idea de que es la ciberseguridad, lo anterior confirma un desconocimiento importante y un aumento en las vulnerabilidades.

Según las respuestas a la pregunta anterior un 92% de personas conocen el concepto de Ciberseguridad, pero al indagar a los encuestados sobre que es dicho término se encontró que su conocimiento no es claro y es allí donde se requiere concientizar para que sea claro a que estamos

expuestos digitalmente y como protegernos ante las diferentes amenazas.

Otro punto clave y de gran interés para las organizaciones es saber si sus empleados están siendo capacitados o no de manera correcta sobre el SGSI (Sistema de Gestión de la seguridad de la información) y si los empleados se toman el tiempo de leer y comprender las políticas que se implementan en sus trabajos.

Las personas encuestadas se encontraron con la pregunta *¿Conoce el SGSI (Sistema de gestión de seguridad de la información) de tu empresa?* Donde se observó que un 33% no conoce el SGSI, el 13% indicó que tal vez tiene conocimiento cifras que afirman que respecto al conocimiento sobre la seguridad de la información y su aplicación no es la más consciente ni eficaz por parte de los teletrabajadores.

Grafica 3 ¿Conoce el SGSI (Sistema de gestión de seguridad de la información) de tu empresa?

Autor 6 Andrés Danilo Arévalo y Camilo Andrés Buitrago

La problemática identificada por medio de la encuesta se obtuvo resultados interesantes respecto a si las organizaciones a la cuales pertenecen los encuestados cuentan con un especialista de Ciberseguridad o también al cual se puede nombrar como un oficial de seguridad, para ello se preguntó *¿Cuenta su empresa con un especialista en Ciberseguridad?*

los resultados fueron un 67% indicó que su organización no contaba con un especialista mientras el 33% respondieron que sí.

Grafica 4 ¿Cuenta su empresa con un especialista en Ciberseguridad?

Autor 7 Andrés Danilo Arévalo y Camilo Andrés Buitrago

La gráfica anterior muestra la importancia de no solo concientizar a los empleados sino también a las organizaciones para que fortalezcan los controles de seguridad si no que se revise si los empleados están siendo bien capacitados y se están dando a conocer no solo las políticas de seguridad, sino que también se informe cómo se compone cada una de las áreas que compone la estructura de la empresa, que en este caso sería quien es el encargado de la seguridad de la información.

A partir de los hallazgos que se obtuvieron en la encuentra realizada, se construyó la propuesta de una guía para concientizar, reforzar y compartir conceptos de ciberseguridad que los teletrabajadores no comprenden de manera amplia y así mitigar los riesgos y vulnerabilidades a los que se expone un teletrabajador en la red.

Ilustración 4 Propuesta de Guía de Buenas Prácticas en el teletrabajo

Autor 8 Andrés Danilo Arévalo y Camilo Andrés Buitrago

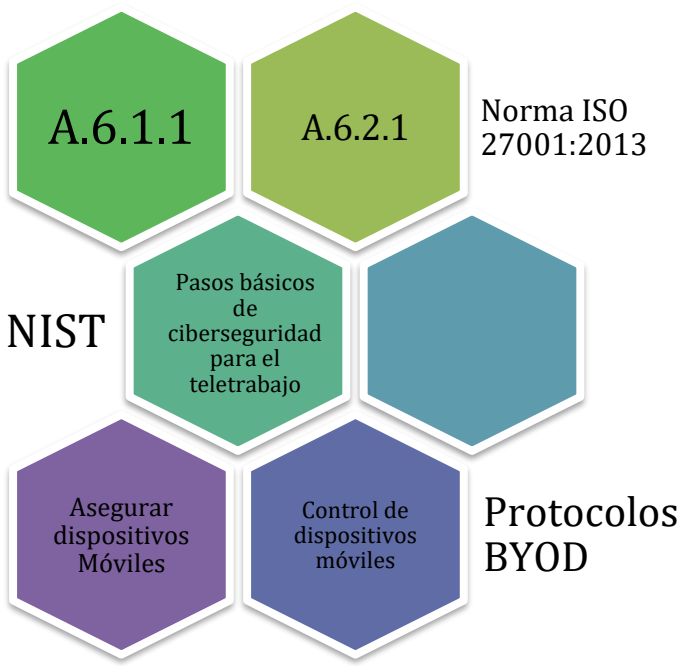
CONCLUSIONES

Los resultados obtenidos dan como conclusión que las brechas de seguridad generadas por empleados que trabajan en la modalidad de teletrabajo son constantes debido al desconocimiento sobre los conceptos y la aplicación de las buenas prácticas de la ciberseguridad. Es importante culturizar a los trabajadores sobre la importancia de la ciberseguridad y la protección de los datos, para ello la propuesta de una guía de buenas prácticas educara a las personas.

La propuesta de la guía se construirá a partir de ciertos referentes y normativa para poder brindar a las personas cierto conocimiento del cual se pueden apoyar para tener más conocimiento sobre

ciberseguridad y así crear conciencia de la importancia de contribuir a la seguridad de la información.

Ilustración 5 Referentes para la Guía de ciberseguridad



Autor 9 Andrés Danilo Arévalo y Camilo Andrés Buitrago

Organizaciones

Desde el aspecto empresarial es importante que se tenga claro la implementación de la seguridad de la información dentro de la organización, definiendo roles y las responsabilidades frente a la seguridad de los datos haciendo uso de la norma *ISO 27001 A.6.1.1* también es fundamental implementar y asegurar una política para dispositivos móviles, que garanticen medidas para el uso de dispositivos móviles contemplado en la norma *ISO 27001 A.6.2.1* con el fin brindar seguridad a dispositivos ajenos a la organización auditando que cumplan con ciertos parámetros de confianza. (internacional)

Empleado (Teletrabajador)

Existen múltiples técnicas y controles que permiten garantizar la seguridad de la información desde el ambiente del teletrabajo para ello a un empleado se le puede educar y concientizar respecto a la ciberseguridad y la implementación de buenas prácticas, algunas de estas pueden ser:

- Consultar y leer las políticas de seguridad de la información de la organización.
- Las conexiones a redes inalámbricas deben ser seguras, por lo cual es recomendable asegurar que nuestra conexión sea segura como por ejemplo verificar que se use la conexión WPA2 Y WPA3, y muy importante que la contraseña de la red sea fuerte.
- El uso de la VPN empresarial para obtener una conexión más segura
- Garantizar el uso del PIN, huella u otros factores biométricos para desbloquear el equipo
- Mantener los equipos actualizados y parchados para suprimir vulnerabilidades.

Lo anterior son pasos básicos pero seguros a la hora de salvaguardar la información y los medios digitales. (Greene, 2020)

REFERENCIAS

Articulo2, L. 1. (2008). *Ley 1221 de 2008* (Artículo 2 ed.). Obtenido de https://www.teletrabajo.gov.co/622/w3-article-8228.html

Brands, E. (04 de marzo de 2022). *El Confidencial.* Obtenido de Tecnología: https://www.elconfidencial.com/tecnologia/2022-03-04/ciberataques-teletrabajo-hp-the-worlf-bra_3342300/

Ciberseguridad, I. n. (2018). *Copias de seguridad, una guía de aproximación para el empresario.* Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

CIBERSEGURIDAD, I. N. (s.f.). *INCIBE*. Obtenido de https://www.incibe.es/

COMUNICACIONES, M. D. (s.f.). *La historia del teletrabajo*. Obtenido de Sala de prensa-Noticias: https://www.teletrabajo.gov.co/622/w3-article-19606.html

Greene, J. (19 de marzo de 2020). *NIST*. Obtenido de Telework Security Basics: https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics

INFOBAE. (23 de octubre de 2022). *INFOBAE*. Obtenido de https://www.infobae.com/america/colombia/2022/10/24/colombia-entre-los-paises-de-america-latina-que-mas-reciben-ciberataques/

internacional, i. (s.f.). *Academia.* Obtenido de NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001 TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS: https://www.academia.edu/40913480/NORMA_T%C3%89CNICA_NTC_ISO_IEC_COLOMBIANA_27001_TECNOLOG%C3%8DA_DE_LA_INFORMACI%C3%93N_T%C3%89CNICAS_DE_SEGURIDAD_SISTEMAS_DE_GESTI%C3%93N_DE_LA_SEGURIDAD_DE_LA_INFORMACI%C3%93N_REQUISITOS

Kapersky. (s.f.). *Kapersky*. Obtenido de Centro de recursos: https://latam.kaspersky.com/resource-center/definitions/what-is-a-vpn

Malwarebytes. (s.f.). *Malwarebytes*. Obtenido de https://es.malwarebytes.com/phishing/