UNIVERSIDAD DON BOSCO
VICERRECTORÍA ACADÉMICA
FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE

Maestro(a) en Seguridad y Gestión de Riesgos Informáticos

PROYECTO

Guía de buenas prácticas aplicadas a la seguridad de la información en el teletrabajo en tiempos de COVID 19 en El Salvador.

PRESENTADO POR

Kevin Alejandro Durán Meléndez

Karina Lourdes García Romero

Carolina Abigail Lovo Guevara

ASESOR

Mg. Rubén Magaña Rodríguez

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América

Junio, 2022

Agradecimientos

Primero dar gracias a Dios, por permitirme concluir con éxito el Post-grado en medio de la adversidad de la pandemia, quien me permitió tener salud, sabiduría y fortaleza, al mismo tiempo a mi esposo por su comprensión y estimulo constante, además por el apoyo incondicional a lo largo de mi carrera profesional.

Agradezco también a nuestro asesor Máster Rubén Magaña por habernos brindado la oportunidad de recurrir a sus conocimientos, experiencias y paciencia en nuestro proyecto de graduación. Al mismo tiempo a todos los formadores de la Universidad don Bosco durante toda la carrera; quienes brindaron sus conocimientos y apoyo para seguir adelante día a día.

Y para finalizar también agradezco a mis compañeros Karina Lourdes García y Kevin Alejandro Durán quienes durante la carrera conformamos un gran equipo de trabajo; lo que nos permitió también establecer una gran amistad y con ello concluir con nuestros objetivos.

Carolina Lovo.

Agradecimientos

Antes que todo dar gracias a Diosito, que nos lleva por caminos que no imaginamos y decisiones que tomamos para mejorar, el permitirme haber tomado esta Maestría en Seguridad y Gestión de Riesgos Informáticos, que es un tema actual y de mucho interés; a pesar de muchos obstáculos como la presencia de la pandemia de COVID-19 que cambio la metodología de clases, las cargas laborales, las adaptaciones, sacrificios; aun así, logramos avanzar hasta llegar a este momento y aplicarlo a nuestros ámbitos laborales.

A mi familia por todo el apoyo y comprensión que me brindaron, se los dedico de todo corazón, especialmente a mi abuelita Payo (Q.D.D.G); a mis compañeros Carito y Kevin, que nos convertimos prácticamente en una familia, compartiendo los buenos, duros, tristes y arduos momentos, estoy muy agradecida de conocer tan lindas personitas y todo el apoyo brindado, al igual que los demás compañeros de carrera: Luis, Oscar, Daniel, Horacio, Erickson y la Cohorte 08.

A nuestro asesor Máster Rubén Magaña, agradecerle su tiempo, paciencia, experiencia y valiosos consejos que nos brindó durante el desarrollo de este trabajo de graduación; gracias por ser un gran guía. Y los demás docentes de la carrera por compartir su experiencia y sobre todo dedicarlo a Máster René Angulo (Q.D.D.G) al haber sido nuestro primer maestro, compartió su conocimiento con humildad y metodología; sentimos una gran pérdida, pero sus enseñanzas quedarán para siempre. A nuestro coordinador Máster Herson Serrano por sus buenas gestiones y la Universidad Don Bosco por innovar con sus carreras.

Karina García.

Agradecimientos

En primer lugar, doy gracias a Dios por permitirme gozar de buena salud, motivación y llenarme de convicción para culminar este camino.

A mi familia, quienes estuvieron en primera línea batallando junto a mí, en medio de la pandemia, a fin de culminar este objetivo, del que también se han apropiado, cargado y colaborado.

A nuestro asesor, Master Rubén Magaña, pieza fundamental en el desarrollo de nuestra investigación, ya que gracias a su experiencia hemos construido una herramienta sustancial con fundamentos teóricos que propiciarán a las organizaciones bases prácticas para el desarrollo de sus esquemas de seguridad.

Finalmente, mis compañeras, Carolina Abigail Lovo y Karina Lourdes García, excelentes profesionales que tuve la bendición y el agrado de conocer, conformando un grupo de trabajo sólido, perseverante y altruista.

Kevin Durán.

Resumen

La actual pandemia del COVID-19, declarada por la Organización Mundial de la Salud (OMS), provocó un distanciamiento social, volviéndose parte del día a día de las personas. Obligando a muchas organizaciones a optar por el teletrabajo para el logro de sus actividades; esta nueva normalidad demuestra hasta qué punto el mundo digital se ha convertido en parte de la vida laboral, por lo que se hace necesario establecer políticas de ciberseguridad para cualquier persona que envíe o reciba información a través de Internet. Este documento presenta una recomendación de guía de buenas prácticas aplicadas a la seguridad de la información en el teletrabajo en tiempos de COVID-19 en El Salvador diferentes organizaciones pueden considerar permitiendo el uso correcto de la información, siendo un activo de suma importancia.

Palabras clave: Buenas prácticas, COVID-19 en El Salvador, Teletrabajo, Ciberseguridad, Protección de Datos.

Abstract

The current COVID-19 pandemic, declared by the World Health Organization (WHO), caused social distancing, becoming part of people's daily lives. Forcing many organizations to opt for work from home to carry out their activities, this demonstrates the extent to which the digital world has become part of labour life, making it necessary to establish cybersecurity policies for anyone who sends or receives information through the Internet. This document presents a recommendation for a guide to good practices applied to information security at work from home during the time of COVID-19 in El Salvador different organizations could consider allowing the correct use of information, since it is one of the most important assets.

Keywords: Good practices, COVID-19 in El Salvador, Remote Work, Cybersecurity, Data Protection.

Tabla de contenido

Índice de figuras

Índice de tablas

Índice de gráficas

CAPITULO 1

1.1 Introducción

El surgimiento de la pandemia de "SRAS-CoV-2 (COVID-19)" **(Organización Mundial de la Salud, 2022)** ha cambiado la vida rutinaria, desde los hábitos de higiene, las interacciones sociales e incluso la forma en la que funcionan los procesos y tareas dentro de una organización. El nuevo cambio de paradigma obligó a la mayoría de las organizaciones a implementar sistemas de teletrabajo para mantener la continuidad del negocio en tiempos de restricciones, y El Salvador no fue la excepción. Esto crea nuevas formas de trabajar, preocupaciones de ciberseguridad y como resultado, cualquier organización tuvo que rediseñar sus sistemas de información y las medidas de seguridad que se tomaron para mitigar los riesgos cibernéticos que planteó el trabajo remoto.

¿El Salvador tenía las bases de seguridad de información establecidas para adoptar la metodología de teletrabajo?, algunas organizaciones adoptaron una continua mejora de la seguridad de información, adquiriendo conocimientos de medidas de teletrabajo y además de conocer un marco legal del mismo; regulando la modalidad a distancia, cumpliendo los objetivos sin afectar la continuidad del negocio y buscando el beneficio tanto de la organización como empleados.

Sin embargo, el cambio de mentalidad del trabajo diario en oficina, ahora está presente en los hogares de quienes están laborando de forma remota; teniendo que aplicar las reglas y normas de las organizaciones en dichos lugares, convirtiendo un espacio del hogar en la estación de trabajo. Además, la administración de la red local ya no está en manos de un empleado especializado en dicha rama, si no que a cargo del mismo usuario y del proveedor de servicios; por lo que se requiere concientizar sobre la importancia de proteger las redes domésticas, ya que son el medio en que se comparte información confidencial, intercambio de correos electrónicos y diversas actividades laborales, tomando en cuenta que esta se distribuye con otros miembros de la familia.

El presente trabajo de investigación sugiere una guía de buenas prácticas aplicables al entorno de la modalidad del trabajo a distancia, siendo está importante para contribuir a la continuidad operativa sin afectar la salud del personal, por las bondades que representa para las organizaciones y sus colaboradores, asociado a otros beneficios como la disminución de la contaminación ambiental, los tiempos de desplazamiento y movilidad en El Salvador; y así mejorar la productividad, competitividad e innovación en las organizaciones.

1.2 Planteamiento del problema

La nueva normalidad a causa de la pandemia COVID-19, trajo cambios repentinos para las empresas, ya que muchas actividades laborales fueron interrumpidas; por lo que diversas organizaciones cambiaron su forma de trabajo, es decir, de la modalidad presencial al trabajo remoto en casa. Por lo tanto, los empleados tuvieron que adaptarse a los nuevos retos que esto conlleva hacia la protección de la información y de forma inmediata.

Esa problemática de resguardar la información, ya no solo depende de las organizaciones y de su infraestructura; si no también de cada empleado, quiénes deben de velar por la seguridad de su entorno de trabajo como su red doméstica, las herramientas y equipos de trabajo, la distribución de la navegación con otros miembros de la familia; como consecuencia las organizaciones no estaban preparadas para abordar estos entornos de forma segura.

1.3 Objetivos

Objetivo general

Establecer una guía de recomendaciones de buenas prácticas de ciberseguridad que puedan ser implementadas para la modalidad de trabajo remoto en tiempos de COVID-19, para ayudar a mitigar los riesgos de inseguridad.

Objetivos específicos

- Identificar los riesgos de ciberseguridad a los que están expuestas las organizaciones en la modalidad de teletrabajo en El Salvador.
- Analizar los factores de riesgos de fuga de información empresarial en el teletrabajo y los impactos legales que conlleva.
- Elaborar una guía de recomendaciones de buenas prácticas y capacitaciones a los empleados que implementan la modalidad a distancia en El Salvador.

1.4 Justificación

A medida que los efectos del COVID-19 se hacen presentes en todo el mundo, las acciones principales de gobiernos y empresas se enfocan, cada vez más, en proteger el bienestar y la seguridad de sus ciudadanos, colaboradores y clientes. La información es un activo esencial y por lo tanto requiere ser protegido adecuadamente. Un dato se vuelve un elemento de valor dentro de cualquier organización, sin importar su rubro o sector; garantizar dicha seguridad no es una labor fácil de cubrir.

Se ha establecido que los principales objetivos de la seguridad son: la confidencialidad, la integridad y la disponibilidad **(Organización Internacional de Normalización, 2022)**; ya que ayudan a aprovechar al máximo la información con el mínimo riesgo. Si alguno de ellos no está presente, dicha seguridad se pierde y por consiguiente la organización se expone a posibles ataques o riesgos.

Las organizaciones tenían definidos sus planes de ciberseguridad o en proceso de maduración en el ambiente de trabajo remoto; sin embargo, ante la crisis sanitaria derivada de la aparición del COVID-19, afectó al mundo entero debido a su alta propagación y posteriormente declarado por la Organización Mundial de la Salud (OMS) como pandemia y generando que las actividades cotidianas, laborales y la comunicación se manejen de forma masiva a través de Internet, exponiéndose a todos los peligros que esto compone.

El nuevo escenario que trajo consigo la pandemia por el COVID-19 sumó retos y preocupaciones a las empresas en el 2020, dado que el perímetro a proteger se extendió por las medidas de confinamiento y el trabajo en casa. Según el Reporte de Seguridad de ESET para Latinoamérica 2020 **(ESET, 2020, pág. 10)**, indica que el 60% de las empresas sufrió al menos un incidente de seguridad en 2019. Con un total de 1,353 empresas encuestadas en Centroamérica; Costa Rica y

Honduras resultaron los países que más ataques han tenido con un 60%, seguidos de El Salvador y Guatemala con un 58%; con el porcentaje más bajo se encuentra Panamá con un 54%. Además, el estudio, reveló que más del 50% de los usuarios encuestados en la región latinoamericana aseguró que la organización para la que trabajan no brindó las herramientas de seguridad necesarias para migrar hacia el teletrabajo en estas condiciones y casi el 45% recibió intentos de "phishing" **(ESET, 2020, pág. 14)** relacionados con la pandemia. ESET dice que se debe de tener en cuenta que al hacerse públicos los datos se vuelve más sencillo para los atacantes crear campañas de "phishing" más dirigidas y efectivas al aprovechar la información.

Con lo anterior se hace evidente la necesidad que toda organización implemente políticas o normas de seguridad de la información, con el objetivo de resguardar y cuidar dichos activos de información, en un ambiente tanto presencial como en modalidad remota.

CAPITULO 2

2.1 Marco teórico

2.1.1 Evolución de pandemia COVID-19 en El Salvador

El 11 de marzo de 2020, la OMS declaró al COVID-19 como pandemia, posteriormente el mismo día en El Salvador; el presidente de la República Nayib Bukele, declaró Estado de Emergencia; a pesar de no tener casos confirmados. A partir del 13 de marzo de 2020, todos los salvadoreños que ingresan al país son enviados a centros de contención para observación. El miércoles 18 de marzo de 2020 se dio la detección del primer caso de COVID-19 en El Salvador, en el municipio de Metapán y poco después se cierran totalmente las fronteras. El 20 de marzo de 2020, el presidente de la República declara cuarentena "domiciliar" y "absoluta" por 30 días en el país. **(Wikipedia, 2022)**

Figura 1

Cronología COVID-19 en El Salvador

Nota. Publicación en red social Twitter por parte del presidente de la República, sobre línea del tiempo del desarrollo del COVID19 en el mundo y la respuesta que El Salvador ha tenido en cada etapa. Twitter.com **(Casa Presidencial-Twitter, 2022)**

Estas decisiones contribuyeron a que empresas e instituciones de diferentes sectores adoptaran modelos de trabajo remoto, como medida de mitigación contra la propagación del virus. Lo anterior contribuyó a reestructurar la comunicación, procesamiento y modalidad de trabajo, siendo estos insumos para desarrollar e implementar tecnologías que se adecuaran a dicho cambio. Un desafío de gran magnitud y que debía ser superado en el menor tiempo posible; sin embargo, el riesgo de exponer los activos de información de las organizaciones crece inevitablemente, siendo este el punto más crítico de esta evolución tecnológica.

El Teletrabajo según el Art. 4 de la Ley de Regulación del Teletrabajo en El Salvador, puede definirse como una forma de organizar y realizar el trabajo de manera no presencial ya sea total o parcialmente, por tiempo determinado o indefinido, fuera del establecimiento o centro de trabajo, pudiendo ser en el domicilio del trabajador o en un lugar ajeno al empleador y utilizando como soporte las tecnologías de la información y la comunicación. **(Asamblea Legislativa de El Salvador, 2020, pág. 2)**

CAPITULO 3

3.1 Marco de referencia

Para conocer la implementación del teletrabajo y las medidas necesarias de ciberseguridad; se efectuó una búsqueda y revisión de artículos académicos asociados al tema de las buenas prácticas de seguridad de la información relacionadas al teletrabajo en tiempos de COVID-19, tomando como referencias bibliotecas académicas, desde el año 2020 cuando el teletrabajo tomo mayor relevancia en las distintas organizaciones.

Se identificaron una cantidad de artículos, de los cuales se seleccionaron temas de interés relacionados con la identificación de los riesgos y vulnerabilidades que las organizaciones puedan presentar en la modalidad de teletrabajo; a continuación, se detallan algunas de las investigaciones:

3.1.1 Retos del teletrabajo en la era del COVID-19

La modalidad de teletrabajo debe superar retos, lo que permite evaluar las ventajas y desventajas que debe enfrentar una organización, porque en la medida en que se tenga la capacidad de comprenderlo, se estará preparado para mitigarlos, entre los principales retos del teletrabajo se encuentran: **(Guimbao, 2020, págs. 7-10)**

- **Organización:** En el trabajo a distancia debe existir una comunicación interna entre empleados y superiores, implementando herramientas técnicas adecuadas, con los objetivos correspondientes; estableciendo metodología de evaluación e indicadores de clave de desempeño y seguimiento de las metas.
- **Resistencia al cambio:** Es necesario acoplarse a los cambios, no solo basado en los elementos tradicionales del trabajo presencial como el cumplimiento de los horarios y en muchos casos,

la supervisión de los empleados, si no conocer las ventajas que las nuevas tecnologías permiten para mejorar rendimientos y productividades.

- **Mantener la cercanía:** El líder debe afrontar este reto para mantener la cercanía y la fluidez con los miembros de su equipo.
- **Gestión del tiempo:** Para el trabajo remoto los horarios laborales son diferentes, debido a que en la modalidad presencial existe un control de marcaciones y horarios estipulados, que a diferencia de la modalidad de teletrabajo no se controlan de la misma forma. La organización debe cuidar el bienestar de los empleados y respetando los periodos necesarios de descanso y desconexión de acuerdo a su contrato laboral.
- **Retroalimentación:** El "feedback" **(Guimbao, 2020, pág. 10)**, de manera continua, es de importancia entre jefe y empleado, con el objetivo de motivar el trabajo bien hecho; generando confianza y compromiso entre ambas partes.
- **Ciberseguridad:** Otro reto al que se enfrentan las organizaciones al implementar la modalidad de teletrabajo es la ciberseguridad. Aplicar "túneles virtuales dentro de Internet para comunicarse" **(Guimbao, 2020, pág. 10)** se ha convertido en una de las herramientas más comunes y seguras. Se tiene la idea que esto depende más del personal informático; sin embargo, también es labor de la alta gerencia realizar campañas de concientización de los empleados sobre la importancia que tiene la seguridad de la información para la organización.
- **Suministro de recursos:** Es tarea de la organización velar porque sus empleados cuenten con insumos y herramientas que les permitan realizar las actividades laborales diarias y de la misma forma el acceso a la información, siempre y cuando el empleado posea los permisos correspondientes.

3.1.2 La seguridad de la información de la organización durante el trabajo remoto

Distintas investigaciones y estudios internacionales como "NIST" **(Instituto Nacional de Normas y Tecnología, 2022)**, atribuyen los ataques cibernéticos más comúnmente a equipos que se encuentran fuera de la organización, esto debido a que no existen equipos perimetrales de seguridad ni normas de uso corporativos fuera de la infraestructura tecnológica. En este sentido, el trabajo remoto provocado por la llegada de COVID-19, ha incrementado la vulnerabilidad de las plataformas de conectividad, dado que existen diversos "hackers" **(Real Academia Española, 2022)** alrededor del mundo que pretenden sacar provecho del incremento de las actividades en línea, mediante ataques de phishing, virus y otros atentados cibernéticos.

Otro factor de riesgo resulta la posibilidad de que los trabajadores puedan conectarse desde sus redes domésticas o mediante cualquier red Wi-Fi sin seguridad, para ingresar a las plataformas de acceso remoto diseñadas por la organización; incrementando el riesgo de ataques cibernéticos a los sistemas e información confidencial.

Además, con el trabajo remoto, algunas organizaciones proporcionan la entrega de dispositivos de su propiedad, o implementan la política de "Trae Tu Propio Dispositivo - BYOD (Bring Your Own Device)" **(Blanco, 2022)**, utilizando "Red Privada Virtual (VPN)" **(Peralta, 2021, pág. 5)**. Por tanto, la organización debe vigilar y proteger la información correspondiente a sus actividades tales como plataformas virtuales, sistemas de información, programas operativos, softwares de organización de labores, servicios de terceros, etc. Siendo necesaria la implementación de políticas y/o protocolos que protejan los activos.

3.1.3 Clasificación de las fuentes de información

Dentro de la clasificación general de las fuentes de información, se encuentran las siguientes:

- Las fuentes de información primaria son las que contienen información original que ha sido publicada por primera vez y que no ha sido filtrada, interpretada o evaluada por nadie más. Son producto de una investigación o de una actividad eminentemente creativa. **(Universidad de Guadalajara, 2022)**
- Fuentes de información secundaria: Contienen información primaria, sintetizada y reorganizada; están diseñadas para facilitar y maximizar el acceso a las fuentes primarias o a sus contenidos. Se apoya de estadísticas realizadas por instituciones u organizaciones que gestionan los procesos administrativos y de contrataciones con base a las leyes del país.

3.2 Hipótesis

La nueva normalidad a causa de la pandemia COVID-19, trajo cambios repentinos para las empresas, ya que muchas actividades laborales fueron interrumpidas; por lo que diversas organizaciones cambiaron su forma de trabajo, es decir, de la modalidad presencial al trabajo remoto en casa. Por lo tanto, los empleados tuvieron que adaptarse a los nuevos retos que esto conlleva hacia la protección de la información y de forma inmediata.

Esta problemática de resguardar la información, ya no solo depende de las organizaciones y de su infraestructura; si no también de cada empleado, que debe de velar por la seguridad de su entorno de trabajo como su red doméstica, las herramientas y equipos de trabajo, la distribución de la navegación con otros miembros de la familia; como consecuencia las organizaciones no estaban

preparadas para abordar estos entornos de forma segura. Por tanto, se determinaron las siguientes hipótesis de estudio:

1. El implementar buenas prácticas de seguridad de la información mejora la competitividad e innovación en las organizaciones.
2. Las condiciones de trabajo remoto cumplen con un porcentaje aceptable de medidas de seguridad de la información, como alternativa de continuidad a las actividades laborales durante la contingencia por la pandemia del COVID-19.
3. La falta de conocimiento sobre la importancia de la seguridad de la información en la modalidad del teletrabajo, puede impactar negativamente en el desarrollo económico financiera de las organizaciones, así como la perdida de datos; tanto en el sector privado como público.

CAPITULO 4

4.1 Marco legal

4.1.1 Ley De Regulación Del Teletrabajo

El Salvador posee una regulación específica del teletrabajo. El 20 de marzo de 2020 y durante la emergencia nacional por la pandemia del COVID-19, la Asamblea Legislativa aprobó el Decreto No. 600, que contiene la Ley de Regulación del Teletrabajo, publicándose en el diario oficial el día 16 de junio de 2020.

Objeto y objetivos: La presente ley tiene como objeto promover, armonizar, regular e implementar el teletrabajo como un instrumento para la generación de empleo y modernización de las instituciones públicas, privadas, autónomas y municipalidades, a través de la utilización de tecnologías de la información y comunicación. (Art.1 L.R.Trb.) **(Asamblea Legislativa de El Salvador, 2020, pág. 1)**

Los principales objetivos del teletrabajo son los siguientes: El aprovechamiento de las tecnologías de la información y comunicación en la prestación de los servicios al público y a la población en general, el aumento y medición de la productividad, mayor eficiencia y transparencia en el uso de los fondos públicos, disminución del gasto, reducción del consumo de energía eléctrica, combustible, alquileres y otros. (Art. 2 L.R.Trb.). **(Asamblea Legislativa de El Salvador, 2020, pág. 2)**

Ámbito de aplicación: Queda comprendido dentro del ámbito de aplicación de la presente ley, las relaciones de trabajo derivadas de cualquier vínculo laboral entre trabajadores, empleadores públicos y privados, cuyos contratos de trabajo se sometan a lo previsto en esta ley, demás leyes laborales vigentes y cualquier otra fuente de derechos y obligaciones laborales. (Art. 3 L.R.Trb.) **(Asamblea Legislativa de El Salvador, 2020, pág. 2)**.

Esta ley promueve derechos y deberes del trabajador en modalidad a distancia en El Salvador, así como la organización de las condiciones laborales, el suministro de equipos, los horarios y la forma pactada en la relación laboral; tanto en el sector público y privado.

4.1.2 Política de Ciberseguridad de El Salvador

Contiene la normativa y lineamientos para la prevención, detección y remediación de posibles vulnerabilidades a las que se puedan exponer los diferentes recursos de información del país y proteger la infraestructura crítica nacional. **(Gobierno de El Salvador, 2022)**

Objetivo: Establecer las líneas de acción y estratégicas que permitan al Gobierno de El Salvador definir los aspectos relevantes enfocados en la prevención de riesgos cibernéticos, así como la gobernanza que debe existir para obtener éxito en este tema. Es de primordial interés definir los criterios de abordaje para el desarrollo de las capacidades de ciberseguridad enfocadas en el aseguramiento de las infraestructuras críticas, el fortalecimiento de los mecanismos de respuesta ante incidentes y el desarrollo de habilidades técnicas y de gestión, para que las instituciones públicas y privadas a nivel nacional y los ciudadanos mismos puedan tomar conciencia del tema de ciberseguridad y los riesgos del uso de las tecnologías de información, que les permitan adoptar medidas de protección ante las ciber amenazas. **(Dirección de Identidad Digital, 2021, pág. 4)**

Se busca la prevención de ciberataques y fraudes financieros en las diferentes instituciones del país, además de la identificación, evaluación y mitigación de los diferentes riesgos cibernéticos.

4.1.3 Ley de Firma Electrónica

La Asamblea Legislativa aprobó el día 1 de octubre de 2015, el Decreto 133 que contiene la Ley De Firma Electrónica, el cual fue sancionada por el presidente de la República y publicado en el Diario Oficial N°196, el 26 de octubre de 2015.

Objeto: Son objeto de la presente Ley los siguientes:

a) Equiparar la firma electrónica simple y firma electrónica certificada con la firma autógrafa;
b) Otorgar y reconocer eficacia y valor jurídico a la firma electrónica certificada, sello electrónico, sello de tiempo, documentos electrónicos y a los mensajes de datos; y,
c) Regular y fiscalizar lo relativo a los proveedores de servicios de certificación, y a los proveedores de servicios de almacenamiento de documentos electrónicos. **(Asamblea Legislativa de El Salvador, 2015, págs. 1-2)**

Esta ley promueve la seguridad jurídica y permite reemplazar con los usuarios documentos en papel a su equivalente en electrónico. Además, regula a los proveedores de servicios, la certificación electrónica, servicios de almacenamiento de documentos electrónicos.

4.1.4 Ley Especial contra los Delitos Informáticos y Conexos

Objeto: Proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la presente Ley. (Art. 1). **(Asamblea Legislativa de El Salvador, 2016, pág. 1)**

Ámbito de Aplicación: La presente Ley se aplicará a los hechos punibles cometidos total o parcialmente en el territorio nacional o en los lugares sometidos a su jurisdicción. También se aplicará a cualquier persona, natural o jurídica, nacional o extranjera, por delitos que afecten bienes jurídicos del Estado, de sus habitantes o protegidos por Pactos o Tratados Internacionales ratificados por El Salvador.

De igual forma, se aplicará la presente Ley si la ejecución del hecho se inició en territorio extranjero y se consumó en territorio nacional o si se hubieren realizado, utilizando Tecnologías de la Información y la Comunicación instaladas en el territorio nacional y el responsable no ha sido juzgado por el mismo hecho por tribunales extranjeros o ha evadido el juzgamiento o la condena. (Art. 2) **(Asamblea Legislativa de El Salvador, 2016, pág. 2)**

Esta ley promueve la protección de la utilización de tecnología de la información y comunicación, en donde la investigación y procesamiento están condicionadas a las diferentes aplicaciones técnicas y periciales informáticas; definiendo las penas y sanciones de los delitos relativos a estafas, espionaje, hurto, daño a la integridad, entre otros.

CAPITULO 5

5.1 Metodología de la investigación

Para la presente investigación se tendrá en cuenta un enfoque cuantitativo, que es el conjunto de estrategias de obtención y procesamiento de información que emplean magnitudes numéricas y técnicas formales y/o estadísticas para llevar a cabo sus análisis, siempre enmarcados en una relación de causa y efecto **(Editorial Etecé, 2022)**. En otras palabras, un método cuantitativo es todo aquel que utiliza valores numéricos para estudiar un fenómeno.

Tabla 1

Métodos y técnicas de producción según metodología

Metodología	Métodos	Técnicas de producción de datos
Cuantitativa	✓ Experimental ✓ Encuesta ✓ Análisis cuantitativo de datos secundarios (estadística)	✓ Cuestionarios ✓ Recopilación de datos existentes (censos, encuestas, estadísticas continuas) ✓ Análisis de contenido de documentos, textos, films, etc.

Nota. La tabla muestra la clasificación de los métodos y técnicas de producción de datos de la metodología cuantitativa. **(GoConqr, 2022)**

Por lo anterior, se utilizarán el método de encuesta por medio de cuestionarios, que conlleva al análisis de datos y presentar cada uno de los resultados que pueden encontrarse, mediante tablas y gráficos para la interpretación y análisis respectivo de datos y bajo el análisis de la Ley de Regulación del Teletrabajo. Asimismo, la investigación nos permitirá determinar cómo se relacionan y se desempeñan los empleados que se encuentran bajo la modalidad de trabajo remoto,

así como en la modalidad presencial en algunas empresas en el país de El Salvador, en el contexto de la pandemia COVID-19.

Figura 2

Fases del proceso de investigación cuantitativa

Nota. Detalle de pasos a seguir en la construcción de la investigación cuantitativa. Slideshare, **(Massuh, 2022, pág. 7)**

5.2 Diseño y muestra del estudio

Dentro de la investigación a realizar en la modalidad de teletrabajo, se identificaron tres principales grupos para poder determinar el análisis de la seguridad de la información en El Salvador, dichos grupos se clasifican:

• Gerencia y Departamentos de Tecnología de la Información (TI).

• Gerencia y Departamentos de Recursos Humanos/ Talento Humano.

• Empleados.

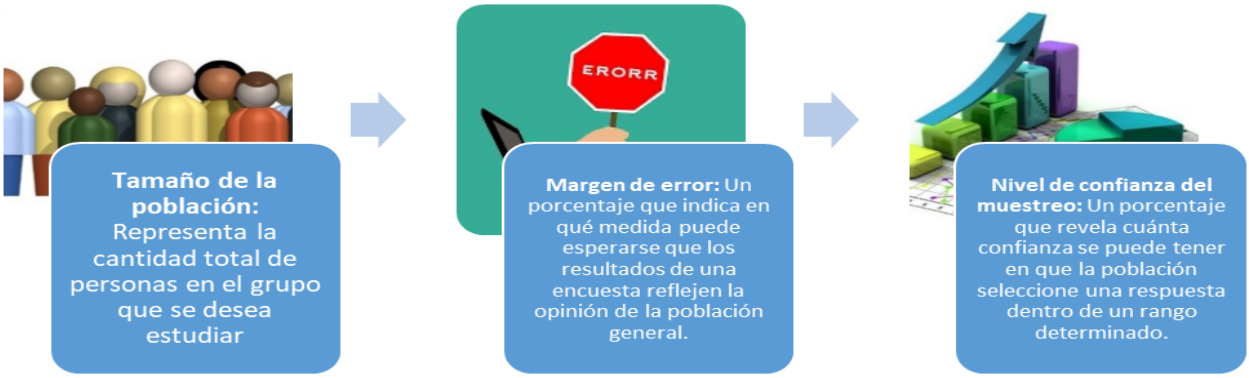
Debido a que no es factible realizar un análisis de todos los elementos de la población de empleados en modalidad de teletrabajo a investigar, se hará uso del muestreo estadístico; seleccionando una muestra, como una parte representativa de dicha población.

5.2.1 Elementos del tamaño de la muestra

Existen tres elementos necesarios para calcular el tamaño de la muestra:

Figura 3

Elementos del muestreo



Nota. La investigación cuantitativa es un procedimiento de decisión, el cual permite analizar y delimitar la población mediante las etapas detallas en esta figura. **(Surveymonkey, 2022)**

5.2.2 Cálculo de la muestra

Para realizar el cálculo de la muestra estadística se utiliza la siguiente fórmula **(Surveymonkey, 2022)**:

$$\boldsymbol{Tamaño\ de\ la\ muestra} = \frac{\frac{\boldsymbol{z^2 \times p(1-p)}}{\boldsymbol{e^2}}}{\boldsymbol{1 + (\frac{z^2 \times p(1-p)}{e^2 N})}}$$

Donde:

N = Tamaño de la población

e = Margen de error (porcentaje expresado con decimales)

p = Es la proporción que se espera encontrar. Como regla general, se usa p=50% si no se cuenta con ninguna información sobre el valor que se espera encontrar. (p = 0.50)

z = Puntuación z, es la cantidad de desviaciones estándar que una proporción determinada se aleja de la media, para encontrar la puntuación z adecuada se utiliza la siguiente tabla:

Tabla 2

Puntuación z según nivel de confianza

Nivel de confianza deseado	Puntuación z
80 %	1.28
85 %	1.44
90 %	1.65
95 %	1.96
99 %	2.58

Nota. Valor de puntuación z, en base al porcentaje de nivel de confianza deseado. **(Surveymonkey, 2022)**

CAPITULO 6

6.1 Desarrollo de la investigación

6.1.1 Fuentes de información primaria

En la presente investigación como fuentes de información primaria, se efectuaron encuestas y cuestionarios dirigidas a los tres principales grupos para poder determinar el análisis de la seguridad de la información, dentro de la modalidad de teletrabajo. Con una muestra de 68 personas divididas en:

• 15 encuestas de Gerencia y Departamentos de Tecnología de la Información (TI).

• 10 encuestas de Gerencia y Departamentos de Recursos Humanos/ Talento Humano.

• 43 encuestas de Empleados.

El objetivo de las encuestas fue conocer aspectos de conocimiento y aplicación de la seguridad de la información a empleados en modalidad de teletrabajo en los que se encuentra la organización, desde el inicio de la pandemia de COVID-19 en El Salvador.

Para desarrollar las encuestas se utilizó la herramienta de Google Forms, enviando enlaces según área de estudio; a diferentes empleados tanto del sector público con una cantidad de 17 encuestados y del sector privado, con una cantidad de 51 encuestados. Dicha herramienta facilitó el obtener información de forma inmediata y ser tabulada para mostrar resultados en línea y mostrando sus respectivas gráficas que servirán para el análisis e insumo de desarrollo de guías de buenas prácticas de seguridad de la información.

6.1.2 Técnica de estadísticas, fuentes secundarias de datos

Para las fuentes de información secundaria se buscaron estadísticas recopiladas por instituciones como Ministerio de Trabajo y Previsión Social y Dirección General de Estadística y Censos de El Salvador (DIGESTYC). Se realizaron visitas al ministerio donde proporcionaron contactos y se realizaron llamadas; pero especificaron que estadísticas puntuales sobre la población en modalidad de teletrabajo, así como estudios respecto a mejora de relaciones laborales, cambios en los contratos de trabajo, entre otras, no se contaba con estudios actuales. En el caso de DIGESTYC tampoco tenía información relacionada con el tema a la fecha.

Por lo anterior se utilizó como referencia el estudio de Teletrabajo En El Salvador Factibilidad y Retos Ante la Pandemia de COVID-19 **(María José Erazo, 2020, pág. 11)**, realizado por Ministerio de Trabajo y Previsión Social; que muestra estadísticas de la población laboral que le es factible realizar teletrabajo, luego de considerar diversos criterios según ocupación y actividad. Los resultados que se obtuvieron de dicho estudio se muestran en la siguiente figura:

Figura 4

Variables sociodemográficas según factibilidad de hacer teletrabajo, 2019

Variable	No puede hacer teletrabajo		Puede hacer teletrabajo	
	Personas	Porcentaje	Personas	Porcentaje
Nacional	2,529,473	87.3%	368,156	12.7%
Sexo				
Hombre	1,515,098	89.5%	178,360	10.5%
Mujer	1,014,375	84.2%	189,797	15.8%
Área de residencia				
Urbano	1,639,452	86.4%	258,849	13.6%
Rural	890,021	89.1%	109,307	10.9%
Edad				
Joven de 16 a 24 años	463,033	91.8%	41,379	8.2%
Joven de 25 a 29 años	325,007	89.0%	40,289	11.0%
Adulto de 30 años a 44 años	871,564	87.6%	123,412	12.4%
Adulto de 45 a 59 años	606,704	85.6%	102,319	14.4%
Adulto mayor de 60 años o más	263,165	81.2%	60,757	18.8%
Nivel de escolaridad				
Ninguno	220,401	87.4%	31,642	12.6%
1 a 3 años	291,594	86.8%	44,267	13.2%
4 a 6 años	433,351	89.6%	50,235	10.4%
7 a 9 años	521,908	91.2%	50,378	8.8%
10 a 12 años	719,979	88.1%	97,379	11.9%
13 años o más	342,241	78.4%	94,256	21.6%

Nota. Se señala el dato de la población salvadoreña que puede realizar teletrabajo, "Teletrabajo en El Salvador Factibilidad y Retos ante la pandemia de COVID-19". **(María José Erazo, 2020, pág. 11)**

6.2 Determinación de tamaño de la muestra

Para la investigación se utilizó el valor de personas que pueden realizar teletrabajo, siendo la cantidad de 368,156 como población de estudio, con un nivel de confianza de 90% y un margen de error de 10%. Se utilizará la siguiente fórmula para calcular el tamaño de la muestra:

$$\textbf{Tamaño de la muestra} = \frac{\frac{\mathbf{z^2 \times p(1-p)}}{\mathbf{e^2}}}{\mathbf{1} + (\frac{\mathbf{z^2 \times p(1-p)}}{\mathbf{e^2 N}})}$$

Al sustituir las variables en la fórmula, donde:

N = Tamaño de la población = 368,156

e = Margen de error (porcentaje expresado con decimales) = 0.10

p = Es la proporción que se espera encontrar. Como regla general, se usa p=50% si no se cuenta con ninguna información sobre el valor que se espera encontrar. (p = 0.50)

z = Puntuación z, para un nivel de confianza del 90% será 1.65

$$\textbf{Tamaño de la muestra} = \frac{\frac{\mathbf{1.65^2 \times 0.50(1-0.50)}}{\mathbf{0.10^2}}}{\mathbf{1} + (\frac{\mathbf{1.65^2 \times 0.50(1-0.50)}}{\mathbf{0.10^2(368,156)}})}$$

$$\textbf{Tamaño de la muestra} = \frac{\frac{\mathbf{2.7225 \times 0.50(0.50)}}{\mathbf{0.01}}}{\mathbf{1} + (\frac{\mathbf{2.7225 \times 0.50(0.50)}}{\mathbf{0.01(368,165)}})}$$

$$\textbf{Tamaño de la muestra} = \frac{\frac{2.7225 \times 0.25}{0.01}}{1 + (\frac{2.7225 \times 0.25}{0.01(368,165)})}$$

$$\textbf{Tamaño de la muestra} = \frac{\frac{0.680625}{0.01}}{1 + (\frac{0.68625}{3,681.65})}$$

$$\textbf{Tamaño de la muestra} = \frac{68.625}{1 + (\frac{0.68625}{3,681.65})}$$

$$\textbf{Tamaño de la muestra} = \frac{68.625}{1 + 0.000186397403}$$

$$\textbf{Tamaño de la muestra} = \frac{68.625}{1.000186397403}$$

$$\textbf{Tamaño de la muestra} = 68.61221086208$$

Aproximando valor de la muestra = **68**

Se obtuvo una muestra de 68 encuestas, que brindaron la información deseada. Por lo anterior el nivel de confianza de 90% se determinó de esta forma; debido a que no se cuenta con un insumo estadístico puntual y actualizado a la fecha de la población en modalidad de teletrabajo durante la pandemia de COVID-19; por lo que el margen de error del 10% pueda no reflejar la opinión de la población general de forma exacta.

CAPITULO 7

7.1 Análisis y resultado de la investigación

De acuerdo a los resultados obtenidos de las encuestas de la muestra de estudio, se procedió a su respectivo análisis por cada grupo objetivo. Por lo tanto, con la investigación se determinó que medidas las organizaciones tomaron en cuenta o cuales no; y a partir de ello formar las sugerencias de guías de buenas prácticas aplicadas a la seguridad de la información. A continuación, se presentan sus gráficas y análisis pertinente.

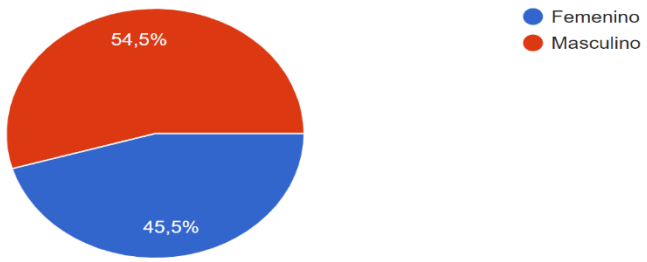
7.2 Encuesta Empleados

Esta encuesta tuvo como objetivo conocer aspectos de seguridad de la información aplicados por empleados en modalidad de trabajo remoto en los que se encuentra la organización, desde el inicio de la pandemia de la COVID-19 en El Salvador.

1. ¿Seleccione su género?

Gráfica 1

Porcentaje género de la muestra de empleado.



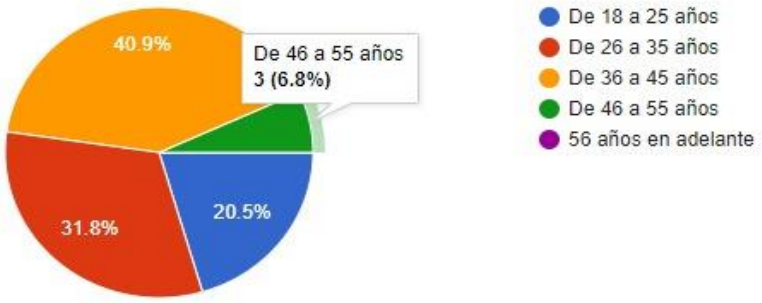
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Con un 54.5% se representa al género masculino, siendo la mayoría de personas encuestadas, mientras que el 45.5% corresponde al género femenino.

2. ¿En qué rango se encuentra su edad?

Gráfica 2

Porcentaje rango de edad de la muestra de empleado



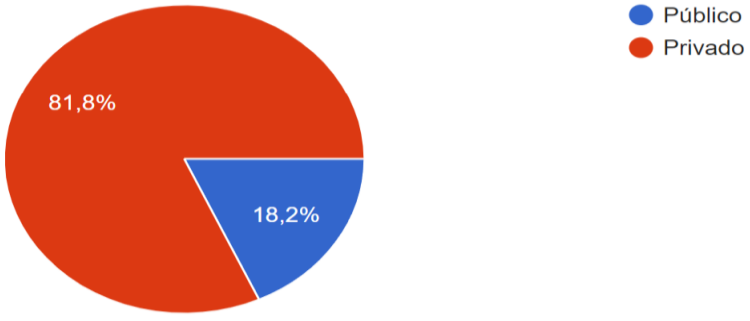
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: La mayoría de personas encuestadas rondan entre los 36 a 45 años de edad con un 40.9%, seguido de un 31.8% con edades entre 26 a 35 años, luego datos de 18 a 25 años con un 20.5%, entre 46 a 55 años 6.8 % y no se registra de 56 años en adelante.

3. ¿A qué sector pertenece la organización?

Gráfica 3

Porcentaje de sector al que pertenece la muestra de empleado



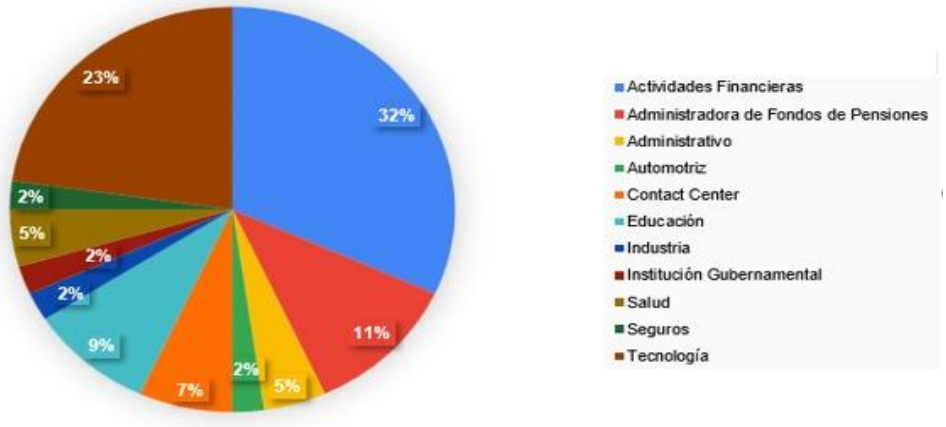
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: El 81.8% de las personas encuestadas pertenece al sector privado y el 18.2% al sector público.

4. ¿Qué actividad realiza la organización?

Gráfica 4

Porcentaje de actividades de la organización de la muestra de empleado



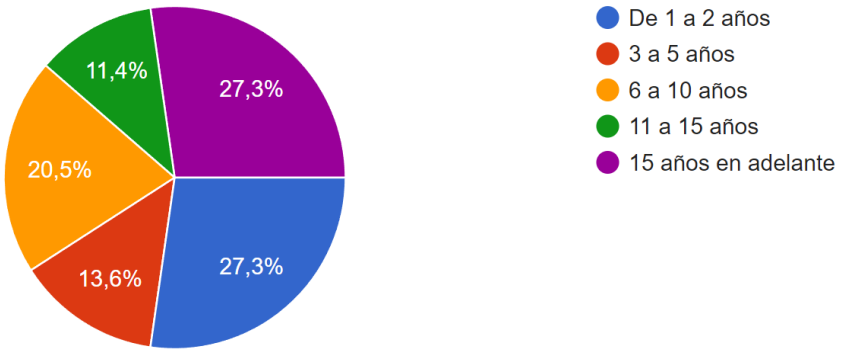
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Las actividades financieras representan el 32%, siendo la mayoría de la muestra poblacional; demostrando que los diferentes rubros económicos también consideran el planteamiento de las buenas prácticas para proteger los intereses productivos.

5. ¿Cuántos años lleva operando en su organización?

Gráfica 5

Porcentaje de años de la muestra de empleado operando en su organización



Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: La mayoría de la población encuestada ha permanecido contratada más de 15 años, o bien apenas comienzan en la organización con 1 a 2 años; siendo estos con un porcentaje del 27.3% cada uno, mientras el 20.5% se encuentra entre 6 a 10 años laborando, el 13.6% corresponde entre 3 a 5 años y el 11.4% de 11 a 15 años laborales.

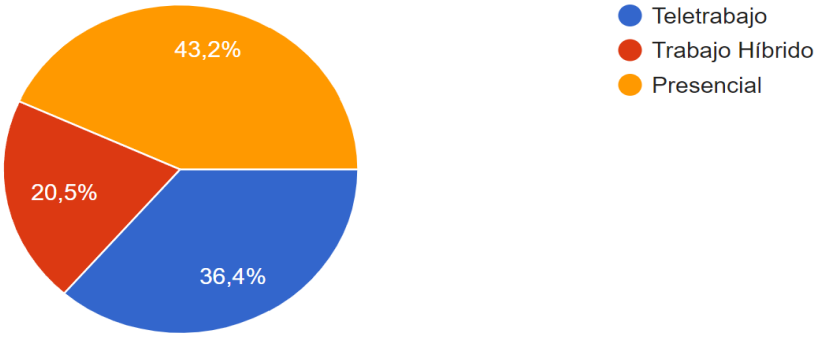
6. ¿En qué modalidad de trabajo está laborando actualmente?

En esta pregunta se especificó para la diferencia de los conceptos:

- Teletrabajo: Según la Ley de Regulación de Teletrabajo, tiene un nuevo contrato laboral o cambio/adenda.
- Trabajo Híbrido: Modalidad mixta, tanto presencial en oficina como trabajo en casa.

Gráfica 6

Porcentaje de modalidad de trabajo de la muestra de empleado



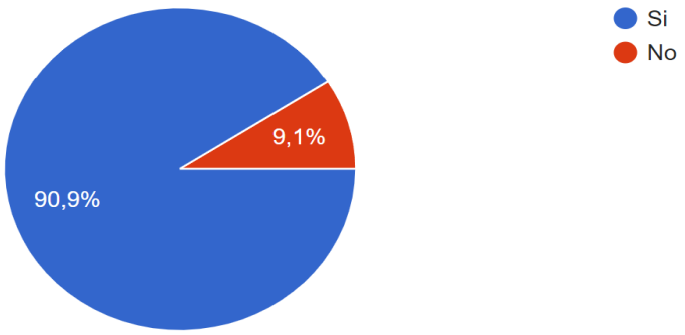
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: La modalidad de trabajo más usada actualmente sigue siendo presencial, con un 43.2%; sin embargo, la tendencia apunta a que el teletrabajo seguirá tomando terreno por las amplias ventajas que trae a las empresas, económicamente hablando, con un 36.4%, mientras que un 20.5% realiza trabajo de forma hibrida.

7. Dentro de la organización ¿Por medio de la modalidad teletrabajo ha logrado coordinar con normalidad tareas con los demás empleados?

Gráfica 7

Porcentaje de coordinación de tareas en modalidad de trabajo de la muestra de empleado



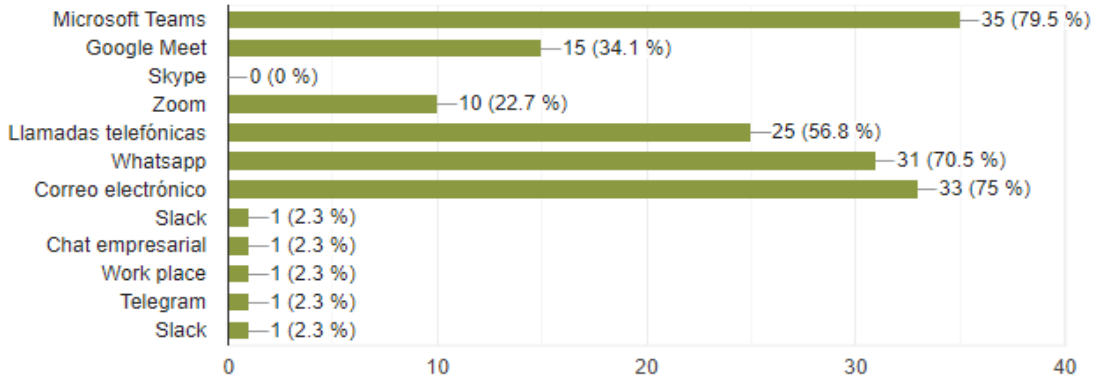
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: La coordinación de actividades grupales y asignaciones han logrado desarrollarse con normalidad en la mayoría de la población con un 90.9%, en contraste con un 9.1% que no logro coordinación con las actividades laborales.

8. ¿Qué medios utilizan para coordinar y planificar tareas asignadas con los otros empleados? (Seleccione una o varias)

Gráfica 8

Porcentaje de medios utilizados para coordinación de tareas



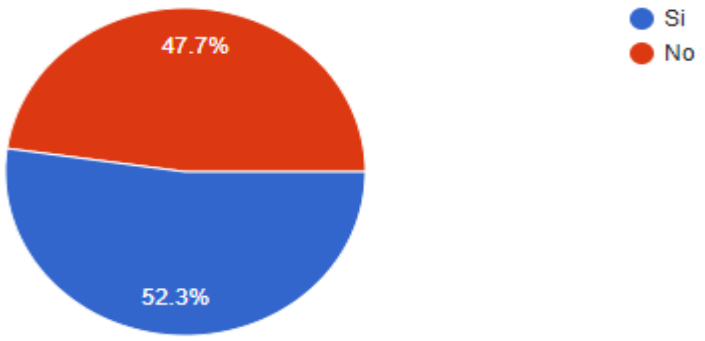
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: En base a los resultados obtenidos en la encuesta se identifica que un 79.5% de los empleados indicó que para coordinar y planificar las actividades asignadas lo realizaron por Microsoft Teams, dejando como segunda posición por medio de correo electrónico con el 75%; y en tercer lugar a Whatsapp con un 70.5%, mientras que las demás herramientas se encuentran dentro de los rangos de porcentajes 2.3% hasta 56.8%. Por lo anterior el resultado obtenido por los empleados, lograron resolver sus actividades laborales en la modalidad de teletrabajo en el tiempo de pandemia COVID-19, bajo las diferentes herramientas establecidas por la organización.

9. Cómo empleado ¿Usted efectuó compras de insumos de oficina para realizar tareas asignadas desde su hogar?

Gráfica 9

Porcentaje de compras de insumos de oficina realizadas por muestra de empleados

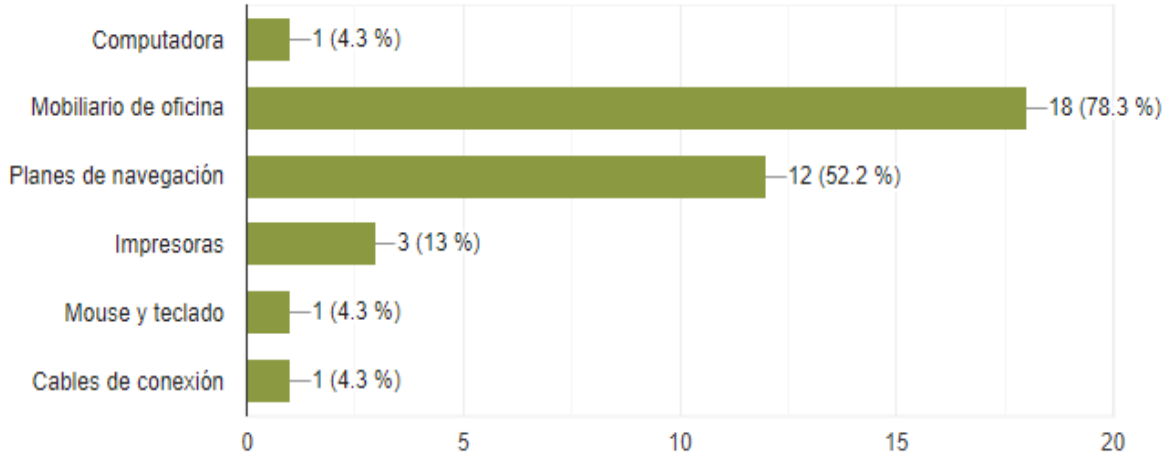


Fuente: Elaboración propia con herramienta Google Forms

Si la respuesta es afirmativa, ¿Qué insumos de oficinas compró?

Gráfica 10

Porcentaje de insumos de oficina que fueron adquiridos por la muestra de empleados



Fuente: Elaboración propia con herramienta Google Forms

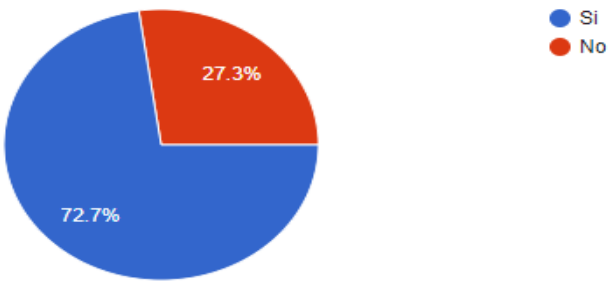
Análisis de resultados: De acuerdo con los resultados obtenidos un 52.3% de empleados realizaron compras de insumos de oficinas para adecuarse a la modalidad de teletrabajo; de los cuales un 78.3% corresponden a compras de mobiliario de oficinas, un 52.2% adquirió planes de navegación, un 13% en compra de impresoras y un 4.3% obtuvo para otros insumos.

Mientras que un 47.7% de los encuestados indicaron no haber efectuado compras de insumos de oficinas, por lo que se adaptaron con lo que tenían disponible desde sus hogares, para continuar con las labores diarias asignadas por la organización.

10. En caso que la empresa haya brindado el equipo de trabajo, este cuenta con medidas de seguridad tales como: bloqueos de periféricos (puertos USB, unidad CD-ROM), conexión a VPN´s, antivirus, políticas de navegación, acceso restringido de Internet.

Gráfica 11

Porcentaje de equipos entregados a muestra de empleados con configuraciones de seguridad.



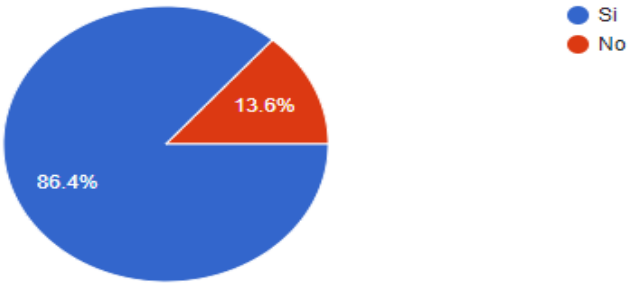
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: De los resultados obtenidos un 72.7% de los encuestados indicaron tener medidas de seguridad bajo la modalidad de teletrabajo, el cual nos permite evaluar que las empresas se prepararon de forma adecuada para proteger la información; mientras que el 27.3% no cuentan con medias de protección en la seguridad de la información lo que puede provocar que la información de datos de la organización se vea comprometida.

11. ¿Cuenta con una conexión a internet que permita una velocidad rápida y estable?

Gráfica 12

Porcentaje de muestra de empleados con conexión a internet con velocidad rápida y estable.



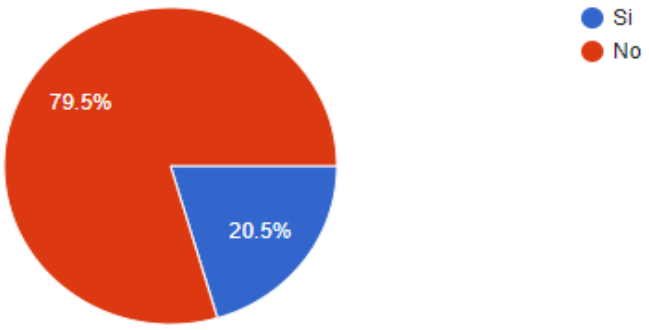
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: De acuerdo con los datos obtenidos un 86.4% de los empleados manifestaron tener una conexión de internet rápida y estable que les permite realizar sus actividades diarias sin inconveniente bajo la modalidad de teletrabajo. Mientras que un 13.6% presentan inconvenientes con la conexión de internet, lo que puede provocar retrasos en las asignaciones laborales.

12. ¿Acostumbra cambiar la contraseña del router de Internet periódicamente?

Gráfica 13

Porcentaje de muestra de empleados que acostumbra a cambiar contraseña de router

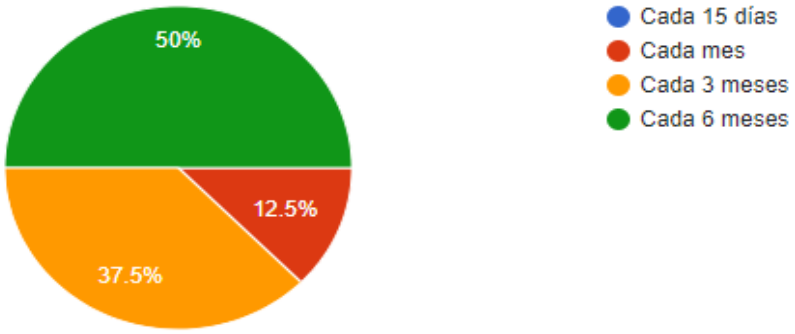


Fuente: Elaboración propia con herramienta Google Forms

Si la respuesta es afirmativa, ¿Con que frecuencia?

Gráfica 14

Porcentaje de frecuencia que se realiza cambio de contraseña



Fuente: Elaboración propia con herramienta Google Forms

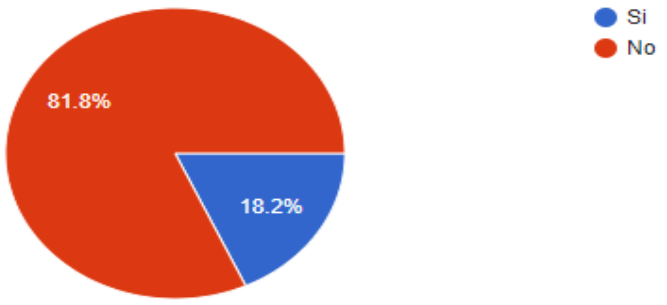
Análisis de resultados: De la muestra de empleados, un 79.5% indico que no realizan de forma periódica el cambio de contraseña del router, por lo que se determina que estando bajo la modalidad de teletrabajo, la información de los datos de la organización se puede ver comprometida y vulnerada ante un ataque cibernético; así como también acceder a dispositivos a los que puede estar conectados.

Por otra parte, un 20.5% de los encuestados indicaron que, si efectúan cambio de contraseña, en donde un 50% lo realiza cada 6 meses, un 37.5% cada 3 meses y un 12.5% cada mes.

13. ¿Acostumbra cambiar la contraseña de su red inalámbrica periódicamente?

Gráfica 15

Porcentaje de muestra de empleados que acostumbra cambiar contraseña de red inalámbrica

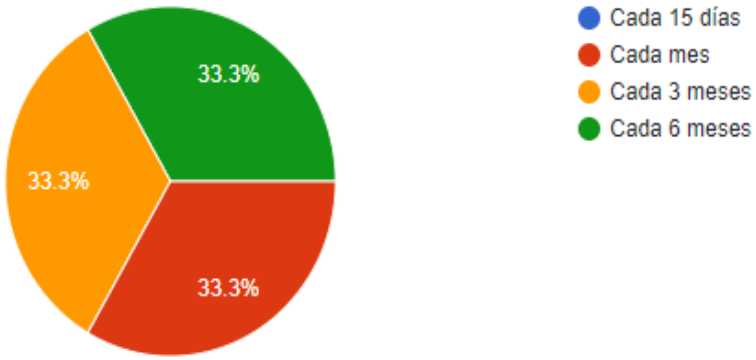


Fuente: Elaboración propia con herramienta Google Forms

Si la respuesta es afirmativa, ¿Con que frecuencia?

Gráfica 16

Porcentaje de frecuencia que se realiza cambio de contraseña



Fuente: Elaboración propia con herramienta Google Forms

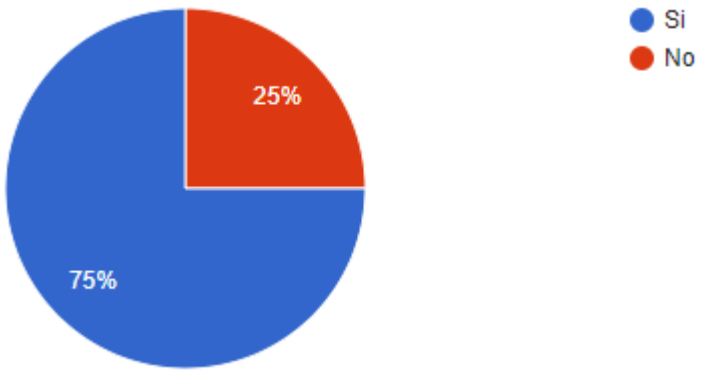
Análisis de resultados: Según los resultados obtenidos un 81.8% de los empleados no realizan un cambio de contraseña en su red inalámbrica, por lo que se concluye que no existe una política de seguridad de red o concientización de parte de la organización hacia los empleados; ya que la verdadera perdida de información o ataques son causados por los mismos usuarios.

Por otra parte, un 18.2% de los empleados que se encuentran bajo la modalidad de trabajo si aplican la buena práctica de cambio de contraseña cada mes, cada 3 meses y cada 6 meses con un 33.3% cada uno.

14. ¿Hace uso de repositorios en la nube (OneDrive, Google Drive, Dropbox, iCloud Drive, etc.) establecidos por la organización para resguardar información o hacer copias de respaldo?

Gráfica 17

Porcentaje de muestra de empleados que utiliza repositorios en la nube



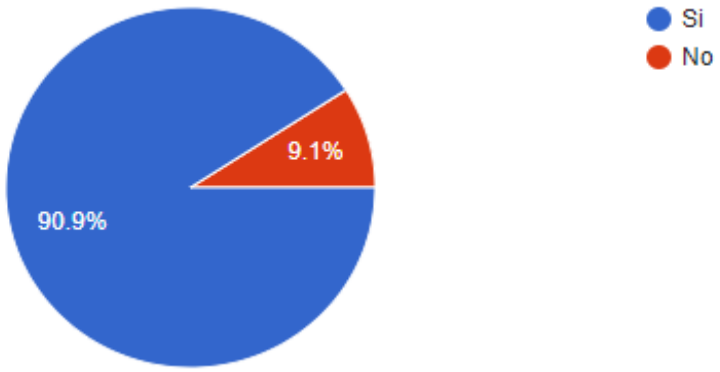
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: De acuerdo con el resultado obtenido el 75% indico que la organización tiene a disposición de los empleados diferentes repositorios en la nube, que les permite resguardar y realizar copias de la información de forma segura; y con ello se aseguran de que la información pueda ser accedida por los empleados en cualquier momento que se requiera. Mientras el 25% manifestó no tener herramientas que les permita resguardar la información.

15. ¿En su equipo de trabajo, hace uso de inicio de sesión de usuario y contraseñas robustas con números, letras, símbolos y mayor a 8 caracteres?

Gráfica 18

Porcentaje de muestra de empleados que utiliza contraseñas robustas



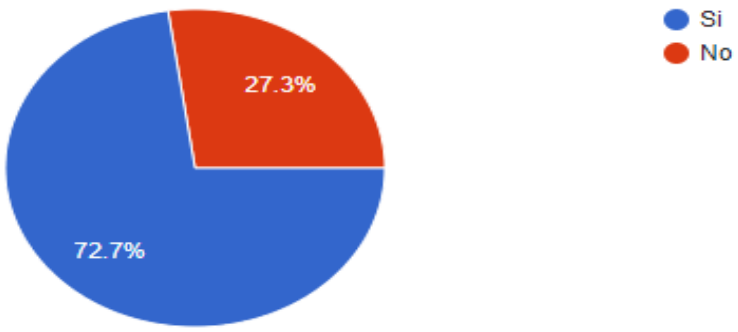
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Según el resultado obtenido, el 90.9% de la muestra de empleados afirman que hacen uso de contraseñas robustas utilizando números, letras, símbolos y con más de 8 caracteres; contra un 9.1% que no hace uso. Identificando que una buena parte de los empleados está consciente de la importancia del uso de contraseñas seguras en inicios de sesiones.

16. ¿En su organización se cuenta con un método de doble factor de autenticación para ingreso a los sistemas, correo electrónico institucional u otros servicios que requieran seguridad?

Gráfica 19

Porcentaje de muestra de empleados que utiliza método de doble factor de autenticación



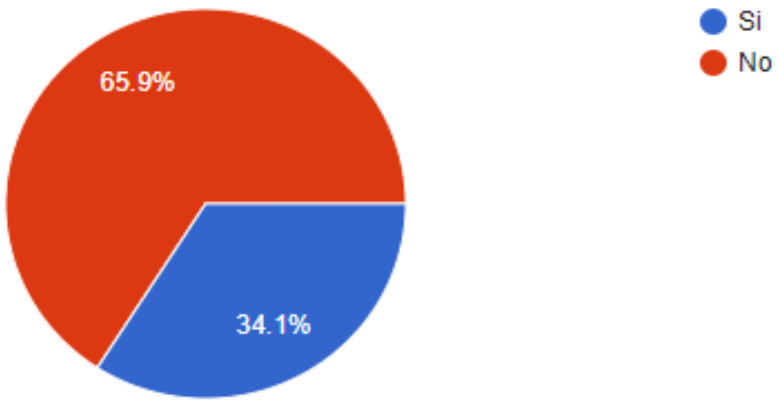
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Según la gráfica, el 72.7% de la muestra de empleados afirma que se cuenta con dicho método para autenticar los ingresos a los sistemas, correos electrónicos entre otros servicios; mientras que un 27.3% no lo utiliza. Por tanto, las organizaciones saben la importancia de la utilización de dicho método como medida de seguridad extra en el ingreso de los sistemas por parte de los usuarios.

17. ¿Cómo empleado, recibió capacitaciones para realizar sus tareas mediante la modalidad de teletrabajo?

Gráfica 20

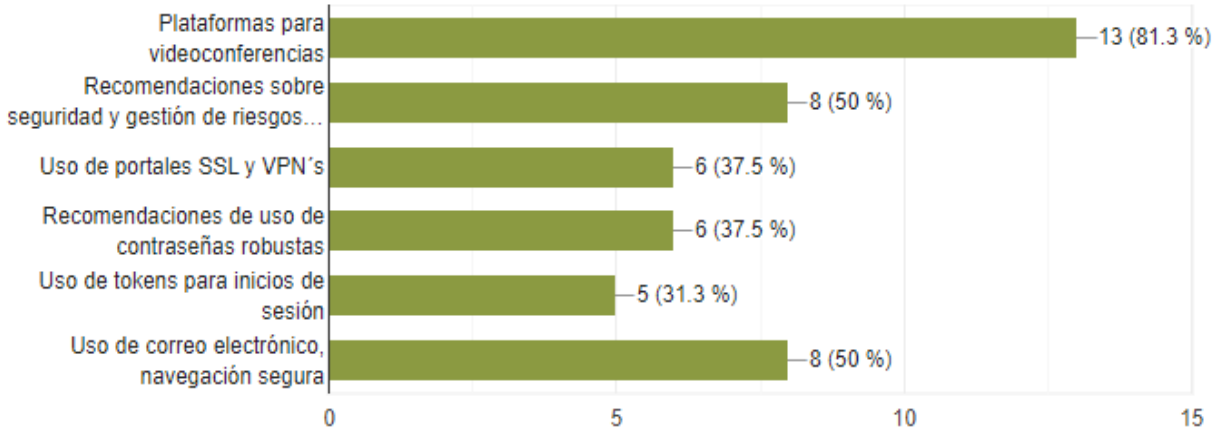
Porcentaje de muestra de empleados que recibió capacitaciones



Fuente: Elaboración propia con herramienta Google Forms

Gráfica 21

Porcentaje de aspectos de capacitaciones brindadas a empleados



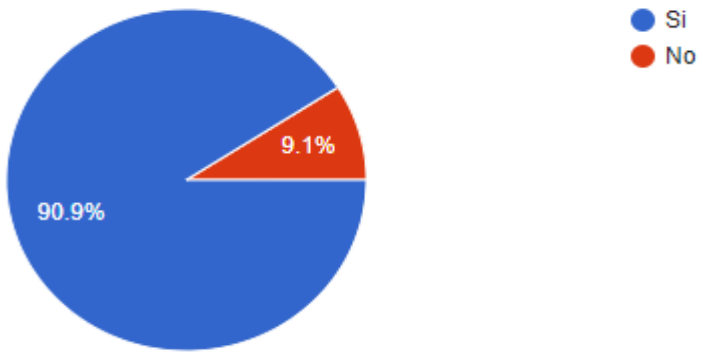
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Los resultados demuestran un valor de 65.9% de la muestra de empleados que no recibieron capacitaciones, con respecto a realizar tareas en la modalidad de teletrabajo; en comparación al 34.1% que si recibió dichas capacitaciones, siendo el 81.3% las plataformas de videoconferencias como primer rubro, el segundo de forma compartida entre Recomendaciones sobre seguridad y gestión de riesgos, y uso de correo electrónico y navegación segura con un 50% cada uno; luego siguen el Uso de portales SSL y VPN´s junto con Recomendaciones de uso de contraseñas robustas con 37.5% cada una y un 31.1% para Uso de tokens para inicios de sesión. Por lo anterior, se denota que la mayoría de empleados tuvieron que aprender por su cuenta y un factor que las organizaciones debieron darle importancia en su momento e incluirlo en un plan de buenas prácticas.

18. ¿Cómo empleado tiene conocimiento que al recibir un correo electrónico sospechoso, debe ser reportando a los canales definidos por la organización?

Gráfica 22

Porcentaje de muestra de empleados que reporta a los canales definidos sobre correos sospechosos.



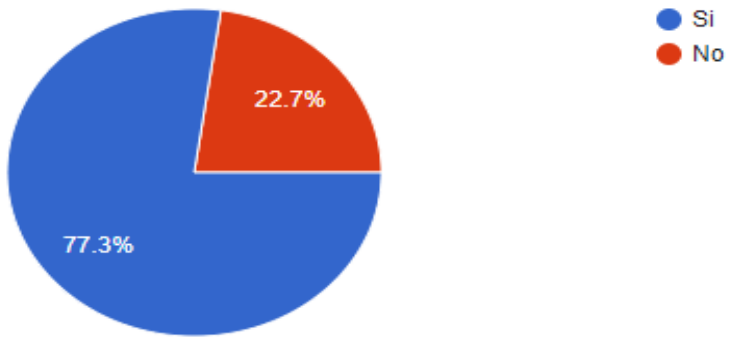
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: La gráfica muestra que el 90.9% de empleados tienen conocimiento que, al recibir un correo electrónico sospechoso, este debe ser reportado a los canales que la organización haya estipulado, siendo de mucho beneficio el contar con dicho conocimiento como medida de seguridad implementada. Mientras que un 9.1% no lo conoce o no se ha implementado.

19. ¿En su equipo de trabajo realiza actualizaciones de antivirus y actualizaciones del sistema operativo para mantenerlo protegido?

Gráfica 23

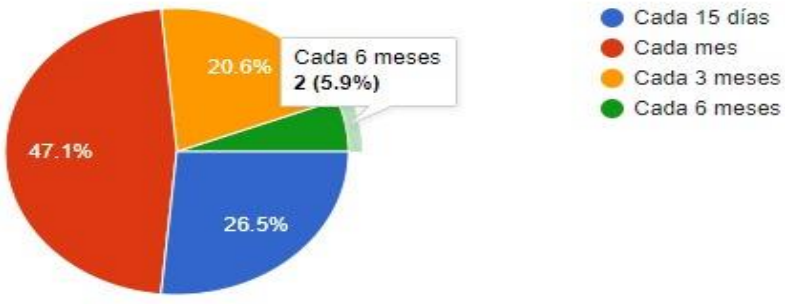
Porcentaje de muestra de empleados que realiza actualizaciones de antivirus y sistema operativo



Fuente: Elaboración propia con herramienta Google Forms

Gráfica 24

Porcentaje de frecuencia que realiza actualizaciones de antivirus y sistema operativo



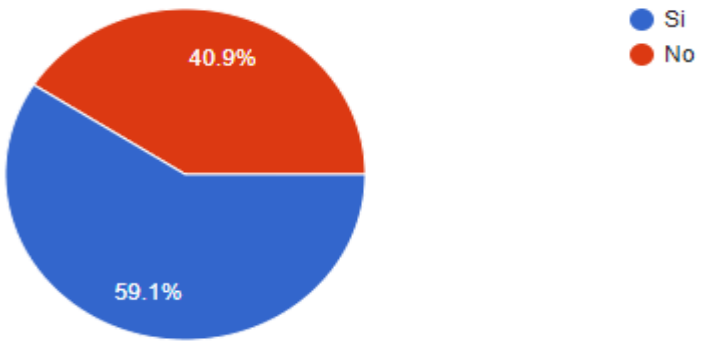
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Los datos reflejan que el 77.3% de la muestra de empleados realizan actualizaciones tanto de antivirus como del sistema operativo, siendo conscientes de que dicha medida brinda protección a los equipos de trabajo y evitar amenazas de seguridad de la información; y la frecuencia con que se realizan, el 47.1% menciono que cada mes, el 26.5% cada 15 días, el 20.6% trimestralmente y 5.9% cada 6 meses. Contra un 22.7% que no realizan dichas actualizaciones.

20. Si usted como empleado posee un dispositivo móvil proporcionado por la organización ¿El uso que le da es para fines únicamente de trabajo?

Gráfica 25

Porcentaje de muestra de empleados con dispositivos móviles para uso laboral



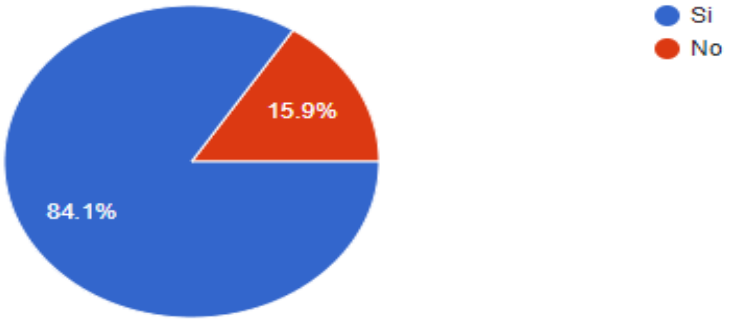
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Los resultados muestran que el 59.1% de la muestra de empleados utilizan un dispositivo móvil proporcionado por la organización solo para fines laborales, contrastando con el 40.9% que lo utiliza con otros propósitos además del laboral. Las organizaciones deben asegurar que al brindar estos dispositivos que el objetivo es únicamente laboral y establecer lineamientos.

21. ¿Acostumbra a bloquear el equipo al levantarse del puesto de trabajo o cerrar sesiones al finalizar su jornada laboral?

Gráfica 26

Porcentaje de muestra de empleados que acostumbra a bloquear el equipo al levantarse



Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Los datos de la gráfica muestran que el 84.1% de empleados considera la importancia de bloquear sesiones al levantarse de su puesto de trabajo o cerrar sesiones cuando finaliza su jornada, aun estando trabajando desde casa; ayudando a mantener la confidencialidad del trabajo. Mientras que un 15.9% no lo pone en práctica.

Como una consulta abierta, se realizó la pregunta:

22. ¿Qué consideraciones, opiniones, mejoras, u observaciones, tiene acerca de los procedimientos que se toman en su organización en cuanto a la preparación que tuvo en la transición a modalidad de teletrabajo?

    Análisis de resultados: La presencia de la pandemia de COVID-19, modifico el ambiente laboral de forma que trasladar los lineamientos de trabajo al hogar, marcó un desafío en las organizaciones y una adaptación “obligatoria” para no interrumpir la continuidad de las tareas de los empleados; entre las opiniones o inconvenientes que se expresaron fueron los siguientes:

- Una mejora es que no se utilice el WhatsApp personal para temas laborales. Menos los dispositivos móviles personales.
- El trabajo presencial para tareas de IT debería desaparecer, Seguir manteniendo la modalidad y no obligar a trabajar en sitio.
- Capacitación y concientización al empleado sobre los phishing, ingeniería social y el manejo adecuado de los recursos de la empresa, brindar talleres prácticos para todos los usuarios.
- Definir mejores políticas de seguridad virtual.
- La empresa dónde trabajó actualmente toma buenas acciones no tengo ninguna observación, Se ha manejado todo de la mejor manera.
- La empresa no estaba preparada y los colaboradores tuvimos que adaptarnos comprando suministros de oficina y mejorar la velocidad de internet para realizar el teletrabajo así mismo ser autodidactas con las plataformas digitales.
- Al conectarse a través de Escritorio Remoto y experimentar problemas para iniciar sesión, la resolución por lo general toma un tiempo considerable y en ocasiones se cae con mucha frecuencia o es muy lento para trabajar normalmente.
- Como empresa se preparó oportunamente para la entrega de laptops para el teletrabajo durante la pandemia; sin embargo, es necesario que refuercen lo importante que es estar bajo esta modalidad por medio de capacitaciones. Para hacer concientización a cada empleado.
- Que puedan ser más humanos y tener empatía. Que sean respetados los horarios de trabajo, ayudando así al personal en su situación de trabajo en casa.

- Mejorar el equipo proporcionado. Deben de brindar el equipo necesario a los empleados para realizar las actividades en teletrabajo.
- Hacer simulacros internos que no se avise a la población laboral, para saber si siguen las normas de seguridad de información, como correos electrónicos ofreciendo beneficios, pidiendo datos personales, clonación de páginas para saber si ellos comprueban, los dominios y certificados de seguridad son originales
- Considerar el gasto que implica trabajar desde casa como Internet y energía eléctrica, además respetar el horario laboral ya que no existen horas extras pagadas.
- Fue buena porque nos brindan las herramientas necesarias para realizarlo.

Existen diversas opiniones con respecto a la implementación del teletrabajo, muchos lo han considerado una buena alternativa y realizar trabajo de forma eficiente; mientras que otros expresan la falta de capacitación tanto en el uso de plataformas, herramientas como las medidas de seguridad. Además del gasto que implico para muchos el invertir el transformar su hogar en su entorno de trabajo. Este gasto se refleja como gasto personal, ya que no están bajo el contrato de teletrabajo de acuerdo a la Ley de Regulación del Teletrabajo en El Salvador, ya que esto permitiría que la empresa asuma dichos gastos de acuerdo al Art. 9 inciso último.

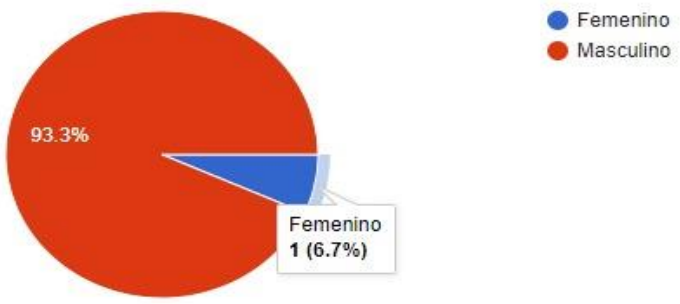
7.3 Encuesta Gerencia y Departamentos de Tecnología de la Información (TI)

Dicha encuesta fue enfocada a la Gerencia y Departamentos de Tecnología de la Información (TI), cuyo objetivo fue conocer aspectos de seguridad de la información aplicados a la modalidad de trabajo remoto, en la organización desde el inicio de la pandemia de COVID-19 en El Salvador.

1. ¿Seleccione su género?

Gráfica 27

Porcentaje de género en muestra de personal de TI



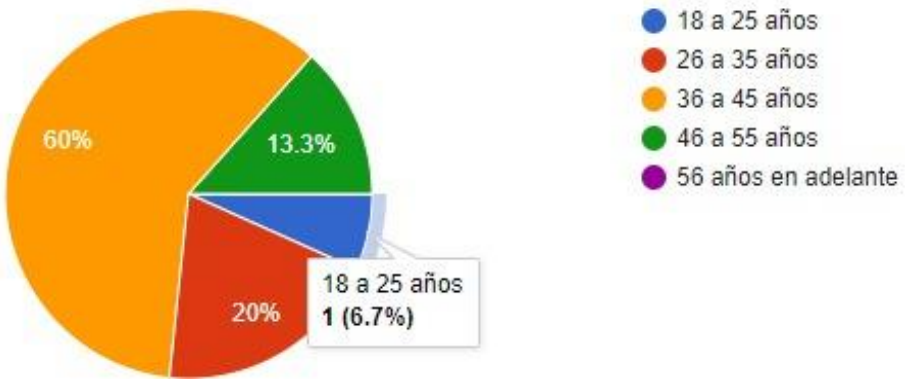
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Se muestra que la distribución de género en el ámbito de TI fue del 93.3% para masculino, abarcando los cargos o responsabilidades de dichas unidades; contra el 6.7% para género femenino.

2. ¿En qué rango se encuentra su edad?

Gráfica 28

Porcentaje de edades de muestra de personal de TI



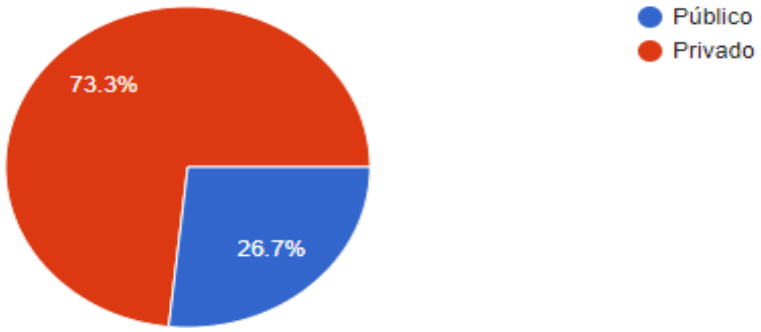
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: La gráfica muestra que el mayor porcentaje radica entre las edades de 36 a 45 años, con un 60% siendo una población adulta joven con años de experiencia en dichas áreas; seguida de un 20% entre las edades de 26 a 35 años, una población mayor entre 46 a 55 años aparece en tercer lugar con un 13.3% y un menor porcentaje de 6.7% entre 18 a 25 años y no se registraron edades de 56 años en adelante. Podemos identificar que es una población joven los responsables de los rubros de TI.

3. ¿A qué sector pertenece la organización donde labora?

Gráfica 29

Porcentaje de sector al que pertenece la organización de la muestra de personal de TI



Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Los resultados demuestran el mayor porcentaje de responsables de TI se encuentran en el sector privado con un 73.3% contra un 26.7% del sector público; puede verse reflejado que al momento de la implementación del teletrabajo se efectuó más en dicho sector que en el ámbito público.

4. ¿Cuál es su cargo funcional?

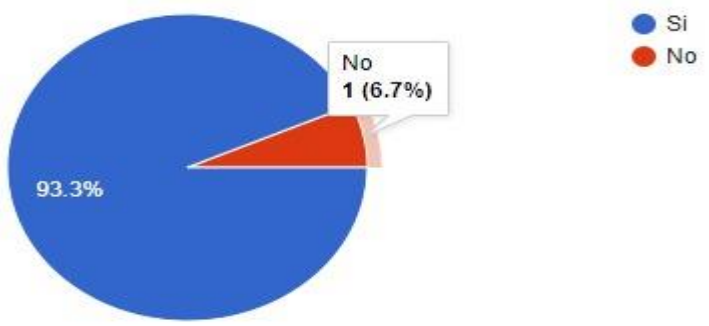
- Administrador de Sistemas
- DBA
- Software Developer
- Coordinador de Centro de Cómputo
- Jefe de Infraestructura
- IT Infrastructure Support
- Técnico en infraestructura de redes
- Colaborador técnico
- Analista Programador
- Analista de Seguridad
- Administrador de base de datos
- Responsable de soporte técnico
- Aplications Developer
- Administración de redes
- Administrador de sistemas

Análisis de resultados: Solicitando que digitaran dicho cargo, se muestra una gama de especialidades de áreas de Tecnologías de la Información, con diferentes responsabilidades, logrando haber más variedad de puestos laborales de TI a nivel de población total de estudio.

5. ¿Para proveer conexiones remotas a los recursos internos de la red institucional, la infraestructura estaba lista para soportar la demanda de usuarios y amenazas del entorno?

Gráfica 30

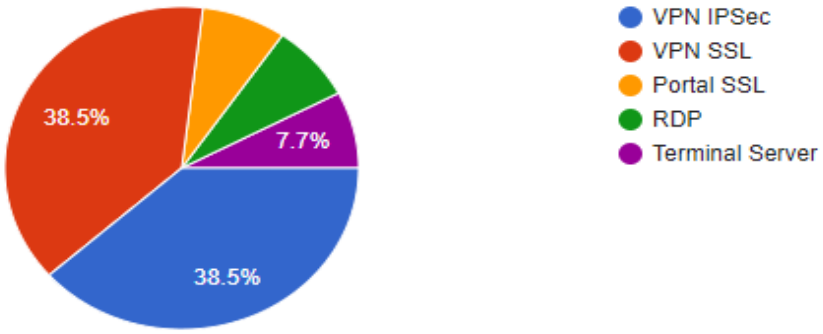
Porcentaje de preparación de la infraestructura



Fuente: Elaboración propia con herramienta Google Forms

Gráfica 31

Porcentaje de herramientas que ayudaron a proveer la conectividad segura



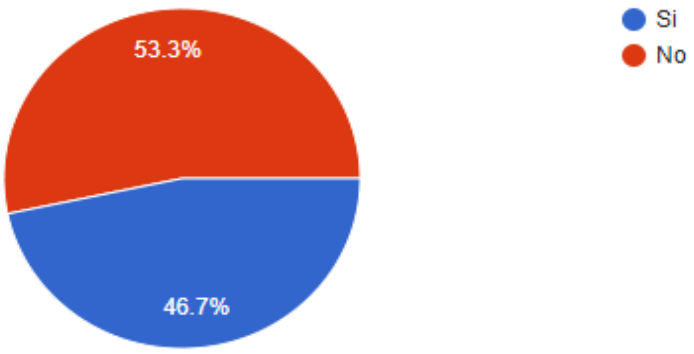
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Los datos reflejan que el 93.3% afirma que la infraestructura estaba lista para soportar la demanda de usuarios y amenazas del entorno, para proveer conexiones remotas, con el cambio del entorno a teletrabajo; de los cuales, las herramientas que ayudaron a proveer la conectividad segura: Un 38.5% lo consideraron tanto para VPN Ipsec como VPN SSL; con las demás opciones de Portal SSL, RDP y Terminal Server con un 7.7% cada uno. Mientras que un 6.7% respondió que la infraestructura no estaba preparada.

6. ¿Cómo área de tecnología, se realizaron capacitaciones a los empleados para realizar sus tareas mediante la modalidad de teletrabajo?

Gráfica 32

Porcentaje de capacitaciones de la muestra de área de TI hacia empleados

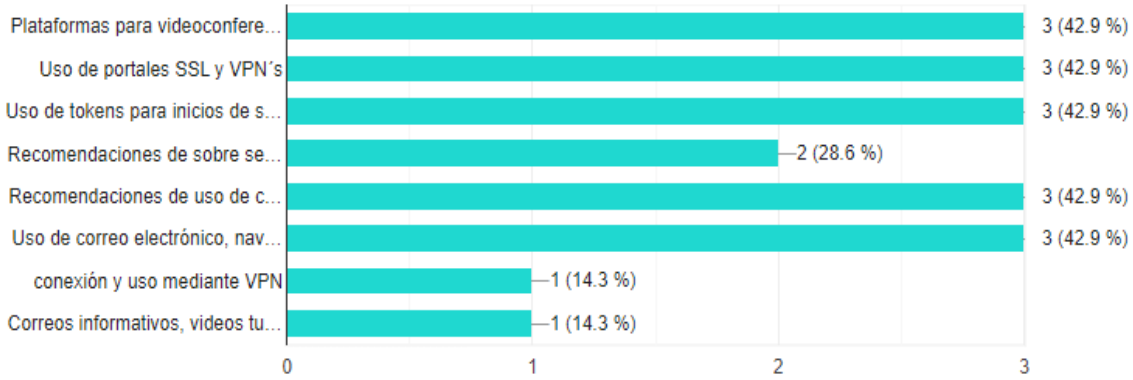


Fuente: Elaboración propia con herramienta Google Forms

En caso de respuesta afirmativa, específicamente ¿en qué áreas? (Seleccione una o varias)

Gráfica 33

Porcentaje de herramientas de capacitaciones brindadas a empleados por personal de TI



Fuente: Elaboración propia con herramienta Google Forms

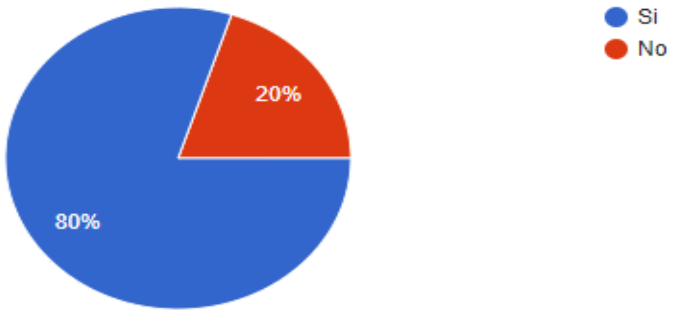
Análisis de resultados: Los resultados muestran que un 53.3% asegura que no se brindaron capacitaciones a los empleados para la realización de sus asignaciones por modalidad de teletrabajo. Mientras un 46.7% responde que, si se brindaron capacitaciones, de este porcentaje que brindo capacitaciones, se destacan los temas de Plataforma para videoconferencias, uso de tokens para inicios de sesión, recomendaciones de uso de contraseñas robustas y uso de correo electrónico, navegación segura con un 42.9% cada uno. Seguido de Recomendaciones de sobre seguridad y gestión de riesgos informáticos con un 28.6% y por último Conexión y uso de VPN, y correos informativos, video tutoriales y manuales con 14.3% respectivamente.

Es de destacar la importancia de brindar capacitaciones dentro de la organización si se desea que se cumplan los objetivos de la mejor forma y no interrumpir las actividades.

7. ¿Los sitios públicos en internet residen en una DMZ para reducir la superficie de contacto entre los clientes externos y la red interna?

Gráfica 34

Porcentaje de medidas que reducen la superficie de contacto en la red interna



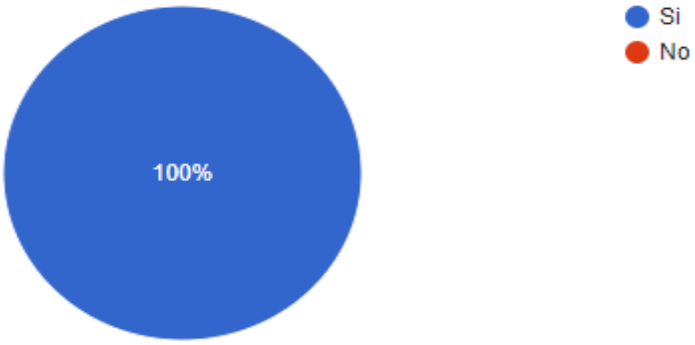
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Según la gráfica se muestra que el 80% de los consultados considera la importancia para reducir la superficie de contacto entre los clientes externos y la red interna, los sitios públicos en internet residen en una DMZ, contra un 20% que no lo implementa de esa forma.

8. ¿Los sitios web públicos aseguran la capa de autenticación con certificados digitales?

Gráfica 35

Porcentaje que utiliza capa de autenticación con certificados digitales



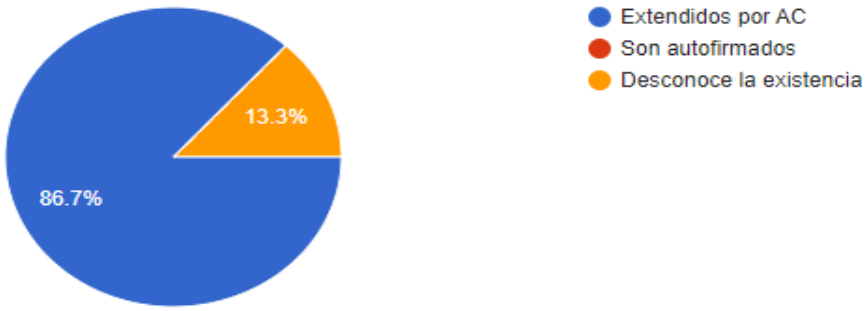
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: De la muestra de empleados encuestados del Área de Tecnología de la Información, el 100% certifica que existe una capa de autenticación en los sitios web públicos lo cual les permiten una identificación exclusiva de una entidad; así como la integridad de los certificados.

9. ¿Los certificados digitales utilizados son extendidos por una AC o son autofirmados?

Gráfica 36

Porcentaje de tipo de certificados digitales utilizados



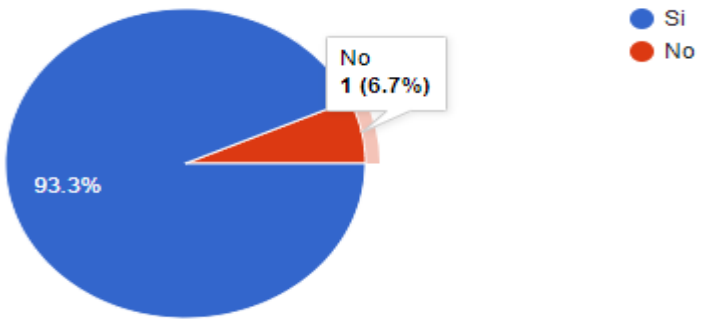
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: De los resultados obtenidos un 86.7% confirmo que los certificados digitales tienen una Autoridad de Certificación (CA) que le permite a la organización verificar que la identidad sea única, confiable, responsable de emitir y revocar certificados digitales utilizados en transacciones y firmas electrónicas. Mientras que el 13.3% desconoce la existencia si la organización cuenta con un CA o certificados autofirmados.

10. ¿Su organización cuenta con un Plan de Continuidad del Negocio ante un evento disruptivo?

Gráfica 37

Porcentaje de organizaciones que cuenta con un Plan de Continuidad del Negocio



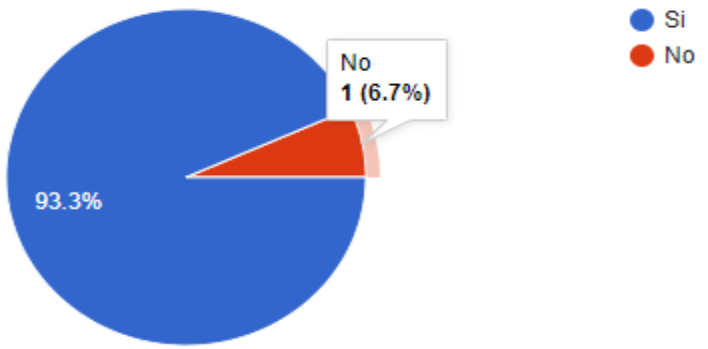
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: De acuerdo al resultado obtenido el 93.3% de las organizaciones cuenta con un Plan de Continuidad del Negocio, el cual les permite prepararse de forma anticipada y garantizar que una organización tenga la capacidad de seguir realizando sus funciones y actividades críticas durante eventos de emergencia o eventos disruptivos. Mientras que el 6.7% de los encuestados indico que la organización para la que laboran no cuenta con un Plan de Continuidad de Negocio.

11. ¿Los equipos corporativos asignados a los teletrabajadores son preparados con medidas de seguridad para restringir y reducir las amenazas fuera de la infraestructura de T.I. de la organización como antivirus, firewall, despliegue del endpoint, etc.?

Gráfica 38

Porcentaje de quipos corporativos que son preparados con medidas de seguridad



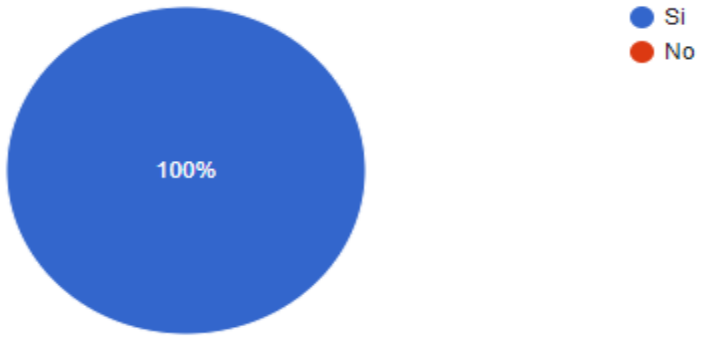
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Según los resultados obtenidos de la muestra de empleados del Área de Tecnología, un 93.3% indico que si implementan medidas de seguridad fuera de la infraestructura de T.I. de la organización; por lo anterior se concluye que al tener un control y políticas de seguridad se logra detectar actividades sospechosas, priorizarla, aislarla y resolverla de forma más rápida. Mientras que el 6.7% de los encuestados manifestó no contar con medidas de seguridad en los equipos conectados a la red.

12. ¿Cómo área de T.I. realizan backup de versiones de bases de datos?

Gráfica 39

Porcentaje que realizan backup de versiones de bases de datos

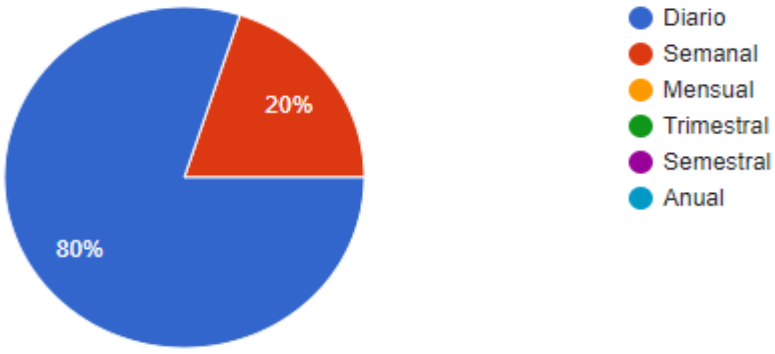


Fuente: Elaboración propia con herramienta Google Forms

En caso de respuesta afirmativa, ¿Con que frecuencia?

Gráfica 40

Porcentaje de frecuencia en que se realizan backup



Fuente: Elaboración propia con herramienta Google Forms

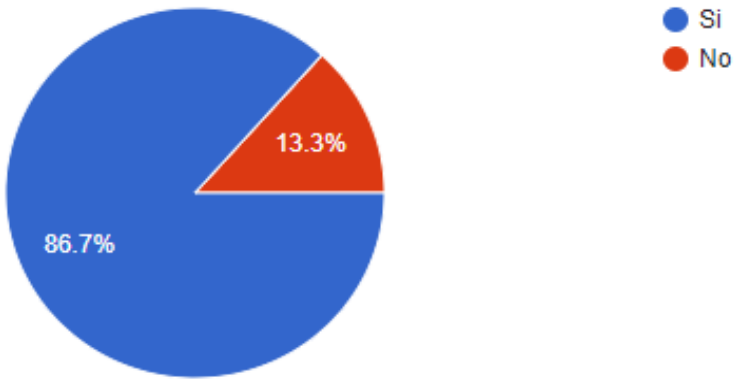
Análisis de resultados: De acuerdo al resultado obtenido el 100% de los encuestados confirmo que, si realizan backup de versiones de bases de datos, donde el 80% lo efectúan de forma diaria y un 20% de forma semanal.

Por lo anterior se concluye que las organizaciones cuentan con estrategias para proteger y recuperar la información ante un robo, hurto, secuestro, pérdida de datos o posibles ataques cibernéticos.

13. ¿Realizan respaldo de programas ejecutables y códigos fuentes de los sistemas en producción?

Gráfica 41

Porcentaje que realizan respaldo de programas ejecutables y códigos fuentes



Fuente: Elaboración propia con herramienta Google Forms

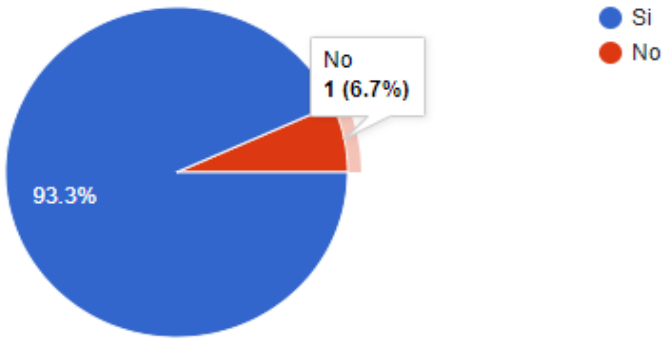
Análisis de resultados: Según los resultados obtenidos de la muestra se define que el 86.7% de los Ingenieros de Infraestructura tienen como buena práctica realizar respaldo de programas y fuentes de los sistemas en producción, mientras que el 13.3% no lo aplica.

De acuerdo al resultado, se concluye que la organización tiene establecidos medidas y procedimientos de respaldo de la información el cual permite garantizar la integridad y disponibilidad de los datos frente a cualquier eventualidad a la que puede estar expuesta de forma parcial o total.

14. ¿En caso de tener sistemas o servicios tercerizados, se les solicitan a los proveedores SLA (Acuerdo de Nivel de Servicio) que se adecuen a las responsabilidades y obligaciones que la organización demanda?

Gráfica 42

Porcentaje de servicios tercerizados con SLA que se adecuan a las responsabilidades de la organización



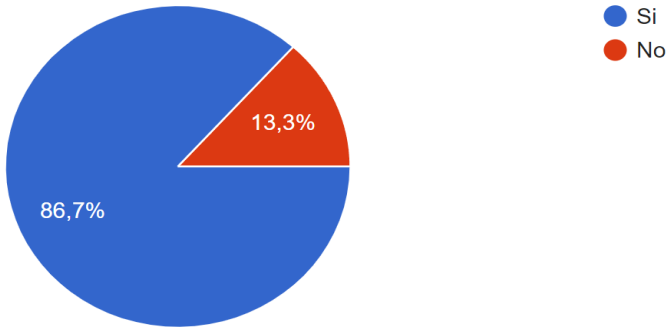
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: De la muestra de empleados del Área de Tecnología encuestados, el 93.3% confirmaron que la organización para la que laboran si cuenta con un Acuerdo de Nivel de Servicio; con ello se concluye que como área de TI tiene procedimientos y medidas de seguridad establecidos que les permite el resguardó de la información con los tres pilares fundamentales de la confidencialidad, disponibilidad e integridad de los datos y se adecuan a las responsabilidades y obligaciones que la organización demanda. Mientras que un 6.7% comento que la organización no tienen un SLA establecido.

15. ¿Las conexiones remotas son validadas por un directorio activo que provea las políticas dictadas por el administrador de red e impuestas al usuario de dominio?

Gráfica 43

Porcentaje de conexiones remotas que son validadas por un directorio activo



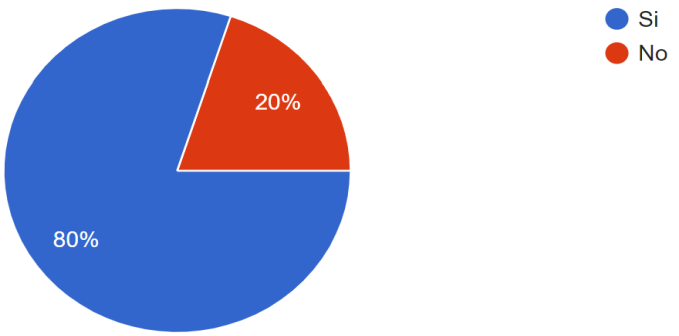
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Se muestra que la mayoría de organizaciones, con un 86.7% si poseen una entidad central autenticadora, siendo un pilar importante para validar a los usuarios y asignarles permisos de acuerdo a su perfil y función. Y el 13.3% no cuentan o desconoce si las conexiones remotas son validadas por un directorio activo.

16. ¿Las conexiones remotas son validadas por un NAC (Network Access Control), que provea las políticas dictadas por el administrador de red?

Gráfica 44

Porcentaje de conexiones remotas que son validadas por un NAC



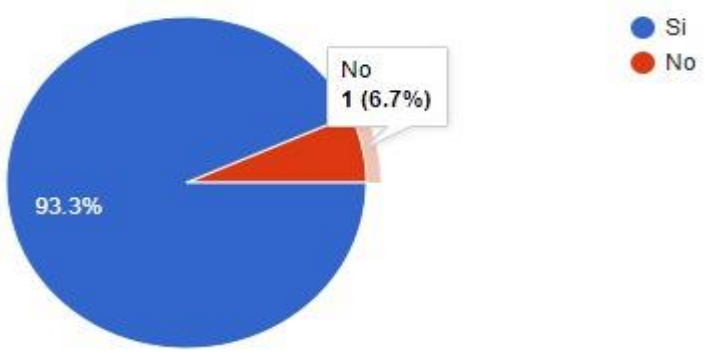
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: El NAC resulta ser muy útil y recomendado para el aseguramiento del acceso a los recursos institucionales, gracias a la asignación dinámica de usuarios dentro de una red corporativa. Esta metodología está siendo usada por la mayoría de las organizaciones encuestadas con un 80%; mientras que un 20% no cuenta o desconoce sobre dichas validaciones.

17. ¿Las conexiones remotas son validadas por perfiles y políticas de navegación establecidas por el firewall perimetral?

Gráfica 45

Porcentaje de conexiones remotas que son validadas por perfiles y políticas de navegación



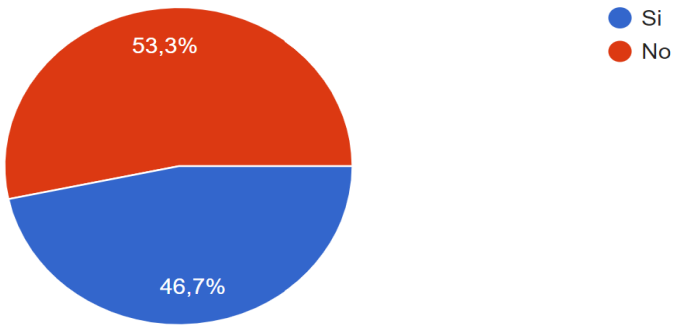
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Una minoría de la muestra, con un 6.7% no tiene implementado o bien desarrollado un firewall perimetral para contener anomalías externas, en contraste el 93.3% si cuentan con las medidas de validación de perfiles y políticas de navegación establecidas por el firewall perimetral.

18. ¿La seguridad de las conexiones remotas son validadas por un doble factor de autenticación?

Gráfica 46

Porcentaje de conexiones remotas que son validadas por un doble factor de autenticación



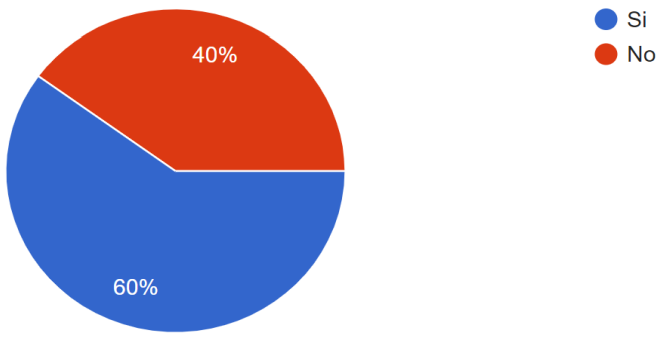
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Con el 53.3%, la mayoría de organizaciones encuestadas, aún no cuentan con doble factor de autenticación; siendo este un método que permite garantizar una validación más segura de los clientes. Mientras que el 46.7% indico que las conexiones remotas son validadas por un doble factor de autenticación.

19. ¿Dentro de la organización cuentan con un SIEM (Security Information and Event Management) o DLP (Data Loss Prevention) para hacer análisis de vulnerabilidades y trazabilidad de la información, para creación y actualización de escenarios de riesgo?

Gráfica 47

Porcentaje de las organizaciones que cuentan con un SIEM o DLP



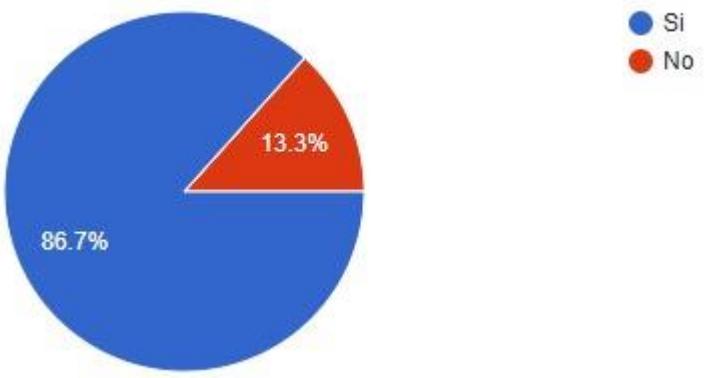
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Según el resultado obtenido, el 60% hace uso de SIEM o DLP, los cuales están implementándose considerablemente hoy en día; sin embargo, deberá de darse a conocer a aquellos sectores que aún no lo aplican, ya que un 40% representa mucha infraestructura que no está recopilando información sobre el comportamiento del tráfico entrante y saliente de sus organizaciones, dejando puntos ciegos a las mismas.

20. ¿Posterior a identificar un evento disruptivo, la información recopilada por los sistemas de monitoreo de eventos, es trasladada a los responsables de la seguridad de la información establecidos por la organización?

Gráfica 48

Porcentaje de la información recopilada por los sistemas de monitoreo de eventos, si es trasladada a los responsables de la seguridad de la información



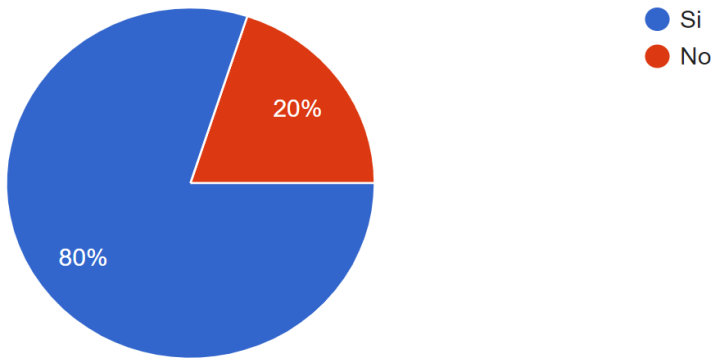
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: La mayoría de la muestra de personal de tecnología encuestada, con un 86.7% poseen un equipo de seguridad especializado, que recibe la información de incidentes, esta es estudiada y llevada a un punto de análisis para identificar los escenarios de riesgo a los que están expuestos. Mientras que el 13.3% no reporta los eventos disruptivos detectados a las áreas correspondientes, establecidas por la organización.

21. ¿Poseen una política y medidas de seguridad de apoyo para gestionar los riesgos de seguridad debido al uso de dispositivos móviles?

Gráfica 49

Porcentaje que posee una política para gestionar los riesgos de seguridad debido al uso de dispositivos móviles



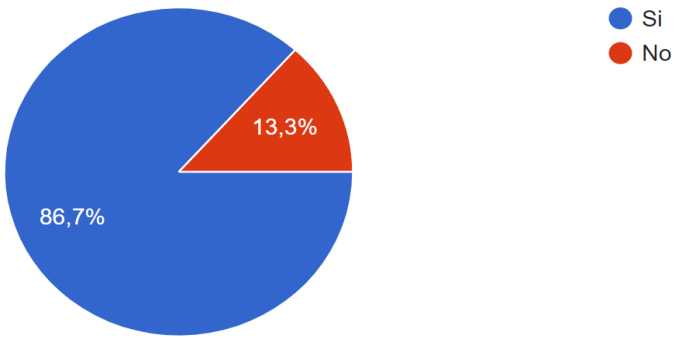
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: El 80% de los encuestados, afirma estar aplicando medidas normativas para gestionar el uso de dispositivos móviles que ingresan a la red corporativa. En contraste el 20% no poseen dichas políticas o las desconocen.

22. ¿Cómo área de tecnología considera que el trabajo remoto cumple con las expectativas de la seguridad de la información establecidas por la organización?

Gráfica 50

Porcentaje que considera que el trabajo remoto cumple con las expectativas de la seguridad de la información



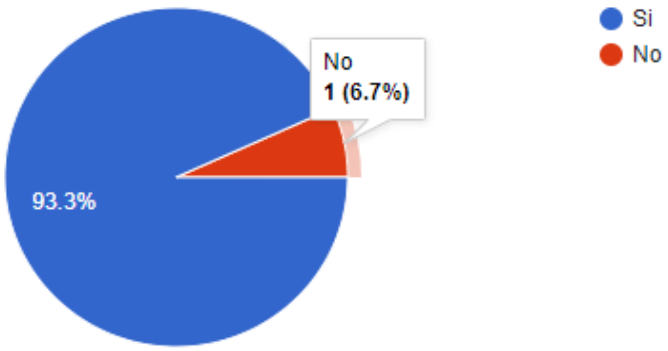
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: La mayoría de la muestra de personal de TI con un 86.7%, afirma estar cumpliendo los requerimientos mínimos que necesitan para proteger sus activos de información. Sin embargo, en las preguntas anteriores se puede notar que aún falta desarrollar mucho en la parte de recopilación, monitoreo, análisis e interpretación de las transacciones generadas en la red. El 13.3% considera que el trabajo remoto no cumple con las expectativas de la seguridad de la información.

23. ¿Considera usted importante que la falta de conocimiento sobre la seguridad de la información en la modalidad del teletrabajo puede impactar negativamente a la organización?

Gráfica 51

Porcentaje que considera que la falta de conocimiento sobre la seguridad de la información en la modalidad del teletrabajo puede impactar negativamente a la organización



Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Según la información dada por la muestra de personal de TI y como se espera, el 93.3% considera que es importante que la falta de conocimiento sobre la seguridad de la información en la modalidad de teletrabajo, puede impactar negativamente a la organización; riesgos como la fuga de información, pérdida y robo de datos, ataques de virus/ malwares, suplantación de identidades, ataque de phishing, entre otros; pueden ser evitados y controlados al capacitar y concientizar al personal sobre dichos riesgos. Solo un 6.7 % considera lo contrario.

Como una consulta abierta, se realizó la pregunta:

24. ¿Qué consideraciones, opiniones, mejoras, u observaciones, tiene acerca de los procedimientos que se toman en su organización en cuanto a la preparación que tuvo en la transición a modalidad de teletrabajo?

    Análisis de resultados: Personal de TI de diferentes organizaciones tuvieron el desafío de adaptar sus recursos a la modalidad de teletrabajo; desde invertir en equipamiento, plataformas, adecuar la infraestructura, capacitaciones a empleados, desarrollo de medidas de seguridad, etc. Entre las opiniones o inconvenientes se expresaron las siguientes:

    - El teletrabajo radica en la confianza sobre los empleados que la desempeñan, para fortalecer la confianza se debe definir un inventario de objetivos a cumplir y habilitar los accesos según las actividades operativas diarias en compañía de las jefaturas inmediatas, es responsabilidad del área informática facilitar los temas relacionados al acceso de programas o sistemas operativos, el garante de las tareas que realizan los empleados corresponde a las jefaturas o mandos medios en pro del bienestar de la empresa.
    - Debe haber una mejor concientización para la utilización de los medios provistos.
    - La infraestructura y el personal no estaba preparado para teletrabajo.
    - Las consideraciones para el teletrabajo con la pandemia, los anchos de banda contratados en las residenciales, no son suficiente para soportar la demanda requerida.
    - Más que todo detalles tales como mayor uso de filtración por direccionamiento MAC, seguridad biométrica, honeypots, loggings en firewalls y switches a nivel general.
    - Fue una medida improvisada, aunque necesaria, ayudó a la continuidad del negocio y requirió de grandes esfuerzos por parte del área de TI.

- Con respecto al teletrabajo considero que mi organización se adaptó de manera oportuna a la situación a través de la preparación de equipos con agentes DLP, SIEM, Antivirus, firewall, entre otros. Así como en la constante capacitación y evaluación de las medidas de seguridad de la información.
- Habilitar las auditorias para evidenciar que los trabajos realizados estén amparados a cambios solicitados no solo confiar en la buena fe de lo que hace.
- Es necesario trabajar en el cambio de mentalidad de parte de la dirección para que se otorgue un valor más alto a la información de la empresa para lograr un mayor involucramiento a la hora de implementar medidas como las que se adoptaron en pandemia. Afinar y probar los planes para afrontar este tipo de crisis también es necesario para no quedarse cortos cuando llegue el momento de actuar.
- Se necesita más exigencia en cuanto al uso de contraseñas robustas.
- Fue un proceso que llevo mucho trabajo y tiempo, ya que se tenían que preparar laptops, gestionar y otorgar permiso de VPN, operaciones administrativas que consumieron tiempo, pero que al final, se logró cubrir y mantener comunicados a todos los usuarios.

La diversidad de opiniones del personal de TI involucrado en la implementación del teletrabajo, demuestra los desafíos y decisiones que se debieron adoptar de forma inmediata; considerando los aspectos tanto de los recursos con los que la organización contaba, la capacidad de infraestructura, la inversión de plataformas y herramientas, conocimiento de los empleados, las medidas de seguridad, entre otros. Para permitir la continuidad operativa y logro de los objetivos, desde localidades diferentes a las oficinas organizativas.

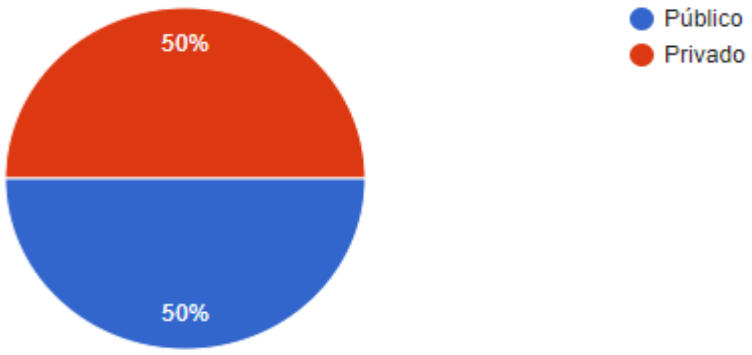
7.4 Encuesta Talento Humano/ Recursos Humanos

La presente encuesta tuvo como objetivo, conocer el tipo de modalidad de trabajo remoto en los que se encuentra la organización desde el inicio de la pandemia de la COVID-19 en El Salvador y las medidas que se gestionaron por parte del área de Talento Humano/ Recursos Humanos.

1. ¿A qué sector pertenece la organización?

Gráfica 52

Porcentaje de sector al que pertenece la muestra de personal de Talento Humano



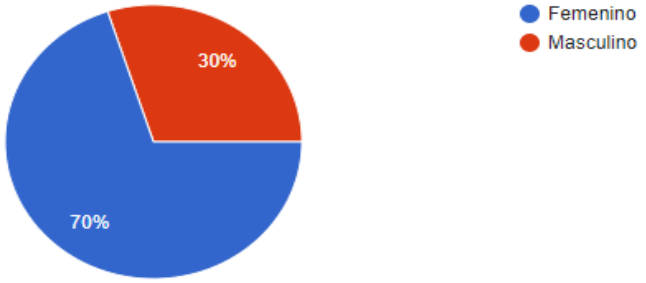
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Se puede apreciar en la gráfica que el porcentaje se distribuye equitativamente en un 50% que pertenece al sector privado como al sector público de la muestra de personal de Talento Humano.

2. ¿Seleccione su género?

Gráfica 53

Porcentaje de género en la muestra de personal de Talento Humano



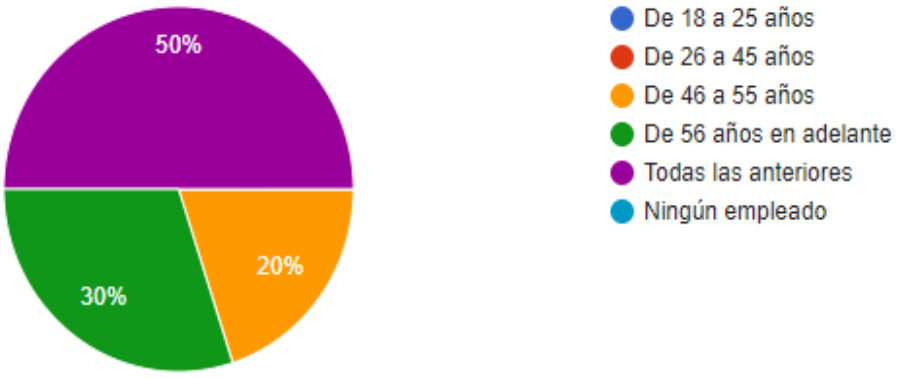
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Se muestra que la distribución de género en el ámbito de Talento Humano se divide 70% para el género femenino y un 30% para masculino.

3. ¿En qué rangos de edades los empleados de la organización fueron enviados en la modalidad de teletrabajo durante la pandemia de COVID-19?

Gráfica 54

Porcentaje de rangos de edades de personal enviado a modalidad de teletrabajo



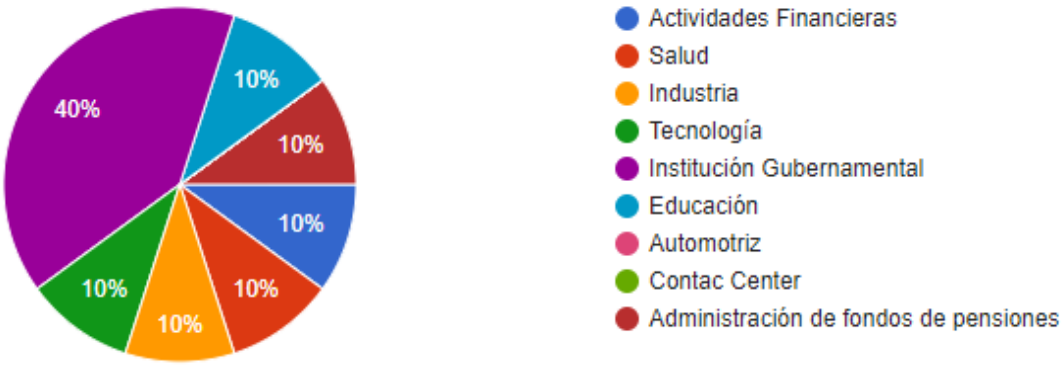
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Dependiendo de las decisiones de cada organización, se presenta diversos porcentajes sobre el rango de edades de empleados que fueron enviados en la modalidad de teletrabajo durante la pandemia de COVID-19. Con un 20% se ubica los rangos entre 46 a 55 años, el 30% fueron personas de 56 años en adelante y la mayoría con un 50% abarcando todas las edades de 18 años en adelante.

4. ¿Qué actividad realiza la organización?

Gráfica 55

Porcentaje de actividades que realizan las organizaciones de la muestra de personal de Talento Humano



Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: En la gráfica se observa la diversidad de actividades que realizan las organizaciones de la muestra de personal de Talento Humano, un 40% perteneciente a Instituciones Gubernamentales y 10% para cada uno de los demás sectores como son: Actividades Financieras, Salud, Industria, Tecnología, Educación y Administración de fondos de pensiones.

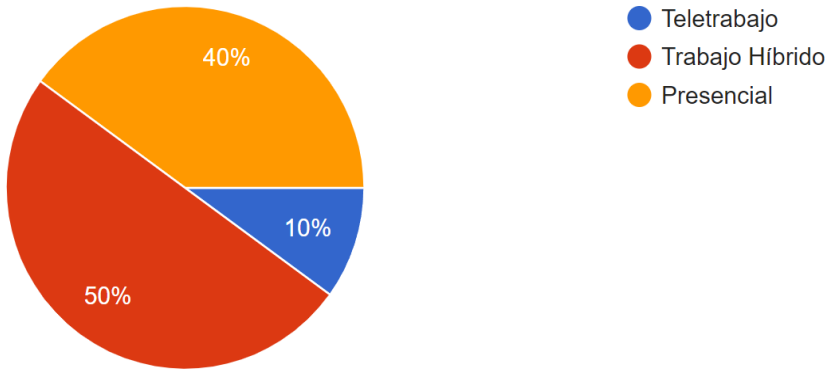
5. En la organización ¿En qué modalidad de trabajo los empleados laboran?

   En esta pregunta se especificó para la diferencia de los conceptos:

   - Teletrabajo: Según la Ley de Regulación de Teletrabajo, tiene un nuevo contrato laboral o cambio/adenda
   - Trabajo Híbrido: Modalidad mixta, tanto presencial en oficina como trabajo en casa

Gráfica 56

Porcentaje de modalidad de trabajo



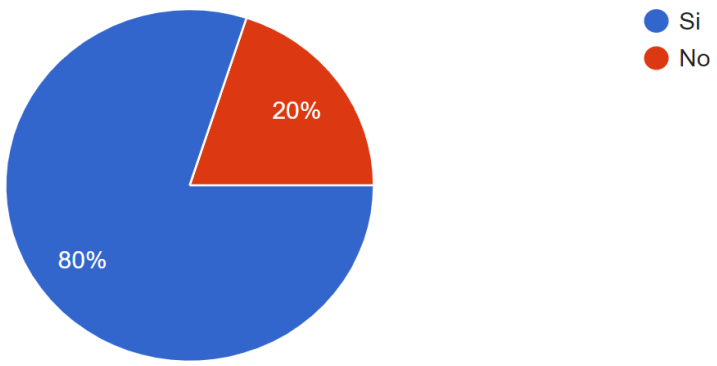
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Según el aporte de las unidades de Talento Humano, la mayoría de empleados están en la modalidad de trabajo híbrido con un 50%, por lo que están haciéndose presentes ciertos días de la semana. Un 40% en modalidad presencial y un 10% en modalidad de teletrabajo.

6. ¿Desde su punto de vista de Unidad de Talento Humano, considera que los empleados de la organización se han adaptado de forma general a realizar sus labores desde la modalidad de teletrabajo?

Gráfica 57

Porcentaje de muestra de personal de Talento Humano que considera que los empleados se han adaptado a la modalidad de teletrabajo



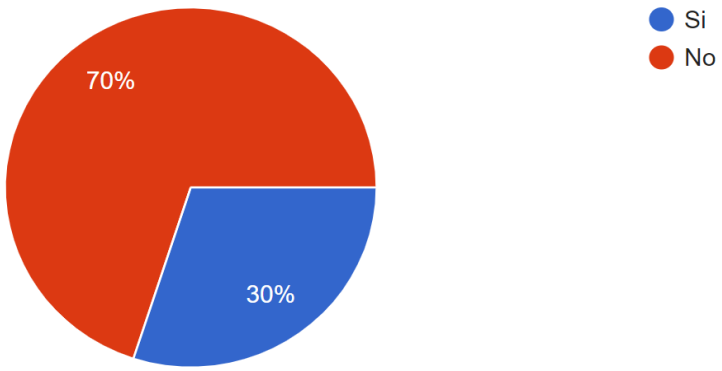
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Según la muestra del personal de Talento Humano, un 80% si ha logrado cumplir sus asignaciones desde casa. Esto es discutible, ya que la mayoría de sugerencias de los empleados están dirigidas a mejoras en la preparación y capacitación del personal. Mientras que un 20% considero que no se logró adaptar bajo la modalidad del teletrabajo desde el tiempo de pandemia de COVID-19.

7. Antes de la pandemia de COVID-19 ¿la organización tenía a algún empleado realizando labores bajo la modalidad de teletrabajo?

Gráfica 58

Porcentaje de organizaciones que tenían empleados realizando teletrabajo antes de pandemia de COVID-19



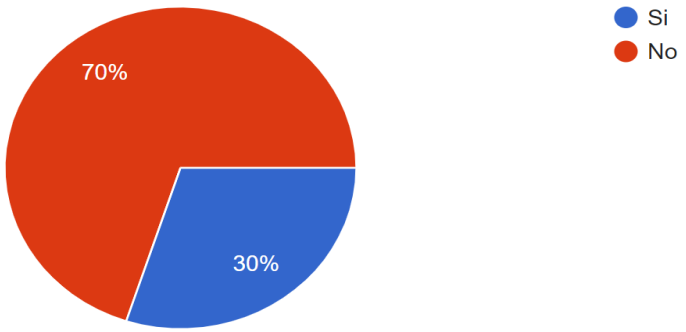
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: El 70% expreso que la organización no contaba con empleados en la modalidad de teletrabajo antes de pandemia de COVID-19. Por lo que se puede comprender que la implementación del teletrabajo en las organizaciones incrementó con la llegada de la Pandemia. Esto motivó al desarrollo de la infraestructura y sistemas de seguridad, medidas de autenticación más robustas y perfiles de seguridad mejor elaborados. Y un 30% ya contaba con persona en modalidad de teletrabajo.

8. Posterior a la pandemia COVID-19 ¿Se planea continuar con empleados en la modalidad de teletrabajo?

Gráfica 59

Porcentaje que considera que se continuará con empleados en la modalidad de teletrabajo



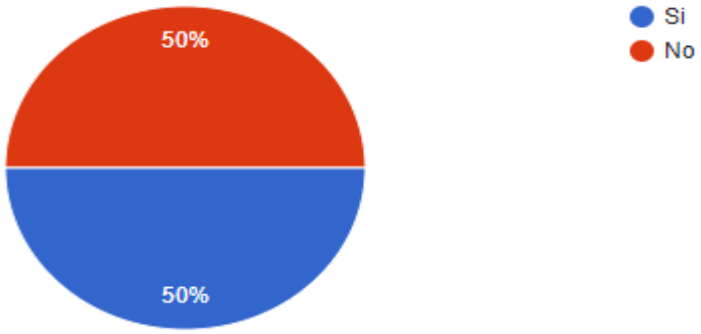
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Con un 70%, la mayoría de empresas no van a considerar seguir la modalidad de teletrabajo, mientras que un 30% considerará continuar bajo dicha modalidad.

9. En caso de respuesta afirmativa, ¿Se modificará el contrato laboral conforme a la ley de regulación de teletrabajo?

Gráfica 60

Porcentaje que considera que se modificará el contrato laboral



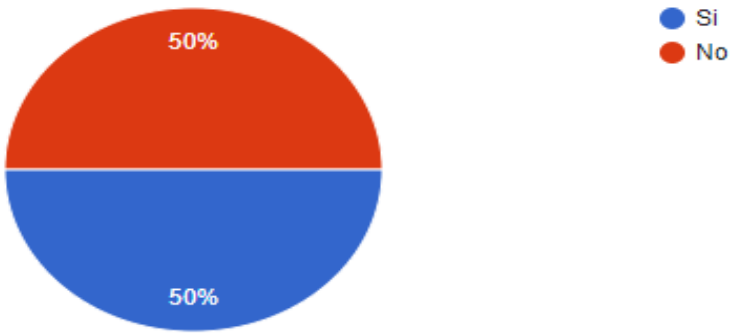
Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: Según resultados obtenidos un 50% de la muestra del Área de Talento Humano, indicó que no estaría realizando modificaciones en el contrato laboral; mientras que el otro 50% si efectuarán las modificaciones correspondientes amparados bajo la Ley de Regulación de Teletrabajo de El Salvador.

10. ¿Cómo organización posee un control de marcaciones de los horarios laborales en modalidad de teletrabajo?

Gráfica 61

Porcentaje que posee un control de marcaciones de los horarios laborales en modalidad de teletrabajo



Fuente: Elaboración propia con herramienta Google Forms

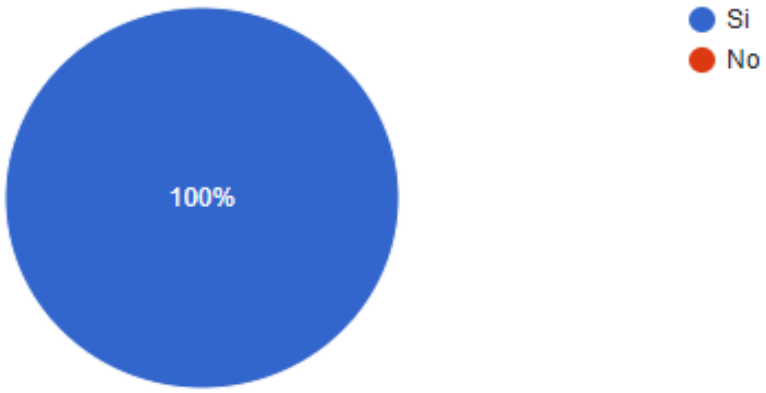
Análisis de resultados: De acuerdo a la gráfica 50% de la muestra, manifestaron no tener un control sobre las marcaciones de los horarios para los empleados que se encuentran bajo la modalidad de teletrabajo; sin embargo, el otro 50% indico que la organización para la que labora si tienen un control de marcaciones, el cual lo realizan por medio de un control de video llamadas, sistemas de conexiones informáticas y GPS, o registros de horario de conexión a los sistemas, etc. Por lo anterior al tener un esquema de trabajo bien definido permitirá a cada empleado lograr los

niveles de desempeño esperados, así como cumplir con los objetivos establecidos según la organización.

11. ¿Ante una crisis como la pandemia de COVID-19, considera el teletrabajo una opción buena e innovadora para la continuidad operativa?

Gráfica 62

Porcentaje que considera el teletrabajo una opción buena e innovadora para la continuidad operativa ante una crisis.



Fuente: Elaboración propia con herramienta Google Forms

Análisis de resultados: De la muestra de empleados del Área de Talento Humano, el 100% manifestó que el trabajar bajo la modalidad de teletrabajo es considerada como una buena opción e innovadora; con ello se logró identificar diferentes aspectos como: la facilidad de la ejecución de las tareas asignadas, la continuidad de las operaciones dentro de la organización no fueron impactadas grandemente, se logró salvaguardar la vida de los empleados en el tiempo de la pandemia de COVID-19, entre otros.

Como una consulta abierta, se realizó la pregunta:

12. ¿Qué consideraciones, opiniones, mejoras, u observaciones, tiene acerca de los procedimientos que se toman en su organización en cuanto a la preparación que tuvo en la transición a modalidad de teletrabajo?

Análisis de resultados

Con la llegada de la pandemia COVID-19 muchas organizaciones tuvieron un gran reto ya que muchos de los empleados fueron obligados a trabajar desde sus casas, adaptándose a nuevas medidas seguridad de los datos. De la muestra de personal de Talento Humano, manifestaron sus diferentes opiniones, mejoras u observaciones acerca de la transición de la modalidad Presencial a la modalidad de Teletrabajo. A continuación, se detallan algunos comentarios al respecto:

- Es necesario considerar como una buena práctica capacitaciones a los empleados, para concientizar sobre la importancia del resguardo y protección de los datos, así como ante un ataque de phishing o un ciberataque, tener el conocimiento adecuado de la acción a realizar ante este evento y el escalamiento al área correspondiente establecido por la organización.
- La mayoría de los empleados debió adaptarse a la modalidad de teletrabajo impulsado por la pandemia el cual tuvieron que invertir en un espacio de trabajo o insumos de oficinas para realizar las actividades laborales asignadas.
- Implementar el desarrollo de un sistema de evaluación de desempeño para el personal administrativo.
- Hay algunos puestos de trabajo que, si existe la posibilidad que se pueden adecuar y otros no se adecuan a la modalidad de teletrabajo, debido que existen muchos procesos manuales y cargos funcionales que requiere la presencia del personal en sitio.

CAPITULO 8

8.1 Desarrollo de guías de buenas prácticas aplicadas a la modalidad de teletrabajo

Debido a la pandemia de COVID-19, la ciberseguridad ocupa un lugar importante hoy en día en cualquier organización; por lo que es necesario adquirir una guía de buenas prácticas de seguridad para la información, que le permita a las organizaciones el poder fortalecer sus defensas ante cualquier amenaza y mitigar los riesgos informáticos.

Cabe mencionar que independientemente del tamaño o rubro de la organización, pueden ser víctimas de ataques ya sean internos o externos.

Con el resultado de las encuestas focalizadas en el Área de TI, Talento Humano y a los empleados de las diferentes organizaciones, se detallan sugerencias de guías de buenas prácticas de ciberseguridad para la modalidad de teletrabajo.

8.1.1 Buenas prácticas de ciberseguridad para empleados en modalidad de teletrabajo

	**1- Configurar y asegurar la red inalámbrica domestica**	**Revisión 1.0**
	Una red doméstica es un grupo de dispositivos como: computadoras, sistemas de juegos, impresoras, teléfonos, tablets y dispositivos portátiles, que se conectan a Internet y entre sí. Una red doméstica segura es de suma importancia, los ciberdelincuentes pueden beneficiarse de redes vulnerables para llevar a cabo una serie de cibercrímenes, como instalar malware, realizar un robo de datos e identidad, etc. Entre las recomendaciones se pueden listar:	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Cambiar la contraseña de router periódicamente cada seis meses o un período similar, debido a que los enrutadores inalámbricos suelen venir previamente configurados con contraseñas predeterminadas. Cambiar a una contraseña robusta con al menos 8 caracteres de largo (idealmente más) y que contenga una mezcla de letras en mayúscula y minúscula, números y símbolos.
b) Fortalecer el cifrado de Wi-Fi, la mayoría de los enrutadores inalámbricos cuenta con una función de cifrado, la cual está normalmente desactivada de forma predeterminada. Activar la configuración de cifrado del enrutador doméstico puede ayudar a proteger la red. Deshabilitar WPS (Wi-Fi Protected Setup), WPA2 y WPA3 son las mejores opciones, ya que son sistemas más recientes y seguros.
c) Crear un acceso SSID diferente para invitados, que también utilice WPA2 o WPA3 y que esté protegida por una contraseña robusta. Utilizar esta red de invitados para las visitas, ya que es posible que utilicen dispositivos comprometidos o infectados con malware.
d) Actualización de firmware del enrutador, una buena práctica de ciberseguridad es mantener actualizado el firmware del enrutador; ya que una versión antigua puede contener vulnerabilidades que los ciberdelincuentes pueden aprovechar.

	**2- Realizar copias de seguridad del empleado**	**Revisión 1.0**
	Es de suma importancia el contar con los respectivos respaldos de la información; de lo contrario, se convierte en un riesgo para la organización, dado que pueden presentarse incidentes, amenazas o perdidas a datos vitales.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Esto permite asegurar la disponibilidad, confidencialidad e integridad de la información, asegurando y protegiendo los datos e información realizando copias de seguridad periódicamente.
b) Establecer procedimiento de backup (forma manual), donde el usuario sea responsable de asegurarse de hacerlo y notificarlo al área asignada por la organización.
c) La organización cuente con herramientas automatizadas que realicen los respaldos en horarios establecidos y que le sean notificado a los empleados.

d) Evitar realizar respaldos de información ajena al ámbito laboral, como son fotos, videos, música, juegos, etc. De índole personal, ya que se corre el riesgo de saturar los espacios asignados.

	3- Asegurar el acceso a sistemas y dispositivos	**Revisión 1.0**
	El realizar teletrabajo desde los hogares, implica el acceso a programas, plataformas o sistemas de la organización, utilizando diferentes equipos a los habituales. Por tanto, se debe considerar los siguientes puntos:	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Utilizando contraseñas robustas y diferentes para cada aplicación y realizar el cambio de forma periódica, así como la autenticación por 2FA (doble factor de autenticación)
b) Evitar el uso de contraseñas como los nombres, fechas de cumpleaños, organización, nombre de un familiar o una persona famosa que pueden ser fáciles de descifrar.
c) Nunca revelar las contraseñas a otras personas.

	4- Protección en correo electrónico	**Revisión 1.0**
	El correo electrónico es una de las herramientas de trabajo más utilizada hoy en día; debido a los múltiples beneficios para la comunicación, por lo que es necesario resaltar la importancia del uso adecuado del correo, ya que el primer objetivo de los ciberdelincuentes es acceder a los datos privados de la empresa a través de ataques de phishing y spam. Por lo anterior se detallan algunas recomendaciones que se deben de tener en consideración:	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) No abrir mensajes o archivos adjuntos con enlaces desconocidos.
b) Nunca descargar software o aplicaciones de enlaces obtenidos por medio de correo electrónico, aplicaciones de mensajería instantánea o redes sociales, ya que puede dirigir a sitios web fraudulentos.
c) No permitir que los empleados usen las direcciones de correo electrónico de la organización para uso personal.
d) Evitar acceder al correo electrónico desde cualquier zona Wi-Fi públicas no conocidas.
e) Nunca proporcionar las contraseñas a terceros.
f) No brindar o solicitar datos sensitivos por medio de correos electrónicos.

	5- Navegación segura	**Revisión 1.0**
	Hoy en día el navegar por internet de forma segura es un gran reto para la mayoría de las organizaciones, debido que es uno de los objetivos principales de la industria del cibercrimen. Por eso, debe de existir formación de buenas prácticas de navegación para los empleados, así como procedimientos y normas que detallen instalaciones y configuraciones seguras en los diferentes equipos del navegador web.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Revisar periódicamente la configuración de privacidad de las cuentas de redes sociales, páginas web, etc.
b) Utilizar los servicios de conexión remota VPN (Red Privada Virtual)
c) Verificar la dirección de una página web sea la correcta en la barra de navegación, ya que los ciberdelincuentes pueden replicar completamente una página web y extraer credenciales.
d) Validar en el navegador web, que la url o enlace del sitio, se inicie con https y aparezca la imagen de un candado, esto asegurará que el sitio es legítimo.
e) Mantener actualizado el antivirus y los diferentes navegadores.

	6- Protección de malware, virus, ransomware, etc.	**Revisión 1.0**
	La protección de las computadoras y dispositivos móviles debe ser un elemento fundamental para los usuarios, ya que con frecuencia se pasa por alto y se tienen consecuencias adversas para el dueño de la computadora. A continuación, se detallan algunas recomendaciones a implementar para evitar ser una víctima de ataques cibernéticos:	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Utilizar y actualizar aplicaciones antimalware con protección en tiempo real.
b) Realizar monitoreos de antivirus periódicamente.
c) Activación y actualización de Firewall.
d) Evitar descargas manuales y automáticas ajenas a las establecidas por la organización, como contenido multimedia en sitios de poca confianza.

	7- Actualización de software	**Revisión 1.0**
	Como una buena práctica de la protección de los sistemas de información de una organización, es necesario realizar una correcta gestión de actualizaciones y parches de seguridad que permitan la prevención de virus o ataques cibernéticos en los equipos de trabajo. A continuación, se recomiendan algunas buenas prácticas a considerar en la modalidad de teletrabajo:	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) En la manera en que los recursos lo permitan tener un entorno de pruebas de aplicación de los parches que permita verificar la funcionalidad de los sistemas previo a la aplicación en producción, para prevenir vulnerabilidades de virus incluyendo el ransomware.

b) Actualizaciones automáticas o manuales de software de los sistemas de la organización.
c) Realizar las verificaciones correspondientes, una vez que se efectúen las actualizaciones de los sistemas, estos se encuentren funcionando correctamente.
d) Evitar sistemas operativos que ya no cuenten con soporte.

	8- Protección de dispositivos móviles	**Revisión 1.0**
	Hoy en día la protección de los dispositivos móviles es de gran importancia; ya que el creciente uso de dichos dispositivos se ha tornado un blanco atractivo de la delincuencia informática.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) No descargar e instalar aplicaciones no autorizadas por la organización.
b) Cerrar sesiones y conexiones al final de su uso.
c) Implementación de contraseñas robustas.
d) Evitar conectar a redes Wi-Fi desconocidas o públicas.
e) Realizar copias de seguridad de los dispositivos.
f) Siempre que el Sistema Operativo notifique las actualizaciones de nueva versión, se puedan aplicar con el objetivo de evitar posibles vulnerabilidades.

	9- Separación de áreas (Personal, familiar, laboral)	**Revisión 1.0**
	Trabajar en casa, hasta hace poco tiempo, solía ser una elección para profesionales de algunas organizaciones. Hoy en día la modalidad de teletrabajo ha tomado mucha importancia; por lo que es necesario separar el trabajo, de las cuestiones familiares para obtener una vida saludable. Así como una conciliación de nuevas oportunidades de desarrollo personal, social y profesional.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Creación de perfiles con particiones y cuentas separadas, los perfiles o niveles de acceso a los recursos y a la información tienen que configurarse en función de los roles de cada empleado.
b) Desactivar cámaras y micrófonos, cuando no son necesarios.
c) No compartir el escritorio cuando este autenticándose al sistema, por error puede ingresar contraseña en el nombre del usuario.
d) Activar bloqueo de pantalla una vez se ausente del área de trabajo y bloqueo automático por inactividad después de 10 minutos.
e) Mantener una política de escritorio limpio.
f) Evitar el uso de post-it con contraseñas a la vista.
g) Firmar una política de seguridad del uso de recursos de la empresa, para propósitos personales y conocer sus sanciones.
h) Las contraseñas son de índole personal y no pueden compartirse bajo ningún motivo.
i) No deben anotarse en libretas o cuadernos, datos de usuarios y contraseñas de sesiones de trabajo, que puedan ser accedidos o usados por otros.

	10- Buen uso de servicios corporativos	**Revisión 1.0**
	Proteger la información hoy día se ha convertido en un reto constante para las organizaciones, por lo que poner en práctica la seguridad de la información debe ser la base fundamental para el funcionamiento de la Ciberseguridad en los servicios corporativos.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Se recomienda evitar la conexión de dispositivos corporativos a la red desde lugares públicos, así como la conexión a redes Wi-Fi abiertas no seguras.
b) Cuando se dispone de un equipo corporativo, no se debe utilizar con fines particulares evitando el acceso a redes sociales, correo electrónico personal, páginas web con publicidad impactante y emergente, así como otros sitios susceptibles de contener virus o favorecer la ejecución de código dañino.
c) Asegurar los dispositivos con contraseñas, PIN o con autenticación de biometría.
d) Se recomienda cerrar las sesiones y conexiones remotas al concluir con las actividades laborales.
e) Como empleado debe tener definidos los roles y accesos con los que deberá contar al momento de la ejecución de las tareas laborales.
f) Realizar bloqueo de la sesión al levantarse del puesto de trabajo, así como la obligación de guardar los documentos de trabajo al terminar la jornada laboral, aplicando la política de escritorios limpios.
g) No efectuar configuraciones en el equipo, e instalar aplicaciones no autorizadas por la organización.

	11- Comunicación y colaboración	**Revisión 1.0**
	Todas las organizaciones, sin importar su sector o tamaño dependen de una comunicación constante entre colaboradores y clientes, por lo que es necesario enfatizar sobre las herramientas a utilizar para dicha comunicación, teniendo en cuenta la seguridad y la protección de los datos de la organización.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Si se detecta una sospecha de que la información de la organización ha sido comprometida es necesario comunicarlo de carácter inmediato a los canales definidos por la organización.
b) Al tener reuniones a través de videoconferencias, se recomienda establecer comunicación solo con usuarios conocidos y bajo las plataformas que la organización tiene autorizadas.
c) Determinar si las personas autorizadas a participar en las reuniones son las que realmente deben ser, verificando la identidad de nuevos contactos en caso de iniciar por primera vez una videoconferencia con ellos.

	**12- Capacitación y concientización de empleados**	**Revisión 1.0**
	El factor humano es un pilar fundamental en la ciberseguridad. El mayor porcentaje de brechas de seguridad se producen en los puestos finales de los empleados mediante campañas maliciosas de phishing o ransomware. Por lo tanto, se proporcionan algunas recomendaciones para ponerse en práctica:	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Cumplir las políticas de seguridad corporativas establecidas por la organización; así como de los procedimientos y las mejores prácticas para el cuidado de la información, tanto personal como de terceros.
b) Evitar abrir correos electrónicos de direcciones desconocidas, descargar música, juegos o videos en los dispositivos corporativos.
c) Los empleados deben aprender y conocer las mejores prácticas y procedimientos para mantener las redes y los datos seguros, así como las consecuencias de no hacerlo.
d) Asistir a las capacitaciones brindadas por la organización sobre seguridad de la información o notificar en caso de no hacerlo y puedan reprogramar la capacitación.

	**13- Guardar la información en los espacios de red habilitados**	**Revisión 1.0**
	Las organizaciones deben contar con políticas, controles que les permita identificar todos los dispositivos y conexiones que se encuentran en la red, con el objetivo de identificar el uso no autorizado o indebido de repositorios en la nube establecidos por la organización.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Evitar almacenar la información de los datos de forma local en los dispositivos, se recomienda realizarlo en los recursos de almacenamiento compartidos o en la nube proporcionados por la organización.
b) Si utiliza la política de “Trae Tu Propio Dispositivo - BYOD (Bring Your Own Device) no utilizar o descargar aplicaciones no autorizadas por la organización.
c) No se debe bloquear o deshabilitar la política de copia de seguridad corporativa definida para cada dispositivo.
d) Evitar el resguardo de información personal en repositorios de la nube y utilizar únicamente los establecidos por la organización.

8.1.2 Buenas prácticas de ciberseguridad para área de TI en modalidad de teletrabajo

	1- Asegurar el acceso a sistemas y dispositivos	Revisión 1.0
	La primera capa de seguridad de cualquier sistema o dispositivo como activo de información, es la validación de autenticación. Asegurar que el ente solicitante sea quien dice ser; garantizará que la información, procesos y servicios se mantengan íntegros.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Limitar el acceso a los empleados a los sistemas de la organización.
b) Establecer que la empresa u organización debe emitir una política que defina las condiciones y restricciones para el teletrabajo. Evaluar qué activos físicos y de información están vinculados a la actividad de teletrabajo, y con base en ello, realizar una evaluación de riesgos aplicada a esos activos, implementando controles adecuados para mitigar y eliminar los riesgos identificados. (ISO 27001/ control A 6.2.2)
c) Establecer una propuesta para definir roles y responsabilidades para implementar un plan de tratamiento de riesgo de seguridad.
d) Es necesario tener mecanismos de protección de autenticación definidos (certificados, contraseñas, tokens, sistemas de doble factor de autenticación) que permita validarse ante los sistemas de control de acceso remoto de la organización.

	2- Protección de malware, virus, ransomware, etc.	Revisión 1.0
	La seguridad contra el malware es la segunda capa importante de protección para las computadoras, servidores o redes. Un paquete de antivirus eficaz es una parte importante de la defensa técnica que debe tener todo sistema informático personal y empresarial. La protección de antivirus bien diseñada tiene varias características. Escanea cualquier programa recién descargado para asegurarse de que esté libre de malware, virus, hasta analizar el comportamiento de archivos para verificar que no estén siendo cifrados por un ransomware.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Activación y actualización de firewall, contratos vigentes de licencia, contratos de soporte y mantenimiento.
b) Implementar mecanismos de filtrado de red, como firewalls y software de detección de intrusos. Hacer cumplir las políticas adecuadas para controlar el tráfico entrante y saliente
c) Establecer una DMZ (Zona Desmilitarizada) con el fin de proteger la red interna.
d) Realizar backups con versiones.
e) Implementación de consola de gestión de antivirus y despliegue del endpoint en equipos de la organización.
f) Actualización de parches de seguridad.

g) En la manera en que los recursos lo permitan tener un entorno de pruebas de aplicación de los parches que permita verificar la funcionalidad de los sistemas previo a la aplicación en producción, para prevenir vulnerabilidades de virus incluyendo el ransomware.

	3- Actualización de software	**Revisión 1.0**
	Las actualizaciones instalan mejoras en la funcionalidad y la seguridad del software. Si no se actualiza el sistema operativo, sus sistemas estarán expuestos a agujeros de seguridad e infracciones que pueden provocar el robo de información personal, la invasión de la privacidad y hasta información corporativa.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Mantener actualizada consola de gestión de antivirus.
b) Monitorear el estado de las actualizaciones de los dispositivos y aplicaciones.
c) Disponer de un sistema de alerta que notifique las vulnerabilidades existentes y la necesidad de realizar actualizaciones, como un SIEM (Security Information and Event Management) o DLP (Data Loss Prevention).
d) Crear un registro de todas las actualizaciones realizadas.

	4- Protección de dispositivos móviles	**Revisión 1.0**
	La protección de dispositivos móviles es un patrón de políticas, tácticas y herramientas diseñadas para fortalecer los dispositivos móviles contra las amenazas de seguridad a los que están expuestos en internet. De no ser por la seguridad aplicada a los dispositivos móviles, las redes corporativas pueden verse vulneradas por el simple hecho de que estos se conecten y formen parte de la red.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Establecer que se debe adoptar una política y medidas de seguridad de apoyo para gestionar los riesgos de seguridad debido al uso de dispositivos móviles. Equipos como portátiles u ordenadores en las condiciones propias del teletrabajo. (ISO 27001/ control A 6.2.1)
b) Ejecución de antivirus.
c) Control de acceso a software, claves, contraseñas, preguntas de seguridad.
d) Instalar soluciones de seguridad en todos los dispositivos.
e) Encriptación de la información.
f) Realizar copias de seguridad periódicamente.
g) Políticas de altas y bajas de dispositivos móviles.

	5- Capacitación y concientización de empleados	**Revisión 1.0**
	Educar al personal sobre temas de protección de equipos corporativos con acceso a los recursos e información, constituye el objetivo fundamental de un programa de sensibilización. Es así como se prepara al eslabón más débil ante cualquier ataque desde internet usando ingeniería social.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 29/06/2022**

a) Establecer que todos los empleados de la organización deben contar con una concientización y con una formación actualizada de manera periódica, para llegar a garantizar que las políticas y procedimientos se implementen de manera correcta. Aunque una buena parte se puede abordar con actividades como reuniones, capacitaciones en línea, foros o publicaciones en la intranet o en carteleras a las que tienen acceso todos los trabajadores. (ISO 27001/ Control A 7.2.2)
b) Solicitar firmas de política de seguridad del uso de recursos de la empresa a los empleados, para evitar su utilización para otros propósitos que no sean laborales.
c) Coordinación del área de TI con los canales establecidos por la organización, de que se cumplan las políticas, lineamientos o participación en las capacitaciones sobre la concientización de la seguridad de la información por parte de los empleados.

	6- Guía para gestionar el riesgo	**Revisión 1.0**
	Es importante realizar un análisis periódico de eventos y factores de riesgo, para identificar amenazas, con el objetivo de mejorar el entendimiento de los factores de riesgo internos y externos asociados.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Realizar controles de eventos y/o registros históricos que puedan proveer un panorama de los posibles factores de riesgos a los activos de TI puedan estar expuestos, en cuanto a fuga de información, intrusiones maliciosas, afectación de la integridad y confidencialidad, de los datos que permita capturar información relevante de cuestiones, incidentes, problemas e investigaciones.
b) Posterior a un evento disruptivo; es necesario analizar y determinar las condiciones específicas que existan o faltan cuando ocurren los eventos.
c) Analizar regularmente que tipos de amenazas son coincidentes para construir y actualizar los escenarios de riesgos.
d) Desarrollar y capturar información sobre el estado del plan de acción para tratar las amenazas; y procedimientos que permitan construir escenarios de riesgos.
e) Informar sobre los resultados del análisis de riesgo a todas las partes interesadas afectadas en términos y formatos útiles para apoyar las decisiones de la organización.
f) Proporcionar a los responsables de la toma de decisiones, la comprensión de los escenarios más probables y peores, exposiciones a pérdidas de información y tecnología.

g) Informar de forma periódica sobre el perfil de riesgo actual a todas las partes interesadas y revisar los resultados de las evaluaciones y revisiones de auditoría interna y de aseguramiento de la calidad.

	**7- Servicios tercerizados**	**Revisión 1.0**
	La tercerización de procesos y servicios resulta ser una manera cómoda y estratégica de las organizaciones para ceder el riesgo. Es decir, que bajo un contrato donde se establecen compromisos ligados a un marco legal, muchos procesos de resolución de problemas serán atendidos por terceros, garantizando una respuesta optima y contundente sobre los escenarios de riesgo y garantizando su resolución.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**
a) Redactar acuerdos con los proveedores que incluyan los requerimientos para abordar los riesgos de la información. (ISO 27001/ A 15.1.3) b) Verificar que dichos requerimientos incluyan toda la cadena de suministros (ISO 27001/ A 15.1.3) c) Establecer un plan de auditorías de seguridad en los servicios que entrega el proveedor (ISO 27001/ A 15.2.1) d) Se debe evitar dejar sesiones abiertas que comprometan o pongan en riesgo información confidencial y pueda ser accesibles por terceros.		

	**8- Reforzamiento de las redes inalámbricas corporativas**	**Revisión 1.0**
	Reforzar la red Wi-Fi de una organización es un desafío para los responsables de las áreas de tecnología, debido a que cualquier falla en la red inalámbrica puede dañar toda la infraestructura de comunicaciones, dichas fallas en la red pueden facilitar la propagación de malwares, virus, filtración de usuarios maliciosos, etc.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**
a) Separar el tráfico proveniente de las redes Wi-Fi corporativas de las redes Wi-Fi de invitados. b) La gestión de las redes de invitados debe tener como capa de autenticación la creación de Tokens, generados por personal certificado y autorizado, como mínimo. c) Las redes Wi-Fi de uso corporativo debe tener como capa de autenticación el uso de la norma 802.11 de la IEEE, con el fin de autorizar el ingreso de los usuarios a las redes inalámbricas; usando como ente autenticador el Active Directory, RADIUS, TACACS+, o bien un NPS. d) Implementar el acceso a la red por sectores, para analizar e identificar quién usa la red, para garantizar una mayor seguridad. Así como en las redes físicas, las redes inalámbricas deben dividirse en función de las necesidades de la organización, con el objetivo de evitar que los usuarios tengan acceso a información restringida.		

	**9- Acceso al medio**	**Revisión 1.0**
	Es el conjunto de mecanismos y protocolos que controlan la forma de acceder al medio de transmisión en redes de difusión, evitando conflictos y errores. Al mismo tiempo caracteriza el funcionamiento de la red y condiciona el rendimiento, fiabilidad y gestión de la misma.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Dentro de la red corporativa es recomendable la implementación de un NAC (Control de Acceso a Red), ya que este será el encargado de gestionar el acceso al medio de forma dinámica en los equipos de conmutación, es decir con base a un perfil de usuario o firma digital, se le asignará una VLAN en específico y por tanto ciertos privilegios de navegación.
b) Elaborar un buen diseño de segmentación lógica de la red, podrá contener aisladas anomalías que pueden perjudicar las redes criticas como la SAN, NAS o Redes de Servidores. Como resultado, proporcionará servicios de seguridad específicos para cada segmento de red, lo que brinda más control sobre el tráfico, optimiza el rendimiento y mejora el entorno de seguridad.
c) Donde el número de clientes conectados a la red sea grande y se tenga segmentada la red lógicamente, es recomendable no definir rutas por defecto en los enrutadores o switches multicapa. En cambio, las rutas deberían apuntar únicamente a las redes donde se encuentren los servicios y recursos internos hechos por la misma empresa. Entonces la navegación de los clientes puede mediarse por un Firewall o un proxy server.
d) Implementación de Firewall de navegación, (o bien un PROXY) para evitar que usuarios accedan a los sitios web, servidores de correo y otras fuentes de información no autorizadas.
e) Implementación de firewall de perímetro, quien se mostrará de frente a las amenazas de internet. Este debe poseer todas las características de defensa Capa 7 que se puedan adquirir: IPS, antivirus, Web Filter, WAF, etc.

	**10- Seguridad de acceso físico**	**Revisión 1.0**
	La organización deberá definir e implantar medidas de seguridad que protejan sus instalaciones, o partes de ellas especialmente sensibles del acceso no autorizado. Teniendo como uno de los objetivos principales los sistemas de información, los sistemas de acceso físico se deberán revisar y actualizar periódicamente.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Implementación de controles de accesos por medio de sistemas biométricos.
b) Implementación y validación de bitácora de ingresos y salidas del personal responsable por medio de tarjetas o códigos personales.
c) Vigilancia 24/7 en zonas externas por personal de seguridad o sistemas de cámaras de videovigilancia y alarmas, para detectar lo posible intrusos de forma inmediata.

d) Para evitar la interrupción de los servicios de la organización, se recomienda la revisión periódica de la climatización y temperatura de los servidores, planta de emergencia, pruebas de descarga controlada de banco de baterías de UPS, tener bitácoras de mantenimiento, cambios de filtros de sedimentos y carbón activado en tomas principales de agua, para el correcto funcionamiento de los Data Center.
e) Protección contra las amenazas externas y ambientales, Se deberá diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes. (ISO 27001/ A 11.1.4)

	11- Dispositivos finales y responsabilidad sobre activos	**Revisión 1.0**
	Los soportes extraíbles constituyen una de las principales amenazas de fuga de información, así como de infección por malware. Se debe evaluar la posibilidad de bloquear estos puertos y eliminar las unidades lectoras/grabadoras de soportes ópticos de los equipos de usuarios. A continuación, se recomiendan algunas buenas prácticas establecidas en los controles de ISO 27001:	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Inventario de activos: Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes. (ISO 27001/ A 8.1.1)
b) Propiedad de los activos: Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización. (ISO 27001/ A 8.1.2)
c) Devolución de activos: Todos los empleados y usuarios de terceras partes deberán devolver todos los activos de la organización que estén en su posesión/responsabilidad, una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo. (ISO 27001/ A 8.1.4)
d) Gestión de soportes extraíbles: Se deberán establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización. (ISO 27001/ A 8.3.1)
e) Eliminación de soportes: Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales. (ISO 27001/ A 8.3.2)
f) Seguridad de los equipos y activos fuera de las instalaciones: Se deberá aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización (Como la situación de la aplicación de modalidad de teletrabajo en tiempos de pandemia de COVID-19) y en consideración de los distintos riesgos. (ISO 27001/ A 11.2.6)
g) Reutilización o retirada segura de dispositivos de almacenamiento: Se deberá verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización. (ISO 27001/ A 11.2.7)

8.1.3 Buenas prácticas de ciberseguridad para área de Recursos Humanos/ Talento Humano en modalidad de teletrabajo

	**1- Formación y capacitación**	**Revisión 1.0**
	La capacitación y la formación del personal son dos tópicos importantes que el área de Talento Humano debe considerar, con el objetivo de concientizar a los empleados sobre las mejores prácticas de seguridad de la información y protección de datos para prevenir brechas de seguridad y así eliminar o mitigar los riesgos.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) Adoptar medidas y controles de ciberseguridad a las nuevas condiciones del teletrabajo y sean aplicadas en el entorno laboral por los empleados.
b) Integrar el teletrabajo dentro de las políticas de ciberseguridad, adaptando un plan de seguridad de la información en la organización.
c) Garantizar el cumplimiento de la responsabilidad del empleado con la organización, respecto a la legislación, normativa y buenas prácticas.
d) Coordinar e informar sobre la formación y concientización a los empleados en modalidad de teletrabajo, en materia de ciberseguridad, al igual que en la modalidad presencial.

	**2- Integridad, confidencialidad y disponibilidad de la información en el teletrabajo**	**Revisión 1.0**
	Es necesario que las organizaciones establezcan centralizar los diferentes servicios tecnológicos que permitan la integridad, confidencialidad, disponibilidad y privacidad de la información.	**Fecha de emisión: 05/04/2022** **Fecha de actualización: 24/05/2022**

a) La organización debe ser responsable de establecer medidas adecuadas, para garantizar la protección de los datos utilizados por los empleados en teletrabajo, con fines laborales.
b) La organización debe velar por que cada empleado cumpla con los contratos de confidencialidad de la información, adoptando todas las normas o políticas para mantenerlo y cumplir con el deber de fidelidad a la misma.
c) Se recomienda la entrega al empleado en teletrabajo de una guía con las responsabilidades, restricciones y sanciones previstas en la legislación vigente y en las normas de la organización.
d) Es responsabilidad del empleado en teletrabajo, comunicar de inmediato a la organización sobre cualquier pérdida, robo, hurto u otro uso indebido de equipos y programas, según lo establecido en los canales de comunicación de la normativa interna.

CAPITULO 9

9.1 Conclusiones

Con base a la investigación y análisis de datos realizados a las diferentes organizaciones en los grupos de Área de Tecnología, Área de Talento Humano y Empleados, donde se expuso la situación de la seguridad de la información en la modalidad de teletrabajo en tiempos de COVID-19 en El Salvador; en donde dicha modalidad fue implementada de forma inmediata y generando un impacto en las actividades laborales de las organizaciones, tanto en el sector público como privado de El Salvador.

Algunas con la preparación adecuada y otras presentando falta de planificación o adecuación de su entorno, o bien no podían ser trasladadas a dicha modalidad, así como también las fallas en las conexiones de red y transferencia de datos, la falta de asesoría y capacitaciones, por lo tanto, para el empleado como para el empleador fue un gran reto. Sin embargo, la respuesta ante dicha crisis puso de manifiesto que la seguridad de la información es un ente vital que no se podía tomar a la ligera, por el hecho que los empleados transformaran sus hogares en oficinas, ya que dichos lugares no poseen la infraestructura física, tecnológica y de seguridad como en las organizaciones. Por tanto, dentro de las hipótesis que generaron el desarrollo de las guías de buenas prácticas aplicadas a la seguridad de la información, se concluye:

- Hipótesis 1: El implementar buenas prácticas de seguridad de la información mejora la competitividad e innovación en las organizaciones.

  Se concluye que la modalidad del teletrabajo tuvo un auge importante en El Salvador, desde la pandemia de COVID-19; sin embargo ante estas dificultades, se determinaron que al implementarse buenas prácticas de seguridad de la información se podría lograr una mejora

competitiva e innovadora en las organizaciones en conjunto con los empleados, ya que no es necesario la presencia física; sino que desde cualquier sitio fuera de la empresa encontrarse conectado y ejecutar las actividades laborales asignadas haciendo uso de las Tecnologías de la Información y las Comunicaciones (TIC).

- Hipótesis 2: Las condiciones de trabajo remoto cumplen con un porcentaje aceptable de medidas de seguridad de la información, como alternativa de continuidad a las actividades laborales durante la contingencia por la pandemia de COVID-19.

  Dentro del estudio se logró determinar que varias organizaciones adoptaron diversas medidas de seguridad de la información para la modalidad de teletrabajo, ya sea invirtiendo en adquirir o mejorar las infraestructuras o en herramienta de seguridad; se consolidaron dichas medidas a fin de sugerirlas y permitir a las organizaciones, fortalecer sus defensas contra posibles ataques y vulnerabilidades informáticas, y permitir la continuidad de las actividades laborales durante la contingencia por la pandemia de COVID-19

- Hipótesis 3: La falta de conocimiento sobre la importancia de la seguridad de la información en la modalidad del teletrabajo, puede impactar negativamente en el desarrollo económico financiera de las organizaciones, así como la perdida de datos; tanto en el sector privado como público.

  Los impactos económicos y financieros fueron determinantes en el futuro de muchas organizaciones, y más en el sector privado, ya que su finalidad principal es incrementar su capital. Es aquí donde el cese en las operaciones presenciales generó que muchas empresas que ofrecen servicios de soporte, instalación y desarrollo de proyectos, y que requerían estar en

> sitio, detuvieran el avance de sus implementaciones. Sin embargo, el trabajo no se detuvo, y adoptaron alternativas que llevaron a continuar su operatividad. El trabajo a distancia es la opción más conveniente para este escenario, y trae a cuenta que un espacio de las organizaciones se mueva a los hogares de los empleados. Es entonces que cobra real importancia la seguridad de los canales de comunicación y las conexiones remotas. Si estos canales de comunicación son interceptados y su información es alterada, podrían acabar con la continuidad operativa y por tanto detener los procesos productivos de las empresas y organizaciones. Resulta fundamental hacer del conocimiento que los cuidados de los activos informáticos garantizan una forma de trabajo segura y por tanto minimizar el riesgo de las amenazas que rondan en el medio del ciberespacio.

Dentro del estudio, muchas empresas adoptaron una modalidad hibrida y eso exige mayor seguridad, debido a la movilidad de un ambiente a otro (oficina/hogar) con la posibilidad que una brecha de seguridad se presente en dicho intercambio, poniendo en riesgo la información de la organización. Este escenario puede provocar que los riesgos de seguridad se materialicen e impactando a una red doméstica y a los equipos de las empresas, teniendo el canal libre para viajar a través de la VPN hacia la infraestructura interna de la organización.

Razón por la cual obliga a que los equipos personales utilizados para trabajar a distancia deberán de protegerse de la misma forma que un equipo corporativo; actualizando parches de sistema, antivirus y restringiendo el acceso a sitios de poca confianza, y cumpliendo exclusivamente su uso para actividades laborales.

9.2 Recomendaciones

- A fin de que las organizaciones puedan garantizar la seguridad de la información que manejan sus empleados en la modalidad de teletrabajo, se recomienda siempre socializar las políticas y lineamientos de ciberseguridad, el no conocerlos puede conllevar a riesgos de pérdida, robo o secuestro de información y además las sanciones ante el mal manejo de esta.

- Crear e incentivar mecanismos para que los empleados de las organizaciones adopten buenas prácticas de ciberseguridad en su entorno de acceso remoto, permitiendo reducir las brechas de seguridad y daños causados por cibercriminales.

- Demostrarle a la organización y hacer énfasis que el eslabón más débil ante una brecha de seguridad es el nivel de concientización del usuario en temas de seguridad de la información, si no se concientiza ante las amenazas y como prevenirlas, se corre el riesgo de cortar la productividad de las organizaciones ante un ataque cibernético, pérdida de información sensible y por consecuencia afectar su valor reputacional y la continuidad operativa.

- Dentro de las instituciones gubernamentales, donde los procesos son burocráticos, formar una comisión conformada por personal de tecnología, financiero, UACI/ DACI y jurídico; donde se busque agilizar los procesos de adquisición de infraestructura tecnológica que fortalezca la seguridad de las organizaciones, ya que los procesos toman demasiado tiempo para ejecutarse. Provocando que las instituciones públicas vayan quedando atrás en el desarrollo de tecnologías y tratamiento de las vulnerabilidades de forma oportuna.

9.3 Bibliografía

- Asamblea Legislativa de El Salvador. (26 de 10 de 2015). Ley de Firma Electrónica. San Salvador, El Salvador: Asamblea Legislativa de El Salvador.
- Asamblea Legislativa de El Salvador. (26 de 02 de 2016). Ley Especial contra los Delitos Informáticos y Conexos. San Salvador, El Salvador: Asamblea Legislativa de El Salvador.
- Asamblea Legislativa de El Salvador. (16 de 06 de 2020). Ley de Regulación del Teletrabajo. San Salvador, El Salvador: Asamble Legislativa de El Salvador.
- Blanco, A. G. (04 de 03 de 2022). Obtenido de https://www.bbva.com/es/teletrabajo-y-ciberseguridad-como-proteger-nuestra-informacion-corporativa-durante-el-confinamiento/
- Casa Presidencial-Twitter. (03 de 03 de 2022). Obtenido de https://twitter.com/PresidenciaSV/status/1239386131252350977
- Dirección de Identidad Digital. (04 de 2021). Politica de ciberseguridad de El Salvador. San Salvador, El Salvador.
- Editorial Etecé. (04 de 03 de 2022). Obtenido de https://concepto.de/metodo-cuantitativo/#:~:text=Los%20m%C3%A9todos%20cuantitativos%2C%20metodolog%C3%ADas%20cuantitativas,relaci%C3%B3n%20de%20causa%20y%20efecto.
- ESET. (2020). Reporte de Seguridad Latinoamérica 2020. 10.
- ESET. (2020). Reporte de Seguridad Latinoamérica 2020. 14.
- Gobierno de El Salvador. (05 de 03 de 2022). Obtenido de https://www.presidencia.gob.sv/ciberseguridad/
- GoConqr. (04 de 03 de 2022). Obtenido de https://www.goconqr.com/c/89311/course_modules/140211-ejercicio-2--teor-as-y-m-todos-en-investigaciones-cualitativas-y-cuantitativas#
- Guimbao, J. F. (2020). El teletrabajo en la era COVID. *Revista del Instituto Español de estudios estratégicos,* 7-10.
- Instituto Nacional de Normas y Tecnología. (04 de 03 de 2022). Obtenido de https://www.nist.gov/
- María José Erazo, D. C. (2020). *TELETRABAJO EN EL SALVADOR FACTIBILIDAD Y RETOS ANTE LA PANDEMIA DE COVID-19.* San Salvador: Ministerio de Trabajo y Previsión Social.
- Massuh, C. (04 de 03 de 2022). Obtenido de https://es.slideshare.net/uatscdhweb/el-proceso-de-la-investigacin-metodologa-cuantitativa

- Organización Internacional de Normalización. (03 de 03 de 2022). Obtenido de https://www.normas-iso.com/iso-27001/
- Organización Mundial de la Salud. (03 de 03 de 2022). Obtenido de https://www.who.int/es/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it
- Peralta, A. J. (2021). La ciberseguridad de la información del empleador y la fiscalización del trabajo remoto: alcances y límites. *Revista LABOREM*, 5.
- Real Academia Española. (04 de 03 de 2022). Obtenido de https://dle.rae.es/j%C3%A1quer
- Surveymonkey. (30 de 04 de 2022). Obtenido de https://es.surveymonkey.com/mp/sample-size-calculator/
- Universidad de Guadalajara. (08 de 04 de 2022). Obtenido de http://biblioteca.udgvirtual.udg.mx/portal/clasificacion-general-de-las-fuentes-de-informacion#:~:text=Fuentes%20primarias%3A%20contienen%20informaci%C3%B3n%20original,de%20una%20actividad%20eminentemente%20creativa.
- Wikipedia. (03 de 03 de 2022). Obtenido de https://es.wikipedia.org/wiki/Pandemia_de_COVID-19_en_El_Salvador

Anexos

Anexo 1. Modelo de encuesta para muestra de empleados en documento y en formato Google Forms

1. ¿Seleccione su género?

☐ Femenino ☐ Masculino

2. ¿En qué rango se encuentra su edad?

☐ 18 – 25 años ☐ 26 -35 años

☐ 36 – 45 años ☐ 46- 55 años

☐ 56 años en adelante

3. ¿A qué sector pertenece la organización?

☐ Público ☐ Privado

4. ¿Qué actividad realiza la organización?

☐ Actividades financieras ☐ Institución gubernamental

☐ Salud ☐ Educación

☐ Industria ☐ Automotriz

☐ Tecnología ☐ Contact Center

☐ Otros Especifique: _____

5. ¿Cuántos años lleva operando en su organización?

☐ 1 – 2 años ☐ 11- 15 años

☐ 3 – 5 años ☐ 15 años en adelante

☐ 6 -10 años

6. ¿En qué modalidad de trabajo está laborando actualmente?

☐ Teletrabajo[1] ☐ Trabajo hibrido[2] ☐ Presencial

7. Dentro de la organización ¿Por medio de la modalidad teletrabajo ha logrado coordinar con normalidad tareas con los demás empleados?

☐ Si ☐ No

8. ¿Qué medios utilizan para coordinar y planificar tareas asignadas con los otros empleados? (Seleccione una o varias)

☐ Microsoft Teams ☐ Llamadas telefónicas

☐ Google Meet ☐ Whatsapp

☐ Skype ☐ Correo electrónico

☐ Zoom ☐ Otros

Especifique: _____

9. Cómo empleado ¿Usted efectuó compras de insumos de oficina para realizar tareas asignadas desde su hogar?

☐ Si ☐ No

Si la respuesta es afirmativa, ¿qué insumos de oficinas compró?

☐ Computadora ☐ Planes de navegación

☐ Mobiliario de oficina ☐ Impresoras

☐ Otros Especifique: _____

[1] Según la Ley de Regulación de Teletrabajo, tiene un nuevo contrato laboral o cambio/adenda

[2] Modalidad mixta, tanto presencial en oficina como trabajo en casa

10. En caso que la empresa haya brindado el equipo de trabajo, este cuenta con medidas de seguridad tales como: bloqueos de periféricos (puertos USB, unidad CD-ROM), conexión a VPN´s, antivirus, políticas de navegación, acceso restringido de Internet.

☐ Si ☐ No

11. ¿Cuenta con una conexión a internet que permita una velocidad rápida y estable?

☐ Si ☐ No

12. ¿Acostumbra cambiar la contraseña del router de Internet periódicamente?

☐ Si ☐ No

Si la respuesta es afirmativa, ¿Con que frecuencia?

☐ Cada 15 días ☐ Cada mes

☐ Cada 3 meses ☐ Cada 6 meses

13. ¿Acostumbra cambiar la contraseña de su red inalámbrica periódicamente?

☐ Si ☐ No

Si la respuesta es afirmativa, ¿Con que frecuencia?

☐ Cada 15 días ☐ Cada mes

☐ Cada 3 meses ☐ Cada 6 meses

14. ¿Hace uso de repositorios en la nube (OneDrive, Google Drive, Dropbox, iCloud Drive, etc.) establecidos por la organización para resguardar información o hacer copias de respaldo?

☐ Si ☐ No

15. ¿En su equipo de trabajo, hace uso de inicio de sesión de usuario y contraseñas robustas con números, letras, símbolos y mayor a 8 caracteres?

☐ Si ☐ No

16. ¿En su organización se cuenta con un método de doble factor de autenticación para ingreso a los sistemas, correo electrónico institucional u otros servicios que requieran seguridad?

☐ Si ☐ No

17. ¿Cómo empleado, recibió capacitaciones para realizar sus tareas mediante la modalidad de teletrabajo?

☐ Si ☐ No

En caso de respuesta afirmativa, específicamente ¿en qué áreas? (Seleccione una o varias)

☐ Plataformas para videoconferencias

☐ Recomendaciones sobre seguridad y gestión de riesgos informáticos

☐ Uso de portales SSL y VPN´s

☐ Recomendaciones de uso de contraseñas robustas

☐ Uso de tokens para inicios de sesión

☐ Uso de correo electrónico, navegación segura

Otros: _____

18. ¿Cómo empleado tiene conocimiento que al recibir un correo electrónico sospechoso, debe ser reportado a los canales definidos por la organización?

☐ Si ☐ No

19. ¿En su equipo de trabajo realiza actualizaciones de antivirus y actualizaciones del sistema operativo para mantenerlo protegido?

☐ Si ☐ No

Si la respuesta es afirmativa, ¿Con que frecuencia?

☐ Cada 15 días ☐ Cada mes

☐ Cada 3 meses ☐ Cada 6 meses

20. Si usted como empleado posee un dispositivo móvil proporcionado por la organización ¿El uso que le da es para fines únicamente de trabajo?

☐ Si ☐ No

21. ¿Acostumbra a bloquear el equipo al levantarse del puesto de trabajo o cerrar sesiones al finalizar su jornada laboral?

☐ Si ☐ No

22. ¿Qué consideraciones, opiniones, mejoras, u observaciones, tiene acerca de los procedimientos que se toman en su organización en cuanto a la preparación que tuvo en la transición a modalidad de teletrabajo?

_____

_____

Anexo 2. Modelo de encuesta para muestra de empleados de Tecnologías de la Información en documento y en formato Google Forms

1. ¿Seleccione su género?

   ☐ Femenino ☐ Masculino

2. ¿En qué rango se encuentra su edad?

   ☐ 18 – 25 años ☐ 26 -35 años

   ☐ 36 – 45 años ☐ 46- 55 años

   ☐ 56 años en adelante

3. ¿A qué sector pertenece la organización donde labora?

   ☐ Público ☐ Privado

4. ¿Cuál es su cargo funcional?

   _____

5. ¿Para proveer conexiones remotas a los recursos internos de la red institucional, la infraestructura estaba lista para soportar la demanda de usuarios y amenazas del entorno?

   ☐ Si ☐ No

Si la respuesta es afirmativa, indique cuales herramientas ayudaron a proveer la conectividad segura:

☐ VPN IPSec ☐ RDP

☐ VPN SSL ☐ Terminal Server

☐ Portal SSL

6. ¿Cómo área de tecnología, se realizaron capacitaciones a los empleados para realizar sus tareas mediante la modalidad de teletrabajo?

☐ Si ☐ No

En caso de respuesta afirmativa, específicamente ¿en qué áreas? (Seleccione una o varias)

☐ Plataformas para videoconferencias

☐ Recomendaciones de sobre seguridad y gestión de riesgos informáticos

☐ Uso de portales SSL y VPN´s

☐ Recomendaciones de uso de contraseñas robustas

☐ Uso de tokens para inicios de sesión

☐ Uso de correo electrónico, navegación segura

☐ Conexión y uso mediante VPN

☐ Correos informativos, videos tutoriales y manual de uso

Otros: _____

7. ¿Los sitios públicos en internet residen en una DMZ para reducir la superficie de contacto entre los clientes externos y la red interna?

☐ Si ☐ No

8. ¿Los sitios web públicos aseguran la capa de autenticación con certificados digitales?

☐ Si ☐ No

9. ¿Los certificados digitales utilizados son extendidos por una CA o son autofirmados?

☐ Extendidos por AC ☐ Son autofirmados ☐ Desconoce la existencia

10. ¿Su organización cuenta con un Plan de Continuidad del Negocio ante un evento disruptivo?

☐ Si ☐ No

11. ¿Los equipos corporativos asignados a los teletrabajadores son preparados con medidas de seguridad para restringir y reducir las amenazas fuera de la infraestructura de T.I. de la organización como antivirus, firewall, despliegue del endpoint, etc.?

☐ Si ☐ No

12. ¿Cómo área de T.I. realizan backups de versiones de bases de datos?

☐ Si ☐ No

En caso de respuesta afirmativa, ¿Con que frecuencia?

☐ Diario ☐ Trimestral

☐ Semanal ☐ Semestral

☐ Mensual ☐ Anual

13. ¿Realizan respaldo de programas ejecutables y códigos fuentes de los sistemas en producción?

☐ Si ☐ No

14. ¿En caso de tener sistemas o servicios tercerizados, se les solicitan a los proveedores SLA (Acuerdo de Nivel de Servicio) que se adecuen a las responsabilidades y obligaciones que la organización demanda?

☐ Si ☐ No

15. ¿Las conexiones remotas son validadas por un directorio activo que provea las políticas dictadas por el administrador de red e impuestas al usuario de dominio?

☐ Si ☐ No

16. ¿Las conexiones remotas son validadas por un NAC (Network Access Control), que provea las políticas dictadas por el administrador de red?

☐ Si ☐ No

17. ¿Las conexiones remotas son validadas por perfiles y políticas de navegación establecidas por el firewall perimetral?

☐ Si ☐ No

18. ¿La seguridad de las conexiones remotas son validadas por un doble factor de autenticación?

    ☐ Si ☐ No

19. ¿Dentro de la organización cuentan con un SIEM (Security Information and Event Management) o DLP (Data Loss Prevention) para hacer análisis de vulnerabilidades y trazabilidad de la información, para creación y actualización de escenarios de riesgo?

    ☐ Si ☐ No

20. ¿Posterior a identificar un evento disruptivo, la información recopilada por los sistemas de monitoreo de eventos, es trasladada a los responsables de la seguridad de la información establecidos por la organización?

    ☐ Si ☐ No

21. ¿Poseen una política y medidas de seguridad de apoyo para gestionar los riesgos de seguridad debido al uso de dispositivos móviles?

    ☐ Si ☐ No

22. ¿Cómo área de tecnología considera que el trabajo remoto cumple con las expectativas de la seguridad de la información establecidas por la organización?

    ☐ Si ☐ No

23. ¿Considera usted importante que la falta de conocimiento sobre la seguridad de la información en la modalidad del teletrabajo puede impactar negativamente a la organización?

    ☐ Si ☐ No

    En qué aspectos:

    _____

    _____

    _____

24. ¿Qué consideraciones, opiniones, mejoras, u observaciones, tiene acerca de los procedimientos que se toman en su organización en cuanto a la preparación que tuvo en la transición a modalidad de teletrabajo?

_____

_____

Universidad Don Bosco

Como parte de proyecto investigativo Guía de buenas prácticas aplicadas a la seguridad de la información en el teletrabajo en tiempos de COVID 19 en El Salvador, de la Maestría en Seguridad y Gestión de Riesgos Informáticos de la Universidad Don Bosco; se pretende estudiar la población del área de tecnologías de la información (TI) y sus roles durante la modalidad de teletrabajo dentro del país.

De antemano agradecemos su apoyo con el llenado del siguiente instrumento, las respuestas son de carácter confidencial y es derivada de manera exclusiva para efectos académicos.

Encuesta a Personal de Tecnologías de la Información

La presente encuesta tiene como objetivo conocer aspectos de seguridad de la información aplicados a la modalidad de trabajo remoto, en la organización desde el inicio de la pandemia de la COVID-19 en El Salvador.

1. ¿Seleccione su género? *

1. Femenino
2. Masculino

Anexo 3. Modelo de encuesta para muestra de empleados de Talento Humano/ Recursos Humanos en documento y en formato Google Forms

1. ¿A qué sector pertenece la organización?

   ☐ Público ☐ Privado

2. ¿Seleccione su género?

   ☐ Femenino ☐ Masculino

3. ¿En qué rangos de edades los empleados de la organización fueron enviados en la modalidad de teletrabajo durante la pandemia de COVID-19?

   ☐ 18 – 25 años ☐ 26 - 45 años

   ☐ 46 – 55 años ☐ 56 años en adelante

   ☐ Todas las anteriores ☐ Ningún empleado

4. ¿Qué actividad realiza la organización?

   ☐ Actividades financieras ☐ Institución gubernamental

   ☐ Salud ☐ Educación

   ☐ Industria ☐ Automotriz

   ☐ Tecnología ☐ Contac Center

   ☐ Otros Especifique: _____

5. En la organización ¿En qué modalidad de trabajo los empleados laboran?

   ☐ Teletrabajo[3] ☐ Trabajo hibrido[4] ☐ Presencial

[3] Según la Ley de Regulación de Teletrabajo, tiene un nuevo contrato laboral o cambio/adenda

[4] Modalidad mixta, tanto presencial en oficina como trabajo en casa

6. ¿Desde su punto de vista en la unidad de Talento Humano, considera que los empleados de la organización se han adaptado de forma general a realizar sus labores desde la modalidad de teletrabajo?

   ☐ Si ☐ No

7. Antes de la pandemia de COVID-19 ¿la organización tenía a algún empleado realizando labores bajo la modalidad de teletrabajo?

   ☐ Si ☐ No

8. Posterior a la pandemia de COVID-19 ¿Se planea continuar con empleados en la modalidad de teletrabajo?

   ☐ Si ☐ No

9. En caso de respuesta afirmativa, ¿Se modificará el contrato laboral conforme a la ley de regulación de teletrabajo?

   ☐ Si ☐ No

10. ¿Como organización poseen un control de marcaciones de los horarios laborales en modalidad de teletrabajo?

    ☐ Si ☐ No

Especifique los controles usados:

_____

_____

_____

11. ¿Ante una crisis como la pandemia de COVID-19, considera el teletrabajo una opción buena e innovadora para la continuidad operativa?

    ☐ Si ☐ No

En qué aspectos:

_____

_____

_____

12. ¿Qué consideraciones, opiniones, mejoras, u observaciones, tiene acerca de los procedimientos que se toman en su organización en cuanto a la preparación que tuvo en la transición a modalidad de teletrabajo?

_____

_____

Universidad Don Bosco

Como parte de proyecto investigativo Guía de buenas prácticas aplicadas a la seguridad de la información en el teletrabajo en tiempos de COVID 19 en El Salvador, de la Maestría en Seguridad y Gestión de Riesgos Informáticos de la Universidad Don Bosco; se pretende estudiar la población de empleados en modalidad de teletrabajo dentro del país.

De antemano agradecemos su apoyo con el llenado del siguiente instrumento, las respuestas son de carácter confidencial y es derivada de manera exclusiva para efectos académicos.

Encuesta Recursos Humanos/ Talento Humano

La presente encuesta tiene como objetivo conocer el tipo de modalidad de trabajo remoto en los que se encuentra la organización desde el inicio de la pandemia de la COVID-19 en El Salvador.

1. ¿A qué sector pertenece la organización? *

Público

Privado

Anexo 4. Modelo de encuesta para obtención de estadísticas respecto a modalidad de teletrabajo para Ministerio de Trabajo y Previsión Social y DIGESTYC

UNIVERSIDAD DON BOSCO

VICERRECTORÍA ACADÉMICA

FACULTAD DE INGENIERÍA

MAESTRÍA EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

Como parte de proyecto investigativo Guía de buenas prácticas aplicadas a la seguridad de la información en el teletrabajo en tiempos de COVID 19 en El Salvador, de la Maestría en Seguridad y Gestión de Riesgos Informáticos de la Universidad Don Bosco; en el cual se pretende estudiar la población de empleados en modalidad de teletrabajo dentro del país. Por lo que solicitamos su apoyo para conocer dentro de esta población:

- Datos según género, la cantidad de hombres y mujeres en esta modalidad

---

- Datos porcentuales de edad de población en modalidad de teletrabajo

---

- Datos de sector de empresa que desarrollan teletrabajo

- Datos de tamaño de empresa que desarrollan teletrabajo

- Datos porcentuales según zonas de organización territorial (occidental, central, paracentral, oriental) que están en la modalidad de teletrabajo

---

- Datos de perfil de los empleados que realizan teletrabajo

Profesional universitario	
Técnicos	
Directivos	
Asistentes	
Otros	

Anexo 5. Modelo de Adenda para Contrato Individual en la modalidad de Teletrabajo en El Salvador

CONTRATO INDIVIDUAL DE TRABAJO

Nombre: _____
_____
Sexo: _____
Edad: _____
Estado Familiar: _____
Profesión u Oficio: _____
Domicilio: _____
Residencia:_____
Nacionalidad: _____
DUI No: _____
Expedido en: _____
, el día_____
Otros datos de Identificación: _____
_____
NIT: _____

Nombre:
Representante Legal:
Sociedad Anónima de capital variable.
De nacionalidad: salvadoreña
Domicilio: San Salvador
Residencia:
NIT:

NOSOTROS: _____ y _____ _____, ambos de generales arriba indicadas y actuando en el carácter que aparece expresado, convenimos en celebrar la presente ADENDA de contrato Individual de Trabajo suscrito por ambas partes el día _____, el cual se encontrará sujeto a las estipulaciones siguientes:

a) CLASE DE TRABAJO O SERVICIO: El trabajador se obliga a prestar sus servicios al patrono como: _____, en la modalidad de TELETRABAJO

b) LUGAR DE PRESTACIÓN DE SERVICIOS El lugar de prestación de los servicios será: en _____, el cual se denominará Telecentro

c) DETERMINACIÓN DE TAREAS: Las funciones a realizar por parte del trabajador desde el telecentro son: _____-

d) HERRAMIENTAS DE TRABAJO:

I. El patrono proporcionará al trabajador los siguientes programas y equipos: _____

Los cuales se entregan en perfectas condiciones y deben ser devueltos así por la persona trabajadora, cuando sean requeridas al efecto por su jefe inmediato, salvo la disminución o deterioro causados por caso fortuito o fuerza mayor, o por la acción del tiempo o por el consumo y uso normal de los mismos.

II. El trabajador, proporcionara las siguientes herramientas de trabajo: _____

e) OTRAS ESTIPULACIONES: CONFIDENCIALIDAD: La persona trabajadora se obliga a no revelar los hechos o términos de su relación comercial con los clientes que atiende a nombre del Patrono, sobre cualesquiera temas, documentación o información relacionados con los servicios que prestan a los clientes y sus negociaciones comerciales, las estrategias, la creatividad, etc., se compromete a no compartir con terceros ninguna información, programa, o documento que se encuentre en su poder, esta cláusula no se aplicará en el evento que revelar los términos de este contrato, su existencia o las cantidades aquí pactadas sea necesario para legalmente hacer valer este Contrato o en la medida que sea requerido legalmente a las partes o sean judicialmente ordenadas a revelar dichos términos, debiendo avisar previamente al Patrono. Si la persona trabajadora no cumple los términos de confidencialidad, la persona trabajadora podrá ser despedida sin responsabilidad para el patrono de conformidad a la causa 4ª del artículo 50 del Código de Trabajo.

En fe de lo cual firmamos el presente documento por triplicado en: San Salvador, _____ _____.

(f)_____ (f)_____
PATRONO O REPRESENTANTE PERSONA TRABAJADORA