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

Ciberseguridad aplicada en entornos de teletrabajo para empresas del sector privado en El Salvador

PRESENTADO POR

Ing. Juan Pablo Góchez Torres

Ing. Melvin Rafael Rivas Hernández

Ing. Juan Francisco Solorzano Merlos.

ASESOR

MSG Nohemy Nathaly Flores Figueroa

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América Junio, 2024

Agradecimientos

Agradecemos profundamente a Dios por permitirnos culminar con éxito este Postgrado, otorgandonos salud, sabiduría y fortaleza durante todo el proceso.

Queremos expresar nuestra más sincero agradecimiento a nuestra asesora, la Magíster Nohemy Nathaly Flores Figueroa, por brindarnos la invaluable oportunidad de contar con sus conocimientos, experiencias y paciencia en el desarrollo de nuestro proyecto de graduación. Su orientación y apoyo fueron fundamentales para alcanzar nuestros objetivos.

Asimismo, extendemos nuestra gratitud a todos los formadores de la Universidad Don Bosco, quienes a lo largo de toda la carrera nos impartieron sus conocimientos y nos brindaron su apoyo incondicional, motivándolos a seguir adelante día a día.

Por último, pero no menos importante, agradecemos a todos aquellos que, de una forma u otra, contribuyeron en este camino de aprendizaje y crecimiento académico, brindando su apoyo y aliento en cada etapa de este importante proceso educativo. Sin su colaboración, este logro no habría sido posible.

Tabla de contenido

1. Introducción

1.1 Contexto y Justificación

En la era digital actual, el teletrabajo ha surgido como una modalidad laboral prominente, especialmente en el contexto de la pandemia de COVID-19, donde la necesidad de distanciamiento social y medidas preventivas ha impulsado a las organizaciones a adoptar esta práctica de trabajo remoto de manera acelerada. En este escenario; El Salvador, al igual que muchas otras naciones, ha presenciado un aumento significativo en la implementación del teletrabajo en empresas del sector privado.

Sin embargo, junto con los beneficios de flexibilidad y eficiencia que ofrece el teletrabajo, surgen desafíos importantes en términos de ciberseguridad. La dependencia de la tecnología y la conectividad remota expone a las organizaciones a una serie de amenazas cibernéticas que pueden comprometer la integridad, confidencialidad y disponibilidad de la información crítica y los sistemas empresariales.

El Salvador, como parte de esta dinámica global, enfrenta desafíos únicos en el ámbito de la ciberseguridad en entornos de teletrabajo. Si bien el país ha experimentado un crecimiento significativo en el uso de tecnologías de la información y la comunicación (TIC) en los últimos años, la madurez en términos de infraestructura digital y conciencia de ciberseguridad aún está en desarrollo. Además, las empresas del sector privado, que abarcan una variedad de industrias, enfrentan presiones adicionales para proteger sus activos digitales mientras se adaptan a este nuevo paradigma de trabajo remoto.

En este contexto, esta investigación propone abordar la cuestión crítica de la ciberseguridad aplicada en entornos de teletrabajo para empresas del sector privado en El Salvador. Se enfocará en analizar los riesgos específicos que enfrentan estas empresas en su transición hacia el teletrabajo, así como en identificar las mejores prácticas y estrategias de ciberseguridad que pueden ayudar a mitigar tales riesgos.

Justificacion

El crecimiento exponencial del teletrabajo en El Salvador, catalizado por la pandemia de COVID-19, ha generado una necesidad imperiosa de abordar los desafíos emergentes en materia de ciberseguridad. En este nuevo paradigma laboral, las empresas del sector privado enfrentan una amplia gama de amenazas cibernéticas, desde ataques de phishing hasta ransomware y vulnerabilidades en la red. La rápida expansión de la infraestructura digital y la multiplicidad de dispositivos utilizados por los empleados han aumentado la complejidad del panorama de seguridad, exponiendo a las organizaciones a un mayor riesgo de comprometer datos sensibles y sufrir pérdidas de información.

Estas amenazas no solo representan una preocupación para la seguridad de la información, sino que también tienen el potencial de impactar negativamente en la continuidad del negocio y en la estabilidad económica de El Salvador. Los ciberataques tienen el potencial de interrumpir las operaciones empresariales, provocar pérdidas financieras significativas y causar daños irreparables a la reputación corporativa. En un momento en que la economía salvadoreña está buscando recuperarse de los efectos adversos de la pandemia, la protección de la infraestructura digital se vuelve crítica para asegurar la resiliencia y el crecimiento sostenible.

La creciente amenaza de ciberataques, pone en alerta a empresas en El Salvador los riesgos de ciberseguridad obligan a implementar medidas para mitigarlos. La falta de conciencia y preparación en materia de ciberseguridad deja a las empresas vulnerables y expuestas a ataques que podrían prevenirse con una planificación adecuada y la implementación de medidas de seguridad robustas. En este contexto, la investigación y la implementación de estrategias efectivas de ciberseguridad se vuelven esenciales para proteger la integridad, confidencialidad y disponibilidad de los datos empresariales, y para garantizar un entorno de teletrabajo seguro y confiable en El Salvador.

1.2 Planteamiento del Problema

El incremento en la adopción del teletrabajo en El Salvador ha sido una respuesta necesaria a los desafíos impuestos por la pandemia de COVID-19 y, en muchos casos, ha llegado para quedarse como una modalidad laboral permanente en numerosas empresas del sector privado. Sin embargo, este cambio hacia el trabajo remoto ha traído consigo una serie de desafíos en términos de ciberseguridad que requieren una atención urgente.

En primer lugar, la expansión de la infraestructura digital para respaldar el teletrabajo ha generado un panorama de seguridad más complejo y fragmentado.. Las empresas se enfrentan al desafío de proteger una red extendida que abarca desde los servidores internos hasta los dispositivos personales de los empleados, lo que aumenta significativamente la superficie de ataque y la dificultad para implementar medidas de seguridad adecuadas.

Además, la diversidad de dispositivos utilizados por los empleados, que van desde computadoras portátiles y teléfonos inteligentes hasta tabletas y dispositivos IoT (Internet de las cosas), introduce una mayor variedad de puntos de acceso potenciales para los atacantes. La gestión de la seguridad en una amplia gama de plataformas y sistemas operativos se convierte en un desafío considerable para las empresas, que deben garantizar la protección de la información sensible independientemente del dispositivo utilizado.

La dependencia de plataformas en la nube para almacenar y compartir datos también plantea desafíos específicos en términos de ciberseguridad. Si bien la nube ofrece numerosos beneficios en cuanto a escalabilidad y accesibilidad, también introduce riesgos inherentes relacionados con la privacidad de los datos, el acceso no autorizado y la vulnerabilidad a ciberataques.

En este contexto, las empresas del sector privado en El Salvador se encuentran expuestas a una amplia gama de amenazas cibernéticas, que van desde ataques de phishing diseñados para engañar a los empleados y robar información confidencial, hasta ataques de ransomware que cifra los datos y exigen rescates financieros para su liberación. Además, las vulnerabilidades en la red, como fallos de seguridad en los sistemas informáticos y la falta de actualizaciones de software, representan riesgos significativos que pueden ser explotados por los ciberdelincuentes para comprometer la seguridad de la información y causar daños financieros y reputacionales a las empresas. Este estudio investiga las prácticas de ciberseguridad actuales implementadas en las empresas de El Salvador y propone estrategias para mejorar la seguridad en entornos de teletrabajo.

1.3 Objetivos de la Investigación

Objetivo general

Desarrollar un marco integral de ciberseguridad adaptado a entornos de teletrabajo para empresas del sector privado en El Salvador, con énfasis en la identificación y gestión de riesgos, así como en la adopción de buenas prácticas basadas en la norma ISO 27002.

Objetivos específicos

- Identificar los principales desafíos en la implementación de controles de ciberseguridad en entornos de teletrabajo para empresas del sector privado de El Salvador, mediante la elaboración de encuestas, entrevistas y análisis de datos.
- Identificar y priorizar los riesgos de ciberseguridad más críticos en los entornos de teletrabajo del sector privado en El Salvador, proponiendo estrategias efectivas de gestión y mitigación.
- Desarrollar una guía de buenas prácticas de ciberseguridad enmarcadas en la norma ISO 27002, como resultado del análisis realizado en tres empresas representativas del sector privado de El Salvador.

1.4 Preguntas de Investigación

1. ¿Qué nivel de madurez poseen las empresas del sector privado de El Salvador en materia de ciberseguridad en entornos de teletrabajo?
2. ¿Cuáles son los desafíos con los que se enfrentan las empresas del sector privado de El Salvador para implementar buenas prácticas de ciberseguridad en entornos de teletrabajo?

3. ¿Las empresas del sector privado de El Salvador conocen e implementan buenas prácticas de ciberseguridad alineadas con el marco de referencia ISO 27002?
4. ¿Existe una cooperación en el sector privado de empresas en EL Salvador para compartir conocimientos en materia de ciberseguridad?

1.5 Estructura del Documento

La estructura del documento se organiza en varias secciones clave que guían al lector a través del proceso de investigación:

1. Introducción

Este capítulo establece el marco inicial de la investigación, proporcionando una visión general de su relevancia y el contexto en el que se lleva a cabo. Aquí se presentan los fundamentos que justifican la necesidad del estudio y se describen claramente los problemas y objetivos de la investigación. También se formulan las preguntas clave que guiarán la investigación y se proporciona una descripción de la organización del documento, destacando brevemente el contenido de cada capítulo.

2. Marco Teórico

Este capítulo ofrece una base teórica para la investigación, definiendo conceptos clave y revisando estudios previos y normativas relevantes. Se analizan estudios y trabajos previos importantes, identificando tendencias, hallazgos y brechas en el conocimiento existente. Además, se describen las principales normativas y estándares internacionales que guían las prácticas de ciberseguridad.

3. Metodología

Este capítulo detalla el enfoque metodológico adoptado para llevar a cabo la investigación, describiendo el diseño, la población estudiada, los instrumentos utilizados y los procedimientos seguidos para la recolección y análisis de datos. Se explica el enfoque general de la investigación, cómo se estructuró el estudio, se detalla la población objetivo y cómo se seleccionó la muestra representativa. Además, se enumeran y describen los instrumentos y técnicas utilizados para recolectar los datos necesarios.

4. Resultados

En este capítulo se presentan los hallazgos de la investigación de manera estructurada y clara. Se utilizan tablas, figuras y gráficos según sea necesario para ilustrar los resultados. Este capítulo proporciona una visión detallada de los datos recopilados y los resultados obtenidos en el contexto del estudio.

5. Discusión

Este capítulo analiza en profundidad los resultados obtenidos, relacionándolos con la literatura revisada y los objetivos de la investigación. Se interpretan y analizan los resultados, destacando hallazgos clave y patrones observados. Además, se discuten las implicaciones prácticas de los resultados para las empresas y otros actores relevantes, y se identifican las limitaciones que pudieron haber afectado los resultados y la interpretación de la investigación.

6. Conclusiones y Recomendaciones

Este capítulo ofrece un resumen de las conclusiones principales del estudio y proporciona recomendaciones prácticas basadas en los hallazgos. Se presentan las conclusiones derivadas del análisis de los resultados, respondiendo a las preguntas de investigación. Además, se sugieren acciones y estrategias para mejorar la ciberseguridad en entornos de teletrabajo.

7. Glosario

Se proporciona un glosario de términos técnicos y conceptos clave utilizados en el documento para facilitar la comprensión del lector.

8. Referencias

Se incluye una lista completa de todas las fuentes citadas en el documento, siguiendo un estilo de citación académico estándar.

9. Anexos

Se presentan materiales adicionales que apoyan el contenido del estudio, como cuestionarios utilizados, datos recopilados, y cualquier otra información relevante.

Índices

- **Índice de Tablas**: Se lista todas las tablas incluidas en el documento.
- **Índice de Figuras**: Se lista todas las figuras incluidas en el documento.
- **Índice de Gráficas**: Se lista todas las gráficas incluidas en el documento.

2. Marco Teórico

2.1 Revisión de la Literatura

Muchas de las empresas e instituciones de diversos sectores en El Salvador han adoptado modelos de trabajo remoto. Esta situación impulsó una reestructuración en la forma de comunicación, procesamiento y modalidad de trabajo, requiriendo el desarrollo e implementación de nuevas tecnologías.

Si bien el trabajo remoto trajo consigo beneficios, también generó desafíos. La rápida adopción de estas tecnologías aumentó el riesgo de exposición de los activos de información de las organizaciones, convirtiéndose en el punto crítico de la 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.

El auge del teletrabajo en El Salvador, ha traído consigo grandes beneficios para las empresas del sector privado y los empleados, pero también nuevos desafíos en materia de ciberseguridad, ya que la descentralización de la fuerza laboral y el uso de dispositivos y redes personales para acceder a información confidencial han incrementado la superficie de ataque y la vulnerabilidad de las empresas del sector privado. Estas deben estar conscientes de los riesgos asociados al teletrabajo y tomar medidas para proteger sus activos informáticos y la información confidencial.

Implementar una estrategia robusta de ciberseguridad es crucial para garantizar la continuidad del negocio, la protección de la reputación y el cumplimiento de las regulaciones.

Ahora bien, hay que considerar que los empleados son la primera línea de defensa contra las amenazas cibernéticas, las empresas necesitan asegurarse de que los empleados están educados en las mejores prácticas de seguridad. Un artículo de una página llamada “Emprendedores” examina la transformación del teletrabajo y su impacto en la educación y el entorno laboral debido a la pandemia de COVID-19. Destaca la necesidad de capacitar a los empleados en habilidades digitales, gestión de datos y trabajo en equipo remoto. Subraya la importancia de que los líderes desarrollen nuevas competencias para gestionar equipos virtuales de manera efectiva. (PEREIRO, 2021)

También una revista digital de España llamada TicPymes, redactó un artículo sobre la importancia de la formación de los empleados para un teletrabajo seguro, en la que enfatiza que la gestión de dispositivos es crucial, especialmente en entornos donde los empleados utilizan sus propios dispositivos. Recomienda implementar medidas para asegurar estos dispositivos y monitorear el comportamiento del usuario para detectar actividades anómalas o sospechosas. La formación continua de los empleados es esencial para mantenerlos actualizados sobre las mejores prácticas de seguridad y las últimas amenazas.
Por último nos dice que la adecuada formación y medidas de seguridad, las empresas pueden mitigar los riesgos del teletrabajo y proteger tanto sus datos como sus sistemas. (TicPymes, 2021)

1. Aumento de acceso al internet en El Salvador

El Salvador ha experimentado un crecimiento significativo en el acceso al internet en los últimos años. De acuerdo a Statista, el crecimiento de usuarios de internet en El Salvador ha sido constante y seguirá así en los próximos años. Para 2021 fueron 3,17 millones los usuarios de internet en El Salvador, y para 2025 serán 4,07 millones. Este acceso generalizado a la red, si bien abre oportunidades, también incrementa los riesgos cibernéticos. (Badia, 2021)

2. Ciberamenazas en El Salvador

El Salvador no es ajeno a las crecientes ciberamenazas que afectan a nivel global. En 2022, la Agencia de la Regulación de las Telecomunicaciones (ARES) reportó un aumento del 30% en los incidentes de ciberseguridad en comparación con 2021. Entre las principales amenazas se encuentran:

Malware: Software diseñado específicamente para dañar o inutilizar ordenadores y sistemas informáticos. Puede utilizarse para robar información personal, borrar archivos o tomar el control de un ordenador.

Phishing: Los delincuentes se hacen pasar por una organización o persona legítima para engañar a las víctimas y conseguir que faciliten información personal o datos financieros. La información se utiliza después para cometer fraude o robo de identidad. Las estafas de phishing suelen realizarse por correo electrónico, pero también pueden producirse a través de mensajes de texto, llamadas telefónicas o redes sociales.

Ransomware: Es un tipo de malware que cifra los archivos de la víctima y exige el pago de un rescate para descifrarlos. La nota de rescate suele indicar al usuario cómo pagar el rescate y descifrar sus archivos. (SKYSNAG,2023)

3. Ciberseguridad en entornos de teletrabajo

La ciberseguridad en entornos de teletrabajo se refiere a la protección de los activos informáticos de una empresa cuando los empleados trabajan de forma remota. Diversos riesgos emergen al trasladar el entorno de trabajo desde oficinas protegidas a espacios domésticos o alternos, y es imperativo que tanto empresas como empleados estén preparados para enfrentarlos.

Esto implica proteger: Dispositivos (computadoras portátiles, tabletas, teléfonos inteligentes, etc), Redes (redes domésticas, redes Wi-Fi públicas, etc), Datos (información confidencial, datos de clientes, propiedad intelectual, etc).

Principales riesgos que presenta el teletrabajo: (Calabuig, 2023)

- Conexiones Inseguras: Las redes Wi-Fi públicas o domésticas no siempre están adecuadamente protegidas, convirtiéndose en puertas de entrada para ciberdelincuentes que pueden interceptar datos transmitidos.
- Uso de Dispositivos Personales: Estos dispositivos pueden no tener configuraciones de seguridad óptimas, o pueden estar comprometidos sin que el usuario lo sepa, poniendo en riesgo la información corporativa.
- Phishing y Malware: Fuera del entorno protegido de la oficina, es más fácil caer en tácticas de phishing, especialmente si los atacantes se disfrazan de entidades conocidas relacionadas con el trabajo.
- Compartir Información por Medios Inseguros: Los trabajadores pueden verse tentados a enviar información a través de aplicaciones de mensajería no seguras o plataformas de almacenamiento en la nube no aprobadas.

- Backup Inseguro: La falta de protocolos de respaldo seguros puede llevar a la pérdida de información importante o a que esta se almacene en lugares accesibles por atacantes.

4. Riesgos de ciberseguridad en entornos de teletrabajo

Los entornos de teletrabajo presentan una serie de riesgos de ciberseguridad que no se encuentran presentes en las oficinas tradicionales. Algunos de los riesgos más comunes incluyen:

- Ataques de phishing y malware.
- Pérdida de datos: Los datos confidenciales pueden perderse o filtrarse fácilmente en entornos de teletrabajo.
- Ataques de denegación de servicio (DDoS): Pueden dirigirse a los empleados que teletrabajan para interrumpir su trabajo y afectar la productividad de la empresa.
- Amenazas internas: Los empleados descontentos o negligentes pueden representar una amenaza interna para la seguridad de la empresa, incluso si trabajan de forma remota.

El Salvador recibió 24 millones de intentos de ciberataques durante el primer trimestre del año, siendo enero (con 11 millones) y marzo (con 9 millones) los meses con mayor actividad, lo cual demuestra que el panorama de amenazas continúa creciendo y evolucionando no solo en el país si no a nivel general, de hecho, la región de América Latina y el Caribe sufrió más de 360 mil millones de intentos de ciberataques en 2022. (Hernández, 2023)

5. Buenas prácticas de ciberseguridad para el teletrabajo

Para mitigar los riesgos de ciberseguridad en entornos de teletrabajo, las empresas del sector privado en El Salvador deben implementar las siguientes buenas prácticas: (IKUSI, 2020)

1. Contar con una Virtual Private Network (VPN): Básicamente, la red privada virtual es una tecnología que posibilita la unión de dos o más dispositivos mediante una conexión particular autenticada, encriptada y segura.
2. Cifrado de información: La criptografía abarca un conjunto de técnicas cuya función principal es proteger la información que se intercambia entre un emisor y un receptor. Este sistema fortalece la seguridad del mensaje o archivo al mezclar su contenido mediante algoritmos matemáticos que codifican los datos del usuario para que solamente el destinatario los pueda entender.
3. Respaldos frecuentes: Durante la jornada de trabajo, las empresas generan una gran cantidad de datos que de no ser almacenados adecuadamente, suelen perderse: para evitar este tipo de problema, es imprescindible que las organizaciones realicen respaldos —backups— frecuentes.
4. Software de protección: Los antivirus y antimalware son soluciones fantásticas, ya que previenen, detectan y eliminan amenazas en los dispositivos. Con todo, existen otras opciones muy útiles que, incluso, pueden considerarse como medidas complementarias.
5. Contraseñas fuertes: El establecimiento de una política de contraseñas eficiente es algo que exige disciplina y la adopción de estrategias que eleven el nivel de la seguridad: implementar claves robustas —que incluyan mecanismos de autentificación por dos factores— es una de las maneras más eficaces de dificultar el acceso de los cibercriminales a los datos.
6. Políticas de ciberseguridad: La política de seguridad de la información es un conjunto de medidas y procedimientos que una empresa define con la intención de orientar el acceso y el uso de los datos, además de soluciones que garanticen su protección en caso de que

ocurran problemas.

6. Recursos para la ciberseguridad en El Salvador

Las empresas del sector privado en El Salvador pueden encontrar una serie de recursos para ayudarlas a mejorar su postura de ciberseguridad en entornos de teletrabajo. Algunos de estos recursos incluyen:

- Superintendencia de Bancos y Seguros (SBS): La SBS ofrece información y recursos sobre ciberseguridad para el sector financiero.
- Secretaría de Innovación de la Presidencia de la República (SI): La SI ofrece programas e iniciativas para promover la ciberseguridad en El Salvador.
- Cámara Salvadoreña de Tecnologías de la Información y las Comunicaciones (CASSATIC): La CASSATICO ofrece información y recursos sobre ciberseguridad para sus miembros.
- Empresas de ciberseguridad: Existen diversas empresas en El Salvador que ofrecen servicios.

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, tomando como referencias bibliotecas académicas, desde el año 2020 cuando hubo un aumento en el teletrabajo y tomó mayor relevancia en las distintas organizaciones.

El "Marco de trabajo de buenas prácticas de ciberseguridad en el teletrabajo para las empresas de desarrollo de software basado en los controles establecidos en la norma ISO 27002:2022 y la NIST SP 800-46" que se enfoca en establecer un conjunto de buenas prácticas de ciberseguridad para las empresas de desarrollo de software que operan bajo modalidades de teletrabajo. Mediante un estudio exploratorio cuantitativo, el autor, Richard Sebastián Esparza Echanique, implementa y evalúa diferentes medidas de seguridad basadas en estándares internacionales. Los resultados indican una mejora significativa en la política de seguridad de la información, la gestión de amenazas, el uso de antivirus, el bloqueo de accesos no autorizados y la actualización constante de las listas de acceso. (Echanique, 2023)

Y el trabajo de Maritza Tobón y Alfredo Alvarez que se centra en el diseño de un programa de seguridad de la información para un call center que maneja operaciones para un cliente del sector bancario en Bogotá, bajo un ambiente de teletrabajo. A raíz del decreto de aislamiento preventivo obligatorio por la pandemia de COVID-19, el call center debió adaptar sus operaciones para permitir que sus empleados trabajaran desde sus casas. Esta situación creó la necesidad de gestionar los riesgos de seguridad de la información de manera eficaz, utilizando como base los estándares de la familia ISO 27000. (Rosero & González, 2021)

Este incremento del teletrabajo trajo consigo varios beneficios pero también algunos 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:

- **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 respetar 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.

2.2 Normativas y Estándares

En El Salvador, existe un marco regulatorio emergente para la ciberseguridad, en esta sección se listaran algunas de las leyes y regulaciones más relevantes, ya que es importante que las empresas del sector privado de nuestro país se mantengan informadas y actualizadas sobre estas y tomen las medidas necesarias para cumplir con ellas.:

1. Ley De Regulación Del Teletrabajo

La ley tiene como objetivo 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. Los principales objetivos del teletrabajo son: aprovechar las tecnologías de la información y comunicación en la prestación de servicios, aumentar y medir la productividad,

mejorar la eficiencia y transparencia en el uso de fondos públicos, reducir gastos y disminuir el consumo de energía eléctrica, combustible, alquileres, entre otros. (Asamblea legislativa, 2020)

2. Ley de Protección de Datos Personales

La ley tiene por objeto la protección integral de los datos personales de las personas naturales en cuanto resulte pertinente, indistintamente en la forma que se almacenen y resguarden, se encuentre en posesión de particulares o de personas jurídicas o entidades públicas y privadas, o cualquier otro tipo de entidad sin personalidad jurídica, con la finalidad de regular su tratamiento legítimo e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas naturales. (Asamblea Legislativa, 2019)

3. Ley especial contra los delitos informáticos y conexos

La ley tiene por 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. (Asamblea legislativa, 2016)

4. 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).** El objetivo es

establecer las líneas de acción y estrategias que permitan al Gobierno de El Salvador definir los aspectos relevantes enfocados en la prevención de riesgos cibernéticos, así como la gobernanza necesaria para abordar con éxito este tema.

Esto incluye definir criterios para el desarrollo de capacidades de ciberseguridad, fortalecer los mecanismos de respuesta ante incidentes y desarrollar habilidades técnicas y de gestión, de modo que las instituciones públicas y privadas y los ciudadanos puedan tomar conciencia de la ciberseguridad y adoptar medidas de protección ante las ciberamenazas.

5. 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. El objeto de la ley:

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.
C. Regular y fiscalizar lo relativo a los proveedores de servicios de certificación, y a los proveedores de servicios de almacenamiento de documentos electrónicos.

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. (Asamblea legislativa, 2015)

6. Norma Técnica Salvadoreña NTS 606:2019

Esta norma establece los requisitos de seguridad para la gestión de la información en las organizaciones. Es aplicable a todos los proyectos, tanto urbanos como rurales, con afluencia de público, de tal manera que todas las obras a construirse sean accesibles para todas las personas. A excepción de los casos de entornos ya edificados, en los que se deberán aplicar los ajustes razonables urbanísticos y arquitectónicos. Norma Técnica Salvadoreña. (2021).

3. Metodología

3.1 Enfoque de Investigación

Para la presente investigación, se adoptará un enfoque cualitativo, el cual se define como el conjunto de estrategias que se utilizan para obtener y procesar información mediante el análisis de datos no numéricos, como textos, entrevistas, y observaciones, así como técnicas interpretativas para llevar a cabo análisis detallados. Este enfoque se caracteriza por su énfasis en la comprensión profunda y contextualizada de los fenómenos y en la subjetividad en la recolección y el análisis de datos. (*Metodología de la investigación* (3ª ed.). (2017). Grupo Editorial Patria.)

Al emplear un enfoque cualitativo, se busca obtener resultados que puedan ser expresados en términos descriptivos, lo que permite realizar interpretaciones ricas y detalladas y establecer relaciones complejas entre variables. Además, este enfoque proporciona una base sólida para la formulación de conclusiones y la toma de decisiones fundamentadas en el entendimiento profundo de las experiencias y perspectivas de los participantes.

Es importante destacar que el enfoque cualitativo implica la utilización de técnicas específicas de análisis, tales como la codificación temática, el análisis de contenido, y el análisis narrativo, entre otras. Estas técnicas permiten explorar patrones, identificar temas emergentes y comprender la significancia de los resultados obtenidos.

.

Fuentes de información primaria

En la presente investigación, se utilizaron como fuentes de información primaria encuestas y entrevistas dirigidas a tres sectores clave de la empresa privada: Industria, Servicios y Comercio. Para cada uno de estos sectores, se diseñaron y aplicaron encuestas y/o entrevistas específicas,

orientadas a los responsables de Ciberseguridad o, en su defecto, a los encargados del área de TI. Estas herramientas de recolección de datos permitieron obtener una visión detallada y precisa sobre las prácticas y desafíos en ciberseguridad que enfrenta cada sector, proporcionando una base sólida para el análisis y las conclusiones del estudio.

El objetivo de las encuestas fue conocer aspectos sobre la identificación de desafíos en la implementación de controles de ciberseguridad en entornos de teletrabajo, Identificación y gestión de riesgos de ciberseguridad de mayor impacto en entornos de teletrabajo, buenas prácticas de ciberseguridad enmarcadas en ISO 27002.

Fuentes secundarias de datos

Para las fuentes de información secundaria, se realizaron búsquedas exhaustivas en artículos disponibles en internet y en libros especializados, enfocándose en los desafíos de seguridad en el contexto del teletrabajo en el sector privado de empresas en El Salvador. Esta investigación incluyó la revisión de publicaciones académicas, informes de organizaciones especializadas en ciberseguridad, y literatura relevante que aborda las problemáticas y soluciones implementadas en el ámbito de la ciberseguridad para el teletrabajo. La información obtenida de estas fuentes permitió enriquecer el análisis, proporcionando una comprensión más profunda y amplia de los retos actuales y las mejores prácticas adoptadas en el sector privado salvadoreño.

3.2 Diseño de la Investigación

El diseño de la investigación consta de una serie de etapas que va desde la elaboración de la encuesta, la identificación y selección de las empresas para la muestra del estudio, el llenado de

las encuestas junto a una entrevista posterior, finalmente la tabulación de los datos y el respectivo análisis de los resultados.

El diseño del estudio se ha estructurado con el objetivo de investigar la aplicación de la ciberseguridad en entornos de teletrabajo en empresas del sector privado en El Salvador. Para ello, se ha seleccionado una muestra representativa que incluye tres empresas: una del rubro de servicios, otra de la industria y una tercera del sector comercial.

Este enfoque de muestreo estratificado permite abordar diversas perspectivas y contextos relacionados con el teletrabajo, así como identificar posibles vulnerabilidades en cada sector específico. Al analizar estas vulnerabilidades, se podrá desarrollar una guía integral de buenas prácticas de seguridad que se adapte a las necesidades y desafíos particulares de cada sector y empresa.

La inclusión de empresas de diferentes sectores económicos garantiza una visión holística de los riesgos y desafíos asociados con el teletrabajo, lo que enriquecerá la calidad y la aplicabilidad de la guía propuesta. Además, al abarcar un espectro diverso de empresas, se podrán identificar patrones comunes y diferencias significativas que contribuyan a una comprensión más completa de la problemática de la ciberseguridad en el teletrabajo.

3.3 Población y Muestra

Para la investigación, se seleccionaron tres empresas representativas del sector privado: una del sector Comercio, una del sector Servicios y otra del sector Industria. La elección de solo una empresa por sector se debió a la complejidad inherente en la obtención de información detallada y confiable de estas organizaciones. Esta muestra limitada permitió enfocarse en profundidad en cada caso, facilitando así la identificación y análisis de los desafíos específicos relacionados con

la implementación del teletrabajo en cada sector. A través de este enfoque, se buscó establecer un panorama claro de las dificultades y mejores prácticas en la adopción del teletrabajo en distintos contextos empresariales.

3.4 Instrumentos de Recolección de Datos

Para el presente trabajo de investigación se han utilizado múltiples instrumentos de recolección de datos. A continuación se detalla cada uno de estos instrumentos:

1. **Encuestas:** Se diseñó una encuesta estructurada en cinco secciones, cada una con cinco preguntas, sumando un total de 25 preguntas abiertas. Estas preguntas están dirigidas a los Gerentes de Tecnología y/o Gerentes de Ciberseguridad de las empresas seleccionadas. La naturaleza abierta de las preguntas permite obtener respuestas detalladas y contextualmente ricas, proporcionando una visión profunda de las prácticas y percepciones en el ámbito de la tecnología y la ciberseguridad.
2. **Entrevistas:** Las entrevistas se emplean como una herramienta complementaria a las encuestas. Su propósito es clarificar y expandir las respuestas obtenidas en las encuestas, permitiendo a los investigadores explorar en mayor profundidad los temas abordados y resolver cualquier ambigüedad. Estas entrevistas se llevaron a cabo con los mismos gerentes, asegurando que las interpretaciones de las respuestas de la encuesta sean precisas y completas. (*Metodología de la investigación* (3ª ed.). (2017). Grupo Editorial Patria.)

3.5 Procedimientos de Recolección y Análisis de Datos

El procedimiento de recolección de datos se realizó con empleados de tres empresas definidas según la muestra de la investigación, se tomaron roles de empleados jefes de área IT y Ciberseguridad, una vez definido esto se realizaron al menos dos sesiones presenciales con cada

empresa participante. La primera sesión se dedicó a la presentación del equipo de investigación y a la entrega de encuestas en la empresa seleccionada. La segunda sesión consistió en una entrevista en profundidad con el Gerente de Tecnología y/o el Gerente de Ciberseguridad de la organización. Esta entrevista tuvo una duración aproximada de 90 minutos y se diseñó para aclarar y profundizar en las respuestas proporcionadas en las encuestas entregadas previamente.

Una vez recolectadas las respuestas, se procedió al análisis de datos. Las respuestas fueron representadas en tablas, diferenciando entre respuestas comunes y no comunes. Esto se debió a que las preguntas eran abiertas y requerían una tabulación detallada conforme al enfoque del estudio. Para esta parte del análisis, se utilizó la herramienta Microsoft Excel, que facilitó la creación de tablas y gráficos necesarios para la visualización y comprensión de los datos obtenidos.

4. Resultados

Parte I. Identificación de desafíos en la implementación de controles de ciberseguridad en entornos de teletrabajo:

1. ¿Cuáles son los principales obstáculos que enfrenta su empresa al implementar controles de ciberseguridad en entornos de teletrabajo?

Respuesta/Sector	*Industria*	*Servicio*	*Comercio*
Presupuesto Limitado	1		
Dispositivos no seguros		1	
Conexiones no seguras		1	
Cultura Ciberseguridad	1	1	
Errores humanos			1
Control en la red de datos			1

Tabla 1, Pregunta 1

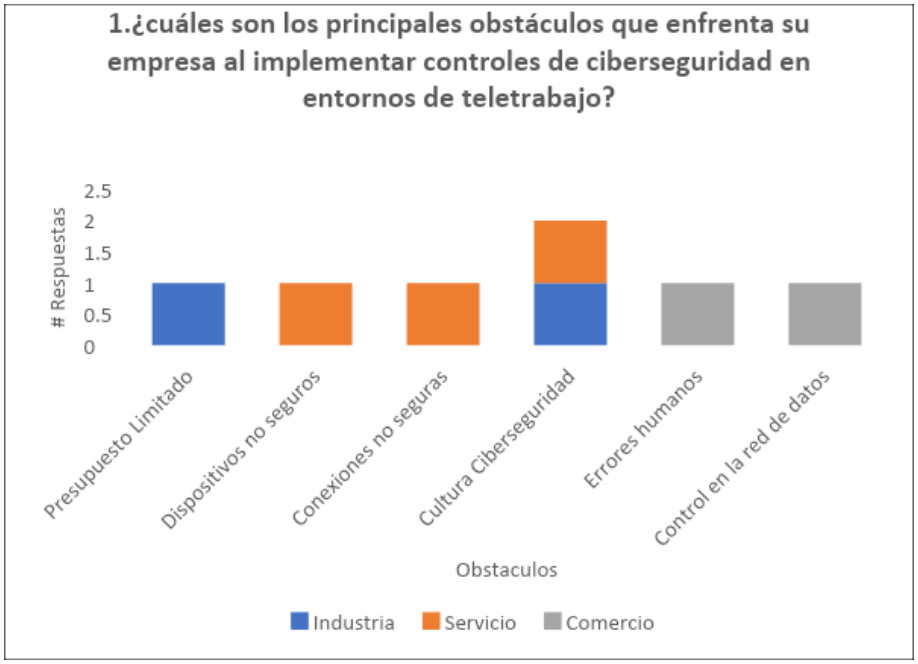

Gráfico 1, pregunta 1

Análisis:

Según los resultados obtenidos para las empresas en estudio unos de los principales obstáculos con los que se enfrentan al momento de implementar controles de Ciberseguridad es la cultura, ya que nos comentan que en ocasiones se brindan las capacitaciones necesarias pero los usuarios se ven un tanto desinteresados respecto a las medidas de seguridad que se brindan en dichos espacios. También hay diversos factores como: los presupuestos limitados, dispositivos no seguros, equipos que no cuentan con las actualizaciones necesarias, sin antivirus, equipos IOT.

2. ¿Cómo evalúa la capacidad de su empresa para educar y concientizar a los empleados sobre las mejores prácticas de ciberseguridad en un entorno de trabajo remoto?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Medio	1	1	
Bajo			1

Tabla 2, Pregunta 2

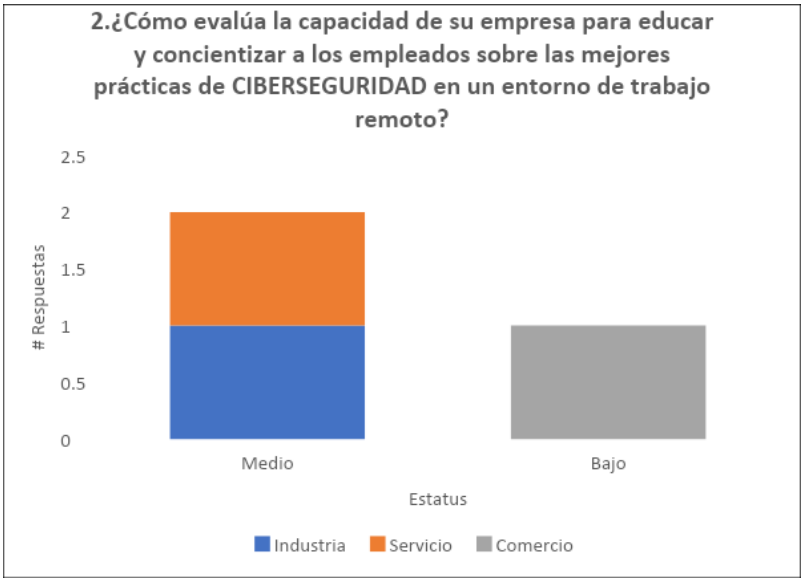

Gráfico 2, Pregunta 2

Análisis:

De acuerdo con los resultados obtenidos para las empresas evaluadas el 66.66% de estas consideran estar en un nivel medio, en cuanto a su capacidad para educar y concientizar respecto a la implementación de buenas prácticas de ciberseguridad, este grupo comenta que ya cuentan con programas de capacitaciones constantes para usuarios sobre seguridad informática, por otro lado, el 33.33% restante aún no cuenta con capacitaciones constantes sobre estas buenas prácticas.

3. ¿Qué medidas ha adoptado su empresa para garantizar la protección de datos confidenciales en entornos de teletrabajo?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Cifrado	1	1	1
Uso VPN	1	1	
Política acceso datos		1	
Control de acceso a sistemas			1
Monitoreo de red			1

Tabla 3, Pregunta 3

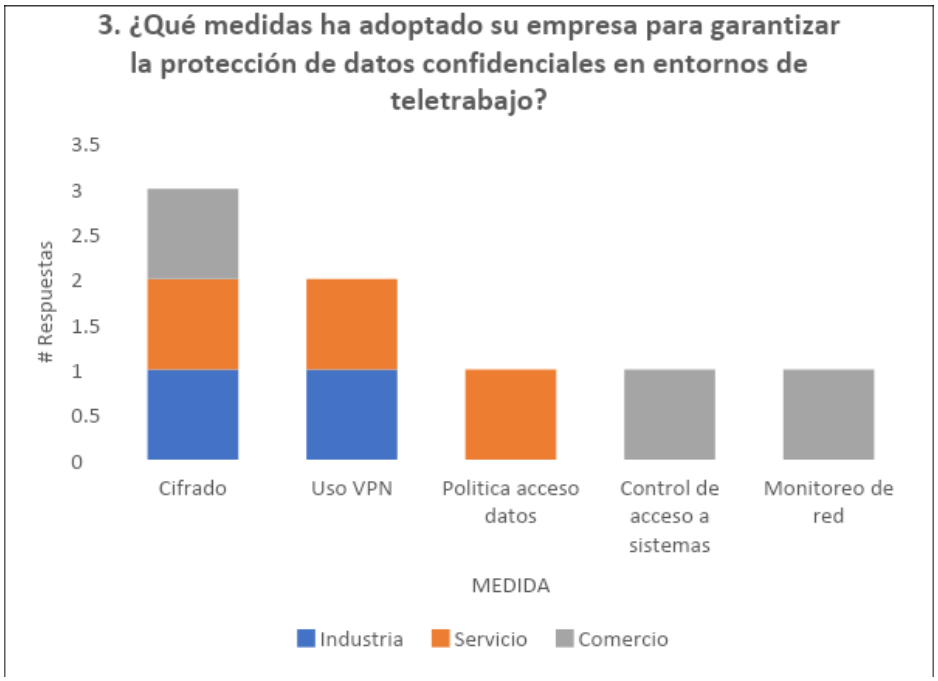

Gráfico 3, Pregunta 3

Análisis:

Según los resultados obtenidos para los casos de estudio seleccionados el 100% de empresas han adoptado o implementado controles de cifrado para garantizar la confidencialidad de los datos de usuarios en modalidad de teletrabajo, también un 66.66% de estas han implementado uso de conexiones VPN para el acceso a sus sistemas, en este sentido la utilización de conexiones VPN por estas organizaciones carecen de doble factor de autenticación, por lo tanto, es una oportunidad de mejora a implementar para estas.

4. ¿Cuáles son los desafíos más comunes que enfrenta su empresa en la gestión de accesos y privilegios en entornos de teletrabajo?

Respuesta/Sector	*Industria*	*Servicio*	*Comercio*
Comunicación Interna	1		
Admin accesos remotos		1	
Actualizaciones políticas de acceso a sistemas		1	
Gestión de contraseñas			1
Gestión de accesos a sistemas			1

Tabla 4, Pregunta 4

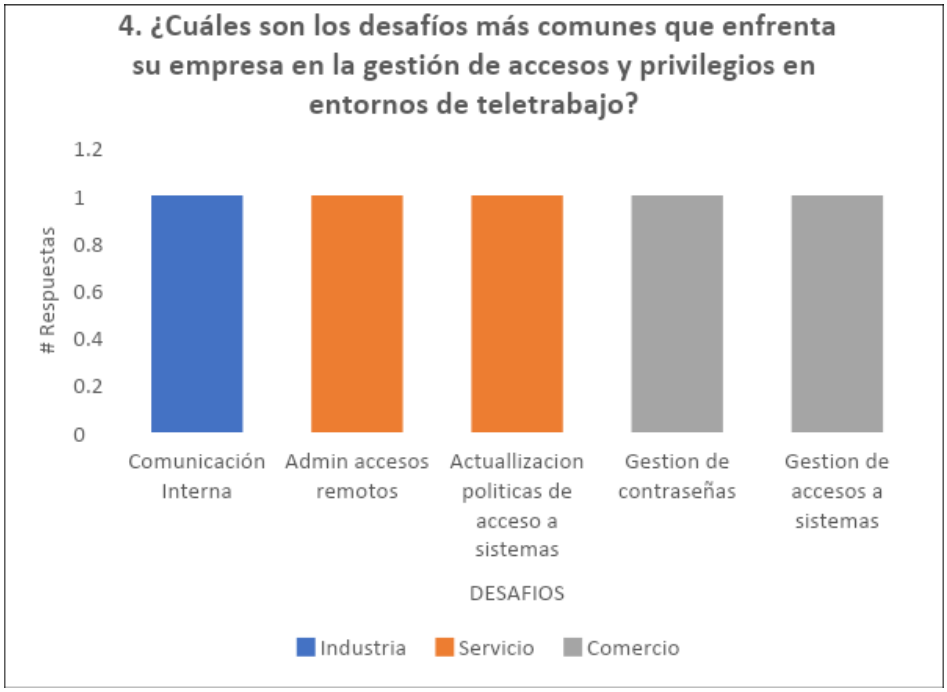

Gráfico 4, Pregunta 4

Análisis:

Conforme a los datos obtenido de la muestra de empresas, todas muestran diferentes desafíos antes la gestión de accesos y privilegios de los sistemas en entorno de teletrabajo,

dentro de los mas significativos se lista el tema de comunicación interna, donde se expresa que en ocasiones no se informa oportunamente cuando un empleado se retira de la organización, trasladando los accesos a otro colaborador, claramente se evidencia una falta de política de bajas de usuarios, también en la parte de actualización de políticas de acceso no se cuenta con un AD implementado que facilite dicha tarea como también la gestión de contraseñas.

5. ¿Cuál es su percepción sobre la eficacia de las VPN en la protección de la información transmitida por empleados que trabajan de forma remota?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Eficaz	1		
Eficaz + otras medidas		1	1

Tabla 5, Pregunta 5

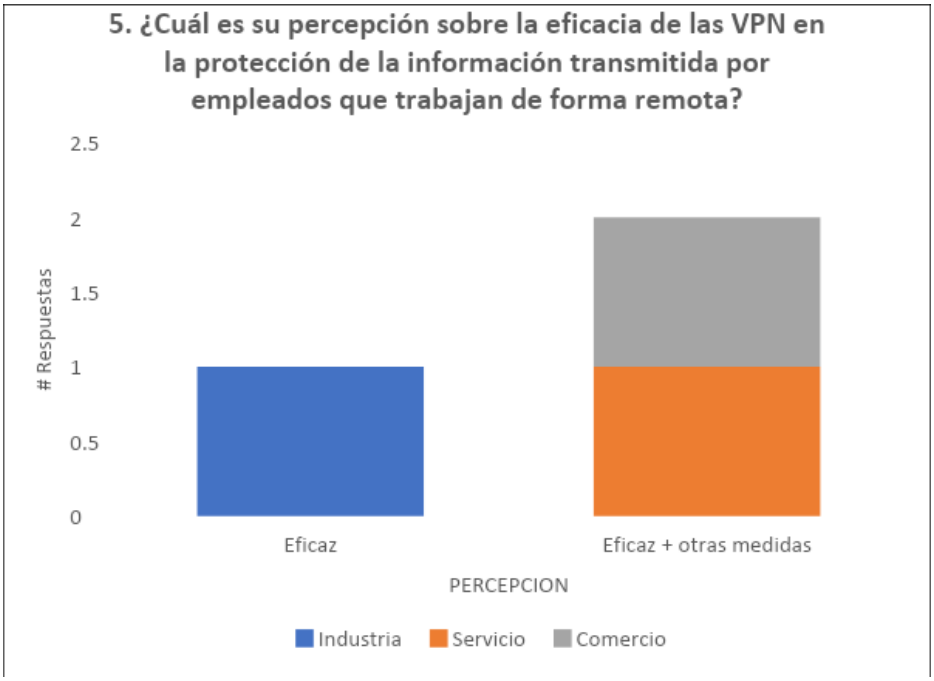

Gráfico 5, Pregunta 5

Análisis:

De acuerdo con las respuestas obtenidas de los 3 casos de estudio, todas están de acuerdo que el uso de conexiones VPN son eficaces para protección de los datos transmitidos desde ubicaciones remotas, sin embargo un 66.6% de estas empresas consideran el uso de VPN eficaz siempre y cuando estas vayan acompañadas con otras medidas de seguridad, por ejemplo el MFA, cabe mencionar que ninguna de estas empresas utiliza doble factor de autenticación en sus conexiones VPN, por lo tanto se vuelve una oportunidad de mejora a implementar.

Parte II. Identificación y gestión de riesgos de ciberseguridad de mayor impacto en entornos de teletrabajo:

1. ¿Cuáles considera que son los riesgos de ciberseguridad más críticos para su empresa en entornos de teletrabajo?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Perdida de Información	1		1
Ataques Ingeniería social		1	1
Ataques Ransomware		1	1

Tabla 6, Pregunta 1

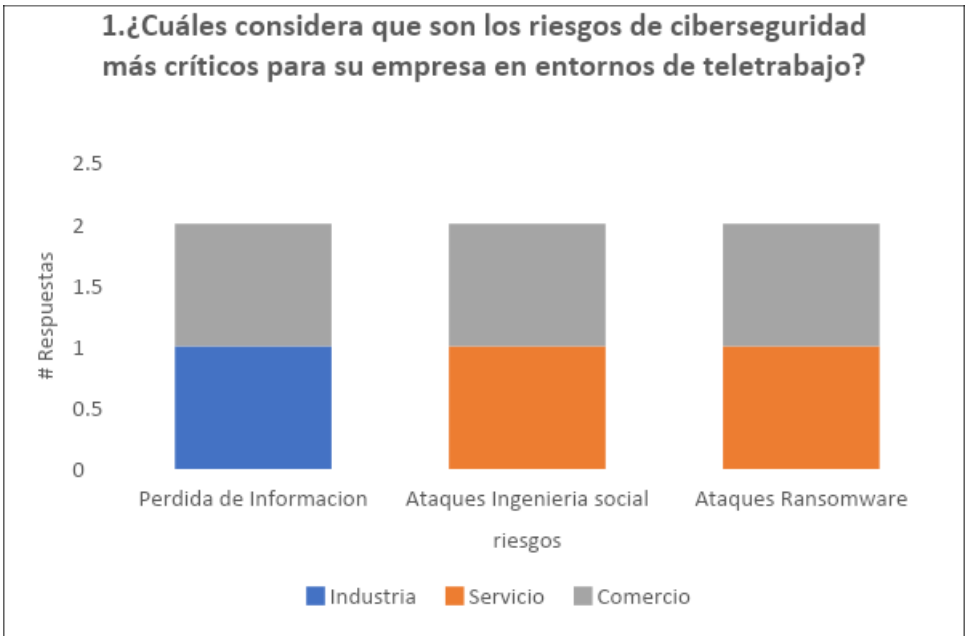

Gráfico 6, Pregunta 1

Análisis:

Según los resultados generados por esta encuesta, las empresas evaluadas consideran La pérdida de información, Ataques de ingeniería social y Ataques Ransomware como riesgos críticos de Ciberseguridad, profundizando un poco más dichas empresas han implementado medidas como: Campañas de concientización de Ciberseguridad, Implementación de IDS , etc. Si bien es cierto carecen de algunos controles necesarios, hay acciones encaminadas a minimizar los impactos de dichos riesgos. La guía de buenas prácticas incluida en este trabajo ayudará a la implementación de nuevas acciones para la prevención de riesgos.

2. ¿Cómo evalúa la preparación de su empresa para enfrentar posibles incidentes de ciberseguridad en un entorno de trabajo remoto?

Respuesta/Sector	*Industria*	*Servicio*	*Comercio*
Bajo	1		
Medio		1	1
Alto			

Tabla 7, Pregunta 2

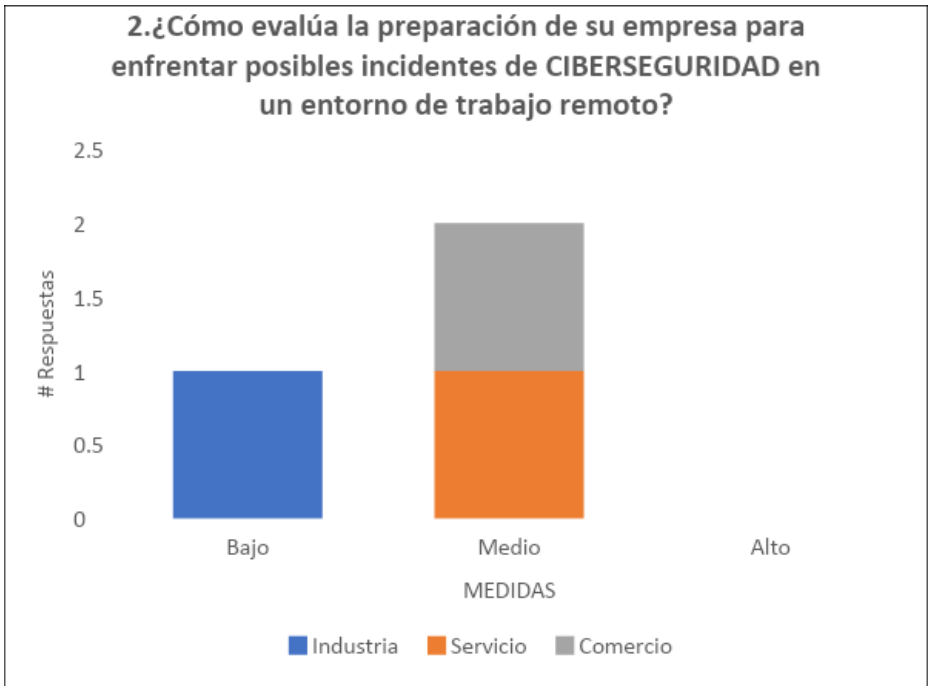

Gráfico 7, Pregunta 2

Análisis:

Respecto a la preparación de las empresas de esta muestra frente a incidentes de Ciberseguridad en entornos de teletrabajo el 66.66% de ellas se encuentra en un nivel medios, estas han aplicado medidas para la evaluación de respuestas ante incidentes de Ciberseguridad, Monitoreos constantes de tráfico de red, políticas de control de acceso, un punto interesante es la realización de simulacros de incidentes de seguridad los cuales

realizan de manera controlada para evaluar los fallos en los controles implementados, por otra parte la empresa del sector industrial tomada en este análisis se encuentra en un nivel bajo ya que están iniciando con la implementación de buenas prácticas de seguridad.

3. ¿Qué medidas ha implementado su empresa para mitigar el riesgo de ataques de phishing dirigidos a empleados que trabajan desde casa?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Concientización en Ciberseguridad	1	1	1
Simulacros de incidentes de Ciberseguridad	1		
Implementación de IDS		1	
Implementación MFA			1

Tabla 8, Pregunta 3

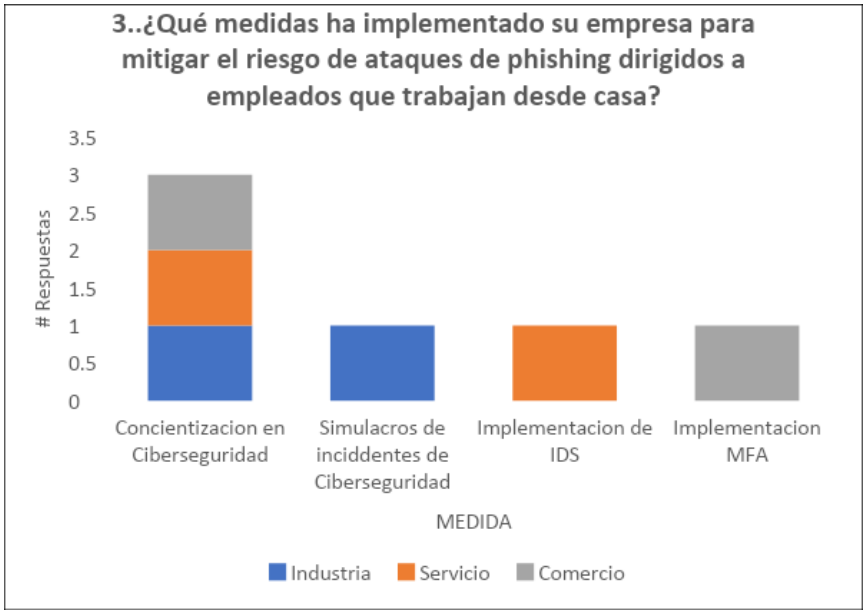

Gráfico 8, Pregunta 3

Análisis:

Según los datos recopilados para las empresas definidas en la muestra, el 100% de estas han realizado campañas de concientización respecto a Ciberseguridad con el propósito de mitigar los riesgos asociados con ataques de Phishing en entornos de teletrabajo, también han implementado medidas como simulacros de Ciberseguridad, implementación de IDS e implementación de MFA para algunos sistemas y plataformas como WhatsApp, Gmail, etc. Si bien es cierto se tienen medidas implementadas, en la guía de buenas prácticas de este documento las empresas podrán tomar de referencias otras prácticas de ciberseguridad.

4. ¿Cuáles son los principales desafíos que su empresa enfrenta en la gestión de dispositivos y acceso a la red en entornos de teletrabajo?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Herramientas especializadas	1		
Cumplimiento políticas de seguridad		1	
Control de dispositivos		1	
Protección de datos			1
Monitoreo de red			1
Gestión actualizaciones (Parches)			1

Tabla 9, Pregunta 4

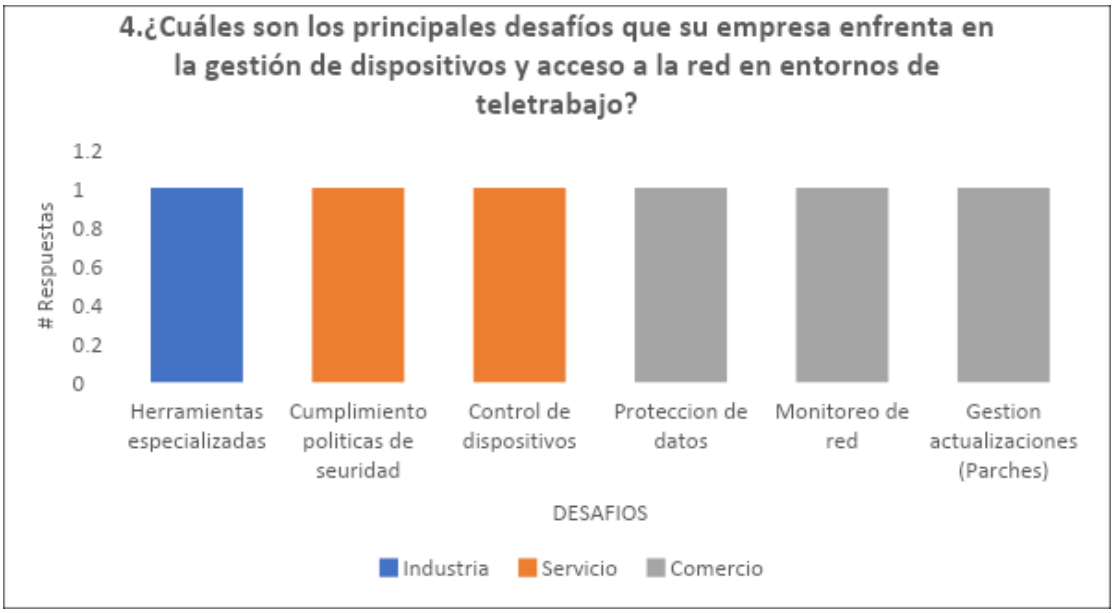

Gráfico 9, Pregunta 4

Análisis:

De acuerdo a los resultados obtenidos, las empresas objeto de estudio consideran como principales desafíos ante la gestión de dispositivos y acceso a la red: La implementación de herramientas personalizadas esto debido al costo de estas y al conocimiento especializado que se debe poseer, también la parte de cumplimiento de las políticas de seguridad en ocasión se vuelve un problema ya que los usuarios no cumplen a cabalidad con dichas medidas, así mismo la actualización de parches de seguridad se vuelve una tarea tediosa ya que no se cuenta con una herramienta centralizada que facilite la tarea.

5. ¿Qué medidas ha adoptado su empresa para garantizar la seguridad de los datos almacenados en dispositivos asignados a empleados que trabajan de forma remota?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Cifrado de datos	1		
Backup a usuarios	1		
políticas BYOD		1	
MDM		1	
Capacitación de Ciberseguridad			1
Implantación Software de seguridad			1
Implementación Política de uso			1

Tabla 10, Pregunta 5

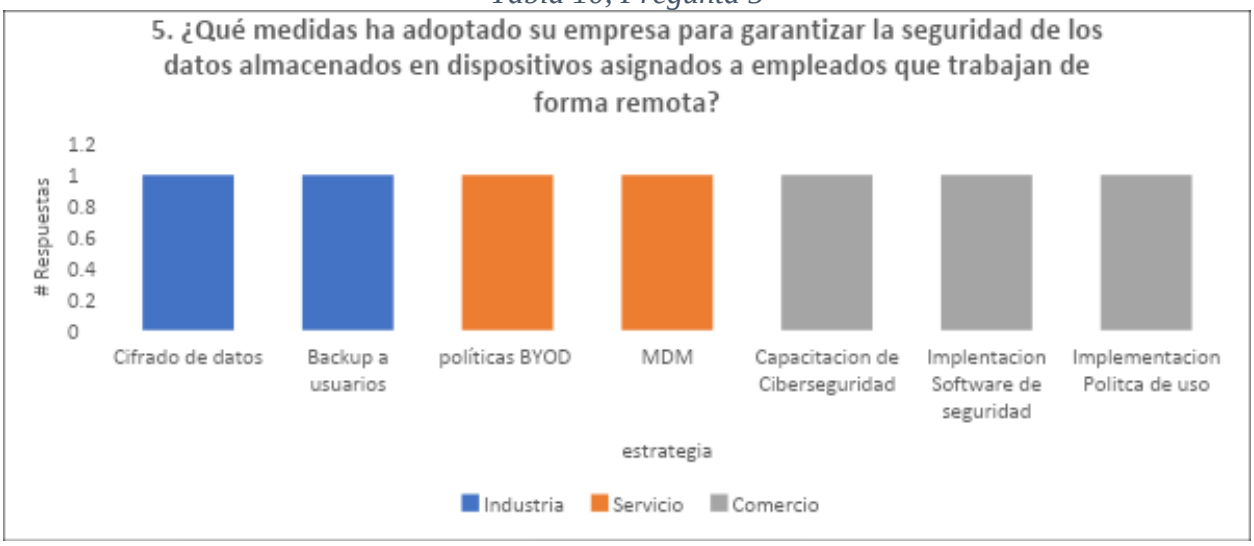

Gráfico 10, Pregunta 5

Análisis:

Conforme a los resultados obtenidos de las empresas que conforman la muestra del presente trabajo de investigación, se listan una cantidad de medidas adoptadas para la protección de los datos en dispositivos de empleados que laboran en la modalidad de teletrabajo, dentro de las medidas más importantes se tiene el cifrado de datos que dicho

fuera de paso esto lo realizan con la herramienta integrada en Windows BitLocker, también cuentan con backup a los documentos de usuarios, dicho respaldo se realiza de manera local en un NAS, pero no se cuentan con réplicas hacia otra ubicación y /o cloud, dicho punto es una acción de mejora que queda para ser implementado.

Parte III. Establecimiento de una guía de buenas prácticas de ciberseguridad enmarcadas en ISO 27002:

1. ¿Está familiarizado/a su empresa con los principios y directrices de ISO 27002 en relación con la ciberseguridad?

Respuesta/Sector	*Industria*	*Servicio*	*Comercio*
Si	1	1	1

Tabla 11, Pregunta 1

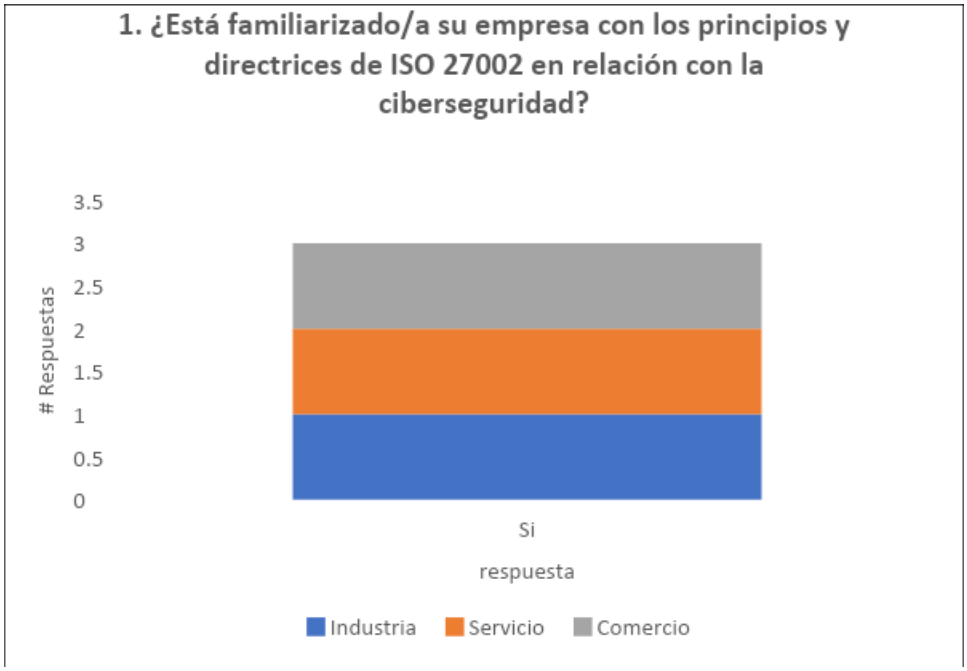

Gráfico 11, Pregunta 1

Análisis:

En cuanto a los datos obtenidos de la muestra establecida, dichas empresas objeto de estudio concuerdan estar familiarizadas con los principios de la ISO 27002, si bien es cierto no existen normas implementados como por ejemplo ISO 27001, es notorio el esfuerzo por la implementación de buenas prácticas de seguridad alineados con ISO 27002, dentro de este trabajo de investigación se listan una serie de buenas prácticas de Ciberseguridad que dichas empresas podrán tomar como referencia para su implementación.

2. ¿Cuáles son las áreas específicas de la norma ISO 27002 que considera más relevantes para su empresa en entornos de teletrabajo?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Control de acceso	1	1	1
Cifrado de datos	1		
Gestión Incidentes			
Ciberseguridad	1		
Gestión activos		1	
Gestión Comunicaciones		1	
Seguridad dispositivos			1
Gestión de riesgos			1

Tabla 12, Pregunta 2

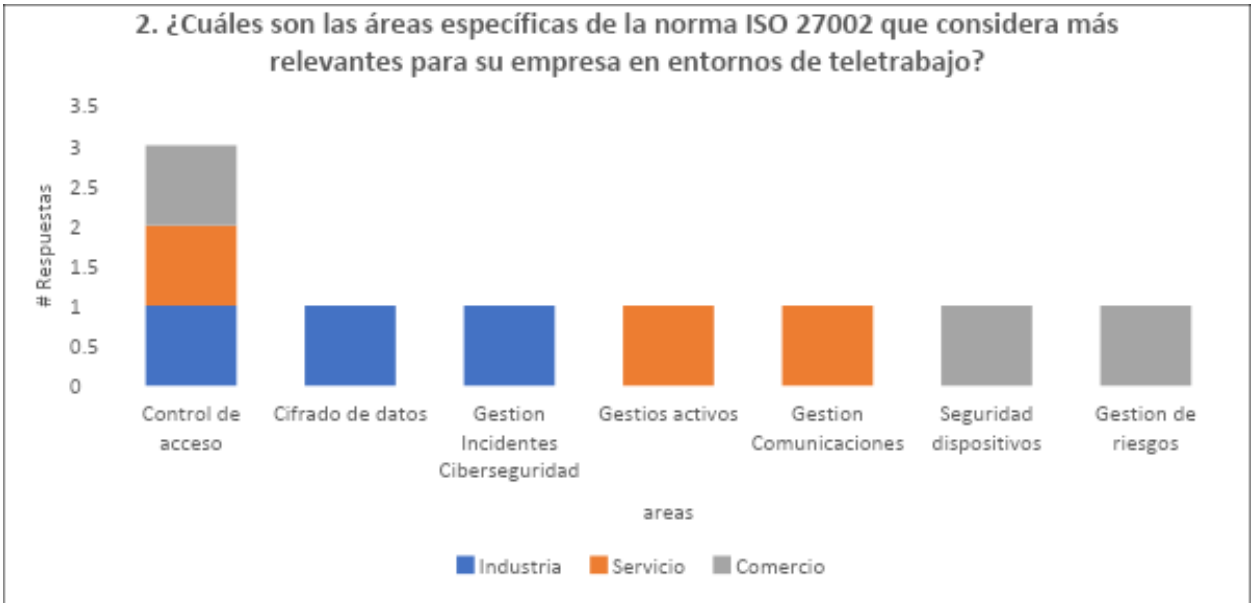

Gráfico 12, Pregunta 2

Análisis:

Respecto a los resultados obtenidos de la encuesta realizada a las empresas que conforman los casis de estudio de la investigación, es importante recalcar que dichas empresas consideran que el Control de acceso es una área relevante enmarcado en la ISO 27002, en ese sentido manifiestan los inconvenientes que presentan al momento de implementar dichos controles, otras áreas relevantes son el Cifrado de datos el cual se realiza con la herramienta propia de Windows (BitLocker), otro aspecto importante es la Seguridad de dispositivos a cual es preocupante ya que se cuentan con dispositivos IOT los cuales no es posible aplicar medidas de seguridad por sus limitaciones de hardware.

3. ¿Qué medidas ha adoptado su empresa para cumplir con los requisitos de ISO 27002 en cuanto a gestión de riesgos de seguridad de la información?

Respuesta/Sector	*Industria*	*Servicio*	*Comercio*
Cifrado de datos	1		
Control de acceso a sistemas	1		
Política de seguridad		1	
Auditorias constantes		1	
Evaluación de riesgos			1
Monitoreo de red			1
Capacitaciones de Ciberseguridad			1

Tabla 13, Pregunta 3

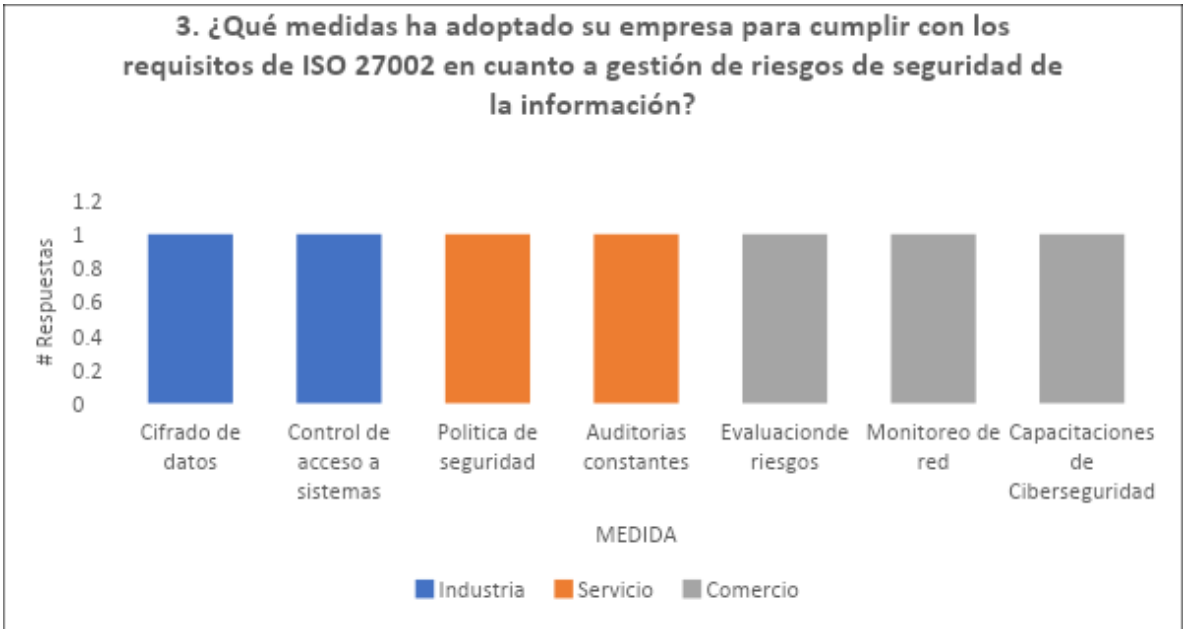

Gráfico 13, Pregunta 3

Análisis:

Según los datos obtenidos, las empresas objeto de estudio han implementado una serie de medidas orientadas a garantizar la seguridad de la información, dentro de estas medidas se listan: Cifrado de datos, Control de acceso a sistemas, Implementación de política de seguridad, Auditorias especializadas constantes, Evaluación de riesgos, Monitoreo de red y finalmente capacitaciones sobre Ciberseguridad, se cuenta con múltiples medidas definidas por la ISO 27002, sin embargo todas estas medidas deberían de ser implementadas en cada una de las empresas, es por ello que acá se evidencia una oportunidad de mejora para la implementación de controles de Ciberseguridad.

4. ¿Cómo evalúa el nivel de cumplimiento de su empresa con los controles de seguridad establecidos en ISO 27002 en un entorno de teletrabajo?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Bajo	1		
Medio		1	1
Alto			

Tabla 14, Pregunta 4

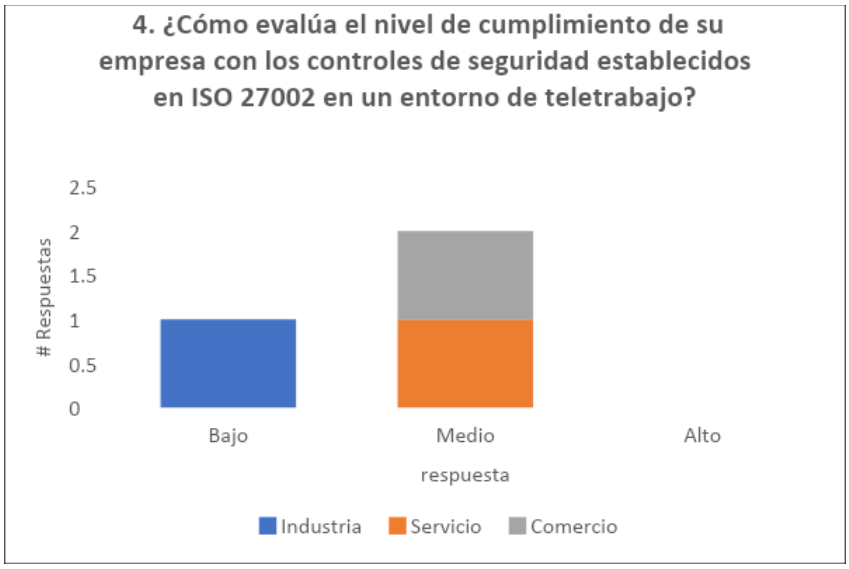

Gráfico 14, Pregunta 4

Análisis:

De acuerdo con las empresas que conforman la muestra de la presente investigación el 66.66% de estas consideran estar en un nivel Medio de cumplimiento de controles de seguridad alineados con las ISO 27002, aca se cuentan con capacitaciones constantes de Ciberseguridad, Auditorías constantes, tienen un grado de madurez mayor y una cultura de Ciberseguridad ya definida, por otro lado la empresa restante del sector comercio se define en un nivel bajo, esto debido a que si bien es cierto cuenta con algunos controles implementados comentan que no tienen una política de seguridad implementada ni una cultura de Ciberseguridad bien establecida en sus usuarios.

5. ¿Cuáles son los desafíos más significativos que su empresa enfrenta al alinear sus prácticas de ciberseguridad con los estándares de ISO 27002?

Respuesta/Sector	*Industria*	*Servicio*	*Comercio*
Presupuesto limitado	1		
Recurso humano calificado	1		
Política de seguridad actualizada		1	
Gestión del cambio		1	
Capacitaciones Ciberseguridad			1
Gestión de riesgos			1
Cooperación			1

Tabla 15, Pregunta 5

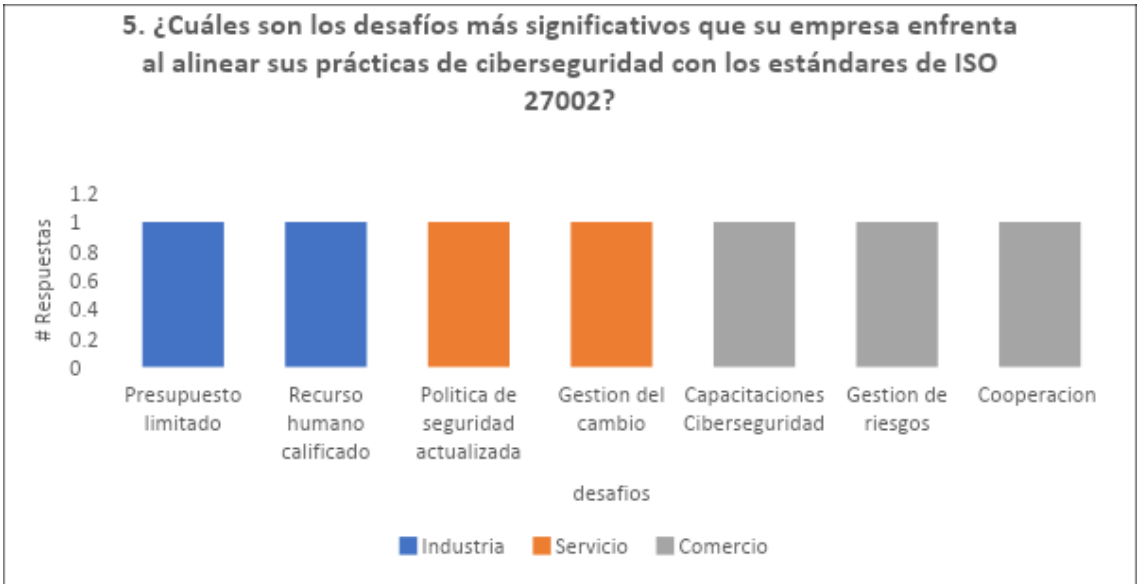

Gráfico 15, Pregunta 5

Análisis:

Conforme a los datos obtenidos, las empresas evaluadas de los diferentes sectores: Comercio, Industria, Servicios, han establecido algunos desafíos que dichas empresas enfrentan al alinear sus prácticas de seguridad con los estándares de la norma ISO 27002, dentro de los desafíos más relevantes se tiene la parte de presupuestos limitados, esto afecta directamente a la inversión de herramientas orientadas a la seguridad de la información, también el recurso humano calificado es un factor determinante para la implementación de herramientas de ciberseguridad.

Parte IV. Análisis de las empresas del sector privado de El Salvador:

1. ¿Cuántas empresas del sector privado en El Salvador han implementado políticas formales de ciberseguridad en entornos de teletrabajo?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Pequeña parte	1	1	
No tiene idea			1

Tabla 16, Pregunta 1

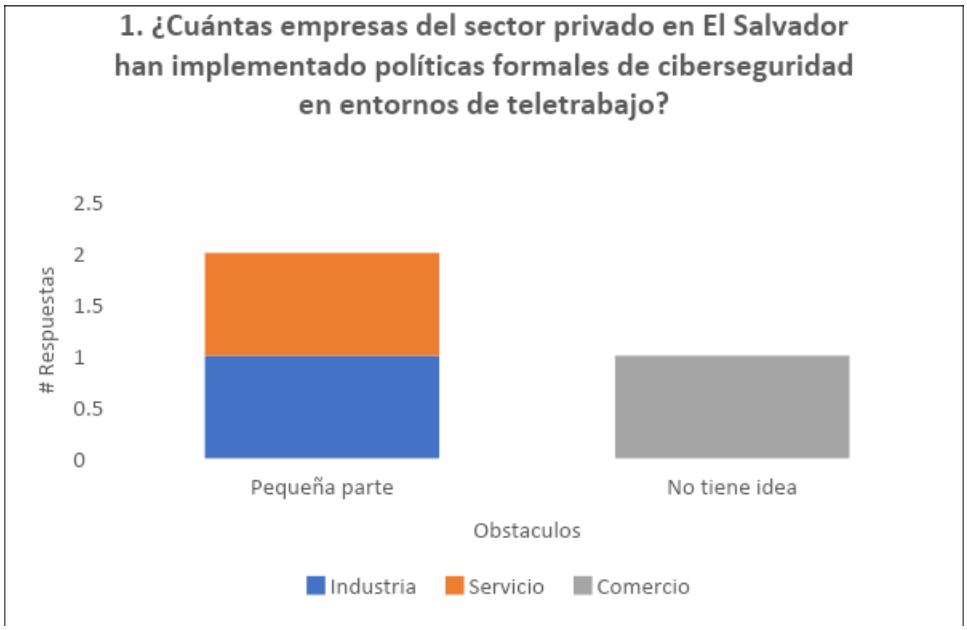

Gráfico 16, Pregunta 1

Análisis:

En cuanto a los resultados obtenidos de las empresas casos de estudio el 66.66% considera que una pequeña parte de las empresas del sector han implementado políticas de ciberseguridad orientadas en entornos de teletrabajo, el resto desconoce de la cantidad. Para las empresas que tienen un mínimo conocimiento de empresas que hayan implementado políticas de ciberseguridad comentan que lo conocen a través de otros colegas ya que no se cuenta con un registro que cuantifique la cantidad de estas organizaciones que adopten dichas buenas práctica de ciberseguridad.

2. ¿Cuáles son las principales prácticas de ciberseguridad que han demostrado ser más efectivas en empresas similares a la suya en El Salvador?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Cifrado de datos	1		
VPN	1		1
MFA		1	
Capacitaciones			
Ciberseguridad		1	
Control de acceso a sistemas			1

Tabla 17, Pregunta 2

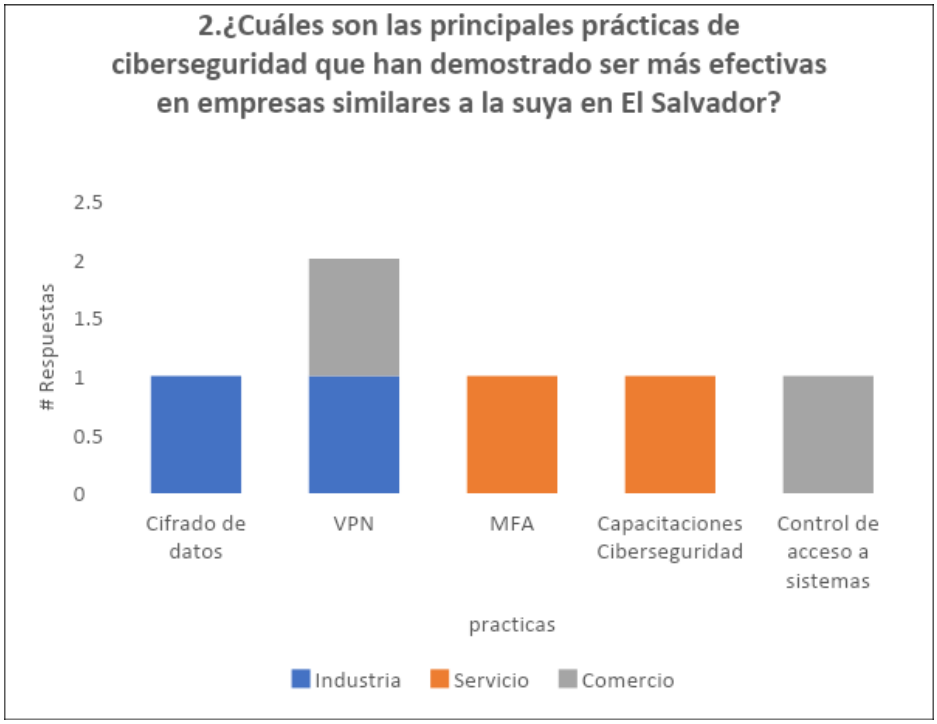

Gráfico 17, Pregunta 17

Análisis:

Conforme a los datos obtenidos de las empresas encuestadas, consideran que una de las principales prácticas se Ciberseguridad que según su experiencia han sido efectivas son el uso de conexiones VPN, también se lista el cifrado de datos tanto en tránsito como en reposo, de igual forma la autenticación de doble factor (MFA), las capacitaciones de Ciberseguridad y finalmente los controles de acceso a sistemas, cabe mencionar que estas medidas son consideradas desde la experiencia de cada empresa encuestada ya que mencionan desconocer la efectividad para otras organizaciones.

3. ¿Ha experimentado su empresa algún incidente de ciberseguridad en un entorno de teletrabajo en el último año?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
No	1		
Si		1	1

Tabla 18, Pregunta 3

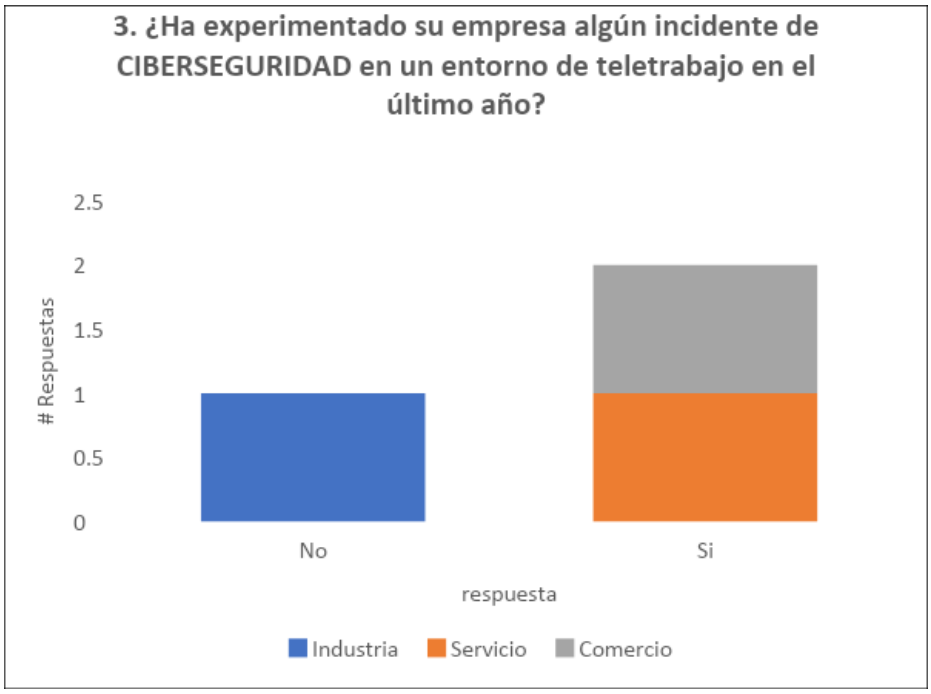

Gráfico 18, Pregunta 3

Análisis:

En cuanto a la aparición de incidentes de ciberseguridad en entornos de teletrabajo en el periodo de un año de las empresas encuestadas el 66.66% afirman si tener incidencias reportadas en ese periodo, el resto no reporta ninguna incidencia. Es importante mencionar que los incidentes reportados hacen referencia a vulnerabilidades generadas por usuarios finales y fallas en políticas de acceso a sistemas. Lo interesante es que las empresas que detectaron estos incidentes tienen muy claras las medidas a implementar para evitar la recurrencia.

4. ¿Qué medidas ha tomado su empresa para mejorar la ciberseguridad después de un incidente en un entorno de teletrabajo?

Respuesta/Sector	*Industria*	*Servicio*	*Comercio*
N/A	1		
Actualización de políticas de control de acceso		1	
Capacitación Ciberseguridad		1	
Implementar MFA			1

Tabla 19, Pregunta 4.

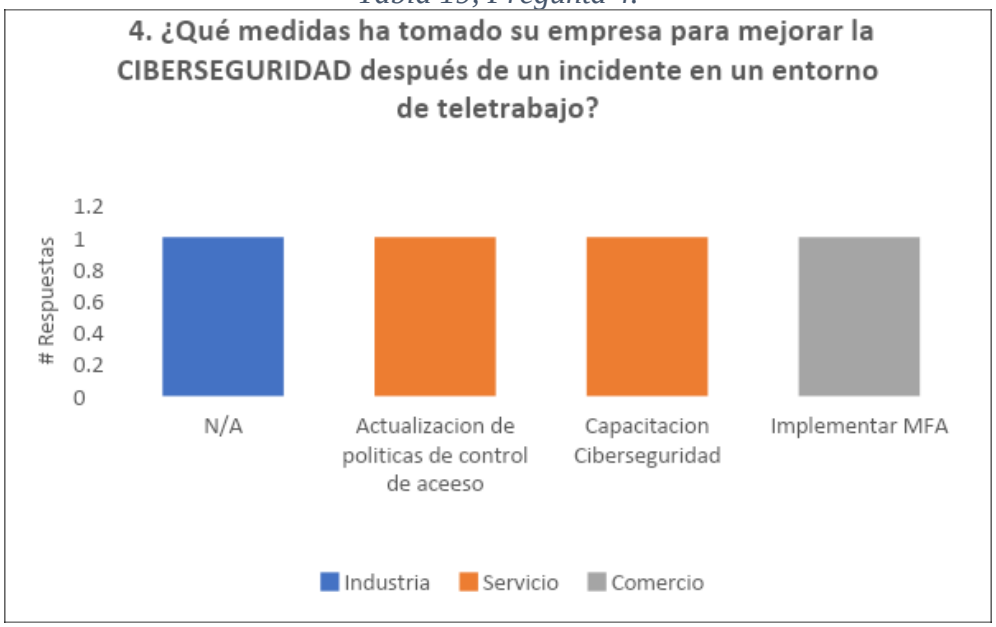

Gráfico 19, Pregunta 4.

Análisis:

Respecto a las medidas de Ciberseguridad implementadas tras un incidente de seguridad, las empresas encuestadas brindan una serie de medidas que aseguran la prevención de riesgos asociados a los incidentes ya materializados, medidas como Actualización de políticas de control de acceso a los sistemas, programación de charlas de Ciberseguridad,

implementación de autenticación multifactorial, etc. Los incidentes materializados van encaminados directamente con usuarios finales y políticas de control de acceso a sistemas mal definidos.

5. ¿Cuál es el nivel de colaboración entre empresas del sector privado en El Salvador en cuanto a compartir información y mejores prácticas de ciberseguridad en entornos de teletrabajo?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Bajo	1		1
Medio		1	
Alto			

Tabla 20, Pregunta 5.

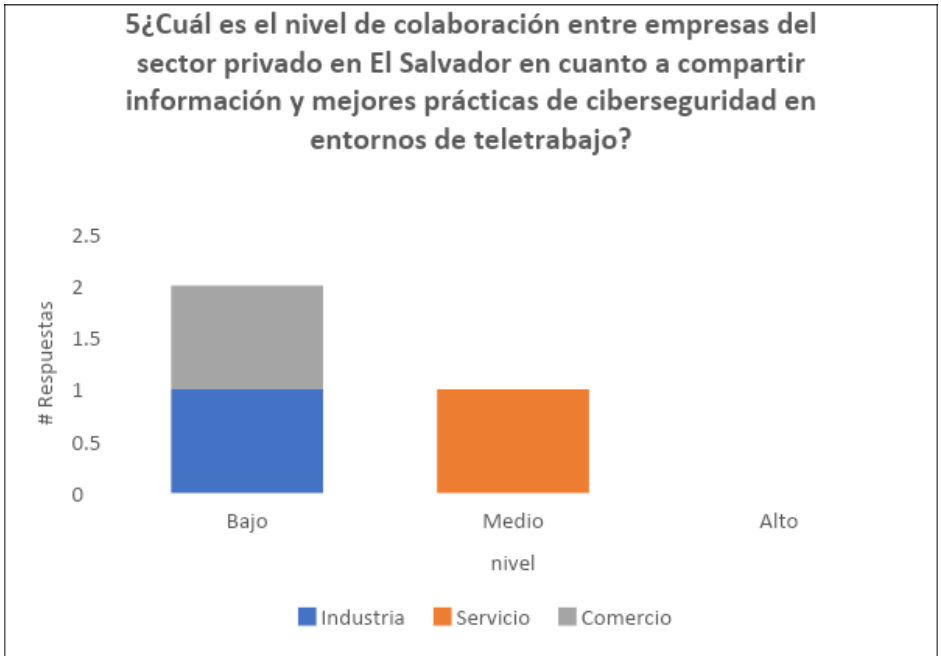

Gráfico 20, Pregunta 5.

Análisis:

Según los datos recopilados de las empresas encuestadas, afirman tener poca colaboración con otras empresas del sector en cuanto a compartir información y mejores prácticas de Ciberseguridad en ambientes de teletrabajo, un 33.33% afirma contar con un nivel de colaboración medio, esto ya que cuenta con el apoyo de algunos colegas que laboran en otras instituciones los cuales comparte conocimiento en materia de Ciberseguridad, claramente nos indican que esta colaboración es un tanto informal y no oficial.

Parte V. Consideraciones adicionales:

1. ¿Cómo evaluaría la preparación general de su empresa para hacer frente a los desafíos emergentes en ciberseguridad en un entorno de teletrabajo?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Bajo	1		1
Medio		1	
Alto			

Tabla 21, Pregunta 1

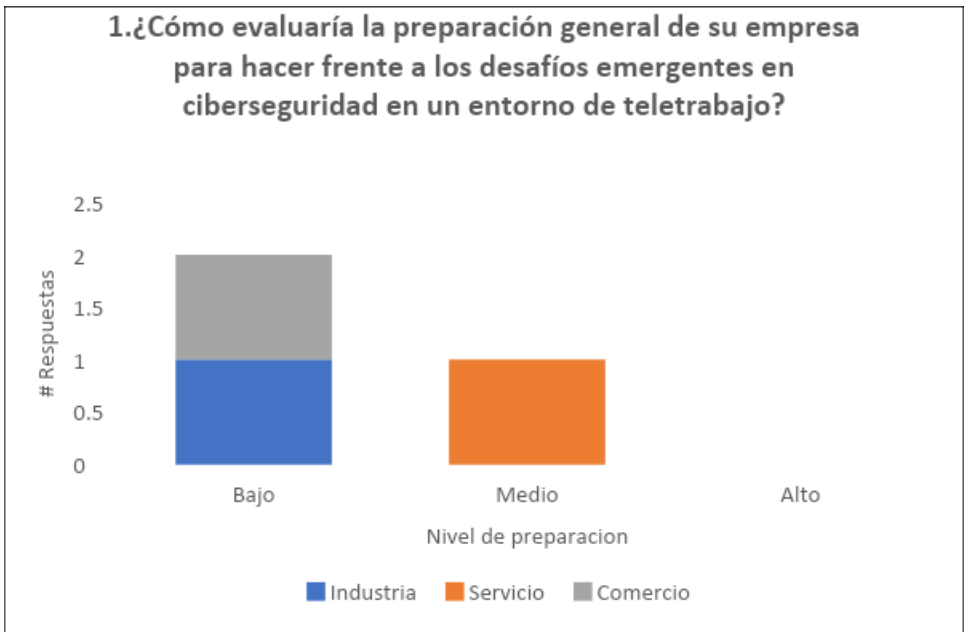

Gráfico 21, Pregunta 1

Análisis:

De acuerdo a los resultados obtenidos el 66.66% de las empresas encuestadas consideran estar en un nivel bajo en cuanto a la preparación ante desafíos emergente de Ciberseguridad en entornos de teletrabajo, el resto considera está en un nivel medio, estas empresas consideran un nivel mayor debido a diversos factores, como: Nivel de cultura de Ciberseguridad ya en desarrollo, realización de auditorías constantes, etc. Mientras que las empresas de nivel bajo comentan que no cuentan con presupuestos adecuados para implementar controles de seguridad ni tampoco cuentan con el personal con la formación idónea para ello.

2. ¿Cuáles son los principales factores que influyen en la eficacia de las medidas de ciberseguridad implementadas en su empresa en entornos de teletrabajo?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Apoyo Gerencia	1	1	
Personal no calificado	1		
Poca Colaboración de usuarios	1	1	1
Actualización tecnológica		1	
Solidez en las políticas Ciberseguridad			1
Implementación eficaz de controles			1

Tabla 22, Pregunta 2.

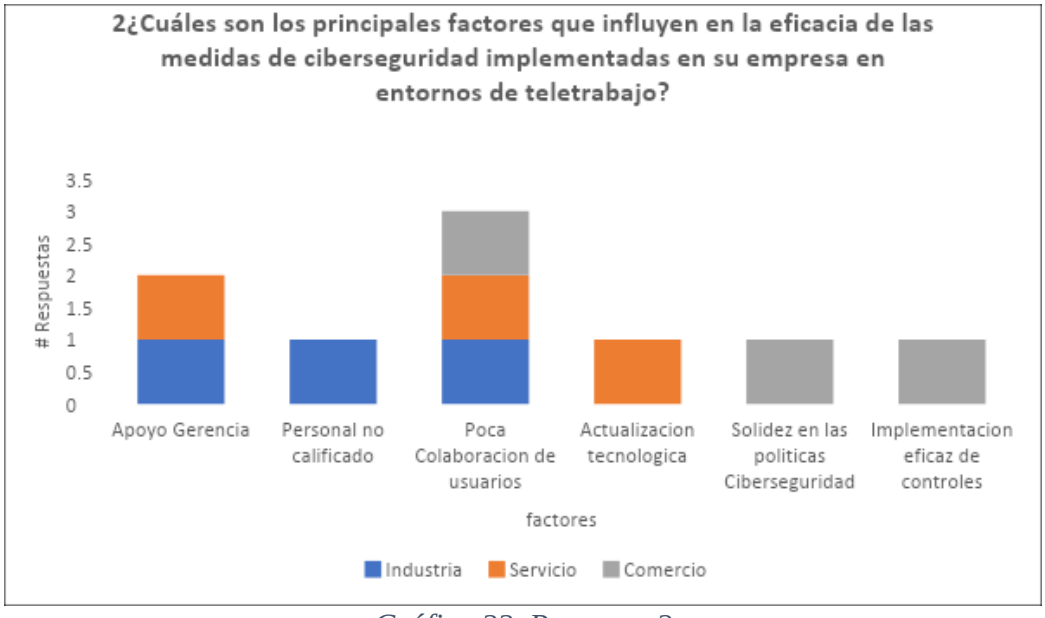

Gráfico 22, Pregunta 2

Análisis:

Conforme a lo datos obtenidos por parte de las empresas que conforman la muestra de esta investigación estas concuerdan que la poca colaboración de usuarios es un factor primordial que afecta la eficacia de las medidas de Ciberseguridad en entornos de teletrabajo, esto obedece a la afirmación que dice que en un ecosistema digital el eslabón más débil siempre es el factor humano, el otro factor es el apoyo a gerencia ya que no se cuentan con el apoyo necesario para la implementación de controles de seguridad ni un presupuesto adecuado para la adquisición de herramientas y equipos que ayuden a la gestión de la Ciberseguridad.

3. ¿Qué recursos adicionales o apoyo necesitaría su empresa para mejorar sus prácticas de ciberseguridad en entornos de teletrabajo?

Respuesta/Sector	***Industria***	***Servicio***	***Comercio***
Inversión en tecnología	1	1	1
Recurso Humano calificado	1		
Formación Ciberseguridad		1	1

Tabla 23, Pregunta 3.

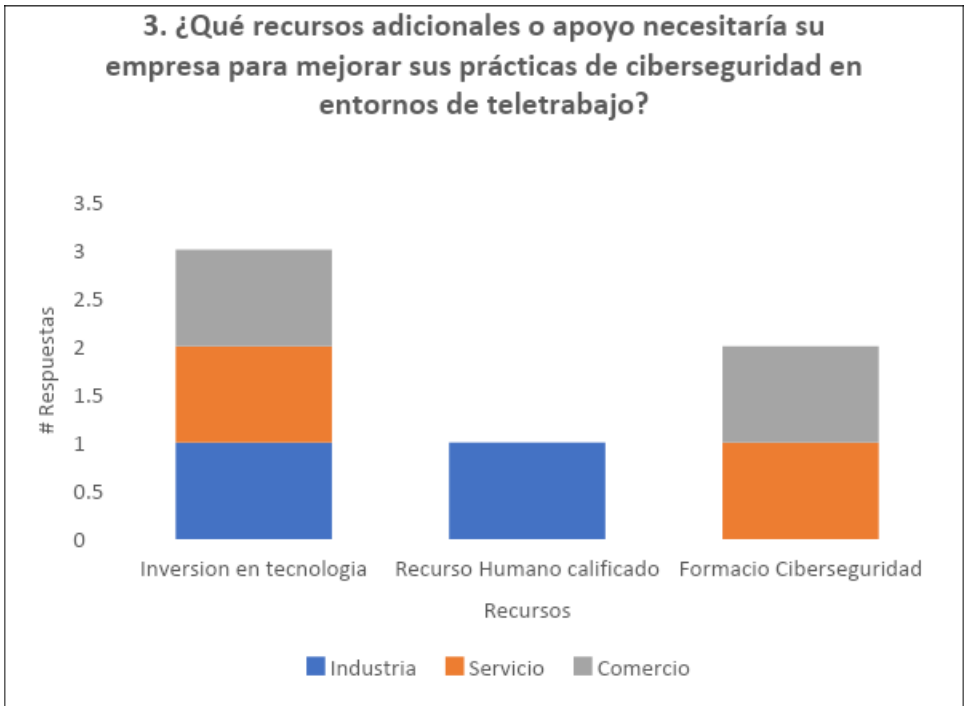

Gráfico 23, Pregunta 3.

Análisis:

En cuanto a los recursos adicionales que necesitan las empresas encuestadas para mejorar sus prácticas de Ciberseguridad, están concuerdan que la parte en la inversión tecnológica es de suma importancia para una correcta implementación de controles de seguridad, también las capacitaciones constantes al personal sobre buenas prácticas de Ciberseguridad, finalmente el contar con el capital humano idóneo se vuelve un recurso valioso a la hora de implementar herramientas tecnológicas para la correcta gestión de la Ciberseguridad.

4. ¿Cómo evalúa la importancia de la colaboración entre el sector privado, el Gobierno y otros actores relevantes en la mejora de la ciberseguridad en El Salvador?

Respuesta/Sector	*Industria*	*Servicio*	*Comercio*
Muy importante	1	1	1

Tabla 24, Pregunta 4.

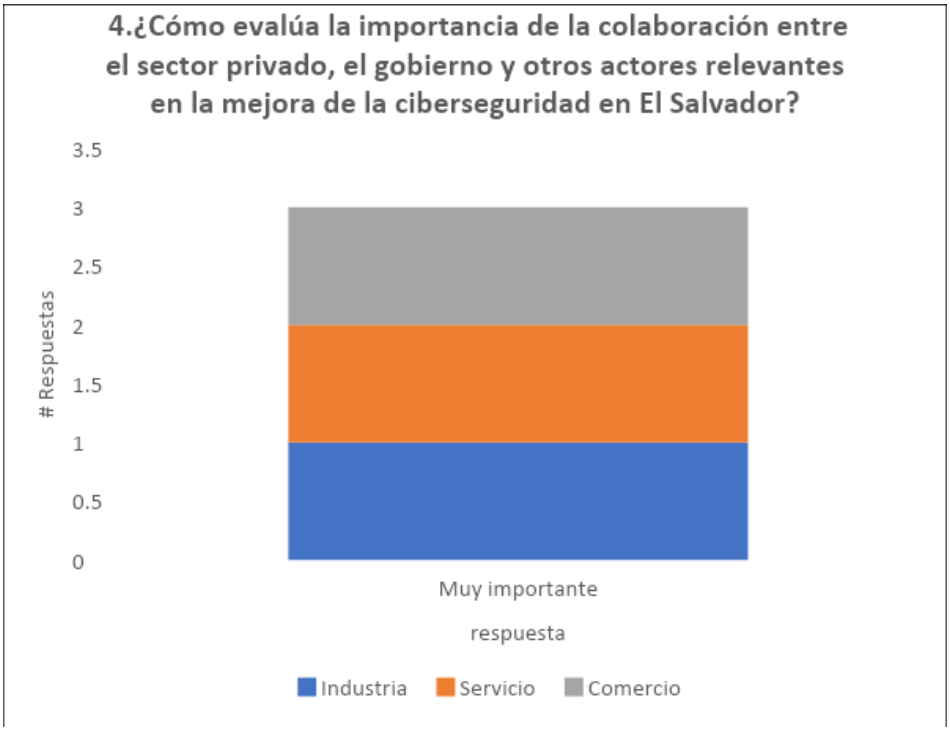

Gráfico 24, Pregunta 4

Análisis:

La colaboración entre el sector privado, el Gobierno y otros actores relevantes es evaluada como muy importante por las empresas encuestadas, para la mejora de la ciberseguridad, se reconoce la crucial importancia de esta cooperación para enfrentar eficazmente los desafíos de Ciberseguridad y fortalecer la seguridad en entornos de teletrabajo. Esta unanimidad subraya la necesidad de un enfoque colaborativo y coordinado para mejorar la ciberseguridad a nivel nacional. Esto a pesar que las empresas consideran un nivel bajo de colaboración entre ellas para compartir conocimiento sobre aspectos de ciberseguridad.

5. ¿Qué medidas de seguridad adicionales considera necesarias para proteger la infraestructura crítica de su empresa en un entorno de teletrabajo?

Respuesta/Sector	*Industria*	*Servicio*	*Comercio*
VPN+MFA	1		
Controles avanzados de acceso a sistemas		1	
Pentesting		1	1
Análisis de vulnerabilidades			1

Tabla 25, Pregunta 5.

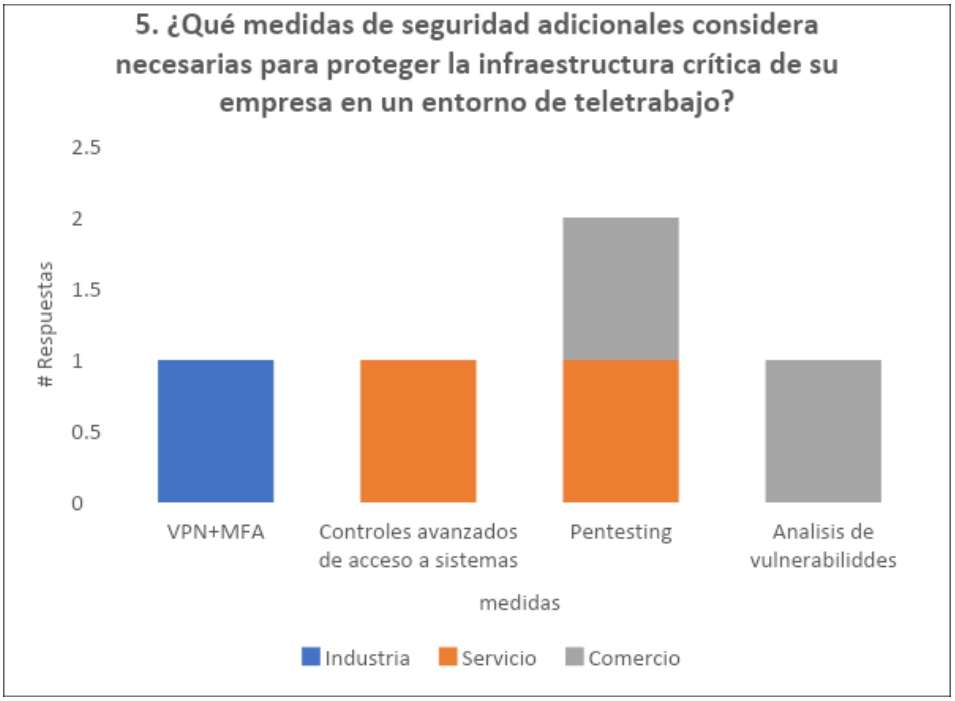

Gráfico 25, Pregunta 54.

Análisis:

Las medidas de seguridad adicionales que las empresas en estudio consideran necesarias para proteger la infraestructura crítica en un entorno de teletrabajo son diversas, dentro de las mas relevantes se tiene las pruebas de Pentesting las cuales ayudan con la identificación de vulnerabilidades y pone a prueba la efectividad de los controles ya implementados, también la utilización de conexiones VPN con doble factor de autenticación es una medida adicional bastante efectiva para la protección de las comunicaciones y datos, el análisis de vulnerabilidades también proporciona un plus en la identificación de riesgos potenciales.

5. Discusión

5.1 Análisis de Resultados

Para el análisis de los resultados se abordará cada una de las cinco partes de encuestas definidas para las 3 empresas casos de estudio seleccionadas del sector privado de El Salvador.

Parte I: Identificación de desafíos en la implementación de controles de ciberseguridad en entornos de teletrabajo

Los desafíos en la implementación de controles de ciberseguridad en entornos de teletrabajo son múltiples y complejos. Uno de los principales obstáculos es la falta de una cultura organizacional sólida en ciberseguridad. Aunque las empresas brindan capacitaciones, muchas veces los empleados muestran desinterés, lo que reduce la eficacia de estas iniciativas. Este problema se agrava con la existencia de presupuestos limitados que impiden la adquisición de equipos seguros y actualizados. La carencia de dispositivos con las actualizaciones necesarias y la falta de antivirus adecuados también se presentan como barreras significativas. Además, la gestión de dispositivos IoT, que frecuentemente carecen de medidas de seguridad adecuadas debido a sus limitaciones de hardware, añade otro nivel de complejidad.

La capacidad de educar y concientizar a los empleados es moderada, con un 66.66% de las empresas considerando que están en un nivel medio, lo que indica la existencia de programas de capacitación aunque no de manera uniforme. En cuanto a la protección de datos, todas las empresas utilizan cifrado, y dos tercios emplean VPN, aunque sin autenticación multifactor, lo que representa una oportunidad de mejora. La gestión de accesos y privilegios es otro desafío

crítico, especialmente debido a problemas de comunicación interna y la falta de políticas claras de bajas de usuarios. Aunque las VPN son vistas como eficaces, su falta de integración con otras medidas de seguridad, como el MFA, limita su efectividad total.

Parte II: Identificación y gestión de riesgos de ciberseguridad de mayor impacto en entornos de teletrabajo

La identificación y gestión de riesgos de ciberseguridad en entornos de teletrabajo se centran en amenazas significativas como la pérdida de datos, ataques de ingeniería social y ransomware. Las empresas reconocen estos riesgos como críticos y han implementado diversas medidas para mitigarlos, incluyendo campañas de concientización y la implementación de sistemas de detección de intrusos (IDS). Sin embargo, aunque estas medidas son un buen comienzo, las empresas aún carecen de algunos controles necesarios, lo que subraya la importancia de la guía de buenas prácticas propuesta en esta investigación para mejorar la preparación y respuesta ante estos riesgos.

La preparación para enfrentar incidentes de ciberseguridad varía entre las empresas. Un 66.66% se considera en un nivel medio de preparación, gracias a la implementación de medidas como monitoreo de tráfico de red y simulacros de incidentes. Sin embargo, la falta de madurez en algunas empresas, especialmente en el sector industrial, destaca la necesidad de continuar desarrollando y fortaleciendo sus estrategias de ciberseguridad. Las medidas para mitigar ataques de phishing incluyen campañas de concientización y simulacros de seguridad, aunque aún hay espacio para mejorar en la implementación de MFA y otras tecnologías avanzadas de seguridad.

La gestión de dispositivos y accesos sigue siendo un desafío, con problemas en la implementación de herramientas personalizadas y la actualización de parches de seguridad.

Parte III: Establecimiento de una guía de buenas prácticas de ciberseguridad enmarcadas en ISO 27002

La familiaridad con los principios y directrices de ISO 27002 es alta entre las empresas encuestadas, aunque la implementación de la norma ISO 27001 no es tan común. Las empresas reconocen la importancia de áreas específicas como el control de acceso y el cifrado de datos, y han adoptado medidas como el uso de BitLocker para cifrar y políticas de seguridad. Sin embargo, la gestión de dispositivos IoT sigue siendo una preocupación debido a las limitaciones inherentes de estos dispositivos. La implementación de auditorías constantes y la evaluación de riesgos muestran un compromiso con la mejora continua, aunque aún existen oportunidades significativas para alinearse completamente con los estándares de ISO 27002.

El nivel de cumplimiento con los controles de seguridad establecidos en ISO 27002 varía, con la mayoría de las empresas considerándose en un nivel medio. Estas empresas han avanzado en la madurez de su cultura de ciberseguridad, realizando capacitaciones y auditorías regulares. No obstante, algunas empresas, especialmente en el sector comercio, se encuentran en un nivel bajo debido a la falta de políticas de seguridad bien definidas y una cultura de ciberseguridad débil entre sus usuarios. Los desafíos más significativos incluyen presupuestos limitados y la falta de recursos humanos calificados, lo que impacta directamente la capacidad de implementar herramientas avanzadas de ciberseguridad.

Parte IV: Análisis de las empresas del sector privado de El Salvador

En el sector privado de El Salvador, la implementación de políticas formales de ciberseguridad en entornos de teletrabajo aún es limitada. Un 66.66% de las empresas considera que pocas organizaciones han adoptado estas políticas, y la falta de un registro formal dificulta la cuantificación precisa. Las prácticas de ciberseguridad más efectivas, según las encuestas, incluyen el uso de VPN, cifrado de datos y MFA, además de capacitaciones continuas en ciberseguridad. Sin embargo, la colaboración entre empresas y el gobierno es crucial para mejorar la ciberseguridad, aunque actualmente es baja, con solo un 33.33% reportando un nivel medio de colaboración basada en relaciones informales.

Los incidentes de ciberseguridad reportados en el último año reflejan vulnerabilidades en las políticas de acceso y la falta de medidas adecuadas. Las empresas que han experimentado incidentes han tomado medidas correctivas como la actualización de políticas de control de acceso y la implementación de autenticación multifactorial. La colaboración entre empresas del sector privado es vista como insuficiente, con un nivel de colaboración informal y no oficial. Esta falta de colaboración subraya la necesidad de establecer redes más formales y estructuradas para compartir información y mejores prácticas en ciberseguridad, lo que podría fortalecer la capacidad de respuesta colectiva ante amenazas cibernéticas.

Parte V: Consideraciones adicionales

La preparación general de las empresas para enfrentar desafíos emergentes en ciberseguridad en entornos de teletrabajo es considerada baja por el 66.66% de las encuestadas. Las principales razones incluyen la falta de presupuesto adecuado para implementar controles de seguridad y la ausencia de personal calificado. Las empresas que se consideran mejor preparadas atribuyen su nivel de preparación a una cultura de ciberseguridad más desarrollada y la realización de auditorías constantes. Sin embargo, el apoyo gerencial y la colaboración de los usuarios siguen siendo factores críticos que afectan la eficacia de las medidas de ciberseguridad.

La colaboración entre el sector privado, el gobierno y otros actores relevantes es vista como crucial para mejorar la ciberseguridad, aunque actualmente es limitada. Las empresas necesitan recursos adicionales como inversión en tecnología y capacitación continua para mejorar sus prácticas de ciberseguridad. La importancia de la colaboración se subraya en la unanimidad de las respuestas, destacando la necesidad de un enfoque coordinado para enfrentar los desafíos de ciberseguridad. Las medidas adicionales recomendadas incluyen pruebas de Pentesting y la implementación de conexiones VPN con doble factor de autenticación, así como análisis de vulnerabilidades para identificar y mitigar riesgos potenciales.

En síntesis

Las empresas enfrentan diversos desafíos en la implementación de controles de ciberseguridad en entornos de teletrabajo. Los principales obstáculos incluyen una cultura organizacional deficiente en materia de ciberseguridad, presupuestos limitados y la utilización de dispositivos no seguros. Aunque algunas empresas han implementado medidas como el cifrado de datos y el uso de VPN, muchas carecen de autenticación multifactorial y políticas claras de gestión de accesos y

privilegios. La educación y concientización de los empleados es moderada, con solo un tercio de las empresas ofreciendo capacitaciones constantes. Estos desafíos resaltan la necesidad de fortalecer la cultura de ciberseguridad y mejorar las prácticas de gestión de riesgos.

La identificación y gestión de riesgos críticos, como la pérdida de información y los ataques de ingeniería social y ransomware, son fundamentales. Las empresas han adoptado medidas como campañas de concientización y la implementación de IDS, pero aún existen brechas significativas en la preparación y respuesta ante incidentes de ciberseguridad. La mayoría de las empresas se considera en un nivel medio de preparación, con simulacros y monitoreos regulares, aunque algunas, especialmente en el sector industrial, están en niveles bajos debido a la falta de madurez en sus prácticas de seguridad. La gestión de dispositivos y el cumplimiento de políticas de seguridad también presentan desafíos importantes debido a la falta de herramientas centralizadas y la colaboración interna.

En el contexto del sector privado de El Salvador, la adopción de políticas formales de ciberseguridad es limitada y la colaboración entre empresas es insuficiente. Las prácticas más efectivas incluyen el uso de VPN, cifrado de datos y MFA, pero la implementación es desigual. Las empresas que han experimentado incidentes han mejorado sus prácticas mediante la actualización de políticas y la implementación de medidas adicionales como la autenticación multifactorial. La colaboración entre el sector privado y el gobierno es crucial para mejorar la ciberseguridad, aunque actualmente es informal y no estructurada. Para enfrentar los desafíos emergentes, las empresas necesitan invertir en tecnología, capacitación continua y fomentar una cultura de ciberseguridad más robusta.

5.2 Implicaciones Prácticas

Sector Comercio

La empresa del sector comercio enfrenta desafíos particulares debido a su nivel relativamente bajo de cumplimiento con las normas de ciberseguridad y una cultura de ciberseguridad no bien establecida. Las implicaciones prácticas incluyen:

1. Mejora en la Cultura de Ciberseguridad: Es crucial implementar programas de capacitación continuos y efectivos para aumentar la concienciación entre los empleados sobre la importancia de las prácticas de ciberseguridad.
2. Políticas de Seguridad Formalizadas: Desarrollar y formalizar políticas de ciberseguridad claras y específicas, incluyendo políticas de acceso y control de usuarios, para asegurar la protección de la información.
3. Recursos y Presupuesto: Abogar por mayores presupuestos y recursos dedicados a la ciberseguridad, incluyendo la adquisición de herramientas tecnológicas avanzadas y la contratación de personal capacitado.
4. Implementación de Monitoreo Continuo: Establecer sistemas de monitoreo continuo de seguridad para detectar y responder rápidamente a posibles incidentes o vulnerabilidades en tiempo real.
5. Auditorías Regulares: Realizar auditorías periódicas de seguridad para evaluar la eficacia de las medidas implementadas y garantizar el cumplimiento con estándares de seguridad establecidos.

Sector Industria

La empresa del sector industrial muestra un nivel bajo de preparación frente a incidentes de ciberseguridad, estando en fases iniciales de implementación de buenas prácticas. Las implicaciones prácticas incluyen:

1. Implementación de Controles de Seguridad Críticos: Priorizar la implementación de controles de seguridad esenciales como el cifrado de datos, el uso de VPN con doble factor de autenticación y la implementación de IDS/IPS para la detección temprana de amenazas.
2. Gestión Proactiva de Vulnerabilidades: Adoptar un enfoque proactivo en la gestión de vulnerabilidades mediante pruebas de penetración regulares y análisis de riesgos para identificar y mitigar posibles puntos débiles en la infraestructura de IT.
3. Capacitación Especializada: Proporcionar formación especializada en ciberseguridad a los empleados para mejorar la conciencia sobre los riesgos y las mejores prácticas de seguridad.
4. Respaldo y Recuperación de Datos: Implementar políticas robustas de respaldo y recuperación de datos para asegurar la continuidad del negocio en caso de incidentes graves como ataques de ransomware o pérdida de datos.
5. Colaboración Sectorial: Fomentar la colaboración con otras empresas del sector industrial para compartir información sobre amenazas y mejores prácticas de ciberseguridad, fortaleciendo así la resiliencia colectiva ante ciberataques.

Sector Servicios

La empresa del sector servicios se encuentra en un nivel medio de preparación y cumplimiento con las normas de ciberseguridad, mostrando esfuerzos continuos en capacitación y auditorías. Las implicaciones prácticas incluyen:

1. Fortalecimiento de Capacitaciones Continuas: Mejorar y expandir los programas de capacitación en ciberseguridad para todos los niveles de empleados, enfatizando la responsabilidad individual en la protección de datos y sistemas.
2. Refuerzo en la Gestión de Accesos: Implementar políticas más estrictas y eficientes de gestión de accesos y privilegios, incluyendo la revisión regular de permisos y la aplicación de autenticación multifactor (MFA) en todos los sistemas críticos.
3. Adopción de Tecnologías Emergentes: Evaluar e implementar tecnologías emergentes como inteligencia artificial y análisis de comportamiento para mejorar la detección y respuesta ante amenazas cibernéticas.
4. Políticas de Seguridad Basadas en Riesgos: Desarrollar políticas de seguridad adaptadas a los riesgos específicos del sector servicios, considerando la sensibilidad de los datos y los requisitos de cumplimiento regulatorio.
5. Colaboración Interdepartamental: Fomentar la colaboración entre departamentos internos para fortalecer la cultura de ciberseguridad y garantizar la coherencia en la implementación de políticas y procedimientos de seguridad.

5.3 Limitaciones del Estudio

Para el desarrollo de la presente investigación se listan una serie de limitantes que se presentaron a lo largo del estudio.

1. **Disponibilidad de tiempo por parte de las empresas en estudio:** En este punto el inconveniente se daba al momento de realizar las respectivas entrevistas en las que se tenía que desplazar a la empresa, en varias ocasiones se reprogramaron las visitas por actividades propias de la empresa.
2. **Disponibilidad de tiempo por parte del equipo de investigación:** Para este punto los tres miembros del equipo de investigación en más de una ocasión presentaron inconvenientes en sus respectivos trabajos por lo que se hacía un poco difícil coordinar las visitas por todo el equipo.
3. **Tamaño de la Muestra**: La muestra de empresas encuestadas fue limitada, lo que puede no representar adecuadamente la diversidad de prácticas y desafíos de ciberseguridad en el sector privado de El Salvador.
4. **Falta de Datos Comparativos**: La ausencia de datos comparativos históricos o regionales puede limitar la capacidad de contextualizar los hallazgos dentro de tendencias más amplias o en comparación con otras regiones o períodos de tiempo.

6. Guia de Buenas Prácticas de Ciberseguridad

Como parte de los objetivos del trabajo y basado en la información recolectada durante la investigación, se ha desarrollado una guía de buenas prácticas en ciberseguridad para entornos de teletrabajo. Esta guía está diseñada para ser utilizada por cualquier empresa del sector privado en El Salvador, proporcionando un marco integral adaptado a las necesidades específicas del teletrabajo.

La guía de buenas prácticas de ciberseguridad está estructurada en varias secciones, cada una de las cuales proporciona información detallada y práctica sobre cómo implementar medidas de seguridad efectivas en entornos de teletrabajo. A continuación, se explica el propósito y el contenido de cada una de estas secciones.

1. Descripción

Propósito: La sección de Descripción proporciona una visión general de la práctica de ciberseguridad específica que se aborda. Se contextualiza dentro de los controles de la norma ISO 27002, lo que ayuda a comprender la relevancia de la práctica en el marco de estándares internacionales de seguridad.

Contenido: Referencia a los controles específicos de ISO 27002 aplicables a la práctica.
Resumen de lo que la práctica implica y por qué es necesaria.
Contexto sobre cómo esta práctica se relaciona con la seguridad de la información en entornos de teletrabajo.

2. Importancia

Propósito: La sección de Importancia destaca por qué es crucial implementar la práctica descrita. Aquí se explica el impacto positivo que tiene en la seguridad general de la organización y cómo contribuye a la protección de la información y los sistemas.

Contenido: Explicación de los riesgos que se mitigan al implementar la práctica.
Beneficios específicos de la práctica para la seguridad y la operación de la organización.
Ejemplos de posibles consecuencias negativas de no implementar la práctica.

3. ¿Cómo?

Propósito: La sección de Cómo proporcionar una guía detallada y práctica sobre cómo implementar la medida de seguridad. Incluye instrucciones específicas y pasos a seguir para asegurar que la práctica se adopte de manera efectiva.

Contenido: Procedimientos detallados para la implementación.
Pasos específicos y acciones necesarias.
Ejemplos y mejores prácticas para asegurar una correcta adopción.
Herramientas y recursos recomendados para facilitar la implementación.

4. Consideraciones adicionales

Propósito: Esta sección aborda aspectos adicionales que deben tenerse en cuenta al implementar la práctica de ciberseguridad. Incluye recomendaciones sobre cómo mejorar y mantener la práctica, así como consideraciones específicas para adaptarla a diferentes contextos y necesidades.

Contenido: Recomendaciones para el cumplimiento de leyes y regulaciones aplicables.
Consejos sobre la evaluación y mitigación de riesgos.
Sugerencias para la formación y concienciación de empleados.
Estrategias para el mantenimiento continuo y la revisión periódica de la práctica.
Consideraciones específicas para adaptarse a diferentes entornos empresariales y tecnológicos.

Esta estructura asegura que las empresas del sector privado en El Salvador puedan adoptar de manera efectiva las buenas prácticas de ciberseguridad, adaptándose a las necesidades específicas del teletrabajo y protegiendo su información corporativa de manera robusta y sostenible y la guía ofrece una cobertura exhaustiva de las mejores prácticas de ciberseguridad necesarias para proteger los entornos de teletrabajo. Cada sección está diseñada para abordar áreas específicas de riesgo y proporcionar soluciones prácticas y herramientas recomendadas para su implementación. La guía no solo establece un estándar de seguridad, sino que también ofrece una hoja de ruta clara para que las empresas puedan mejorar su postura de seguridad de manera continua y efectiva.

1. Política De Teletrabajo	
Descripción:	Para Política De Teletrabajo, hace referencia a los controles de ISO 27002: A.6.2.1: Política de dispositivos móviles A.6.2.2: Teletrabajo
Esquema 1. Introducción 1.1 Contexto y Justificación 1.2 Planteamiento del Problema 1.3 Objetivos de la Investigación Objetivo general Objetivos específicos 1.4 Preguntas de Investigación 1.5 Estructura del Documento 2. Marco Teórico 2.1 Revisión de la	Establecer una política clara de teletrabajo asegura que los empleados comprendan sus responsabilidades y expectativas relacionadas con la seguridad de la información mientras trabajan fuera de la oficina ISO/IEC. (2013). . Esto minimiza el riesgo de incidentes de seguridad y asegura que se sigan prácticas coherentes y seguras en entornos remotos.

Literatura 1. Aumento de acceso al internet en El Salvador 2. Ciberamenazas en El Salvador 3. Ciberseguridad en entornos de teletrabajo 4. Riesgos de ciberseguridad en entornos de teletrabajo 5. Buenas prácticas de ciberseguridad para el teletrabajo 6. Recursos para la ciberseguridad en El Salvador 2.2 Normativas y Estándares	

1. Ley De Regulación Del Teletrabajo 2. Ley de Protección de Datos Personales 3. Ley especial contra los delitos informáticos y conexos 4. Política de Ciberseguridad de El Salvador 5. Ley de Firma Electrónica 6. Norma Técnica Salvadoreña NTS 606:2019 3. Metodología 3.1 Enfoque de Investigación Fuentes de información primaria	

Fuentes secundarias de datos 3.2 Diseño de la Investigación 3.3 Población y Muestra 3.4 Instrumentos de Recolección de Datos 3.5 Procedimientos de Recolección y Análisis de Datos 4. Resultados Parte I. Identificación de desafíos en la implementación de controles de ciberseguridad en entornos de teletrabajo: Parte II. Identificación y gestión de riesgos	

de ciberseguridad de mayor impacto en entornos de teletrabajo: Parte III. Establecimiento de una guía de buenas prácticas de ciberseguridad enmarcadas en ISO 27002: Parte IV. Análisis de las empresas del sector privado de El Salvador: Parte V. Consideraciones adicionales: 5. Discusión 5.1 Análisis de Resultados	

5.2 Implicaciones Prácticas 5.3 Limitaciones del Estudio 6. Guia de Buenas Prácticas de Ciberseguridad 1. Política De Teletrabajo 2. Autenticación Fuerte 3. Uso De Vpn 4. Actualizaciones De Seguridad 5. Cifrado De Datos En Reposo 6. Cifrado De Datos En Tránsito 7. Gestión De Dispositivos 8. Formación En	

Ciberseguridad 9. Seguridad Física 10. Seguridad De Wi-Fi 11. Seguridad De Correo Electrónico 12. Seguridad De Dispositivos Móviles 13. Seguridad De Conexiones Remotas 14. Seguridad De Datos En La Nube 15. Seguridad Física De Dispositivos Remotos 16. Seguridad En Videoconferencias 17. Seguridad En El Acceso Aplicaciones Web 18. Seguridad De Redes Personales	

Activar la compatibilidad con lectores de pantalla

Para habilitar la compatibilidad con lectores de pantalla,

pulsa Ctrl+Alt+Z.

Para obtener información acerca de las combinaciones de teclas, pulsa Ctrl+barra diagonal.

Buscar y reemplazar

l

u

s

c

a

r

l

a

i

n

f

o

r

n a c i ó n n i e n t r a s t r a b a j a n f u e	

r a d e l a o f i c i n a Importancia:	

¿Cómo?:	Cómo realizar: Desarrollar una política escrita que defina claramente las expectativas y responsabilidades de los empleados en teletrabajo, incluyendo procedimientos de seguridad, uso de dispositivos, acceso a datos, y manejo de información sensible. Comunicar y distribuir la política a todos los empleados, asegurando que la comprendan y la acepten. Revisar y actualizar la política periódicamente. Herramientas: Microsoft Word: Para crear y mantener documentos de políticas. Confluence: Para gestionar y compartir la política de teletrabajo con toda la organización.

Consideraciones adicionales:	Cumplimiento Legal y Normativo: Asegurarse de que la política de teletrabajo cumpla con las leyes y regulaciones locales y sectoriales. Evaluación de Riesgos: Realizar evaluaciones periódicas de riesgos para identificar y mitigar posibles vulnerabilidades relacionadas con el teletrabajo. Soporte Técnico: Establecer un sistema de soporte técnico eficiente para asistir a los empleados remotos con problemas de conectividad y seguridad.

Tabla 22, Política de trabajo

2. Autenticación Fuerte	
Descripción:	Para Autenticación Fuerte, hace referencia a los controles de ISO 27002: A.9.4.2: Procedimientos de inicio de sesión seguro A.9.4.3: Sistema de gestión de contraseñas
Importancia:	La autenticación multifactorial añade una capa adicional de seguridad, dificultando el acceso no autorizado a los sistemas corporativos ISO/IEC. (2013). . Esto es especialmente crucial para proteger información sensible y recursos corporativos accesibles desde ubicaciones remotas.

¿Cómo?:	Cómo realizar: Implementar la autenticación multifactor (MFA) para todos los accesos remotos a los recursos corporativos. Configurar políticas que requieran el uso de MFA para aplicaciones críticas y acceso a datos sensibles Herramientas: Duo Security: Proporciona MFA para proteger el acceso a las aplicaciones Duo Security. (n.d.). Google Authenticator: Ofrece autenticación de dos factores (2FA) mediante generación de códigos temporales Google. (n.d.)..

Consideraciones adicionales:	Facilidad de Uso: Asegurarse de que el método de MFA sea fácil de usar para los empleados, minimizando las fricciones y problemas de acceso. Compatibilidad: Verificar la compatibilidad de la MFA con todas las aplicaciones y sistemas utilizados por la organización. Redundancia: Tener mecanismos de respaldo en caso de falla de uno de los factores de autenticación, como códigos de recuperación.

Tabla 24, Autenticación fuerte

3. Uso De Vpn	
Descripción:	Para Uso De Vpn, hace referencia a los controles de ISO 27002: A.13.1.1: Controles de red A.13.1.3: Segregación en redes
Importancia:	Las VPNs aseguran que las conexiones remotas a la red corporativa sean seguras y encriptadas, protegiendo los datos en tránsito de posibles interceptaciones y accesos no autorizados ISO/IEC. (2013). . Esto es esencial para mantener la integridad y confidencialidad de la información transmitida desde ubicaciones remotas.

¿Cómo?:	Cómo realizar: Configurar una red privada virtual (VPN) para que los empleados se conecten de forma segura a la red corporativa desde ubicaciones remotas. Establecer políticas que requieran el uso de VPN para cualquier acceso remoto. Herramientas: OpenVPN: Una solución de VPN de código abierto que permite conexiones seguras OpenVPN. (n.d.).. Cisco AnyConnect: Una solución de VPN que ofrece conectividad segura y confiable Cisco Systems, Inc. (n.d.). .

Consideraciones adicionales:	Capacidad y Rendimiento: Asegurar que la infraestructura de la VPN pueda manejar el volumen de tráfico esperado sin afectar el rendimiento. Registros y Auditoría: Implementar sistemas de registro y auditoría para monitorear el uso de la VPN y detectar posibles intentos de intrusión. Actualización y Mantenimiento: Mantener la VPN actualizada con los últimos parches y mejoras de seguridad.

Tabla 25, Uso de VPN

4. Actualizaciones De Seguridad	
Descripción:	Para Actualizaciones De Seguridad, hace referencia a los controles de ISO 27002: A.12.6.1: Gestión de vulnerabilidades técnicas

Importancia:	Mantener los dispositivos remotos actualizados con los últimos parches de seguridad y software es crucial para proteger contra vulnerabilidades conocidas que pueden ser explotadas por atacantes Kanade, S. S. (2018).. Esto ayuda a prevenir incidentes de seguridad y asegurar la protección continua de los datos corporativos.

¿Cómo?:	Cómo realizar: Implementar un sistema de gestión de parches que supervise y aplique actualizaciones de seguridad a todos los dispositivos remotos. Establecer políticas de actualización automática para garantizar que los dispositivos estén siempre al día. Herramientas: Microsoft Endpoint Configuration Manager: Para gestionar y desplegar actualizaciones de software Microsoft. (n.d.). . Patch My PC: Para automatizar la aplicación de parches de seguridad Patch My PC. (n.d.)..

Consideraciones adicionales:	Pruebas Previas: Realizar pruebas de parches y actualizaciones en un entorno de prueba antes de implementarlas en producción para evitar problemas de compatibilidad. Comunicación: Informar a los empleados sobre las actualizaciones y posibles interrupciones de servicio. Automatización: Automatizar el proceso de actualización para minimizar errores humanos y asegurar la consistencia.

Tabla 26, Actualizaciones de Seguridad

5. Cifrado De Datos En Reposo	
Descripción:	Para Cifrado De Datos En Reposo, hace referencia a los controles de ISO 27002: A.10.1.1: Política sobre el uso de controles criptográficos A.10.1.2: Gestión de claves
Importancia:	El cifrado de disco completo protege la información almacenada en dispositivos remotos, asegurando que los datos sensibles no sean accesibles en caso de pérdida o robo del dispositivo ISO/IEC. (2013). . Esto es esencial para mantener la confidencialidad de la información.

¿Cómo?:	Cómo realizar: Implementar cifrado de disco completo en todos los dispositivos remotos para proteger la información almacenada. Establecer políticas que requieran el uso de cifrado en dispositivos que manejen datos sensibles. Herramientas: BitLocker: Una herramienta de cifrado de disco completa integrada en Windows Microsoft. (n.d.). . VeraCrypt: Una solución de cifrado de disco completa y de código abierto VeraCrypt. (n.d.)..

Consideraciones adicionales:	Gestión de Claves: Implementar una gestión robusta de claves para asegurar que las claves de cifrado estén protegidas y sean accesibles solo a personal autorizado. Desempeño del Sistema: Evaluar el impacto del cifrado en el desempeño del sistema y ajustar las configuraciones según sea necesario. Recuperación de Datos: Establecer procedimientos claros para la recuperación de datos en caso de fallos en el cifrado o pérdida de claves.

Tabla 27, Cifrado de Datos en Reposo

6. Cifrado De Datos En Tránsito	
Descripción:	Para Cifrado De Datos En Tránsito, hace referencia a los controles de ISO 27002: A.13.2.3: Mensajería electrónica A.13.1.1: Controles de red

Importancia:	Cifrar todas las comunicaciones entre dispositivos remotos y la red corporativa asegura que los datos transmitidos estén protegidos contra interceptaciones y accesos no autorizados ISO/IEC. (2013). . Esto es especialmente importante cuando se utilizan redes públicas o no seguras.
¿Cómo?:	Cómo realizar: Implementar protocolos de cifrado para todas las comunicaciones entre dispositivos remotos y la red corporativa, como SSL/TLS. Configurar políticas para que todas las conexiones remotas utilicen comunicaciones cifradas. Herramientas: OpenSSL: Para implementar cifrado SSL/TLS en comunicaciones OpenSSL. (n.d.).. WireGuard: Una solución de VPN moderna y rápida con cifrado fuerte WireGuard. (n.d.). .

Consideraciones adicionales:	Protocolo Adecuado: Asegurarse de utilizar el protocolo de cifrado adecuado según la sensibilidad de los datos y la naturaleza de la comunicación. Certificados SSL/TLS: Gestionar adecuadamente los certificados SSL/TLS, incluyendo su renovación y revocación cuando sea necesario. Compatibilidad: Verificar la compatibilidad del cifrado con todos los dispositivos y aplicaciones utilizados por la organización.

Tabla 28, Cifrado de Datos en Tránsito

7. Gestión De Dispositivos	
Descripción:	Para Gestión de dispositivos, hace referencia a los controles de ISO 27002: A.6.2.1: Política de dispositivos móviles A.9.2.1: Registro y eliminación de usuarios

Importancia:	Las políticas de gestión de dispositivos móviles (MDM) permiten a las organizaciones administrar y asegurar dispositivos remotos, incluyendo la capacidad de borrar datos de forma remota en caso de pérdida o robo ISO/IEC. (2013). . Esto ayuda a proteger la información sensible y asegura el cumplimiento de las políticas de seguridad de la organización.

¿Cómo?:	Cómo realizar: Implementar una solución de gestión de dispositivos móviles (MDM) para administrar y asegurar dispositivos remotos. Establecer políticas de seguridad y capacidad de borrar datos de forma remota en caso de pérdida o robo. Herramientas: Microsoft Intune: Para gestionar y asegurar dispositivos móviles y aplicaciones Microsoft. (n.d.).. AirWatch (VMware Workspace ONE): Una solución de gestión de dispositivos móviles completa.

Consideraciones adicionales:	Políticas de Uso Aceptable: Definir y comunicar claramente las políticas de uso aceptable para dispositivos móviles. Seguridad de Aplicaciones: Monitorear y controlar las aplicaciones instaladas en los dispositivos para evitar software malicioso. Soporte Multi-Plataforma: Asegurar que la solución MDM soporte todos los tipos de dispositivos utilizados en la organización (iOS, Android, Windows, etc.).

Tabla 29, Gestión de Dispositivos

8. Formación En Ciberseguridad	
Descripción:	Para Formación En Ciberseguridad, hace referencia a los controles de ISO 27002: A.7.2.2: Concienciación, educación y formación en seguridad de la información
Importancia:	Proporcionar formación regular en seguridad de la información a los empleados que trabajan de forma remota asegura que estén conscientes de las amenazas y sepan cómo responder adecuadamente ISO/IEC. (2013). . Esto reduce el riesgo de incidentes de seguridad causados por errores humanos o falta de conocimiento.

¿Cómo?:	Cómo realizar: Desarrollar y proporcionar programas de formación continua en seguridad de la información a todos los empleados, especialmente aquellos que trabajan de forma remota. Utilizar plataformas de e-learning para facilitar el acceso a la formación. Herramientas: KnowBe4: Una plataforma de formación y concienciación en seguridad KnowBe4. (n.d.).. Coursera: Para cursos de formación en ciberseguridad y buenas prácticas.

Consideraciones adicionales:	Frecuencia de Formación: Programar formaciones regulares y actualizaciones frecuentes para mantener a los empleados al día con las últimas amenazas y técnicas de seguridad. Evaluación de Conocimientos: Realizar evaluaciones periódicas para medir la efectividad de la formación y identificar áreas que requieran refuerzo. Personalización: Adaptar los programas de formación según los roles y responsabilidades de los empleados.

Tabla 30, Formación en Ciberseguridad

9. Seguridad Física	
Descripción:	Para Seguridad Física, hace referencia a los controles de ISO 27002: A.11.2.6: Seguridad de los equipos y activos fuera de las instalaciones
Importancia:	Asegurar que los dispositivos remotos estén físicamente seguros en entornos domésticos ayuda a prevenir el acceso no autorizado y el robo de equipos que contienen información sensible ISO/IEC. (2013). . Esto es crucial para mantener la seguridad y la integridad de la información corporativa.

¿Cómo?:	Cómo realizar: Establecer directrices para asegurar físicamente los dispositivos remotos, como el uso de candados de seguridad y almacenamiento seguro cuando no estén en uso. Concienciar a los empleados sobre la importancia de la seguridad física en entornos domésticos. Herramientas: Kensington Security Slot: Candados de seguridad para portátiles y otros dispositivos Kensington. (n.d.).. Targus DEFCON CL: Cables de seguridad con cerradura para portátiles Targus. (n.d.). .

Consideraciones adicionales:	Entornos Compartidos: Considerar la seguridad de dispositivos en entornos compartidos o públicos, como cafeterías o espacios de co-working. Políticas de Viaje: Establecer políticas específicas para la seguridad de dispositivos durante viajes de negocios. Dispositivos de Respaldo: Utilizar dispositivos de respaldo para minimizar el impacto de la pérdida o daño de un dispositivo.

Tabla 31, Seguridad Física

10. Seguridad De Wi-Fi	
Descripción:	Para. Seguridad De Wi-Fi, hace referencia a los controles de ISO 27002: A.13.1.1: Controles de red
Importancia:	Configurar las redes Wi-Fi domésticas con cifrado WPA2 o WPA3 y contraseñas seguras protege las comunicaciones inalámbricas de ser interceptadas por terceros no autorizados ISO/IEC. (2013). .. Esto es fundamental para asegurar que las conexiones a la red corporativa sean seguras y los datos transmitidos estén protegidos.

¿Cómo?:	Cómo realizar: Configurar las redes Wi-Fi domésticas con cifrado WPA2 o WPA3 y establecer contraseñas seguras. Proporcionar guías y formación a los empleados sobre cómo configurar y asegurar sus redes Wi-Fi domésticas. Herramientas: Router con soporte WPA3: Como los de marcas Netgear o Asus Netgear. (n.d.).. Wi-Fi Analyzer: Herramientas como NetSpot o Acrylic Wi-Fi para analizar y optimizar la seguridad de la red Wi-Fi NetSpot. (n.d.). .

Consideraciones adicionales:	Configuración Inicial: Proporcionar asistencia o guías detalladas para la configuración inicial de las redes Wi-Fi seguras. Monitoreo y Mantenimiento: Realizar auditorías periódicas de seguridad en las redes Wi-Fi para detectar y solucionar vulnerabilidades. Separación de Redes: Configurar redes separadas para el trabajo y el uso personal para minimizar riesgos de seguridad.

Tabla 32, Seguridad WIFI

11. Seguridad De Correo Electrónico	
Descripción:	Para seguridad de Correo Electrónico, hace referencia a los controles de ISO 27002: A.12.2.1: Protección contra malware.
Importancia:	Proteger el correo electrónico contra amenazas como phishing, malware y spam es crucial para mantener la seguridad de la información y la integridad de los sistemas corporativos ISO/IEC. (2013). . El correo electrónico es un vector común de ataque y asegurar su uso es vital para prevenir compromisos de seguridad y pérdidas de datos.

¿Cómo?:	Como realizar: ● Implementar filtros avanzados de spam y malware en los servidores de correo electrónico. ● Utilizar técnicas de autenticación de correo como SPF, DKIM y DMARC para verificar la legitimidad de los correos entrantes. ● Realizar campañas de concienciación y formación sobre phishing para educar a los empleados. Herramientas: ● Soluciones de Seguridad de Correo Electrónico: Herramientas como Proofpoint, Mimecast Mimecast. (n.d.). o Microsoft Defender for Office 365 para proteger el correo electrónico. ● Servicios de Autenticación: Implementar SPF, DKIM y DMARC a través de servicios como DMARC Analyzer DMARC Analyzer. (n.d.). o Valimail. ● Plataformas de Formación: Utilizar plataformas como KnowBe4 KnowBe4. (n.d.). o Cofense para entrenar a los empleados sobre el reconocimiento de correos electrónicos fraudulentos.

Consideraciones adicionales:	Monitoreo Continuo: Realizar monitoreos y análisis continuos de los patrones de correo electrónico para detectar y mitigar nuevas amenazas. Evaluaciones de Seguridad: Realizar evaluaciones periódicas de la seguridad del correo electrónico y actualizar las políticas y herramientas según sea necesario. Seguridad de Contraseñas: Implementar políticas de gestión de contraseñas fuertes y autentificación multifactor para las cuentas de correo. Respaldo de Correos: Asegurar que se realicen copias de seguridad regulares de los correos electrónicos críticos.

Tabla 33, Seguridad de Correo Electrónico

12. Seguridad De Dispositivos Móviles	
Descripción:	Para seguridad de Dispositivos Móviles, hace referencia a los controles de ISO 27002: A.6.2.1: Política para el uso de dispositivos móviles.

Importancia:	Asegurar los dispositivos móviles utilizados para el trabajo es crucial para proteger los datos corporativos accesibles a través de estos dispositivos ISO/IEC. (2013). . La movilidad y el acceso remoto presentan riesgos específicos que deben ser mitigados para mantener la integridad y confidencialidad de la información.

¿Cómo?:	Cómo realizar: ● Implementar políticas de seguridad específicas para dispositivos móviles, incluyendo la obligatoriedad de cifrado de datos y el uso de contraseñas fuertes. ● Utilizar soluciones de gestión de dispositivos móviles (MDM) para monitorear y gestionar la seguridad de los dispositivos. ● Configurar mecanismos de bloqueo remoto y borrado de datos en caso de pérdida o robo del dispositivo. Herramientas: ● Soluciones MDM: Herramientas como MobileIron MobileIron. (n.d.)., AirWatch o Microsoft Intune para gestionar y asegurar dispositivos móviles. ● Cifrado de Dispositivos: Utilizar soluciones de cifrado integradas en el sistema operativo como BitLocker para Windows o FileVault para macOS. ● Aplicaciones de Seguridad: Implementar aplicaciones de seguridad como Norton Mobile Security o Lookout Mobile Security.

Consideraciones adicionales:	Actualizaciones Regulares: Asegurar que todos los dispositivos móviles reciban actualizaciones regulares de software y parches de seguridad. Seguridad de Aplicaciones: Revisar y aprobar las aplicaciones que se pueden instalar en dispositivos móviles para evitar software malicioso. Formación: Proporcionar capacitación a los empleados sobre las mejores prácticas de seguridad para el uso de dispositivos móviles. Segmentación de Red: Implementar segmentación de red para limitar el acceso de dispositivos móviles a recursos sensibles de la red corporativa.

Tabla 34,Seguridad de Dispositivos Móviles

13. Seguridad De Conexiones Remotas	
Descripción:	Para seguridad de Conexiones Remotas, hace referencia a los controles de ISO 27002: A.13.2.3: Conexión de red externa.

Importancia:	Asegurar las conexiones remotas es vital para proteger la integridad y confidencialidad de la información transmitida entre los dispositivos remotos y la red corporativa ISO/IEC. (2013). . Las conexiones no seguras pueden ser interceptadas, poniendo en riesgo datos sensibles.

¿Cómo?:	Cómo realizar: ● Implementar redes privadas virtuales (VPN) para todas las conexiones remotas a la red corporativa. ● Configurar el uso de túneles cifrados y protocolos seguros como SSL/TLS para la transmisión de datos. ● Monitorear y gestionar activamente las conexiones remotas para detectar y responder a actividades sospechosas. Herramientas: ● Soluciones VPN: Herramientas como Cisco AnyConnect Cisco Systems, Inc. (n.d.)., NordVPN Teams o OpenVPN para establecer conexiones seguras. ● Firewalls de Próxima Generación: Utilizar firewalls como Palo Alto Networks, Fortinet o Check Point para monitorear y asegurar el tráfico de red. ● Sistemas de Detección y Prevención de Intrusiones (IDS/IPS): Herramientas como Snort, Suricata o Cisco Firepower para identificar y mitigar amenazas en tiempo real.

Consideraciones adicionales:	Autenticación Fuerte: Implementar autenticación multifactor (MFA) para todas las conexiones remotas. Políticas de Uso Aceptable: Definir y comunicar políticas claras sobre el uso aceptable de las conexiones remotas. Segmentación de Red: Asegurar que las conexiones remotas están segmentadas para limitar el acceso a recursos críticos. Monitoreo Continuo: Realizar monitoreo continuo de las conexiones remotas para identificar y responder rápidamente a cualquier anomalía.

Tabla 35, Seguridad de Conexiones Remotas

14. Seguridad De Datos En La Nube	
Descripción:	Para seguridad de Datos en la Nube, hace referencia a los controles de ISO 27002: A.14.2.1: Seguridad en el desarrollo y soporte de sistemas.
Importancia:	Asegurar los datos almacenados y procesados en la nube es fundamental para proteger la información sensible y cumplir con las regulaciones de privacidad ISO/IEC. (2013). . La migración a servicios en la nube introduce nuevos riesgos que deben ser gestionados adecuadamente para mantener la seguridad.

¿Cómo?:	Cómo realizar: ● Implementar políticas de seguridad específicas para el uso de servicios en la nube, incluyendo la clasificación y cifrado de datos. ● Utilizar soluciones de gestión de identidad y acceso (IAM) para controlar y monitorizar el acceso a los recursos en la nube. ● Configurar mecanismos de monitoreo y alertas para detectar y responder a actividades sospechosas en la nube. Herramientas: ● Soluciones IAM: Herramientas como AWS IAM Amazon Web Services. (n.d.). , Azure Active Directory o Google Cloud IAM para gestionar accesos en la nube. ● Plataformas de Seguridad en la Nube: Soluciones como Prisma Cloud, AWS Security Hub o Microsoft Defender for Cloud para asegurar el entorno en la nube. ● Herramientas de Cifrado: Utilizar servicios de cifrado como AWS KMS, Azure Key Vault o Google Cloud KMS para proteger los datos.

Consideraciones adicionales:	Evaluación de Proveedores: Realizar evaluaciones de seguridad y cumplimiento de los proveedores de servicios en la nube. Backup de Datos: Asegurar que se realicen copias de seguridad regulares de los datos almacenados en la nube. Formación de Empleados: Capacitar a los empleados sobre las mejores prácticas y riesgos asociados al uso de servicios en la nube. Revisión de Contratos: Revisar y asegurar que los contratos con proveedores de servicios en la nube incluyan cláusulas de seguridad y cumplimiento.

Tabla 36, Seguridad de Datos en la Nube.

15. Seguridad Física De Dispositivos Remotos	
Descripción:	Para seguridad Física de Dispositivos Remotos, hace referencia a los controles de ISO 27002: A.11.1.1: Controles de seguridad física.

Importancia:	Asegurar físicamente los dispositivos remotos es crucial para prevenir el acceso no autorizado y el robo de datos ISO/IEC. (2013). . La protección física de los dispositivos asegura que la información corporativa no caiga en manos equivocadas y mantiene la integridad de los sistemas.
¿Cómo?:	Cómo realizar: ● Establecer políticas claras sobre la seguridad física de los dispositivos utilizados para el teletrabajo. ● Proveer a los empleados de equipos de seguridad como candados de seguridad para laptops y mochilas anti-robo. ● Fomentar el almacenamiento seguro de dispositivos cuando no estén en uso, evitando dejarlos desatendidos en lugares públicos. Herramientas: ● Candados de Seguridad: Dispositivos como los candados Kensington para asegurar laptops Kensington. (n.d.).. ● Software de Rastreo y Recuperación: Herramientas como Prey, Absolute LoJack o Find My Device para rastrear y recuperar dispositivos perdidos o robados. ● Mochilas de Seguridad: Mochilas con características

	anti-robo de marcas como Pacsafe o XD Design.

Consideraciones adicionales:	Seguros: Considerar la contratación de seguros que cubran la pérdida o robo de dispositivos. Protocolos de Respuesta: Establecer protocolos claros para la respuesta rápida en caso de pérdida o robo de un dispositivo. Revisión y Actualización: Revisar y actualizar regularmente las políticas y prácticas de seguridad física para asegurar que se adapten a las nuevas amenazas. Auditorías de Seguridad: Realizar auditorías periódicas para asegurar que los empleados cumplen con las políticas de seguridad física.

Tabla 37, Seguridad Física de dispositivos Remotos

16. Seguridad En Videoconferencias	
Descripción:	Para seguridad en Videoconferencias, hace referencia a los controles de ISO 27002: A.13.2.3: Aseguramiento de los servicios de red.

Importancia:	Garantizar la seguridad en videoconferencias es esencial para proteger la confidencialidad y la integridad de la información compartida durante las reuniones virtuales ISO/IEC. (2013). . Las videoconferencias son susceptibles a diversas amenazas, como la intercepción no autorizada y la interrupción maliciosa (zoombombing).
¿Cómo?:	Cómo realizar: ● Utilizar plataformas de videoconferencia que ofrezcan cifrado de extremo a extremo. ● Configurar reuniones privadas con contraseñas y controles de acceso. ● Capacitar a los empleados sobre las mejores prácticas para la seguridad en videoconferencias. Herramientas: ● Plataformas de Videoconferencia Seguras: Zoom con configuración segura, Microsoft Teams, Cisco Webex Zoom. (n.d.).. ● Cifrado de Videoconferencias: Utilizar opciones de cifrado proporcionadas por las plataformas de videoconferencia. ● Gestión de Acceso: Configurar listas de participantes y usar salas de espera para controlar el acceso a las

	reuniones.

Consideraciones adicionales:	Revisión de Configuraciones: Revisar y actualizar regularmente las configuraciones de seguridad de las plataformas de videoconferencia. Protocolos de Respuesta: Establecer protocolos claros para manejar incidentes de seguridad durante las videoconferencias. Actualización de Software: Asegurar que el software de videoconferencia esté siempre actualizado con los últimos parches de seguridad. Políticas de Grabación: Definir políticas claras sobre la grabación de videoconferencias y el almacenamiento seguro de esas grabaciones.

Tabla 38. Seguridad en Videoconferencias.

17. Seguridad En El Acceso Aplicaciones Web	
Descripción:	Para seguridad en el Acceso a Aplicaciones Web, hace referencia a los controles de ISO 27002: A.9.4.1: Uso de servicios gestionados de autenticación.

Importancia:	Asegurar el acceso a las aplicaciones web utilizadas por empleados remotos es crucial para proteger los datos corporativos y prevenir accesos no autorizados. Las aplicaciones web son un objetivo común para los ataques de ciberdelincuentes.
¿Cómo?:	Cómo realizar: ● Implementar autenticación multifactor (MFA) para el acceso a todas las aplicaciones web. ● Configurar políticas de acceso basadas en roles y necesidades específicas. ● Monitorear y registrar todos los intentos de acceso a las aplicaciones web. Herramientas: ● Soluciones MFA: Authy, Google Authenticator, Microsoft Authenticator Google. (n.d.).. ● Gestión de Accesos: Okta, OneLogin, Microsoft Azure AD. ● Registro y Monitoreo: Splunk, LogRhythm, ELK Stack.

Consideraciones adicionales:	Educación del Usuario: Capacitar a los empleados sobre la importancia de usar MFA y las mejores prácticas para mantener la seguridad. Política de Contraseñas: Asegurar que las políticas de contraseñas sean robustas y aplicadas a todas las aplicaciones web. Revisión de Permisos: Realizar revisiones periódicas de permisos y accesos para asegurarse de que los empleados solo tengan acceso a lo necesario. Evaluaciones de Seguridad: Realizar evaluaciones de seguridad y pruebas de penetración periódicas en las aplicaciones web.

Tabla 39, Seguridad en el Acceso a Aplicaciones Web

18. Seguridad De Redes Personales	
Descripción:	Para seguridad de Redes Personales, hace referencia a los controles de ISO 27002: A.13.1.1: Controles de red.
Importancia:	Asegurar las redes personales de los empleados es esencial para proteger la información corporativa transmitida a través de ellas. Las redes domésticas pueden ser vulnerables a ataques si no están adecuadamente protegidas ISO/IEC. (2013). .

¿Cómo?:	Cómo realizar: ● Configurar redes Wi-Fi con cifrado WPA3 y contraseñas seguras. ● Asegurar que los routers domésticos tengan el firmware actualizado. ● Desactivar el acceso remoto al router y cambiar las credenciales predeterminadas. Herramientas: ● Routers Seguros: Netgear Nighthawk, Asus RT-AX88U con soporte WPA3 Netgear. (n.d.).. ● Herramientas de Análisis de Red: Fing, Wi-Fi Analyzer. ● Software de Seguridad de Red: Bitdefender Home Scanner, Norton Core Security.

Consideraciones adicionales:	Seguridad Física: Asegurar que el router esté en un lugar seguro y no accesible para personas no autorizadas. Red de Invitados: Configurar una red de invitados separada para dispositivos no corporativos. Monitoreo de Red: Monitorear el tráfico de la red doméstica para detectar actividades sospechosas. Formación: Proveer guías y capacitación a los empleados sobre cómo asegurar sus redes personales.

Tabla 40, Seguridad en Redes Personales

19. Seguridad De Datos En Dispositivos Externos	
Descripción:	Para seguridad de Datos en Dispositivos Externos, hace referencia a los controles de ISO 27002: A.8.3.3: Manejo de soportes físicos.
Importancia:	Proteger los datos almacenados en dispositivos externos, como discos duros y memorias USB ISO/IEC. (2013). , es crucial para prevenir el acceso no autorizado y la pérdida de información sensible.

¿Cómo?:	Cómo realizar: ● Implementar políticas de cifrado obligatorio para todos los datos almacenados en dispositivos externos. ● Controlar el uso de dispositivos externos mediante políticas de acceso y monitoreo. ● Proveer dispositivos externos aprobados y seguros para su uso en la organización. Herramientas: ● Software de Cifrado: VeraCrypt, BitLocker, FileVault Sirur, M. (2015). . ● Dispositivos USB Seguros: Kingston DataTraveler Vault Privacy, IronKey. ● Soluciones DLP (Prevención de Pérdida de Datos): Symantec DLP, McAfee Total Protection for DLP.

Consideraciones adicionales:	Inventario de Dispositivos: Mantener un inventario de todos los dispositivos externos utilizados en la organización. Política de Uso: Definir y comunicar claramente la política de uso de dispositivos externos a todos los empleados. Capacitación: Formar a los empleados sobre los riesgos asociados al uso de dispositivos externos y las mejores prácticas para mitigarlos. Auditorías: Realizar auditorías periódicas del uso de dispositivos externos y el cumplimiento de las políticas de seguridad.

Tabla 41, Seguridad de Datos en Dispositivos Externos

20. Gestión De Parcheo Y Actualizaciones	
Descripción:	Para gestión de Parcheo y Actualizaciones, hace referencia a los controles de ISO 27002: A.12.6.1: Gestión de vulnerabilidades técnicas.
Importancia:	Mantener todos los sistemas y aplicaciones actualizados con los últimos parches de seguridad es esencial para proteger contra vulnerabilidades conocidas y prevenir ciberataques ISO/IEC.

	(2013). .
¿Cómo?:	Cómo realizar: ● Implementar un sistema centralizado para la gestión y distribución de parches y actualizaciones. ● Configurar actualizaciones automáticas siempre que sea posible para minimizar el riesgo de sistemas desactualizados. ● Realizar pruebas de compatibilidad y seguridad antes de desplegar parches críticos en el entorno de producción. Herramientas: ● Soluciones de Gestión de Parches: Microsoft WSUS, Ivanti Patch Management, SolarWinds Patch Manager Kanade, S. S. (2018).. ● Sistemas de Actualización Automática: Utilizar las configuraciones de actualización automática en sistemas operativos como Windows Update o macOS Software Update. ● Herramientas de Monitoreo: Nagios, Zabbix para monitorear el estado de los parches y actualizaciones en todos los sistemas.

Consideraciones adicionales:	Prioridad de Parches: Establecer un sistema de priorización para la instalación de parches críticos. Documentación: Mantener registros detallados de todas las actualizaciones y parches aplicados. Comunicación: Informar a los empleados sobre la importancia de mantener sus sistemas actualizados y cómo proceder en caso de problemas con actualizaciones. Evaluaciones de Seguridad: Realizar evaluaciones de seguridad periódicas para identificar sistemas que puedan estar desactualizados o vulnerables.

Tabla 42, seguridad de Parcheo y Actualizaciones

7. Conclusiones y Recomendaciones

7.1 Conclusiones

- Los entornos de teletrabajo son más vulnerables a los ciberataques que los entornos de oficina tradicionales. Esto se debe a que los empleados remotos a menudo utilizan sus propios dispositivos y redes, que pueden no estar tan bien protegidos como los dispositivos y redes de la empresa.
- Es importante evaluar los riesgos de seguridad asociados con el teletrabajo e implementar controles de seguridad adecuados para mitigar esos riesgos. Los controles de seguridad pueden incluir el uso de una VPN, el cifrado de datos y la autenticación multifactor.
- Es importante concienciar a los empleados remotos sobre los riesgos de la ciberseguridad y sobre cómo protegerse de esos riesgos. La formación sobre seguridad debe cubrir temas como la ingeniería social, el phishing y el malware.
- Es importante tener un plan de gestión de incidentes en vigor para responder a los ciberataques. El plan de gestión de incidentes debe incluir pasos para identificar, contener y erradicar los ciberataques.

- El teletrabajo ha aumentado significativamente en El Salvador debido a la pandemia de COVID-19, trayendo consigo beneficios de flexibilidad y eficiencia. Sin embargo, esta modalidad también ha expuesto a las empresas a una serie de amenazas cibernéticas que comprometen la integridad, confidencialidad y disponibilidad de la información crítica.

- A pesar del crecimiento en el uso de tecnologías de la información, la infraestructura digital y la conciencia sobre ciberseguridad en El Salvador aún están en desarrollo. Muchas empresas carecen de una comprensión adecuada de los riesgos cibernéticos y de las medidas necesarias para mitigarlos.

- Las empresas enfrentan desafíos significativos en la protección de una infraestructura digital extendida y diversa. La multiplicidad de dispositivos y la dependencia de plataformas en la nube aumentan la complejidad de la gestión de la seguridad. Los ataques de phishing, ransomware y las vulnerabilidades en la red son amenazas constantes.
- La implementación de estrategias efectivas de ciberseguridad es crucial para proteger la integridad, confidencialidad y disponibilidad de los datos empresariales. Las empresas necesitan un enfoque integral que incluya políticas claras, gestión de riesgos, formación de empleados y el uso de tecnologías avanzadas.
- Basado en el análisis de tres empresas representativas del sector privado en El Salvador, se desarrolló una guía de buenas prácticas de ciberseguridad enmarcadas en la norma ISO 27002. Esta guía proporciona un marco detallado y práctico para ayudar a las empresas a mejorar su seguridad en entornos de teletrabajo.

7.2 Recomendaciones

- Desarrollar e implementar una política de seguridad integral que cubra todos los aspectos de la ciberseguridad en el teletrabajo.
- Proporcionar formación y concienciación continuas a los empleados sobre los

riesgos de ciberseguridad y las mejores prácticas para protegerse.

- Implementar soluciones de seguridad adecuadas para proteger los dispositivos y las redes, como firewalls, software antivirus y sistemas de detección de intrusos.
- Establecer un plan de respuesta a incidentes para hacer frente a las ciberamenazas, que incluya procedimientos para la identificación, contención y recuperación de incidentes.
- Revisar y actualizar periódicamente la política de seguridad y las soluciones de seguridad para garantizar que estén al día con las últimas amenazas.
- Se recomienda que las empresas del sector privado en El Salvador adopten la guía de buenas prácticas de ciberseguridad desarrollada en esta investigación. La guía ofrece un enfoque estructurado y práctico para mitigar los riesgos cibernéticos en entornos de teletrabajo.
- Las empresas deben desarrollar y comunicar políticas claras de teletrabajo y ciberseguridad. Estas políticas deben incluir procedimientos de seguridad, uso de dispositivos, acceso a datos y manejo de información sensible.
- Es esencial invertir en la formación continua y la concienciación de los empleados sobre ciberseguridad. Los empleados deben estar capacitados para identificar y responder a amenazas cibernéticas como el phishing y el ransomware.
- Las empresas deben realizar evaluaciones periódicas de riesgos para identificar y priorizar los riesgos de ciberseguridad más críticos. Es crucial implementar estrategias efectivas de gestión y mitigación de estos riesgos.
- Mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad es fundamental para proteger contra vulnerabilidades conocidas. Se debe

implementar un sistema centralizado para la gestión y distribución de parches y actualizaciones.

- Las empresas deben utilizar tecnologías avanzadas de ciberseguridad, como autenticación multifactor (MFA), soluciones de gestión de acceso e identidad (IAM), y herramientas de cifrado de datos. Estas tecnologías ayudan a asegurar los datos y los sistemas en entornos de teletrabajo.
- Implementar sistemas de monitoreo continuo y establecer protocolos claros de respuesta a incidentes es vital para detectar y mitigar actividades sospechosas y responder rápidamente a incidentes de ciberseguridad.
- Las empresas deben colaborar con organismos reguladores y otras entidades del sector para mantenerse al día con las mejores prácticas y cumplir con las leyes y regulaciones locales e internacionales de ciberseguridad.

8. Glosario

1. Actualizaciones de seguridad:

Revisiones de software diseñadas para corregir vulnerabilidades y mejorar la seguridad del sistema.

2. Agencia de la Regulación de las Telecomunicaciones (ARES):

Entidad que reporta y regula incidentes de ciberseguridad en El Salvador.

3. Análisis forense digital:

Investigación de incidentes de ciberseguridad para identificar la causa y el impacto.

4. Antivirus:

Software que detecta, previene y elimina programas maliciosos.

5. Autenticación fuerte:

Uso de mecanismos de autenticación avanzados, como MFA, para aumentar la seguridad de los accesos.

6. Autenticación multifactor:

Método de control de acceso que requiere más de una forma de verificación para conceder acceso a un sistema o información.

7. Ataques DDoS:

Actos que buscan saturar y hacer inoperables los sistemas informáticos mediante el envío masivo de solicitudes.

8. Auditoría de seguridad:

Evaluación formal de la seguridad de los sistemas y procedimientos de una organización.

9. Backup y recuperación:

Procedimientos para realizar copias de seguridad de datos y restaurarlos en caso de pérdida.

10. Cámara Salvadoreña de Tecnologías de la Información y las Comunicaciones (CASSATIC):

Organización que ofrece información y recursos sobre ciberseguridad.

11. Ciberamenazas:

Riesgos y ciberataques que pueden comprometer la seguridad de sistemas y datos informáticos.

12. Ciberseguridad:

Medidas y prácticas para proteger los sistemas informáticos y la información confidencial contra ciberamenazas y ataques.

13. Cifrado de datos:

Proceso de convertir información en un código para prevenir el acceso no autorizado.

14. Concientización sobre seguridad:

Programas educativos para informar y capacitar a los empleados sobre prácticas seguras y amenazas potenciales.

15. Controles de acceso:

Restricciones y medidas para asegurar que solo las personas autorizadas puedan acceder a recursos específicos.

16. Controles de seguridad basados en riesgo:

Enfoque de seguridad que prioriza los recursos y esfuerzos en función del nivel de riesgo de diferentes activos y actividades.

17. Copia de seguridad:

Proceso de duplicar datos para protegerlos y permitir su recuperación en caso de pérdida o daño.

18. Dispositivo móvil seguro:

Estrategias y medidas de seguridad para proteger dispositivos móviles y la información que contienen.

19. Doble factor de autenticación (2FA):

Método de autenticación que requiere dos formas de verificación para acceder a una cuenta.

20. Evaluación de vulnerabilidades:

Proceso de identificar y medir las vulnerabilidades en un sistema para mitigarlas.

21. Firewall:

Software o hardware que controla y filtra el tráfico de red entre dos o más redes, protegiendo los sistemas informáticos contra accesos no autorizados.

22. Gestión de contraseñas:

Estrategias y herramientas para crear, almacenar y gestionar contraseñas de manera segura.

23. Gestión de incidentes:

Proceso de identificar, analizar y corregir riesgos de seguridad para minimizar el impacto de incidentes.

24. Ingeniería social:

es la combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano

25. Inteligencia Artificial (IA):

Red de dispositivos físicos que se comunican y comparten datos entre sí a través de Internet.

26. IoT (Internet de las cosas):

Red de dispositivos físicos conectados a Internet que pueden recopilar y compartir datos.

27. Ley de Delitos Informáticos:

Tipifica actos relacionados con la ciberseguridad, como el acceso no autorizado a sistemas y el robo de datos.

28. Ley de Firma Electrónica:

Equipara la firma electrónica con la firma autógrafa y regula su uso y validez jurídica.

29. Ley de Protección de Datos Personales:

Legislación que establece obligaciones para las empresas en cuanto a la protección de datos personales.

30. Ley de Regulación del Teletrabajo:

Legislación salvadoreña que regula el teletrabajo, promoviendo su implementación y estableciendo los derechos y deberes de trabajadores y empleadores.

31. Malware:

Software malicioso diseñado para dañar o robar información de sistemas informáticos.

32. Monitoreo de seguridad:

Supervisión continua de sistemas y redes para detectar y responder a incidentes de seguridad.

33. Normativa Técnica Salvadoreña NTS 606:2019:

Establece requisitos de seguridad para la gestión de la información en las organizaciones en El Salvador.

34. Normativas de cumplimiento:

Regulaciones y estándares que las organizaciones deben seguir para proteger datos e información.

35. Pentesting:

Pruebas de penetración para evaluar la seguridad de un sistema mediante simulación de ataques.

36. Phishing:

Técnica de engaño utilizada para obtener información confidencial haciéndose pasar por una entidad confiable en comunicaciones electrónicas.

37. Plan de continuidad del negocio:

Estrategias y procedimientos para asegurar que las operaciones críticas continúen durante y después de una interrupción significativa.

38. Política de privacidad:

Declaración que describe cómo una organización recopila, maneja y protege los datos personales de sus usuarios.

39. Política de teletrabajo:

Directrices y controles para el trabajo remoto, estableciendo responsabilidades y expectativas para minimizar riesgos de seguridad.

40. Política de uso aceptable:

Normas que describen el comportamiento y uso aceptable de los recursos de tecnología de una organización.

41. Protección de datos:

Medidas y prácticas para asegurar que los datos sean accesibles solo por usuarios autorizados.

42. Ransomware:

Software que secuestra información y exige un pago para liberarla.

43. Red privada virtual (VPN):

Tecnología que crea una conexión segura y cifrada sobre una red menos segura, como Internet.

44. Resiliencia de la red:

Capacidad de una red para continuar operando correctamente a pesar de fallos o ataques.

45. Resistencia al cambio:

Dificultad de las organizaciones y empleados para adaptarse a nuevas tecnologías y modalidades de trabajo.

46. Seguridad de la información:

Protección de la información contra accesos no autorizados y daños, asegurando su confidencialidad, integridad y disponibilidad.

47. Seguridad en el ciclo de vida del software (SDLC):

Incorporación de prácticas de seguridad en cada etapa del desarrollo de software.

48. Seguridad en la nube:

Prácticas y tecnologías para proteger datos y aplicaciones alojadas en servicios de computación en la nube.

49. Seguridad física:

Medidas para proteger el hardware y la infraestructura de daños físicos y accesos no autorizados.

50. Sistema de detección de intrusos (IDS):

Software o dispositivo que monitorea redes y sistemas en busca de actividades maliciosas o violaciones de políticas.

51. Superficie de ataque:

El conjunto de puntos vulnerables a través de los cuales un atacante puede intentar acceder a un sistema informático.

52. Teletrabajo:

Forma de organizar y realizar el trabajo de manera no presencial, utilizando tecnologías de la información y comunicación, definido por la Ley de Regulación del Teletrabajo en El Salvador.

53. Túneles virtuales:

Canales seguros dentro de Internet utilizados para comunicarse de forma protegida, comúnmente mediante VPNs.

54. Uso de VPN:

Implementación de redes privadas virtuales para asegurar conexiones remotas y proteger datos en tránsito.

9. Referencias

PEREIRO, R. (2021, 07 28). Educar para un nuevo estilo de vida sin oficinas. Recuperado de https://emprendedores.es/formacion/educar-para-un-nuevo-estilo-de-vida-sin-oficinas/

TicPymes. (2021, 05 05). La importancia de la formación de los empleados para un teletrabajo seguro. Recuperado de https://www.ticpymes.es/formacion/la-importancia-de-la-formacion-de-los-empleados-para-un-teletrabajo-seguro/

Badia, R. (Ed.). (2021, diciembre 23). El comercio electrónico en El Salvador. r ICEX España Exportación e Inversiones. Available: https://www.icex.es/content/dam/es/icex/oficinas/101/documentos/2022/03/documentos-anexos/DOC2022901378_2.pdf

SKYSNAG. (2023, October 11). Ransomware, malware y phishing. ¿Cuál es la diferencia? Skysnag. Available: https://www.skysnag.com/es/blog/ransomware-vs-malware-vs-phishing-what-is-the-difference/

Calabuig, D. (2023, septiembre 18). Ciberseguridad Teletrabajo: Riesgos y Consejos para Empresas. Ymant. Available:https://www.ymant.com/blog/ciberseguridad-teletrabajo-riesgos-y-consejos/

Hernández, A. (2023, September 12). País recibió 24 millones de intentos de ciberataques - Noticias de El Salvador. El Diario de Hoy. Available:https://www.elsalvador.com/noticias/negocios/ataques-ciberneticos-el-salvador-empresas/1089503/2023/

IKUSI. (n.d.). (2020) Ciberseguridad en el teletrabajo: 6 recomendaciones para resguardar la información de tu empresa - Ikusi. Ikusi EN. Available:https://www.ikusi.com/mx/blog/ciberseguridad-en-el-teletrabajo-6-recomendaciones-para-resguardar-la-informacion-de-tu-empresa/

Esparza Echanique, R. S. (2023). Marco de trabajo de buenas prácticas de ciberseguridad en el teletrabajo para las empresas de desarrollo de software basado en los controles establecidos en la Norma ISO 27002:2022 y la NIST SP 800-46 [Tesis de maestría, Universidad Técnica del Norte]. Recuperado de https://repositorio.utn.edu.ec/handle/123456789/15305

Álvarez Rosero, A., & Tobón González, M. (2021). Diseño de un programa de seguridad de la información en la operación que maneja un call center para un cliente del sector bancario, en un ambiente de teletrabajo (Trabajo de grado, Universidad Piloto de Colombia). Facultad de Ingeniería, Especialización en Seguridad Informática. Recuperado de https: https://repository.unipiloto.edu.co/handle/20.500.12277/10812

(2020, June 16) DECRETO No. 600 LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE EL SALVADOR, CONSIDERANDO: I. Que el artículo 37 de la Constitució. (n.d.). Portal

de Transparencia - El Salvador.
Available:https://www.transparencia.gob.sv/institutions/rree/documents/408863/download

(2019, June 24). Asamblea Legislativa.
Available:https://www.asamblea.gob.sv/sites/default/files/documents/correspondencia/2A326CE8-F13A-4828-8640-648235C228BF.pdf

(2016, February 26). ASAMBLEA LEGISLATIVA - REPUBLICA DE EL SALVADOR _ DECRETO N. (n.d.). Fiscalía General de la República.
Available:https://www.fiscalia.gob.sv/medios/portal-transparencia/normativas/normativas-de-interes/ley-especial-contra-delitos-ciberneticos.pdf

(2015, October 26) DECRETO N° 133 LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE EL SALVADOR, CONSIDERANDO: I. Que el Art. 101 de la Constitución de. (n.d.). Firma Electrónica. Available:https://firmaelectronica.economia.gob.sv/wp-content/uploads/2023/11/Ley-de-Firma-Electronica-Con-Membrete-nuevo.pdf
Metodología de la investigación (3a ed.). (2017). Grupo Editorial Patria.

ISO/IEC. (2013). ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls. International Organization for Standardization.

Duo Security. (n.d.) Duo Security. Retrieved from https://duo.com

Google. (n.d.). Google Authenticator. Retrieved from https://support.google.com/accounts/answer/1066447

OpenVPN. (n.d.). OpenVPN. Retrieved from https://openvpn.net

Cisco Systems, Inc. (n.d.). Cisco AnyConnect Secure Mobility Client. Retrieved from https://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/index.html

Kanade, S. S. (2018). Patch management: A comparative study. In 2018 IEEE International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). Coimbatore, India. https://doi.org/10.1109/ICCCI.2018.8449885

Microsoft. (n.d.). Microsoft Endpoint Configuration Manager. Retrieved from https://www.microsoft.com/en-us/microsoft-365/endpoint-management

Patch My PC. (n.d.). Patch My PC. Retrieved from https://patchmypc.com/

Sirur, M. (2015). Comparative analysis of data encryption algorithms. IEEE Xplore. Retrieved from https://ieeexplore.ieee.org/document/7252395

Microsoft. (n.d.). BitLocker Drive Encryption Overview. Retrieved from https://support.microsoft.com/en-us/windows/bitlocker-drive-encryption-overview-1b1bfab7-d7e1-4516-8d94-10c42cd6d13b

VeraCrypt. (n.d.). VeraCrypt. Retrieved from https://www.veracrypt.fr/

Netgear. (n.d.). Nighthawk AX12 12-Stream AX6000 Wi-Fi Router. Retrieved from https://www.netgear.com/home/products/networking/wifi-routers/RAX120.aspx

OpenSSL. (n.d.). OpenSSL. Retrieved from https://www.openssl.org/

WireGuard. (n.d.). WireGuard. Retrieved from https://www.wireguard.com/

Zoom. (n.d.). Zoom Security Guide. Retrieved from https://zoom.us/security

Microsoft. (n.d.).Microsoft Intune. Retrieved from https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/in-tune-mobile-device-management

Kensington. (n.d.). Kensington Security Slot. Retrieved from https://www.kensington.com/

Amazon Web Services. (n.d.). AWS Identity and Access Management (IAM). Retrieved from https://aws.amazon.com/iam/.

KnowBe4. (n.d.). KnowBe4. Retrieved from https://www.knowbe4.com/.

Cisco Systems, Inc. (n.d.). Cisco AnyConnect Secure Mobility Client. Retrieved from https://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/index.html

Kensington. (n.d.). Kensington Security Slot. Retrieved from https://www.kensington.com

Targus. (n.d.). Targus DEFCON CL. Retrieved from https://www.targus.com

MobileIron. (n.d.). MobileIron Unified Endpoint Management (UEM). Retrieved from https://www.mobileiron.com

Netgear. (n.d.). NETGEAR Routers with WPA3. Retrieved from https://www.netgear.com/home/products/networking/wifi-routers/.

NetSpot. (n.d.). NetSpot. Retrieved from https://www.netspotapp.com/

KnowBe4. (n.d.). KnowBe4. Retrieved from https://www.knowbe4.com/

DMARC Analyzer. (n.d.). DMARC Analyzer. Retrieved from https://www.dmarcanalyzer.com/

Mimecast. (n.d.). Mimecast Email Security. Retrieved from https://www.mimecast.com/products/email-security/..

Norma Técnica Salvadoreña. (2021).Accesibilidad al Entorno Físico: Urbanismo y Arquitectura. Retrieved from https://conaipd.gob.sv/wp-content/uploads/2021/04/Norma-T%C3%A9cnica-

Salvadore%C3%B1a-Accesibilidad-al-Entorno-F%C3%ADsico-Urbanismo-y-Arquitectura-2021.pdf

10. Anexos

CUESTIONARIO

Empresa: _____ Fecha: _____

Sector: ☐Industria ☐Comercio ☐Servicio

Parte l. Identificación de desafíos en la implementación de controles de Ciberseguridad en entornos de teletrabajo:

1. ¿Cuáles son los principales obstáculos que enfrenta su empresa al implementar controles de Ciberseguridad en entornos de teletrabajo?

2. ¿Cómo evalúa la capacidad de su empresa para educar y concienciar a los empleados sobre las mejores prácticas de Ciberseguridad en un entorno de trabajo remoto?

3. ¿Qué medidas ha adoptado su empresa para garantizar la protección de datos confidenciales en entornos de teletrabajo?

4. ¿Cuáles son los desafíos más comunes que enfrenta su empresa en la gestión de accesos y privilegios en entornos de teletrabajo?

5. ¿Cuál es su percepción sobre la eficacia de las VPN en la protección de la información transmitida por empleados que trabajan de forma remota?

Parte II. Identificación y gestión de riesgos de Ciberseguridad de mayor impacto en entornos de teletrabajo:

1. ¿Cuáles considera que son los riesgos de Ciberseguridad más críticos para su empresa en entornos de teletrabajo?

2. ¿Cómo evalúa la preparación de su empresa para enfrentar posibles incidentes de Ciberseguridad en un entorno de trabajo remoto?

3. ¿Qué medidas ha implementado su empresa para mitigar el riesgo de ataques de phishing dirigidos a empleados que trabajan desde casa?

4. ¿Cuáles son los principales desafíos que su empresa enfrenta en la gestión de dispositivos y acceso a la red en entornos de teletrabajo?

5. ¿Qué estrategias ha adoptado su empresa para garantizar la seguridad de los datos almacenados en dispositivos personales de empleados que trabajan de forma remota?

Parte III. Establecimiento de una guía de buenas prácticas de Ciberseguridad enmarcadas en ISO 27002:

1. ¿Está familiarizado/a su empresa con los principios y directrices de ISO 27002 en relación con la ciberseguridad?

2. ¿Cuáles son las áreas específicas de la norma ISO 27002 que considera más relevantes para su empresa en entornos de teletrabajo?

3. ¿Qué medidas ha adoptado su empresa para cumplir con los requisitos de ISO 27002 en cuanto a gestión de riesgos de seguridad de la información?

4. ¿Cómo evalúa el nivel de cumplimiento de su empresa con los controles de seguridad establecidos en ISO 27002 en un entorno de teletrabajo?

5. ¿Cuáles son los desafíos más significativos que su empresa enfrenta al alinear sus prácticas de Ciberseguridad con los estándares de ISO 27002?

Parte IV. Análisis de las empresas del sector privado de El Salvador:

1. ¿Cuántas empresas del sector privado en El Salvador han implementado políticas formales de Ciberseguridad en entornos de teletrabajo?

2. ¿Cuáles son las principales prácticas de Ciberseguridad que han demostrado ser más efectivas en empresas similares a la suya en El Salvador?

3. ¿Ha experimentado su empresa algún incidente de Ciberseguridad en un entorno de teletrabajo en el último año?

4. ¿Qué medidas ha tomado su empresa para mejorar la Ciberseguridad después de un incidente en un entorno de teletrabajo?

5. ¿Cuál es el nivel de colaboración entre empresas del sector privado en El Salvador en cuanto a compartir información y mejores prácticas de Ciberseguridad en entornos de teletrabajo?

Parte V. Consideraciones adicionales:

1. ¿Cómo evaluaría la preparación general de su empresa para hacer frente a los desafíos emergentes en Ciberseguridad en un entorno de teletrabajo?

2. ¿Cuáles son los principales factores que influyen en la eficacia de las medidas de Ciberseguridad implementadas en su empresa en entornos de teletrabajo?

3. ¿Qué recursos adicionales o apoyo necesitaría su empresa para mejorar sus prácticas de Ciberseguridad en entornos de teletrabajo?

4. ¿Cómo evalúa la importancia de la colaboración entre el sector privado, el gobierno y otros actores relevantes en la mejora de la Ciberseguridad en El Salvador?

5. ¿Qué medidas de seguridad adicionales considera necesarias para proteger la infraestructura crítica de su empresa en un entorno de teletrabajo?

Índice de Tablas

Pág.

Índice de Gráficas

Pág.