REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

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.

Trabajo de Titulación previo a la obtención del Título de Magíster en

Computación con mención en Seguridad Informática

AUTOR: Ing. Richard Sebastián Esparza Echanique

DIRECTOR: MSc. Pedro David Granda Gudiño

IBARRA - ECUADOR

2023

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1723266407		
APELLIDOS Y NOMBRES:	ESPARZA ECHANIQUE RICHARD SEBASTIAN		
DIRECCIÓN:	GONZALO MARTÍN E2-346 Y JUAN GUTIÉRREZ		
EMAIL:	rsesparzae@utn.edu.ec		
TELÉFONO FIJO:	2645823	**TELÉFONO MÓVIL:**	0963848474

DATOS DE LA OBRA	
TÍTULO:	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.
AUTOR (ES):	ESPARZA ECHANIQUE RICHARD SEBASTIAN
FECHA: DD/MM/AAAA	27/11/2023
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ☒ **POSGRADO**
TITULO POR EL QUE OPTA:	Magíster en Computación con Mención en Seguridad Informática
ASESOR /DIRECTOR:	**Director:** MSc. Granda Gudiño Pedro David **Asesor:** MSc. Guevara Vega Vicente Alexander

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 27 días del mes de noviembre de 2023.

EL AUTOR:

Nombre: ESPARZA ECHANIQUE RICHARD SEBASTIAN

UNIVERSIDAD TÉCNICA DEL NORTE

RESOLUCIÓN 173-SE-33-CACES 2020

26 de octubre del 2020

FACULTAD DE POSGRADO

Ibarra, 22 de noviembre de 2023

Dra. Lucía Yépez
DECANA
FACULTAD DE POSTGRADO

ASUNTO: Conformidad con el documento final

Señora Decana:

Nos permitimos informar a usted que revisado el Trabajo final de Grado "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" del maestrante ESPARZA ECHANIQUE RICHARD SEBASTIÁN, de la Maestría de Computación con Mención en Seguridad Informática, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	**Firma**
Tutor	MSc. Granda Gudiño Pedro David	Pedro David Granda Gudiño — Firmado digitalmente por Pedro David Granda Gudiño Fecha: 2023.11.22 09:29:09 -05'00'
Asesor	MSc. Guevara Vega Vicente Alexander	VICENTE ALEXANDER GUEVARA VEGA — Firmado digitalmente por VICENTE ALEXANDER GUEVARA VEGA Fecha: 2023.11.22 10:12:14 -05'00'

DEDICATORIA

A mi amada familia que siempre ha estado ahí apoyándome y motivándome cada día a superarme. En especial a mi padre Jaime Arturo Esparza Telcán, quien, a lo largo de los años, entre buenos y malos momentos me ha enseñado a nunca rendirme, a luchar en todo momento por lo que quiero y sobre todo a no perder la esperanza incluso en los momentos donde parece no haber nada más que oscuridad. Por enseñarme que sin importar la dificultad de las situaciones siempre hay una luz al final del túnel y que de toda situación siempre se puede aprender algo y utilizarlo para mejorar constantemente como personas y como profesionales, por guiarme en mi camino con sus sabias palabras. Este trabajo te lo dedico a ti, porque gracias a ti, hoy soy quien soy y se hacia dónde quiero ir.

Richard Esparza.

AGRADECIMIENTOS

En primer lugar, me gustaría agradecer a Dios por permitirme llegar a este punto en mi vida de crecimiento profesional, por darme la salud y por permitirme compartir este momento con quienes más amo en el mundo, mi familia.

En segundo lugar, gracias a mis amados padres y hermanos, quienes siempre me han brindado su apoyo incondicional y por siempre estar dispuestos a ayudarme sin importar la situación.

En tercer lugar, agradezco de todo corazón el apoyo que me han brindado mis amigos Gabriela Villacís, Mario Guano y José Hernández. Gracias por sus consejos, ideas, ocurrencias, y en general por hacer de este un proceso disfrutable y placentero más allá de cualquier dificultad que se haya presentado.

Por último, agradezco a la Universidad Técnica del Norte y a todos los docentes que han formado parte de este proceso formativo, por todos los conocimientos compartidos y el apoyo brindado a lo largo de este viaje de crecimiento profesional.

Richard Esparza.

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

El objetivo de esta investigación fue establecer un marco de trabajo de buenas prácticas de ciberseguridad en el teletrabajo para las empresas de desarrollo de software, a través de la síntesis de resultados de un estudio exploratorio. Para ello se trabajó desde un enfoque cuantitativo y se estableció como diseño de estudio el no experimental y transversal. En cuanto al tipo de investigación seleccionado se trata del descriptivo, exploratoria y de campo. Para la recolección de datos se empleó la técnica de la encuesta y se aplicaron dos cuestionarios a los trabajadores de Plugthem S.A. El desarrollo de la investigación se realizó con todos los permisos del caso por parte de la empresa y empleados de la desarrolladora de software Plugthem S.A. En relación con los resultados, luego de aplicar la propuesta, en cuanto al tratamiento de temas relacionados con la política de seguridad de la información, alcanzó un 3,56%. En el análisis de la información relacionada a amenazas de seguridad, se obtuvo un 3,06%. En el uso de antivirus en los equipos 2,06%. Bloqueo del acceso a personas no autorizadas mediante cortafuegos 1,72%. Actualización constante de las listas de acceso al uCXP 1,72%, mostrando un impacto positivo después de aplicar el marco de seguridad. Se concluye para garantizar buenas prácticas de ciberseguridad debe realizarse un adiestramiento, permanente en el área de seguridad informática, monitorear los incumplimientos en torno a la instalación de sistemas y medidas de seguridad, tener directrices claras. Es necesario promover estrategias que fomenten la flexibilidad y el desarrollo continuo. Se requiere fortalecer los controles de acceso a las instalaciones y vigilar las posibilidades de fugas de la información.

Palabras clave: Ciberseguridad, protección de datos, buenas prácticas.

ABSTRACT

The objective of this research was to establish a framework of good cybersecurity practices in teleworking for software development companies, through the synthesis of results from an exploratory study. To achieve this, we worked from a quantitative approach and established the non-experimental and cross-sectional study design. Regarding the type of research selected, it is descriptive, exploratory and field. To collect data, the survey technique was used and two questionnaires were applied to the workers of Plugthem S.A. The development of the investigation was carried out with all the necessary permissions by the company and employees of the software developer Plugthem S.A. In relation to the results, after applying the proposal, in terms of the treatment of issues related to the information security policy, it reached 3.56%. In the analysis of information related to security threats, 3.06% was obtained. In the use of antivirus on computers 2.06%. Blocking access to unauthorized persons through firewalls 1.72%. Constant updating of uCXP 1.72% access lists, showing a positive impact after applying the security framework. It is concluded that to guarantee good cybersecurity practices, permanent training must be carried out in the area of computer security, monitoring non-compliance regarding the installation of systems and security measures, and having clear guidelines. It is necessary to promote strategies that encourage flexibility and continuous development. It is necessary to strengthen access controls to facilities and monitor the possibilities of information leaks.

Keywords: Cybersecurity, data protection, good practices.

CAPITULO I
EL PROBLEMA

1.1. Problema de Investigación

Al tratar la ciberseguridad en la actualidad, se habla de una obligación de proteger los activos de información para las organizaciones, independientemente del sector sobre el cual estas desarrollen sus actividades, ya sea público o privado (Gayo, 2021). De hecho, tal y como señalan Medina *et al*. (2020) el objetivo principal de la ciberseguridad es generar confianza entre los clientes, proveedores y el mercado en general sobre la información que manejan en la red, ya que vivimos en un mundo hiperconectado, en el que la mayoría de las actividades son registradas por internet y dispositivos electrónicos.

Motivado en gran parte por la pandemia del Covid-19 y a la instauración del teletrabajo como la nueva modalidad de trabajo a nivel mundial, se ha hecho evidente que la ciberseguridad es un problema para el que muchas organizaciones simplemente no estaban preparadas (Tosca, 2022). Esto es así debido a que la ciberseguridad en el teletrabajo comprende tanto a la seguridad de los diferentes servicios y plataformas que permiten el desarrollo de las actividades remotas (software de videoconferencias, programas para trabajar de forma colaborativa, redes empresariales, entre otros), así como también a la de los dispositivos electrónicos desde los cuales se accede a este tipo de herramientas (laptops, computadoras de escritorio, celulares), ya sean personales o corporativos (Gómez & Becerra, 2020).

Hoy más que nunca las empresas alrededor del mundo se enfrentan grandes desafíos en materia de ciberseguridad, por ejemplo, el garantizar la integridad de los datos que maneja la empresa, la confidencialidad de todas las comunicaciones ya sea por videoconferencia o mensajes, inclusive la limitación y acceso a los distintos sistemas y soluciones de trabajo colaborativo (Corrallo, *et al*. 2021).

De acuerdo con Experian (2015) casi la mitad de las organizaciones comerciales sufren al menos un incidente de seguridad por año y el número de incidentes sigue aumentando. De hecho, el teletrabajo que ha supuesto una oportunidad para las empresas al permitir el desarrollo de las actividades en remoto, también lo es para los ciberdelincuentes, ya que ahora muchos de sus ataques van dirigidos hacia el usuario, el cual siempre ha sido considerado como el eslabón más débil de la cadena en materia de ciberseguridad (Incibe, 2019).

A pesar de los esfuerzos por desarrollar e implementar sistemas seguros, muy pocas organizaciones pueden sentir que su infraestructura es invulnerable (Bilge, *et al*. 2017). Más allá de todo esto, en el Ecuador, incluso con el surgimiento de estándares y normas establecidos a nivel mundial por organismos internacionales de gran importancia y poder como la Organización Internacional para la Estandarización (ISO), el Instituto Nacional de Estándares para la Tecnología (NIST), el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), entre otros; se ha demostrado que ninguna empresa, en ningún tipo de entorno, ya sea público o privado, ha podido realizar acciones para proteger sus activos de información de manera eficaz (Ron, *et al*. 2019).

En muchos casos la falta de garantía de seguridad de la información se traduce como pérdida de dinero, daños a la reputación de las organizaciones, pérdida de propiedad intelectual, fraudes financieros, entre otros. Además, se ha visto agravado por la falta de políticas, normas y recomendaciones claras de ciberseguridad con relación al teletrabajo (Corallo, *et al.* 2021). Es por esta razón que el enfoque del presente trabajo de investigación es establecer un marco de trabajo de buenas prácticas de ciberseguridad en el teletrabajo para así contribuir a la protección de los activos y la información de las empresas de desarrollo de software.

1.2. Interrogantes de la Investigación.

RQ1: ¿Cómo se pueden implementar buenas prácticas de ciberseguridad en el teletrabajo para las empresas de desarrollo de software?

RQ2: ¿Cómo evaluar adecuadamente un marco de trabajo de ciberseguridad dentro de una empresa de desarrollo de software?

1.3. Objetivos de la Investigación.

1.3.1. Objetivo General

Establecer un marco de trabajo de buenas prácticas de ciberseguridad en el teletrabajo para las empresas de desarrollo de software, a través de la síntesis de resultados de un estudio exploratorio.

1.3.2 Objetivos Específicos

Identificar las prácticas de ciberseguridad utilizadas por las empresas que operan bajo la modalidad de teletrabajo.

Diseñar un marco de trabajo con los mecanismos y procedimientos de ciberseguridad en el teletrabajo apropiados para las empresas de desarrollo de software basada en los controles establecidos en la norma ISO 27002:2022 y la NIST SP 800-46.

Evaluar el impacto del marco de trabajo de ciberseguridad en la ejecución de los procesos de desarrollo de software de la empresa Plugthem S.A.

1.4. Justificación

Según la National Qualifications Authority (NQA, 2013) organismo que actúa a nivel global como certificador en procesos a las empresas, la ciberseguridad, es la protección de la integridad, confidencialidad y disponibilidad de los datos; por lo que la creación y aplicación de normas, políticas y estándares entre otros, es fundamental para proteger los activos de información de las organizaciones de ataques cibernéticos, fuga de datos, robo de identidad, ransomware, malware, ingeniería social, phishing y otras amenazas relacionadas con la seguridad cibernética (Ron, *et al.* 2019).

La ciberseguridad en las organizaciones es de suma importancia debido a que a medida que las tecnologías de internet y las aplicaciones móviles aumentan en uso, volumen y complejidad, los ataques cibernéticos maliciosos están evolucionando y como resultado la sociedad se enfrenta a mayores riesgos de seguridad en el ciberespacio más que nunca (Li, *et al*. 2019). Tanto es así que, de acuerdo con Abdullah, *et al.* (2019) en años recientes los ciberdelitos, llevados a cabo en gran parte con la intención de afectar maliciosamente información crítica y confidencial, han provocado la pérdida de miles de millones de dólares afectando no solo a la economía de las empresas y a la global.

Sin embargo, a pesar del gran valor que representa la ciberseguridad, la mayoría de las actividades económicas de las empresas se han desarrollado a través de las redes informáticas, muchas veces sin las garantías necesarias, lo que ha generado graves problemas de ciberseguridad (Ron, *et al*. 2019). Esto se ha hecho aún más evidente en tiempos actuales, donde el teletrabajo se ha impuesto casi de forma obligatoria en todas las organizaciones debido a la pandemia del Covid-19 (Adeva y Vera, 2020) puesto que trabajar fuera de las instalaciones de la organización requiere tener en cuenta el riesgo para los activos de la información, ya que tanto estos como las personas trabajadoras están expuestos a múltiples desafíos y amenazas de seguridad cibernética; dando lugar a la necesidad de adoptar e implementar medidas de seguridad de los datos o ciberseguridad con la finalidad de reducir los riesgos hasta niveles controlables (Gayo, 2021).

Los esfuerzos de ciberseguridad son esenciales para mejorar y asegurar los aparatos electrónicos y redes digitales para promover la continuidad de las actividades económicas. Es fundamental establecer la seguridad de la información porque prácticamente la totalidad de dispositivos, aplicaciones y sistemas son vulnerables a los ataques cibernéticos (Hijji & Alam, 2021).

Bajo esta premisa, algunas instituciones reconocidas a nivel internacional como la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) y el Instituto Nacional de Estándares para la Tecnología (NIST), así como ciertas entidades nacionales en varios países, han propuesto recomendaciones de ciberseguridad en tiempos de teletrabajo (CISA, 2022); (CCN-CERT, 2020); (Incibe, 2020); pero, aún no se ha establecido un estándar o norma que brinde una solución definitiva a los desafíos a los que se están enfrentando las empresas actualmente, mucho menos en el Ecuador que apenas cuenta con un par de leyes y una política general.

Ante esta realidad es preciso realizar esfuerzos (proponer modelos, marcos de trabajo, herramientas, normas, lineamientos, políticas) enfocados a tratar los diversos desafíos de ciberseguridad que se presentan en el desarrollo de las actividades económicas bajo la modalidad de teletrabajo, para así contribuir a la protección de los activos de información de las empresas.

El presente trabajo está enmarcado dentro del Objetivo de Desarrollo Sostenible 16 de la ONU sobre Paz, justicia e instituciones sólidas, que a su vez se encuentra alineado con el objetivo 10 del Plan de Creación de Oportunidades 2021-2025 en el cual se establece una política que busca fortalecer la triada CID (confidencialidad, integridad y disponibilidad) frente a las amenazas provenientes del ciberespacio. Por último, este proyecto se relaciona con la línea No. 10 de investigación científica aprobada por el Honorable Consejo Universitario de la UTN concerniente al Desarrollo, aplicación de software y cyber security (seguridad cibernética) (UTN, 2023).

CAPITULO II
MARCO REFERENCIAL

2.1. Antecedentes

El incremento en el uso de las tecnologías de la información, dentro de las actividades que se realizan en el día a día, ha dado lugar a que la seguridad informática se convierta un elemento imprescindible (Khraisat, *et al.* 2019). En la actualidad, y motivado en gran parte por la pandemia de la Covid-19, más de 500 millones de personas en todo el mundo se han visto en la obligación de adoptar el trabajo desde casa, popularizándose el concepto del teletrabajo haciendo uso de diferentes plataformas y software que facilitan el desarrollo de las tareas de forma remota, lo cual ha hecho a las organizaciones replantearse a la ciberseguridad como la búsqueda de una protección que vaya mas allá del perímetro (Adeva y Vera, 2020).

A pesar de la importancia de la seguridad informática, tanto el sector público, privado y la sociedad en general, no han sabido tomar medidas proactivas para mejorar su ciberseguridad (Ron, *et al*. 2019). Informes recientes muestran que el número de ataques cibernéticos sigue aumentando a nivel mundial (Okutan *et al*. 2018). De hecho, cada día se incrementan los casos relacionados con el robo de computadoras, nuevos virus, ciberataques, ciberguerras, entre otros, que afectan directamente a la economía de las empresas objeto de ataque (Bustamante, *et al*. 2018).

Desafíos como dar soporte remoto en caso de que el usuario tenga problemas, reaccionar frente a la posible pérdida o hurto del equipo en los desplazamientos, limitar y asegurar el acceso de colaboradores externos y proveedores desde sus propios dispositivos, prever y reducir los riesgos de intercepción y desviación de tráfico de los aparatos electrónicos, siguen presentes en la mayoría de organizaciones sin que estas sepan cómo afrontarlos de la manera adecuada (Gómez y Becerra, 2020).

Está claro entonces que existe una necesidad aparente y urgente de implementar mecanismos de ciberseguridad para prevenir amenazas y vulnerabilidades. Hoy en día se considera que una organización que no es cibersegura se encuentra condenada al fracaso, además, la implementación de diferentes estándares y políticas es una de las fuerzas motivadoras más poderosas detrás de la mayoría de las inversiones comerciales debido al impacto financiero o reputacional que implica (Marotta & Madnick, 2021). Aunque el cumplimiento no siempre es igual a la seguridad, se ha demostrado que en algunos casos puede ayudar a aumentarla (Sommestad, *et al.* 2014).

Desde esta perspectiva, se han presentado algunas propuestas con diferentes lineamientos, normas, guías, entre otros, destacándose especialmente la labor realizada por el Centro de Ciberseguridad Nacional español (CCN) que en mayo de 2020, actualizó sus recomendaciones de seguridad para trabajar en casa (CCN-CERT, 2020), o la guía dirigida a organizaciones sobre la ciberseguridad en el desempeño de actividades a distancia publicada por el Instituto Nacional de Ciberseguridad de España, que incluye varias directrices y políticas para el trabajo remoto (Incibe, 2020); incluso en Estados Unidos, los principales organismos expertos en el tema elaboraron varios documentos con referencia teletrabajo y asimismo la Agencia de Ciberseguridad y Seguridad de Infraestructura creó una plataforma web en la cual fueron publicados numerosos informes (CISA, 2022).

En el Ecuador, sin embargo, apenas se están dando los primeros pasos enfocados a la ciberseguridad en general con la publicación de la Política Nacional de Ciberseguridad y un par de propuestas puntuales como la de (Vilcacundo, 2021) en la cual se establecen políticas de ciberseguridad en el teletrabajo de una institución de educación superior, y la propuesta de (Silva, 2022) que pretende establecer mecanismos para el uso adecuado de los dispositivos electrónicos de teletrabajo en una institución financiera. Esto denota que aún no se ha establecido una cultura y conciencia en materia de ciberseguridad en el país debido en gran parte a la naturaleza altamente cambiante y evolutiva de los ataques cibernéticos y a los costos que supone protegerse contra ellos, lo que los convierte en un riesgo fundamental y un determinante de éxito y supervivencia para las organizaciones (Marotta & Madnick 2021).

De acuerdo con (Gayo, 2021), el teletrabajo es una oportunidad, pero también supone un reto para las organizaciones ya que, si no se adoptan medidas de seguridad informática o ciberseguridad adecuadas, sus activos de información pueden quedar expuestos a vulnerabilidades que representan un riesgo para la confidencialidad, integridad y disponibilidad de los datos. Desafortunadamente, enfrentar ataques cibernéticos es ahora la norma y no la excepción, por lo que es necesario establecer defensas proactivas. De hecho, Bilge, *et al*. (2017) afirman que las empresas deben estar preparadas para minimizar los daños cuando finalmente se produzcan ciberataques, para este fin, necesitan implementar múltiples capas de seguridad, incluidos servicios de seguridad administrados, asesores de seguridad confiables, programas de capacitación para empleados, entre otros, además de los mecanismos tradicionales de defensa contra amenazas cibernéticas.

2.2. Marco Teórico

2.2.1. Seguridad de la Información

El concepto de la seguridad de la información se refiere a garantizar que la información tenga las siguientes características denominadas como triada CID: confidencialidad, integridad y disponibilidad. Sin embargo, hoy en día, autores como Wang, *et al.* (2018) consideran que también deben incluirse las características de autenticidad, identificación, y no repudio.

En el Ecuador, a través de la norma para la gestión del riesgo operativo, define la seguridad de la información como un conjunto de métodos y directrices que posibilitan la preservación de la triada CID (Superintendencia de Bancos, 2021). Además, en el artículo 25 de esta misma norma, que se basa en gran medida en lo dispuesto por la Internacional Organization for Standardization (ISO 27000, 2022) , se establecen los requisitos mínimos para una adecuada gestión de la seguridad de la información como: Roles y responsabilidad concretamente definidos, establecimiento de un comité de seguridad de la información, definición de un área dedicada a velar por la correcta gestión de la seguridad de la información y un oficial responsable.

2.2.2. Seguridad Informática

Soriano (2014) define a la seguridad informática como el conjunto de herramientas y medidas técnicas que se implementan con el objetivo de salvaguardar los datos contenidos en equipos informáticos contra posibles ataques de hackers malintencionados. Por otro lado, Figueroa, *et al*. (2018) la considera como un área cuya finalidad es asegurar que los recursos como los programas no sean utilizados con fines bélicos o maliciosos.

En la actualidad, gracias al Índice Global de Ciberseguridad creado por la UIT (Unión Internacional de Telecomunicaciones), es posible saber cuáles son los países con un mayor compromiso por implementar estrategias y acciones enfocadas a mejorar de forma continua su seguridad informática, destacándose sobre todo Singapur y Estados Unidos entre los países con mejor índice en la materia ya que es evidente el esfuerzo que hacen los gobiernos de estas naciones para salvaguardar su espacio e infraestructura cibernética. Más allá de esto, a nivel de Latinoamérica el Ecuador se encuentra en el sexto lugar con mejor índice de ciberseguridad respecto a los 19 países que forman parte de la estadística en la región (Alvarado, 2021). Esto gracias a las acciones implementas por el gobierno a través del Ministerio de Telecomunicaciones (MINTEL) en conjunto con el Centro de Respuesta a Incidentes Informáticos del Ecuador (EcuCERT).

2.2.3. Teletrabajo y su Importancia

De acuerdo con Medina *et al.* (2020) el teletrabajo podría entenderse como el desarrollo de una actividad laboral remunerada, para la cual se utilizan las tecnologías de la información y la comunicación (TIC), siempre y cuando se realice fuera del lugar físico laboral y con los medios provistos por la empresa, no exigiendo la presencia permanente del trabajador en ella. Hoy en día es un modelo que brinda mayor accesibilidad y flexibilidad a los trabajadores, atrayendo y manteniendo el talento humano. Pero más allá de esto, posee las siguientes características: está orientado a resultados y no a horas trabajadas, se realiza fuera de las instalaciones de la organización, depende en gran medida de las TIC, presenta un nuevo equilibrio entre autonomía y supervisión, tiene una alta capacidad de adaptación al cambio, flexibilidad de horarios, formación continua, entre otros

En el Ecuador, este tipo de modalidad de trabajo se ha popularizado motivado en gran parte por la pandemia del COVID-19, siendo de gran interés sobre todo para las nuevas generaciones que, de acuerdo con González (2023) hoy más que nunca buscan como opción de empleo aquellos que ofrezcan una modalidad 100% remota o híbrida. Tanto es así que alrededor de 165.000 personas en la actualidad cuentan con una labor bajo esta modalidad según los datos recabados por Sistema Único de Trabajo del Ministerio de Telecomunicaciones (Delgado, 2023).

2.2.4. Prácticas de Ciberseguridad

La ciberseguridad se refiere a la práctica de defender computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos (Joyanes, 2017). Puede definirse entonces como el conjunto de procedimientos y herramientas que se implementan para proteger la información digital (López et al. (2019) (Nakhodchi & Dehghantanha, 2020).

A nivel de Ecuador, el gobierno considera a la ciberseguridad como un tema vital para asegurar la supervivencia de la nación en esta nueva era digitalizada en donde una protección adecuada y una actualización continua son la clave para el triunfo, de ahí que gracias a los esfuerzos del Estado en conjunto con organizaciones privadas y de la academia, el Ecuador cuenta ahora con una Estrategia Nacional de Ciberseguridad (ENC), enfocada sobre todo a garantizar que los datos personales y la información de los ciudadanos se encuentre protegida, al mismo tiempo que promueve un acceso seguro a las tecnologías de la información (MINTEL, 2022).

Un elemento importante dentro de las prácticas de ciberseguridad lo constituye el adiestramiento del personal que no son otra cosa que una serie de capacitaciones organizadas,

con un alto sentido pedagógico y tecnológico para garantizar que el personal pueda desarrollar capacidades que le permitan garantizar el cumplimiento de pasos y le fortalezcan habilidades para enfrentar situaciones laborales asociadas a las vulneraciones de la seguridad. En ese sentido, Huaman, (2021) señalo que la instrucción implica que el personal adquiera habilidades mediante la experiencia de aprendizaje, preparándolos para enfrentar desafíos laborales. Por ello el adiestramiento en operaciones cibernéticas implica desarrollar conocimientos específicos para la ciberdefensa, aprovechando el potencial cognitivo del individuo.

Allauca, (2022) mencionó que una de las principales dificultades señalada por los clientes corporativos es la interrupción del servicio. Para contrarrestar esta situación, los departamentos de Tecnologías de la Información (TI) de cada empresa implementarán métodos y técnicas de seguridad, además de capacitar al personal, llevar a cabo pruebas de seguridad y realizar inversiones en seguridad empresarial. Esto se hace con el propósito de mitigar los impactos y estar preparados para enfrentar posibles ataques a la red corporativa.

Villacís (2022) manifestó que la carencia de empleados capacitados en las empresas para abordar de manera rápida estas circunstancias, los desafíos al implementar proyectos de actualización tecnológica y su integración con las plataformas ya establecidas, e incluso la limitación presupuestaria para gestionar adecuadamente la seguridad, son factores que dificultan la efectiva prevención de los ciberataques.

De manera que, si las empresas no adoptan medidas de ciberseguridad y no gestionan adecuadamente el riesgo en sus infraestructuras tecnológicas y en los procesos del negocio, estarán expuestas a numerosas amenazas. En caso de que un ciberdelincuente explote las vulnerabilidades, los activos de información de las empresas podrían verse gravemente comprometidos (Allauca, 2022). Para ello requerirán instalación de sistemas y medidas de seguridad.

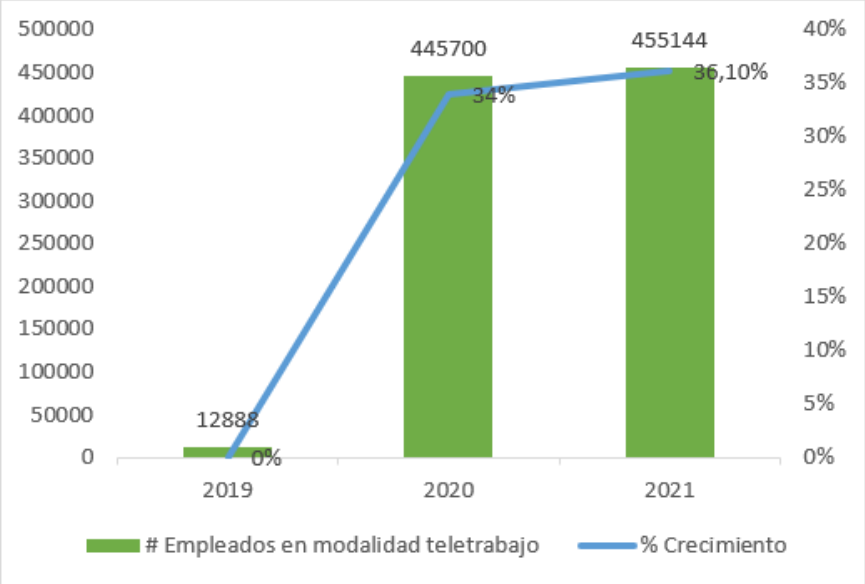
2.2.4.1. Ciberseguridad en el Teletrabajo. De acuerdo con Khan, *et al*. (2022) la ciberseguridad en el teletrabajo se refiere al cumplimiento de estándares, normas e implementación de políticas enfocadas a mantener un entorno de trabajo seguro fuera de la organización. Esto evidencia como, la transformación digital de la sociedad ha ampliado el acceso a herramientas de trabajo remoto de alto rendimiento: las computadoras son poderosas, las redes son rápidas y confiables, el software de videoconferencia es más fuerte que nunca y las herramientas de administración y almacenamiento en la nube brindan acceso remoto a todos los datos operativos de una determinada organización (ISECM, 2023). En resumen, ya no existen barreras tecnológicas reales para la práctica generalizada del teletrabajo.

Sin embargo, esta misma noción de teletrabajo crea una dinámica desconcertante desde un punto de vista puramente de ciberseguridad pues la administración de TI (Tecnologías de la Información) termina brindando protección a una multitud de pequeñas unidades de trabajo independientes, administradas de manera autónoma y, a menudo, bordeando el límite de lo que pertenece a la organización y lo que forma parte de la vida privada del trabajador (Ukwen & Karabatak, 2021).

Durante la pandemia de Covid-19, hubo un aumento sin precedentes en la cantidad de empleados que trabajan fuera de la infraestructura de TI de las organizaciones debido al uso de dispositivos personales. De hecho, tan solo en Ecuador, desde el año 2019 hasta el 2021 hubo un crecimiento de más del 35% en la cantidad de empleados que se encuentran operando bajo la modalidad de teletrabajo (Niubox, 2021). (ver figura 1).

Figura 1

Crecimiento del teletrabajo en Ecuador



Nota: tomado de *Niubox* (2021).

Un dato interesante, es que la escala y la sofisticación de los ataques cibernéticos continúan aumentando después del Covid-19 y ahora más que nunca se ha vuelto fundamental para las empresas proteger su información y activos de TI (Hijji & Alam, 2021). Por consiguiente, es necesario implementar acciones que permitan garantizar la protección de la información.

2.2.4.2. Desafíos de Ciberseguridad en el Teletrabajo. Los autores Abukari & Bankas (2020) manifiestan que los desafíos de ciberseguridad en el teletrabajo son aquellos problemas que se encuentran enmarcados dentro las siguientes cinco categorías que hasta el momento son los más relevantes (ver figura 2).

Figura 2

Desafíos de la ciberseguridad

Nota: tomado de Abukari & Bankas (2020).

El gran aumento de ciberataques exitosos en la actualidad se atribuye directamente a la cantidad de personas que desempeñan sus actividades laborales bajo la modalidad de teletrabajo o trabajo remoto. Según un estudio realizado por Borkovich & Skovira (2020) el desafío más grande de ciberseguridad son las personas ya que muchas veces no tienen una conciencia de seguridad y se exponen a ciberataques al abrir vínculos; tener un mayor acceso a los datos o más permisos de administrador de los necesarios; descargar información confidencial en memorias USB; reenviar correos electrónicos de trabajo a cuentas personales; o compartir documentos que no deberían.

En el Ecuador, de acuerdo CON CSIRT CELEC EP, (2022) los principales desafíos a los que se enfrentan las organizaciones además de los mencionados anteriormente también incluyen: falta de capacidad para soportar conexiones seguras a la infraestructura de TI de la empresa, errores de configuración e implementación de mecanismos de acceso seguro, y la falta de cifrado de discos en los dispositivos del usuario final, entre otros.

2.2.5. Políticas de Ciberseguridad

Según lo expuesto por Abukari & Bankas (2020) las políticas de ciberseguridad son documentos de tecnología de información generalmente utilizados por las organizaciones y agencias gubernamentales para ayudar a mejorar sus medidas de seguridad cibernética contra posibles ataques de ingeniería social y piratas informáticos malintencionados. Bukley et al. (2014) mencionan que en este caso se requiere afianzar las políticas ya que generalmente se utilizan para agilizar el comportamiento del personal.

Ahora bien, según una investigación realizada por Aldawood, & Skinner, (2019) desarrollar e instituir procedimientos integrales de ciberseguridad es una de las mejores medidas de seguridad para reducir los ciberataques. En general, una política que aborde este aspecto debería contemplar lineamientos para el comportamiento del personal y medidas punitivas, de ingeniería social, preventivas, la de escritorio, identificadores de llamadas, monitoreo, redes sociales, auditoría y el cumplimiento, pues de acuerdo con Abukari & Bankas (2020) estos son componentes claves.

En este contexto, es preciso mencionar que en el año 2021 y motivado en gran medida por el preocupante incremento en la cantidad de incidentes cibernéticos nacionales, el Ecuador aprobó mediante acuerdo ministerial 006-2021, la primera Política Nacional de Ciberseguridad que a grandes rasgos establece lineamientos y directrices relacionados a una adecuada gestión, tratamiento y mitigación de riesgos de ciberseguridad (MINTEL, 2021).

2.2.6. Familia de Normas ISO/IEC 27000:2022

La familia de normas ISO/IEC 27000 se publicó originalmente como British Standard 7799 en 1995 y posteriormente como ISO 17799. Estas proporcionan recomendaciones de mejores prácticas sobre la gestión, los riesgos y los controles de la seguridad de la información en el contexto de un Sistema de gestión de la seguridad de la información (Rianafirin & Kurniawan, 2017).

De acuerdo con Tjirare & Shava (2017) la implementación de la familia de normas ISO 27000 puede traer los beneficios que se enumeran a continuación para una organización: ayuda a llevar a cabo una planificación estructurada para reconocer, administrar, supervisar y mejorar de forma proactiva los desafíos de seguridad de la información y sus riesgos correspondientes.

Los procedimientos y métodos para gestionar la seguridad de la información serán establecidos, registrados y aplicados en la práctica. Se mostrará el compromiso de la organización con la el aseguramiento de los datos lo que también asegurará la asignación correcta de recursos, la definición de roles y responsabilidades, así como la provisión de la formación adecuada. De igual manera, se menciona que se implementarán medidas de seguridad para resguardar los datos contra accesos no permitidos, al tiempo que se garantizará su disponibilidad para aquellos usuarios autorizados que lo necesiten.

De manera que, la adopción de las normas ISO 27000 ofrece una estructura integral que permite a las organizaciones reconocer, administrar, monitorear y mejorar proactivamente los desafíos de seguridad de la información y sus riesgos asociados. Proporciona un marco sólido que fortalece la seguridad de la información y promueve prácticas efectivas para su gestión integral en las organizaciones.

Otros de los beneficios mencionados se relacionan con evidenciar una gestión eficiente de la continuidad del negocio en una organización mejorará su imagen y aumentará las posibilidades de crecimiento en el ámbito comercial. Es factible proteger los derechos de propiedad intelectual. Finalmente, una empresa que verifique de manera independiente el cumplimiento de las regulaciones puede asegurar que ha respetado adecuadamente las leyes pertinentes en cuanto a la protección de datos personales (Tjirare & Shava, 2017).

2.2.6.1. Norma ISO/IEC 27001:2022. La norma ISO/IEC 27001 es uno de los estándares de seguridad de la información más utilizados y aceptados en todo el mundo (Malatji, 2023). El 25 de octubre de 2022, se publicó la tercera edición de la norma como ISO/IEC 27001:2022 para abordar los desafíos globales de ciberseguridad y mejorar la confianza digital.

En general, esta norma provee orientaciones para apoyar a las organizaciones a establecer las mejores prácticas para implementar un sistema de gestión de seguridad de la información, especificando requisitos que permitan la selección e implementación de controles de seguridad adecuados (Longras *et al*. 2018). Este estándar ayuda a las organizaciones a proteger sus activos de información, alcanzar sus niveles adecuados de seguridad y así alcanzar sus objetivos comerciales. La implementación de esta se realiza a través de un proceso de cuatro fases como se muestra en la figura 3.

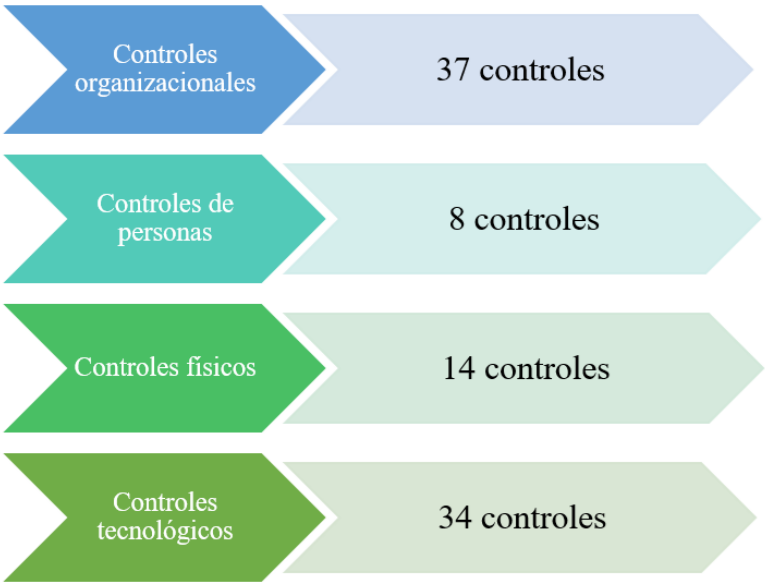
Figura 3.
Fases de implementación de la norma ISO/IEC 27001

Nota: Tomado de ISO 27001 (2023).

Es importante mencionar también que esta norma es aplicable a todo tipo de organización independientemente de su tamaño o giro de negocio ya que lo que se pretende sobre todo es proteger la información. Además, es una norma sobre la cual se puede obtener una certificación que avale el cumplimiento y compromiso con la seguridad de la información.

2.2.6.1. Norma ISO/IEC 27002:2022. Es uno de los derivados de la familia ISO/IEC 27000 creada por La Organización Internacional de Normalización (ISO), y sirve como guía para explicar la implementación de la seguridad de la información utilizando controles para lograr los objetivos de seguridad establecidos por la organización (Sulistyowati, Suryanto, & Handayani, 2020). Esta norma no requiere una forma particular de control, sino que más bien deja que el usuario seleccione e implemente el control adecuado de acuerdo con sus necesidades. teniendo en cuenta los resultados de una evaluación de riesgos previa. Fue actualizada en el año 2022, cambiando así su organización y quedó ahora constituida por 93 controles (en lugar de 114) distribuidos en 4 categorías o cláusulas según el contexto de aplicación de cada control, esto se puede apreciar en la figura 4.

Figura 4.
Organización de la Norma ISO/IEC 27002:2022



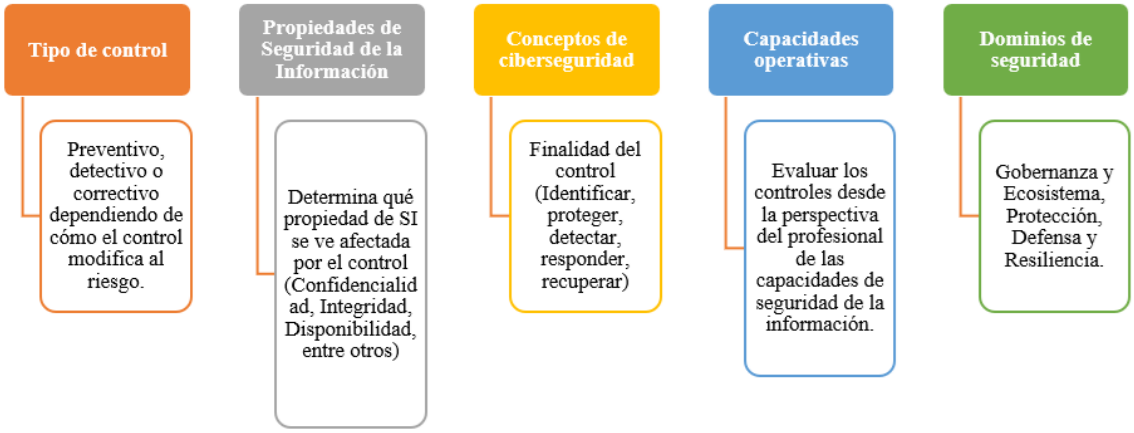
Nota: Tomado de ISO 27002, (2022)

Sin embargo, la norma es bastante flexible en cuanto a esta categorización por lo que provee una definición bastante general de cada acción haciendo énfasis en que la categorización puede y debe adaptarse según el contexto de cada organización que desee implementar estos controles (ISO 27000, 2022). La definición de cada categoría sería la siguiente:

Controles organizacionales, que se adaptan a las necesidades específicas de cada organización. Los de personas que involucran a individuos, se centran en regular el comportamiento humano dentro de un entorno organizativo para fortalecer la seguridad de la información y reducir los riesgos asociados con las acciones de las personas en el uso, acceso y manipulación de datos y sistemas. Controles físicos: Todos los controles en donde se ven involucrados objetos físicos. Los tecnológicos, que están centrados en el aspecto técnico de la seguridad de la información, utilizando herramientas y sistemas para proteger activamente los recursos digitales de una organización y mitigar las amenazas cibernéticas.

La norma ISO 27001 define cinco atributos específicos para cada control con el propósito de ofrecer una comprensión más detallada del impacto que tendría la implementación de dicho control en una organización. Estos atributos proporcionan una visión más clara y detallada sobre cómo afectaría o contribuiría a la seguridad de la información de la organización, esto se puede visualizar en la figura 5.

Figura 5.
Atributos de los controles de la norma ISO 27002:2022



Nota: Tomado de ISO 27002, (2022)

2.2.6.1.1. Controles Relacionados al Teletrabajo. Considerando que el presente trabajo toma como base los controles antes descritos, se presenta a continuación el detalle de aquellos más relevantes identificados con relación a la ciberseguridad en esta modalidad tomando en cuenta también los atributos definidos por la norma para una mejor comprensión:

Tabla 1.

Controles organizacionales

Id	Nombre	Descripción	Tipo de Control	Propiedades de Seguridad de la información	Dominios de Ciberseguridad
5.1	Políticas de Seguridad de la información	Se debe definir, aprobar, publicar, comunicar y mantener adecuadamente una política de seguridad de la información para la organización con el objetivo de cumplir con las normas y estatutos requeridos de forma legal y contractual.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Gobernanza y ecosistema, Resiliencia
5.2	Roles de Seguridad de la Información y Responsabilidades	Los roles y responsabilidades de seguridad de la información deben definirse de acuerdo con las necesidades de las organizaciones.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Gobernanza y ecosistema, Protección, Resiliencia
5.4	Gestión de responsabilidades	Todo el personal debe regirse a la política de seguridad definida.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Gobernanza y ecosistema
5.7	Inteligencia de amenazas	La información relacionada a amenazas de seguridad debe ser recolectada y analizada.	Preventivo, Detectivo, Correctivo	Confidencialidad, Integridad, Disponibilidad	Defensa, Resiliencia
5.9	Inventario de información y activos asociados	Se debe desarrollar y mantener un inventario de los activos de información, así como los datos de sus dueños.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Gobernanza y ecosistema, Protección
5.10	Uso aceptable de la información y otros activos asociados	Desarrollo y gestión de reglas y procedimientos para el uso adecuado de los activos de información.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Gobernanza y ecosistema, Protección

5.11	Devolución de activos	Todo el personal debe devolver los activos a su cargo una vez que ha finalizado su relación con la organización o por algún otro acuerdo.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Protección
5.14	Transferencia de información	Se deben establecer reglas, procedimientos y acuerdos para la transferencia de información dentro de la organización y con terceros.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Protección
5.15	Control de acceso	Se debe establecer e implementar reglas que controlen el acceso físico y lógico de las personas a la información.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Protección
5.18	Derechos de acceso	Es necesario gestionar adecuadamente los permisos de acceso y actualizarlos conforme se requiera de acuerdo con las políticas de control de acceso definidas.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Protección
5.23	Seguridad de la información para el uso de servicios en la nube	Los procesos para adquirir, usar y remover servicios basados en la nube deben ser establecidos.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Gobernanza y ecosistema, Protección
5.24	Planificación y preparación para la gestión de incidentes de seguridad de la información	La organización debe prepararse para gestionar incidentes de seguridad definiendo los procesos, roles y responsabilidades pertinentes.	Correctivo	Confidencialidad, Integridad, Disponibilidad	Defensa
5.36	Cumplimiento de reglas, políticas y estándares de seguridad de la información	Debe existir una revisión regular del cumplimiento de las políticas de la organización y otros estándares.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Gobernanza y ecosistema

Nota: Tomado de ISO 27002, (2022)

Tabla 2.

Controles de personas

Id	Nombre	Descripción	Tipo de Control	Propiedades de Seguridad de la información	Dominios de Ciberseguridad
6.3	Concientización, educación y entrenamiento en seguridad de la información	Todo el personal de la organización debe recibir capacitación en materia de seguridad sobre los elementos relevantes para el adecuado desempeño de sus funciones.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Gobernanza y ecosistema
6.5	Responsabilidades al cambio o término de relación laboral	Se deben establecer y comunicar las responsabilidades que se mantendrán al término o cambio de la relación laboral con la organización	Preventivo	Confidencialidad, Integridad, Disponibilidad	Gobernanza y ecosistema
6.7	Trabajo remoto	Es necesario implementar todas las medidas necesarias para proteger la información que es accedida, procesada y almacenada fuera de la organización.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Protección
6.8	Reporte de eventos de seguridad de la información	La organización debe proveer mecanismos para que personal pueda reportar eventos de seguridad observados a través de canales apropiados.	Detectivo	Confidencialidad, Integridad, Disponibilidad	Defensa

Nota: Tomado de ISO 27002, (2022)

Tabla 3.

Controles físicos

Id	Nombre	Descripción	Tipo de Control	Propiedades de Seguridad de la información	Dominios de Ciberseguridad
7.3	Aseguramiento de oficinas, habitaciones e instalaciones	Los controles físicos adecuados para acceder a las diferentes instalaciones deben ser implementados	Preventivo	Confidencialidad, Integridad, Disponibilidad	Protección
7.7	Escritorio y pantalla limpios	Las reglas de escritorio y pantalla limpios se deben cumplir a cabalidad para reducir el riesgo de acceso no autorizado a información confidencial.	Preventivo	Confidencialidad	Protección
7.9	Seguridad de los activos fuera de las instalaciones	Todos los dispositivos que se puedan utilizar fuera de la organización para acceder a la información deben ser protegidos.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Protección
7.14	Eliminación segura o reutilización de equipos	Cualquier equipo utilizado para almacenar información o que contenga algún tipo de software perteneciente a la organización debe ser verificado para asegurar su correcta eliminación.	Preventivo	Confidencialidad	Protección

Nota: Tomado de ISO 27002, (2022)

Tabla 4.

Controles tecnológicos

Id	Nombre	Descripción	Tipo de Control	Propiedades de Seguridad de la información	Dominios de Ciberseguridad
8.1	Dispositivos de usuario final	Toda la información accedida, procesada o almacenada en dispositivos del usuario final debe ser protegida.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Protección
8.5	Autenticación segura	Se debe implementar procedimientos y tecnologías de autenticación segura basados en políticas.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Protección
8.12	Prevención de fuga de datos	La implementación de medidas para evitar fugas en todos los sistemas, redes y otros dispositivos por los que circula la información debe ser asegurada.	Preventivo, Detectivo	Confidencialidad	Protección, Defensa
8.18	Uso de programas de utilidad privilegiados	Es necesario controlar/reducir el uso de programas que permitan evadir los controles establecidos en las aplicaciones y sistemas.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Protección
8.19	Instalación de software en sistemas operativos	Se deben implementar las medidas y mecanismos apropiados para gestionar la instalación del software en los diferentes sistemas.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Protección
8.20	Seguridad de la red	Toda la red y los dispositivos que forman parte de esta deben ser asegurados, gestionados y controlados para proteger la información.	Preventivo, Detectivo	Confidencialidad, Integridad, Disponibilidad	Protección
8.25	Ciclo de vida de desarrollo seguro	Se requiere el establecimiento y aplicación de reglas para el desarrollo de aplicaciones y sistemas seguros.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Protección
8.28	Codificación segura	Durante el desarrollo de software deben aplicarse principios de codificación segura.	Preventivo	Confidencialidad, Integridad, Disponibilidad	Protección
8.30	Desarrollo tercerizado	La organización debe velar por una correcta dirección, monitoreo y revisión de todas las actividades realizadas por medio de terceros.	Preventivo, Detectivo	Confidencialidad, Integridad, Disponibilidad	Gobernanza y ecosistema, Protección

Nota: Tomado de ISO 27002, (2022)

2.2.7. Serie NIST SP 800

Las publicaciones de la serie Special Publication (SP) 800 de NIST presentan información de interés para los interesados en seguridad informática. La serie comprende pautas, recomendaciones, especificaciones técnicas e informes anuales de las actividades de ciberseguridad del NIST (NIST, 2018).

Creada en 1990, la serie informa sobre la investigación, las pautas y los esfuerzos de divulgación realizados por el laboratorio de tecnología de la información en materia seguridad informática, incluyéndose además sus actividades de colaboración con la industria, el gobierno y las organizaciones académicas.

2.2.7.1. NIST SP 800-46. Esta publicación realizada por el NIST proporciona información sobre consideraciones de seguridad para empleados que trabajan de forma remota y varios tipos de soluciones de acceso remoto. También ofrece recomendaciones para asegurar una variedad de tecnologías de teletrabajo, acceso remoto y BYOD (Bring Your Own Device) y brinda recomendaciones sobre la creación de políticas de ciberseguridad de teletrabajo (Souppaya & Scarfone, 2016). A modo de resumen, se explica a continuación los tópicos que aborda la publicación en sus diferentes apartados:

Seguridad del acceso remoto para personas y visión general del teletrabajo donde se describe de una manera breve las vulnerabilidades y amenazas comunes a las que se enfrentan las empresas, así como métodos de seguridad recomendados para garantizar un acceso remoto adecuado. Además, discute potenciales riesgos inherentes al uso de dispositivos BYOD dentro de las redes empresariales. También se hace mención de la seguridad del acceso remoto para las empresas y visión general del teletrabajo que trata sobre los mecanismos que deberían considerarse para proteger las soluciones de acceso remoto, incluyendo los servidores, ubicación del software, entre otros. En el mismo orden de ideas se plantea la seguridad de dispositivos de usuario final en el teletrabajo, donde se proveen recomendaciones para asegurarlos de manera efectiva y al mismo tiempo proteger la información contenida en estos (Souppaya & Scarfone, 2016).

Finalmente se establecen consideraciones para el teletrabajo, abordando en forma y con ejemplos sobre cómo elaborar una política de seguridad y diseñar e implementar buenas prácticas particularmente útiles en la materia. Dentro de lo más relevante que ofrece esta publicación se encuentra también un modelo de ciclo de vida de 5 fases diseñado para ayudar a las organizaciones a implementar recomendaciones en puntos clave de su estrategia de teletrabajo, esto se puede visualizar en la figura 6.

Figura 6.
Modelo de Ciclo de Vida de una solución de teletrabajo

Nota: Adaptado de Souppaya & Scarfone (2016).

2.2.7.1.1. Controles Relacionados al Teletrabajo. Como ítem clave, esta publicación proporciona en su Anexo A un conjunto de controles específicos relacionados al teletrabajo, tecnologías BYOD y acceso remoto seguro que se encuentran directamente asociados a los controles de seguridad y privacidad para sistemas de información de la NIST SP 800-53. Por lo que los más relevantes identificados para esta investigación se describen a continuación:

Tabla 5.
Controles del Anexo A

Id	Nombre	Descripción
AC-2	Gestión de cuentas	Establece que debe existir una adecuada gestión de autenticación de uno o varios factores para los usuarios por medio de contraseñas, certificados digitales o algún tipo de token.
AC-17	Acceso remoto	Involucra a todo el proceso que se debe seguir para garantizar un acceso remoto seguro, va desde la documentación de requisitos de acceso hasta la encriptación de todas las conexiones.
AC-19	Control de acceso para dispositivos móviles	Define los requisitos que deben cumplir los dispositivos móviles controlados por la organización para acceder a sus sistemas.
AC-20	Uso de sistemas de información externos	Regula el uso de dispositivos BYOD personales o de terceros para acceder, procesar y transmitir información.
CP-9	Respaldos de sistemas de información	Se debe mantener un respaldo adecuado de la información contenida en los sistemas de información ya sea de forma local o remota.
IA-3	Identificación y autenticación de dispositivos	Es necesario que exista una autenticación mutua entre los diferentes dispositivos antes de establecer cualquier conexión o intercambio de información entre ellos.

IA-11	Re-autenticación periódica	Controles periódicos para asegurar que los usuarios tienen autorización para acceder a determinada información cuando han tomado descansos entre largas sesiones de trabajo remoto.
RA-3	Evaluación de riesgos	Se requiere realizar una evaluación de riesgos previo a implementar cualquier método de acceso remoto a los sistemas de la organización.
SC-7	Protección de límites	Establece que la red debe ser segmentada apropiadamente para separar componentes públicos de los privados.
SC-8	Confidencialidad e Integridad de las transmisiones	Debería utilizarse la criptografía como mecanismo para salvaguardar la confidencialidad e integridad de la información contenida en los diferentes sistemas.

Nota: Tomado de NIST (2018).

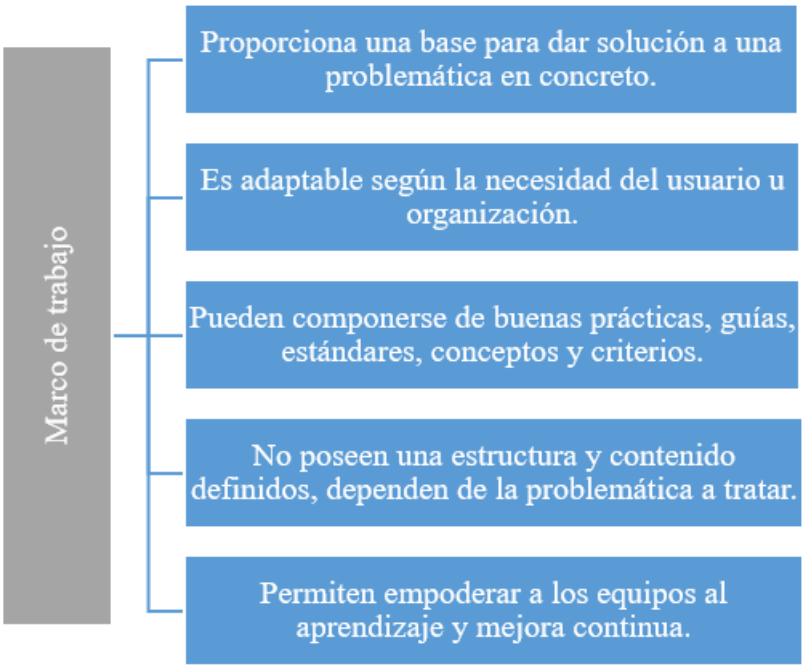
2.2.8. Marco de Trabajo

De acuerdo con Marín, et al. (2018), un marco de trabajo o framework se puede definir como un conjunto de buenas prácticas, recomendaciones, conceptos y criterios enfocados a tratar una temática o problema en particular, siendo su aplicación libre para el usuario final ya que no establece lineamientos y la aplicación de los diferentes conceptos dependerá de cada usuario y su necesidad específica.

En general, los marcos de trabajo no están ligados a una disciplina en particular por lo que su aplicabilidad es extensa y sobre todo en materia de ciberseguridad, a manera de ejemplo, es importante mencionar al Cybersecurity Framework del NIST (NIST, 2018) que fue desarrollado con el objetivo de ayudar a las organizaciones de todo tipo y tamaño a gestionar de forma adecuada los riesgos de ciberseguridad a los que pueden estar sujetos en el desarrollo de sus actividades diarias. Sin embargo, su contenido es extenso y no aborda específicamente la temática objeto de estudio en esta investigación, es decir, el teletrabajo.

2.2.8.1. Características de un Marco de Trabajo. El autor Martínez, (2020) que un marco de trabajo, evidencia una estructura flexible que sirve como base para abordar y resolver problemas específicos. Se adapta a las necesidades de usuarios u organizaciones y puede incluir buenas prácticas, guías, estándares, conceptos y criterios relevantes para la situación particular. No tiene una estructura rígida y su contenido varía según la problemática a tratar. Permite capacitar a los equipos, fomentando el aprendizaje y la mejora continua. Estas características se presentan en la figura 7.

Figura 7.
Características de un marco de trabajo



Nota: adaptado de Martínez, (2020).

2.3. Marco Legal

Las bases legales que sustentan 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 son las siguientes:

La Laye Orgánica de Telecomunicaciones (2015) que expone en el Artículo 7 que el gobierno de Ecuador debe asegurar la protección de las comunicaciones, lo que abarca resguardar la información y los datos personales en el ámbito de las telecomunicaciones.

De igual manera, el Código Orgánico de la Economía Social de los Conocimientos, creatividad e innovación (2016) en el Artículo 87, expones que las compañías que funcionan en la industria digital deben implementar medidas de seguridad para resguardar la información y los datos personales de sus clientes.

El Reglamento de Teletrabajo del Ministerio del Trabajo (2022) expone en el Artículo 11 las empresas que empleen personal en modalidad de teletrabajo tienen la responsabilidad de implementar medidas de seguridad para salvaguardar la información y los datos personales de sus empleados.

El presente trabajo toma como referencia las directrices y lineamientos establecidos en el acuerdo ministerial No. MDT-2022-237 publicado en el Registro Oficial No. 234 con fecha 20 de enero del 2023, y que fue creado con el objetivo de regular el ejercicio de la actividad del teletrabajo en el territorio ecuatoriano, así como garantizar el derecho a la desconexión de los empleados.

El Acuerdo Ministerial No. 025-2019 (MINTEL, 2019) y su anexo EGSI versión 2.0, contiene las buenas prácticas que las instituciones públicas deben implementar sobre seguridad de la información y medidas de protección a su infraestructura; así como a los sistemas informáticos que custodian con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos de seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados, minimizando los riesgos ante posibles ataques y amenazas que pretendan acceder o alterar la información del Estado. Tiene como base la norma técnica ecuatoriana INEN ISO/IEC 27001:2013 y está compuesto por 14 dominios y 114 controles que deben ser implementados de manera obligatoria.

Para el caso de esta investigación este instrumento legal tiene un gran peso puesto que la base para establecer el marco de buenas prácticas está alineada con los controles de norma ISO 27002:2022. Además, el EGSI ha sido realizado en base a un análisis que permite enmarcar lo más relevante de la norma internacional y delimitarlo o encasillarlo dentro de las necesidades que tiene el Ecuador en cuanto a gestión de seguridad de la información y al mismo tiempo asegura el cumplimiento de otras normativas legales como la Ley Orgánica de Protección de Datos Personales (LOPDP) y la Política Nacional de Ciberseguridad que fue creada con el objetivo de construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población y la protección de los bienes jurídicos del Estado en el ciberespacio, encaminando acciones para garantizar un ciberespacio seguro.

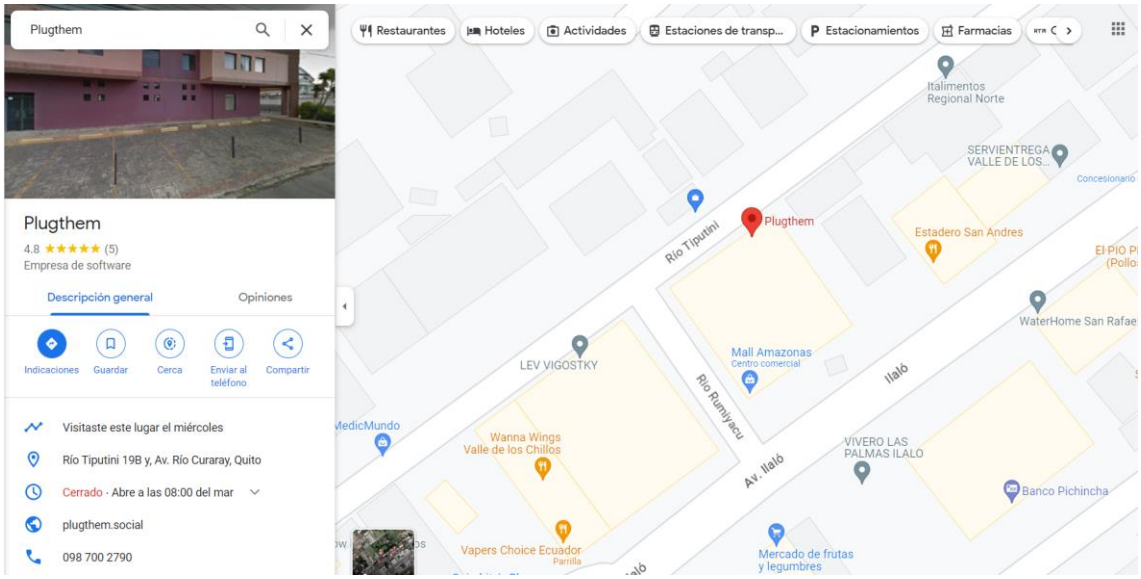
CAPITULO III
MARCO METODOLÓGICO

3.1. Descripción del área de estudio / Descripción del grupo de estudio

El proyecto de investigación fue ejecutado en la empresa de Desarrollo de software y Business Analytics Plugthem S.A., ubicada en la Ciudad de Quito, Provincia de Pichincha. La empresa se especializa en desarrollar software a medida y transformar datos de experiencia del cliente (CX Data) mediante herramientas propietarias que permiten escuchar la voz de los clientes en tiempo real.

Figura 8

Ubicación de la empresa de desarrollo de software Plugthem S.A.



Fuente: Tomado de Google Maps (2023).

Actualmente cuenta con un aproximado de 40 empleados distribuidos en 6 áreas organizativas dentro de su sede principal en la ciudad de Quito: Comercial, Productos, Proyectos, Talento Humano, Financiero y Tecnologías de la Información. La empresa tiene presencia en varios países de la región como Colombia, México, Estados Unidos, entre otros, y entre sus principales herramientas de innovación tecnológica se encuentran el programa VOC (Voice of the Customer), programa VOE (Voice of the Employee), la plataforma de e-learning PlugTraining y la plataforma de reconocimiento de empleados PlugRewards.

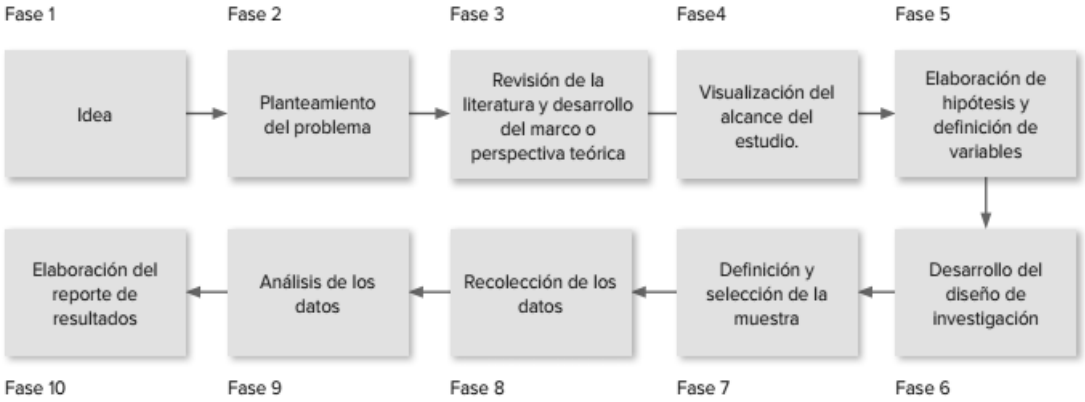
3.2. Enfoque y tipo de investigación

El enfoque de la presente investigación es de carácter cuantitativo, ya que de acuerdo con Hernández y Mendoza (2018) permite determinar características del objeto de estudio, mediante la importancia asignada a la recolección de datos y aplicación de métodos estadísticos. Además, se ejecuta de forma sistematizada, siguiendo una serie de pasos rigurosos.

En torno al enfoque cuantitativo, destaca a existencia de pasos que deben ser considerados para el desarrollo del estudio. Cada uno de ellos debe ser seguido con rigurosidad, al respecto Hernández y Mendoza (2018) sostienen que estos procesos se encuentran ordenados secuencialmente. El punto de partida inicia con la definición de una idea que se acota, lo que conduce a la formulación de objetivos y preguntas de investigación. Luego, se lleva a cabo una revisión exhaustiva de la literatura existente, lo que permite construir un marco teórico sólido. Luego, se determinan y definen las variables clave. Seguidamente se cumplen otras fases, a continuación, se presenta la figura 8, para una ilustración completa de los pasos a seguir.

Figura 9

Pasos del enfoque cuantitativo



Nota: Tomado de Hernández y Mendoza (2018).

En lo relacionado con este estudio, el surgimiento de la idea parte de la actividad que se lleva a cabo en la empresa Desarrollo de software y Business Analytics Plugthem S.A., razón por la cual se consideró pertinente establecer un marco de trabajo de buenas

prácticas de ciberseguridad en el teletrabajo para las empresas de desarrollo de software, a través de la síntesis de resultados de un estudio exploratorio.

También es necesario mencionar, que se estableció como diseño de estudio el no experimental y transversal. El primero permite entender que no se realizó manipulación de las variables que, para este estudio son propuestas que en este caso son: prácticas de ciberseguridad, teletrabajo, controles establecidos en la norma ISO 27002:2022 y la NIST SP 800-46, desarrollo de software. Es decir, que la información se recogió sin alterar los datos y ninguna de las condiciones o comportamientos. Lo que quiere decir que se trataron de manera objetiva. Para ello se seleccionaron cuidadosamente los casos o las unidades a medir, teniendo en cuenta el contexto específico en términos de lugar y tiempo.

En cuanto al tipo de investigación seleccionado se trata del descriptivo, exploratoria y de campo. El carácter descriptivo, como bien lo menciona describe los elementos presentes a partir de los datos obtenidos. Mientras que el exploratorio se adquiere cuando se trata de conocer acerca de las variables; además, permite identificar de manera clara un problema. En relación con lo de campo viene determinado porque los datos se recogen directamente del lugar donde ocurren los hechos (Pereyra, 2022).

Esta investigación, trata el tema de la ciberseguridad en el teletrabajo por consiguiente fue necesario describir los elementos que subyacen a partir de la actividad de desarrollo de software. Al adentrarse en la exploración se profundizó en las variables que ya fueron mencionadas, todo en el contexto de la empresa Desarrollo de software y Business Analytics Plugthem S.A.

3.3. Procedimiento de Investigación

Fase 1. Identificar las prácticas de ciberseguridad utilizadas por las empresas que operan bajo la modalidad de teletrabajo.

Se realizó una revisión analítica de la literatura en bases digitales de carácter científico como IEEE Xplore, Scopus y Google Académico tanto en idioma inglés como en español utilizando palabras clave y descriptores que permitan identificar información relevante en relación con las variables. Posteriormente se extrajo la información de forma sintetizada.

Fase 2. Diseñar un marco de trabajo con los mecanismos y procedimientos de ciberseguridad en el teletrabajo apropiados para las empresas de desarrollo de software basada en los controles establecidos en la norma ISO 27002:2022 y la NIST SP 800-46.

El marco de trabajo se diseñó según los controles relacionados con el teletrabajo especificados en la norma ISO 27002:2022 y las buenas prácticas establecidas en la NIST SP 800-46 junto con los resultados de la revisión analítica de la literatura. Para esto se estableció un conjunto de fases y procedimientos con enfoque en la ciberseguridad en el teletrabajo para las empresas de desarrollo de software.

Fase 3. Evaluar el impacto del marco de trabajo de ciberseguridad en la ejecución de los procesos de desarrollo de software de la empresa Plugthem S.A.

Se aplicó el marco de trabajo y se realizaron encuestas a los trabajadores de la empresa Plugthem S.A. con el fin de conocer cuál es su percepción en torno a los beneficios y facilidades del marco diseñado, así como para identificar posibles puntos de mejora. Las encuestas se aplicaron utilizando la herramienta Microsoft Forms y contaron con preguntas de tipo opción múltiple con el fin de poder tabular y analizar los resultados de forma más objetiva.

3.4. Consideraciones Bioéticas

El desarrollo de la investigación se realizó con todos los permisos del caso por parte de la empresa desarrolladora de software Plugthem S.A., cuyas autoridades emitieron una autorización por escrito para poder llevar a cabo el proceso de validación del marco de trabajo que se pretende diseñar.

Así mismo, los empleados de Plugthem S.A. fueron informados oportunamente sobre los aspectos relevantes que comprenden a esta investigación de modo que puedan conocer la importancia de su participación en el proceso, así como sus obligaciones, derechos y beneficios a los que estarán sujetos. Además, se mantuvo y respetó el anonimato de todos los participantes e involucrados.

CAPITULO IV
RESULTADOS Y DISCUSIÓN

En este apartado se presentan los resultados y la discusión de una manera organizada, estos se desarrollaron según la etapa de la investigación y los objetivos planteados, su principal acción es ayudar a comprender y expresar coherentemente los hallazgos de la investigación y exponer el razonamiento del investigador a lo largo del capítulo. Para Hernández y Mendoza (2018), esto implica incluir reflexiones y puntos de vista partiendo de la interpretación de los datos.

4.1. Resultados

El orden que sigue para este capítulo inicia con la presentación de los datos obtenidos del análisis del Alfa de Cronbach, a tales efectos se puede visualizar una tabla que contiene el rango la fiabilidad del instrumento. En ese sentido, Rodríguez y Reguant (2020) señalaron que los valores entre 0,70 y 0,90 denotan que hay buena consistencia interna, para el caso de este estudio el resultado se muestra en la tabla 6.

Tabla 6.
Alfa de Cronbach

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
0,829	17

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Luego, se realizó el análisis factorial para ello fue necesario aplicar lo recomendado por Rodríguez y Reguant (2020) quienes manifestaron que el Alfa de Cronbach puede mejorarse a partir de la eliminación de elementos. Por esta razón, se decidió eliminar uno para obtener mayor rango de fiabilidad esto se puede observar en la tabla 7 donde se muestra el rango si se elimina un elemento.

Tabla 7.

Análisis factorial

Estadísticas de total de elemento				
	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
¿La empresa le ha ofrecido capacitación acerca de seguridad informática?	55,87	108,375	0,268	0,797
¿Usa redes de WIFI en todo lugar?	54,83	121,623	-0,297	0,829
¿El trabajo que se ejecuta se mide por resultados y no por horas laboradas?	54,62	110,071	0,132	0,807
¿Las actividades de teletrabajo se pueden ejecutar desde cualquier espacio?	54,46	106,955	0,196	0,805
¿El teletrabajo desarrollado permite adaptarse a cambios?	54,25	100,283	0,460	0,785
¿Hay flexibilidad de horarios al desarrollar el teletrabajo?	54,00	110,348	0,117	0,808
¿El teletrabajo permite que ocurra capacitación continua?	54,58	101,906	0,590	0,780
¿Se tratan temas relacionados con la política de seguridad de la información?	55,17	107,884	0,305	0,795
¿Los roles de Seguridad de la información y Responsabilidades se encuentran claramente definidas con todos los clientes y empleados?	54,92	95,384	0,686	0,769
¿El personal se rige de acuerdo con la política de seguridad definida?	54,46	100,868	0,553	0,780
¿Se recoge y analiza la información relacionada a amenazas de seguridad?	55,12	101,418	0,480	0,784
¿Se menciona la existencia de un inventario de activos y los responsables de estos?	54,79	99,563	0,432	0,787
¿Usa las normas o reglas para el uso adecuado de activos de información?	54,21	103,998	0,496	0,785
¿El personal devuelve activos al finalizar la relación laboral?	53,21	108,433	0,333	0,794
¿Se gestionan de manera adecuada permisos de accesos y las actualizaciones necesarias?	54,00	102,870	0,486	0,785
¿Están establecidos los procesos de acceso, uso y remoción de la información en la nube?	54,92	92,775	0,669	0,768

¿La empresa está preparada para la gestión de incidentes de seguridad, incluso hay roles definidos?	54,71	100,476	0,447	0,786
¿Se revisa constantemente que se cumplan las políticas de seguridad?	55,04	99,346	0,643	0,775

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Posteriormente sigue en orden y por variable la presentación de la interrogante, tabla y gráfico, sí como la interpretación y análisis de los datos, de las encuestas aplicadas en este caso a los empleados de diferentes áreas y a los que son desarrolladores, finalmente se puede visualizar la discusión generada a partir de los hallazgos obtenidos al aplicar la encuesta a los empleados de la empresa Plugthem, S.A.

Variable: prácticas de ciberseguridad

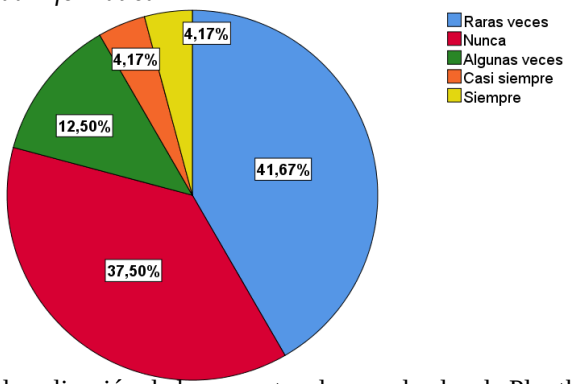
Pregunta 1: ¿La empresa le ha ofrecido adiestramiento acerca de seguridad informática? (Ver tabla 8 y figura 9).

Tabla 8.
Adiestramiento acerca de seguridad informática

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Raras veces	10	41,7	41,7	41,7
	Nunca	9	37,5	37,5	79,2
	Algunas veces	3	12,5	12,5	91,7
	Casi siempre	1	4,2	4,2	95,8
	Siempre	1	4,2	4,2	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 10
Adiestramiento acerca de seguridad informática



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si la empresa les ha ofrecido adiestramiento en seguridad informática, los consultados respondieron de la siguiente manera 41.7% raras veces lo que sugiere que en la mayoría de las ocasiones no se proporciona capacitación. 37.5% nunca lo que indica que en Plugthem S.A. no se ha abordado este punto. 12.5% algunas veces lo que permite conocer con esa frecuencia se les ha facilitado información relacionada con el tema. 4,2% refirieron que casi siempre y siempre, lo que muestra que una minoría de trabajadores han recibido capacitaciones con regularidad. De manera que, 62,5% de los empleados reconoce que se ofrece formación en este punto. Sin embargo, un 37,5% señala que nunca han recibido.

Variable: teletrabajo

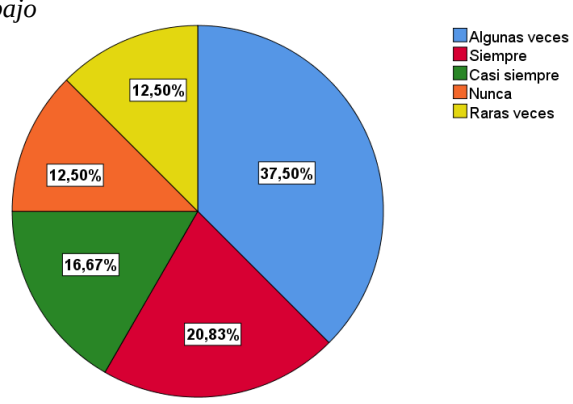
Pregunta 2: ¿El trabajo que se ejecuta se mide por resultados y no por horas laboradas? (Ver tabla 9 y figura 10).

Tabla 9.
Forma de medir el teletrabajo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Algunas veces	9	37,5	37,5	37,5
	Siempre	5	20,8	20,8	58,3
	Casi siempre	4	16,7	16,7	75,0
	Nunca	3	12,5	12,5	87,5
	Raras veces	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 11
Forma de medir el teletrabajo



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar sobre si el trabajo que realizan se mide por resultados y no por horas laboradas, los encuestados respondieron de la siguiente manera 37.5% algunas veces lo que sugiere que existe cierta flexibilidad en la forma en que se evalúa el desempeño, pero no es constante. 20.8% siempre esto indica que un grupo significativo de trabajadores experimenta una valoración basada en lo resultante. 16.7% casi siempre lo que muestra una tendencia hacia una ponderación direccionada al logro. 12.5% nunca lo que demuestra que una minoría siente que la forma en que rinden está estrictamente ligada al tiempo dedicado. 12.5% raras veces lo que refleja una falta de consistencia al ejecutar evaluaciones de rendimiento en Plugthem S.A. Finalmente se evidencia que 87,5% de los empleados confirman que los resultados de teletrabajo se miden por resultados. Frente un 12,5% que no lo considera así.

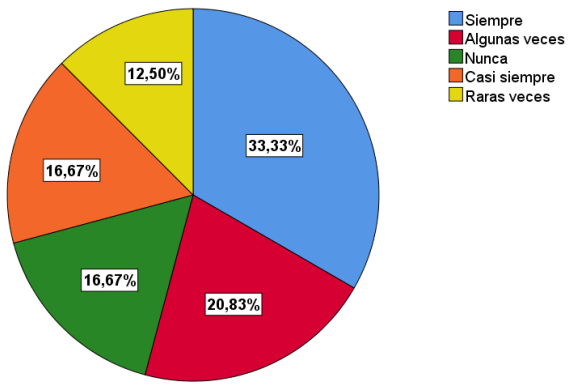
Pregunta 3: ¿Las actividades de teletrabajo se pueden ejecutar desde cualquier espacio? (Ver tabla 10 y figura 11).

Tabla 10.
Actividades de teletrabajo y espacios

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	8	33,3	33,3	33,3
	Algunas veces	5	20,8	20,8	54,2
	Nunca	4	16,7	16,7	70,8
	Casi siempre	4	16,7	16,7	87,5
	Raras veces	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 12
Actividades de teletrabajo y espacios



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Ante la pregunta sobre si las actividades de teletrabajo se pueden ejecutar desde cualquier espacio. Respondieron de la siguiente forma 33.3% siempre, lo que evidencia que un tercio experimenta una alta flexibilidad en términos de dónde llevar a cabo sus labores. 20.8% algunas veces lo que indica que, en ocasiones, escogen el lugar del cual trabajan, pero no de manera constante.16.7% afirmó que nunca se les hace fácil realizar sus tareas en diversos lugares. Esto sugiere algunas restricciones o limitaciones en cuanto a la elección del sitio para trabajar. 16.7% de señaló que casi siempre lo que muestra una tendencia flexible, aunque no constantemente. 12.5% de los empleados mencionó que raras veces lo que refleja una falta de consistencia en la posibilidad de cumplir la jornada en diferentes sitios. Los datos reflejan que 83,3% de los encuestados pueden realizar su labor desde diferentes lugares. Frente un 16,7% que no puede lograrlo.

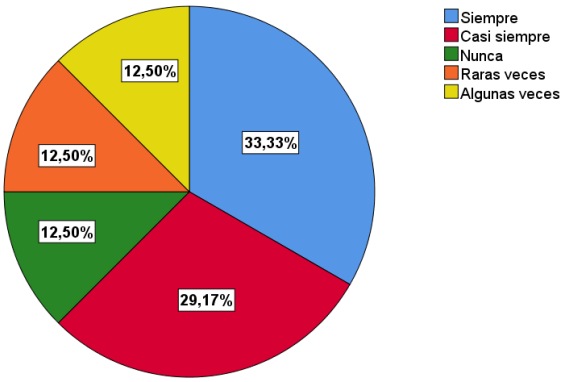
Pregunta 4: ¿El teletrabajo desarrollado permite adaptarse a cambios? (Ver tabla 11 y figura 12).

Tabla 11.
Teletrabajo y cambios

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	8	33,3	33,3	33,3
	Casi siempre	7	29,2	29,2	62,5
	Nunca	3	12,5	12,5	75,0
	Raras veces	3	12,5	12,5	87,5
	Algunas veces	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 13
Teletrabajo y cambios



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar a los empleados si el teletrabajo desarrollado les permite adaptarse a cambios, las respuestas fueron las siguientes 33.3% siempre, lo que sugiere que un tercio

de los colaboradores siente que esta modalidad les proporciona una alta capacidad de acomodo a situaciones variables. 29.2% mencionó que casi siempre lo que indica que una proporción significativa que trabajar de esa forma les brinda ofrece solidez para afrontar tareas y responsabilidades.12.5% nunca lo que muestra que una minoría considera que no tienen efectividad ante situaciones cambiantes. 12.5% raras veces lo que refleja falta de consistencia para ajustarse en este contexto. 12.5% algunas veces, demostrando que en ocasiones pueden enfrentar transformaciones, pero no de manera constante. Los datos reflejan que 77,5% de los consultados se han podido ajustar a cambios a partir de la modalidad establecida. Frente un 12,5% que no lo ha logrado.

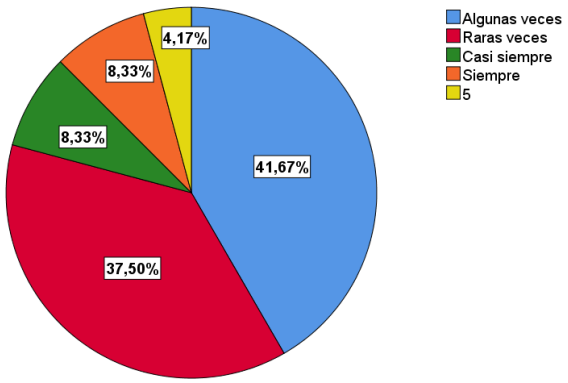
Pregunta 5: empresa ¿El teletrabajo permite que ocurra capacitación continua? (Ver tabla 12 y figura 13).

Tabla 12.
Teletrabajo y capacitación

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Algunas veces	10	41,7	41,7	41,7
	Raras veces	6	25,0	25,0	66,7
	Casi siempre	4	16,7	16,7	83,3
	Siempre	4	16,7	16,7	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 14
Teletrabajo y capacitación



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar a los empleados si el teletrabajo permite que ocurra capacitación continua, respondieron de la siguiente forma 41.7% algunas veces, lo que sugiere que una parte significativa de los colaboradores experimenta aprendizaje durante esta modalidad,

aunque no de manera constante. 25.0% raras veces esto indica que una proporción considerable siente que la adquisición de conocimiento es limitada cuando trabajan de remotamente. 16.7% casi siempre, lo que demuestra que un grupo minoritario ha experimentado oportunidades regulares para capacitarse. 16.7% siempre, de modo que un porcentaje similar a la categoría anterior considera que pueden aprender de constantemente en el entorno. Los resultados demuestran que 100% de los consultados han podido recibir capacitación permanente.

Variable control organizacional

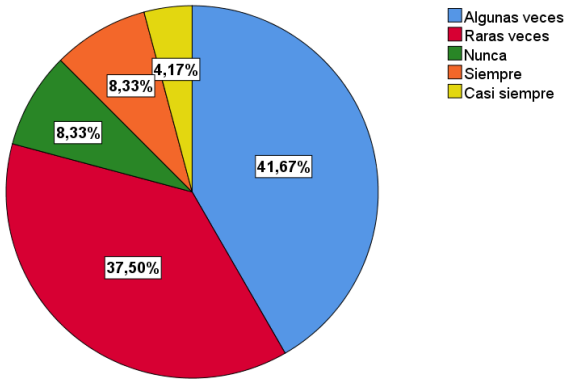
Pregunta 6: ¿Se tratan temas relacionados con la política de seguridad de la información? (Ver tabla 13 y figura 14).

Tabla 13.
Políticas de seguridad en la empresa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Algunas veces	10	41,7	41,7	41,7
	Raras veces	9	37,5	37,5	79,2
	Nunca	2	8,3	8,3	87,5
	Siempre	2	8,3	8,3	95,8
	Casi siempre	1	4,2	4,2	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 15
Políticas de seguridad en la empresa



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar a los empleados si sobre si se abordan temas relacionados con la política de seguridad de la información, respondieron así 41.7% algunas veces, lo que sugiere que una parte significativa experimenta discusiones y capacitación relacionadas con la temática, pero no de forma constante. 37.5% mencionó que raras veces, lo que

demuestra que algunos consideran que el tema se aborda de manera poco frecuente. 8.3% afirmó que nunca se mencionan estas políticas. 8.3% señaló que siempre se reflejando un porcentaje similar a la categoría anterior. 4.2% indicó que casi siempre lo que muestra que una minoría ha recibido capacitaciones acerca de este punto. Los resultados demuestran que 91,7% de los consultados conocen información relativa a la seguridad y las políticas. Frente un 8,3% que señala no saber del tema.

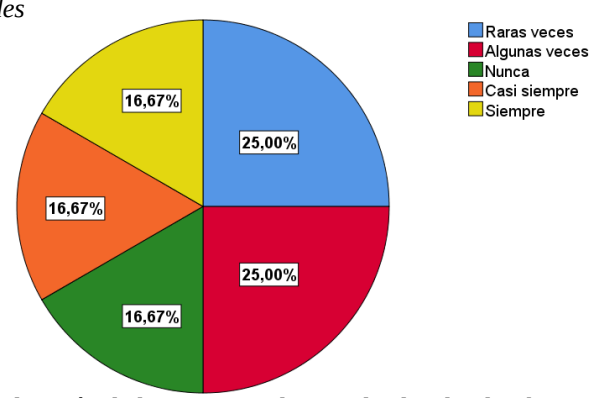
Pregunta 7 ¿Los roles de Seguridad de la información y Responsabilidades se encuentran claramente definidas con todos los clientes y empleados? (Ver tabla 14 y figura 15).

Tabla 14.
Definición de roles y responsabilidades

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Raras veces	6	25,0	25,0	25,0
	Algunas veces	6	25,0	25,0	50,0
	Nunca	4	16,7	16,7	66,7
	Casi siempre	4	16,7	16,7	83,3
	Siempre	4	16,7	16,7	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 16
Definición de roles y responsabilidades



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar acerca definición de roles y responsabilidades 25.0% indicó que raras veces. Lo que permite conocer que un cuarto de los empleados percibe es poco común. 25.0% mencionó que algunas veces. Lo que refleja una percepción similar a la categoría anterior y sugiere que la claridad es intermitente. 16.7% afirmó que nunca, lo que demuestra que una minoría siente que esto es inexistente en la organización. 16.7%

consideró que casi siempre de manera que una proporción parecidos a los resultados anteriores aprecia que con frecuencia se establecen. 16.7% contestó que siempre lo que muestra que pocos conocen lo establecido en referencia a la temática. Los resultados muestran que 82,3 de los encuestados conocen de los roles y responsabilidades con los clientes. Frente un 16,7% que indica no saberlo.

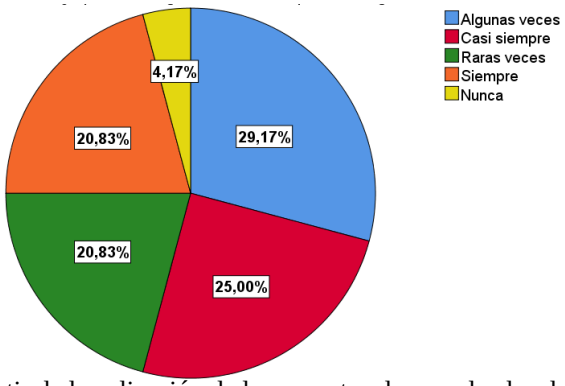
Pregunta 8 ¿El personal se rige de acuerdo con la política de seguridad definida? (Ver tabla 15 y figura 16).

Tabla 15.
Personal y políticas definidas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Algunas veces	7	29,2	29,2	29,2
	Casi siempre	6	25,0	25,0	54,2
	Raras veces	5	20,8	20,8	75,0
	Siempre	5	20,8	20,8	95,8
	Nunca	1	4,2	4,2	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 17
Personal y políticas definidas



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si el personal se rige de acuerdo con la política de seguridad definida 29.2% indicó que algunas veces. Esto sugiere que una parte significativa percibe que es intermitente. 25.0% mencionó que casi siempre lo que indica que un grupo importante experimenta un alto nivel de responsabilidad en cumplir lo establecido. El 20.8% de los empleados afirmó que raras veces lo que evidencia que una proporción considerable de opina que es poco frecuente. 20.8% señaló que siempre lo que refleja que algunos sienten que se cumple de manera constante. Finalmente 4.2% respondieron que nunca lo que

demuestra que una minoría siente que este aspecto es inexistente. Los resultados demuestran que un 95,8% de los consultados siguen la política definida. Frente un 4,2 que indica no realizarlo.

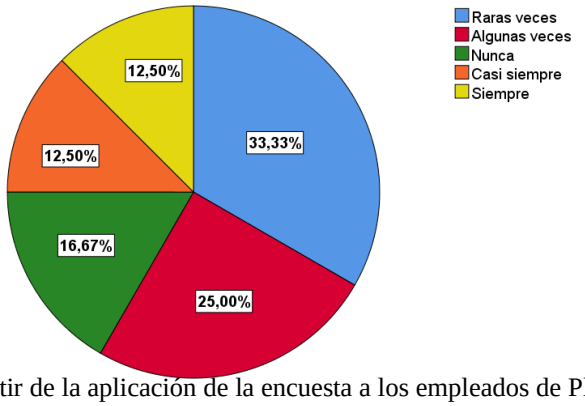
Pregunta 9 ¿Se recoge y analiza la información relacionada a amenazas de seguridad? (Ver tabla 16 y figura 17).

Tabla 16.
Tratamiento de información relacionada con amenazas de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Raras veces	8	33,3	33,3	33,3
	Algunas veces	6	25,0	25,0	58,3
	Nunca	4	16,7	16,7	75,0
	Casi siempre	3	12,5	12,5	87,5
	Siempre	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 18
Tratamiento de información relacionada con amenazas de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si se recoge y analiza la información relacionada a amenazas de seguridad 33.3% indicó que raras veces. Esto sugiere que una parte significativa de los empleados perciben que la actividad es poco común. 25.0% mencionó que algunas veces. Lo que indica que entienden que en ocasiones se realiza, pero no de manera constante. 16.7% afirmó que nunca, evidenciando que una minoría siente que este control es inexistente en la organización. 12.5% respondió que casi siempre lo que demuestra que una proporción menor considera que la recopilación y análisis son frecuentes. 12.5% señaló que siempre, reflejando una percepción similar a la categoría anterior, se puede señalar que algunos conocen que se ejecuta esta acción permanentemente. Los resultados

demuestran que 83,3% de los encuestados conocen que se recoge la información aerca de amenaza de la seguridad y se analiza. Frente un 16,7% que desconoce este procedimiento.

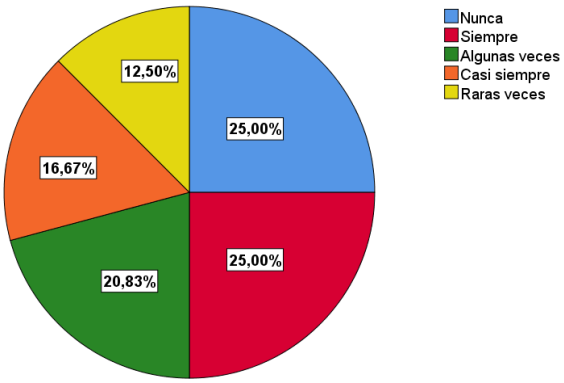
Pregunta 10 ¿Se menciona la existencia de un inventario de activos y los responsables de estos? (Ver tabla 17 y figura 18).

Tabla 17.
Inventario y responsables

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	6	25,0	25,0	25,0
	Siempre	6	25,0	25,0	50,0
	Algunas veces	5	20,8	20,8	70,8
	Casi siempre	4	16,7	16,7	87,5
	Raras veces	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 19
Inventario y responsables



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si se menciona la existencia de un inventario de activos y los responsables de estos, 25.0% indicó que nunca. Esto sugiere que una cuarta parte de los empleados siente que esta información no se aborda o informa en la organización. 25.0% mencionó que siempre evidenciando que un porcentaje similar a la categoría anterior conoce acerca del tema. 20.8% afirmó que algunas dejando ver que, en ocasiones se trata, pero no de manera constante. 16.7% respondió que casi siempre lo que permite señalar que una proporción menor maneja la temática. Los resultados evidencian que 75% de los empleados conoce acerca del inventario de activos. Frente un 25% que no está claro.

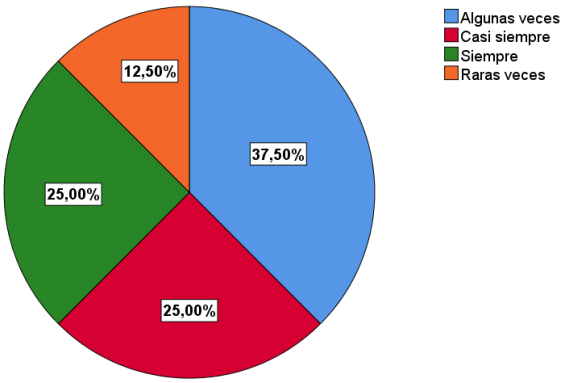
Pregunta 11 ¿Usa las normas o reglas para el uso adecuado de activos de información? (Ver tabla 18 y figura 19).

Tabla 18.
Normas y uso adecuado de activos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Algunas veces	9	37,5	37,5	37,5
	Casi siempre	6	25,0	25,0	62,5
	Siempre	6	25,0	25,0	87,5
	Raras veces	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 20
Normas y uso adecuado de activos



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si se usan las normas o reglas para el uso adecuado de activos de información, 37.5% indicó que algunas veces, esto sugiere que una parte significativa de los empleados las utiliza intermitentemente. 25.0% mencionó que casi siempre lo que indica que un grupo importante cumple lo pautado. 25.0% señaló que siempre, reflejando que una proporción similar a la categoría anterior cumplen de manera constante. 12.5% respondió que raras veces por lo que se demuestra que una minoría siente que lo estipulado se sigue con poca frecuencia. Los resultados demuestran que 100% de los consultados siguen las normas para el cuidado de la información.

Pregunta 12 ¿El personal devuelve activos al finalizar la relación laboral? (Ver tabla 19 y figura 20).

Tabla 19.
Devolución de activos

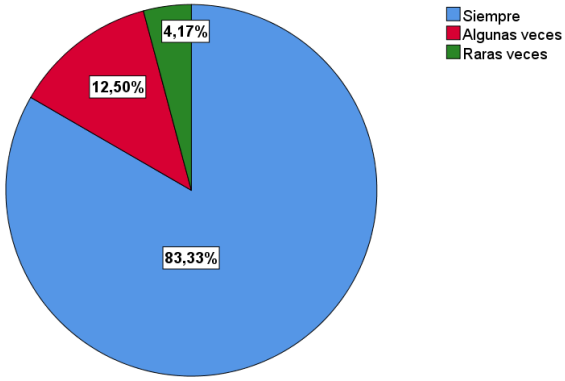
	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado

Válido	Siempre	20	83,3	83,3	83,3
	Algunas veces	3	12,5	12,5	95,8
	Raras veces	1	4,2	4,2	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 21

Devolución de activos



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si el personal devuelve activos al finalizar la relación laboral, 83.3% indicó que siempre el personal devuelve activos. Esto sugiere que la gran mayoría siente que la devolución de estos al finalizar la relación laboral es una práctica constante y consistente. 12.5% de los empleados mencionó que algunas veces lo que indica que un grupo minoritario considera que puede ser intermitente en algunos casos. 4.2% afirmó que raras veces, mostrando que una minoría aún menor percibe que poco común.

Pregunta 13 ¿Se gestionan de manera adecuada permisos de accesos y las actualizaciones necesarias? (Ver tabla 20 y figura 21).

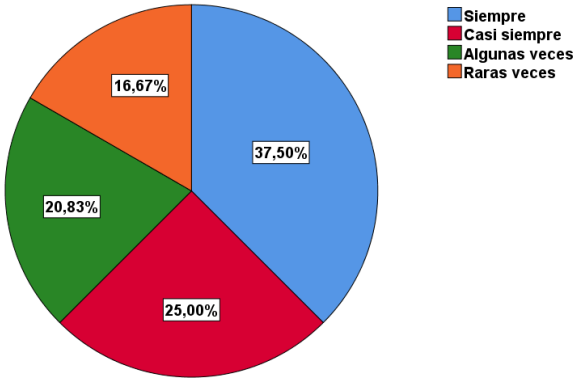
Tabla 20.

Gestión de permisos y actualizaciones

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	9	37,5	37,5	37,5
	Casi siempre	6	25,0	25,0	62,5
	Algunas veces	5	20,8	20,8	83,3
	Raras veces	4	16,7	16,7	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 22
Gestión de permisos y actualizaciones



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si se gestionan de manera adecuada los permisos de accesos y las actualizaciones necesarias, 37.5% indicó que siempre, lo que sugiere que una parte significativa percibe que la gestión es constante y efectiva. 25.0% mencionó que casi siempre, demostrando que un grupo siente que es mayoritariamente eficiente, aunque puede haber excepciones. 20.8% afirmó que algunas veces, lo que muestra que una proporción considerable capta que es intermitente. 16.7% respondió que raras veces, reflejando que una minoría considera que la acción es poco común. Los resultados demuestran que 100% de los consultados conocen que se gestionan de manera adecuada permisos y actualizaciones.

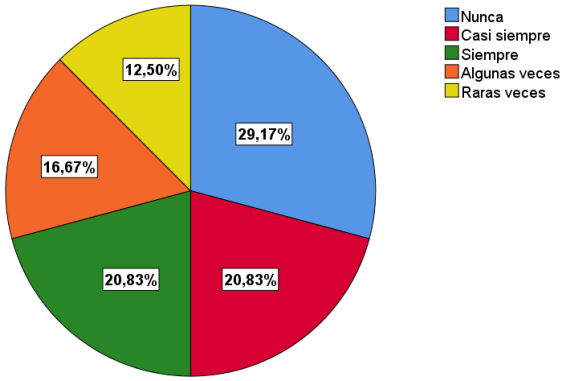
Pregunta 14 ¿Están establecidos los procesos de acceso, uso y remoción de la información en la nube? (Ver tabla 21 y figura 22).

Tabla 21.
Procesos de gestión en la nube

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	7	29,2	29,2	29,2
	Casi siempre	5	20,8	20,8	50,0
	Siempre	5	20,8	20,8	70,8
	Algunas veces	4	16,7	16,7	87,5
	Raras veces	3	12,5	12,5	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 23
Procesos de gestión en la nube



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si sobre si están establecidos los procesos de acceso, uso y remoción de la información en la nube, 29.2% indicó que nunca, lo que permite conocer que una parte significativa siente que nunca se establece esta acción. 20.8% mencionó que casi siempre lo que demuestra que un grupo considera que estas acciones son mayoritariamente establecidas y seguidas. 20.8% señaló que siempre, reflejando una percepción similar a la categoría anterior y sugiere que se lleva a cabo de forma constante. 16.7% afirmó que algunas lo que denota que una proporción considerable percibe que es intermitente. 12.5% respondió que raras veces, de manera que una minoría cree que es una práctica poco común en la empresa. Los resultados demuestran que 71,8 de los consultados conocen el proceso a ejecutarse en la nube. Frente un 29,2% que no lo sabe. Esto probablemente se encuentra asociado al departamento donde se desempeñan.

Pregunta 15 ¿La empresa está preparada para la gestión de incidentes de seguridad, incluso hay roles definidos? (Ver tabla 22 y figura 23).

Tabla 22.
Preparación para incidentes de seguridad

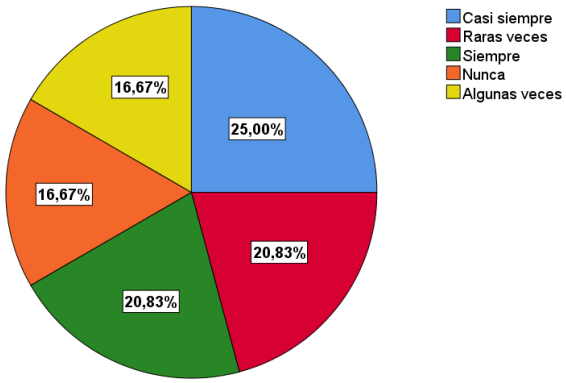
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	6	25,0	25,0	25,0
	Raras veces	5	20,8	20,8	45,8
	Siempre	5	20,8	20,8	66,7

	Nunca	4	16,7	16,7	83,3
	Algunas veces	4	16,7	16,7	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 24

Preparación para incidentes de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si sobre si la empresa está preparada para la gestión de incidentes de seguridad, incluso si hay roles definidos, 25.0% que la empresa está preparada lo que sugiere que un grupo significativo siente que la empresa cuenta con una preparación sólida en este aspecto. 20.8% mencionó raras veces, lo que implica que esta acción es poco común o poco consistente. 20.8% respondió que siempre, reflejando que una proporción similar a la categoría "Raras veces" siente que la preparación es constante. 16.7% nunca, lo que sugiere que para este grupo hay ineficiencias en torno al punto. 16.7% afirmó algunas veces, lo que evidencia intermitencia en este aspecto. Los resultados demuestran que en un 83,3% la empresa está preparada y con roles definidos en caso de incidentes. Frente un 16,7% que no lo considera así.

Pregunta 16 ¿Se revisa constantemente que se cumplan las políticas de seguridad? (Ver tabla 23 y figura 24).

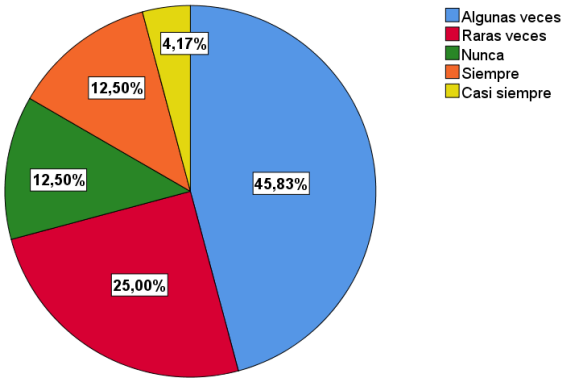
Tabla 23.

Revisión constante de cumplimiento de normas de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Algunas veces	11	45,8	45,8	45,8
	Raras veces	6	25,0	25,0	70,8
	Nunca	3	12,5	12,5	83,3
	Siempre	3	12,5	12,5	95,8
	Casi siempre	1	4,2	4,2	100,0
	Total	24	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Figura 25
Revisión constante de cumplimiento de normas de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si se revisa constantemente que se cumplan las políticas de seguridad 45.8% indicó que algunas veces, esto sugiere que una parte significativa de los empleados percibe que la revisión del cumplimiento de políticas de seguridad es intermitente. 25.0% mencionó que raras veces, demostrando que un siente que esta revisión es poco común. 12.5% afirmó que nunca lo que muestra que para una minoría esta revisión nunca ocurre. 12.5% señaló que siempre lo que evidencia que para algunos la revisión es constante. 4.2% de respondió que casi siempre se revisa sumándose la percepción al grupo que respondió que siempre. Los resultados demuestran que la empresa en un 77,5 % realiza revisiones constantes para garantizar el cumplimiento de las políticas de seguridad. No obstante, para 12,5% de los empleados no se percibe igual.

Encuesta aplicada a los empleados desarrolladores de la empresa.

Variable reducción de vulnerabilidades

Pregunta 1 ¿Se usa contraseñas en cada uno de los procesos y clientes que se administran? (Ver tabla 24 y figura 25).

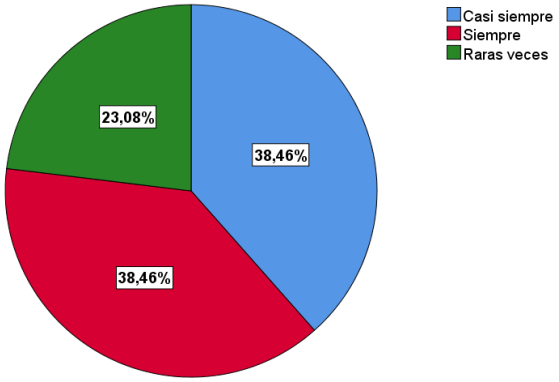
Tabla 24.
Uso de contraseña

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	5	38,5	38,5	38,5
	Siempre	5	38,5	38,5	76,9
	Raras veces	3	23,1	23,1	100,0

	Total	13	100,0	100,0

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 26
Uso de contraseñas



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Los resultados de la pregunta sobre el uso de contraseñas en cada uno de los procesos y clientes administrados revelan que el 38.5% de los encuestados indicaron que casi siempre, mientras que otro 38.5% afirmó que siempre se emplean. El 23.1% mencionó que raras veces. Estos datos sugieren una diversidad en la frecuencia de uso de estas, con una parte significativa indicando prácticas de seguridad constantes también se evidencia un grupo que admite un uso menos regular o esporádico. De acuerdo con la información un 100% de los desarrolladores reconoce que, si se usan claves.

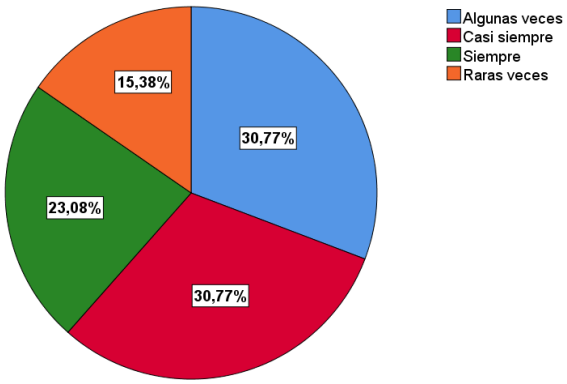
Pregunta 2 ¿Se cifra o encripta información de manera constante? (Ver tabla 25 y figura 26).

Tabla 25.
Cifrado o encriptado

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Algunas veces	4	30,8	30,8	30,8
	Casi siempre	4	30,8	30,8	61,5
	Siempre	3	23,1	23,1	84,6
	Raras veces	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 27
Cifrado o encriptado



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

La interpretación de los resultados revela que la práctica de cifrar muestra cierta variabilidad entre los encuestados. Un 61.5% indicó que esta medida se realiza algunas veces o casi siempre, sugiriendo que hay una aplicación intermitente. Por otro lado, el 23.1% afirmó que se cifra información siempre, lo que indica una consistencia en la aplicación de medidas de seguridad. Sin embargo, el 15.4% que mencionó raras veces sugiere una brecha. Finalmente, de acuerdo con los resultados se puede señalar que 100% de los desarrolladores reconocen que sí se o encripta la información.

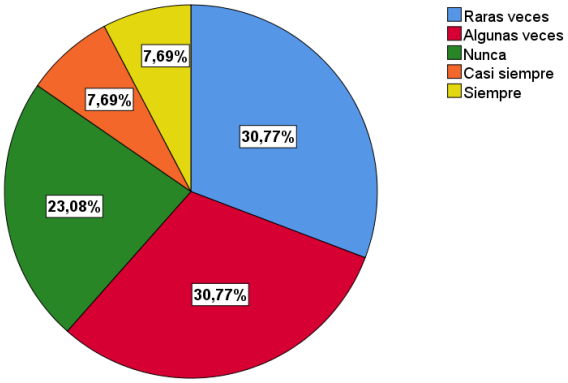
Pregunta 3 ¿Se realiza control de procesos que logran detectar actividades inusuales? (Ver tabla 26 y figura 27).

Tabla 26.
Control de actividades inusuales

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Raras veces	4	30,8	30,8	30,8
	Algunas veces	4	30,8	30,8	61,5
	Nunca	3	23,1	23,1	84,6
	Casi siempre	1	7,7	7,7	92,3
	Siempre	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 28
Control de actividades inusuales



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

La evaluación de las respuestas indica que hay diversidad en la aplicación del control de procesos para detectar actividades inusuales. Un 61.5% de los encuestados mencionó que esto ocurre raras veces o algunas veces lo que sugiere que no es una práctica consistente en la mayoría de los casos. Por otro lado, el 15.4% indicó que nunca se realiza, evidenciando una brecha significativa en la implementación de medidas para divisar estos problemas. En contraste, el 15.4% restante afirmó que se hace casi siempre o siempre señalando regularidad en los controles para la detección de comportamientos anómalos. Los resultados destacan la importancia de fortalecer el monitoreo para identificar y abordar los eventos de manera más efectiva. Finalmente, de acuerdo con la información se puede señalar que 76,9% de los desarrolladores reconocen que sí se ejecuta este proceso de monitorear anomalías, frente al 23,1% que no lo considera así o lo desconoce.

Variable instalación de sistemas y medidas de seguridad

Pregunta 4 ¿Se emplea antivirus en todos los equipos de los empleados? (Ver tabla 27 y figura 28).

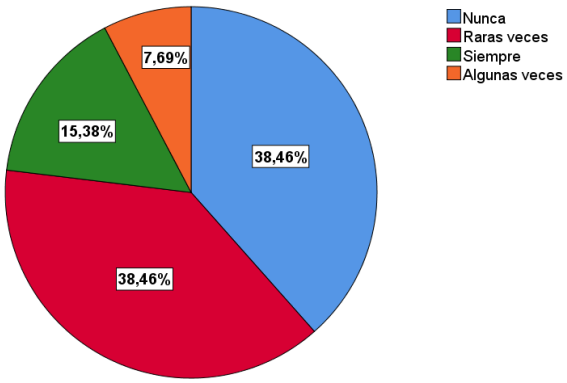
Tabla 27.
Uso de antivirus

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	5	38,5	38,5	38,5
	Raras veces	5	38,5	38,5	76,9
	Siempre	2	15,4	15,4	92,3
	Algunas veces	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 29

Uso de antivirus



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Un 38.5% de los encuestados indicó que nunca y 38.5% mencionó raras veces, lo que sugiere que una proporción significativa de empleados no cuenta con esta aplicación en sus dispositivos. El hallazgo plantea preocupaciones sobre la vulnerabilidad potencial de los sistemas informáticos. Por otro lado, el 15.4% respondió que siempre, lo cual es una práctica más segura y consistente. Un 7.7% afirmó que algunas veces, indicando que hay cierta variabilidad en el uso de medidas en este aspecto. En general, la información obtenida resalta la importancia de este punto garantizar la protección contra posibles amenazas informáticas. Finalmente debe mencionarse que el 61,5% de los empleados reconoce que, si se usan antivirus, frente 38,5% que no lo considera así.

Pregunta 5 ¿Se logra bloquear el acceso a personas no autorizadas mediante cortafuegos? (Ver tabla 28 y figura 29).

Tabla 28.

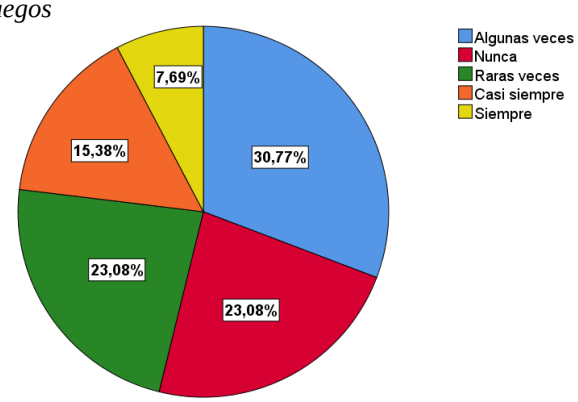
Bloqueo mediante corta fuegos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Algunas veces	4	30,8	30,8	30,8
	Nunca	3	23,1	23,1	53,8
	Raras veces	3	23,1	23,1	76,9
	Casi siempre	2	15,4	15,4	92,3
	Siempre	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 30

Bloqueo mediante corta fuegos



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Los resultados indican que el uso de cortafuegos para bloquear el acceso a personas no autorizadas varía en la empresa. Un 30.8% de los encuestados menciona que esto se hace algunas veces, lo que sugiere una implementación inconsistente de la medida. Además, un 23.1% afirma que nunca, lo cual es una preocupación significativa, ya que podría dejar la red vulnerable a posibles amenazas. Por otro lado, un 15.4% afirmó que casi siempre, mientras que un 7.7% dijo que siempre se logra. La información señala la necesidad de una revisión y fortalecimiento de las prácticas de seguridad, asegurando consistencia en el uso de organismos para proteger la red contra accesos no autorizados.

Pregunta 6 ¿Se actualizan de manera constante las listas de acceso al uCXP? (Ver tabla 29 y figura 30).

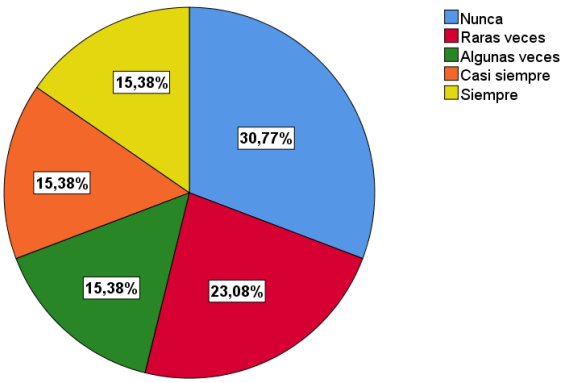
Tabla 29.

Actualización de accesos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	4	30,8	30,8	30,8
	Raras veces	3	23,1	23,1	53,8
	Algunas veces	2	15,4	15,4	69,2
	Casi siempre	2	15,4	15,4	84,6
	Siempre	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 31
Actualización de accesos



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Los resultados de la encuesta indican que la actualización constante de las listas de acceso al uCXP no es una práctica regular en la empresa. Un 30.8% de los encuestados respondió nunca. Además, un 23.1% indicó que esto ocurre raras veces. Solo un 15.4% afirmó que algunas veces, casi siempre o siempre. Esta información sugiere la necesidad de mejorar y regularizar los procesos para garantizar la seguridad y la gestión eficiente de los recursos. Finalmente se demuestra que 62,8% de los encuestado reconocen que si se realizan actualizaciones de la información de las personas que acceden al uCXP. Frente a un 30,8 que no lo considera así.

Variable control de personas

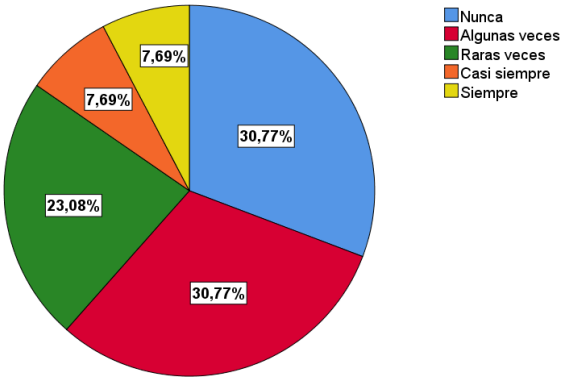
Pregunta 7 ¿Existen mecanismos que permiten reportar eventos de seguridad a través de canales apropiados? (Ver tabla 30 y figura 31).

Tabla 30.
Mecanismos para reportar eventos de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	4	30,8	30,8	30,8
	Algunas veces	4	30,8	30,8	61,5
	Raras veces	3	23,1	23,1	84,6
	Casi siempre	1	7,7	7,7	92,3
	Siempre	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 32
Mecanismos para reportar eventos de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Los datos revelan que hay un espacio para mejorar la existencia y eficacia de mecanismos para reportar eventos de seguridad a través de canales apropiados. El hecho de que un 61.6% de los encuestados haya indicado que estas prácticas ocurren nunca o algunas veces sugiere que la implementación actual puede no ser lo suficientemente consistente o eficiente. Solo un 15.4% indicó que sucede casi siempre y otro 7.7% siempre. Esto destaca la importancia de fortalecer la cultura de reporte para garantizar una identificación y respuesta efectiva a los sucesos inusuales. Por ello se considera necesaria una revisión y mejora de estos canales para fomentar una participación más activa y una comunicación fluida en relación con este aspecto. Finalmente, de acuerdo con la información 60,2% de los participantes afirmó que existen estos mecanismos, frente un 30,8% que no lo considera así.

Variable control físico

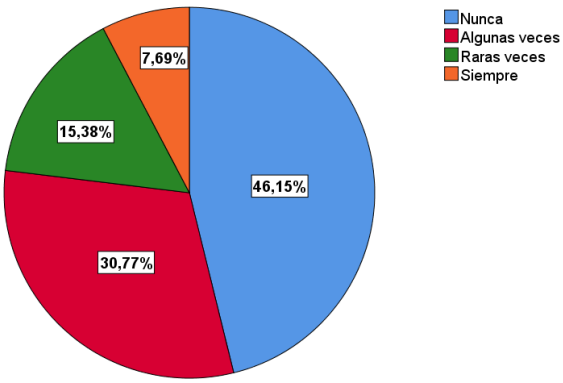
Pregunta 8 ¿Existen controles físicos para el acceso a las instalaciones? (Ver tabla 31 y figura 32).

Tabla 31.
Controles de acceso

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	6	46,2	46,2	46,2
	Algunas veces	4	30,8	30,8	76,9
	Raras veces	2	15,4	15,4	92,3
	Siempre	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 33
Controles de acceso



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

La información proporcionada sugiere que la implementación de controles físicos para el acceso a las instalaciones presenta áreas de mejora en la empresa. La mayoría de las respuestas indican que estos controles físicos 46% considera que nuca se aplican. 30,8% que ocurre algunas veces. 15,4%; 7,7% raras veces, lo que sugiere una falta de consistencia en la aplicación de medidas de seguridad física. Finalmente se puede señalar que 54% de los participantes si evidencia controles de este tipo frente un 46% que no.

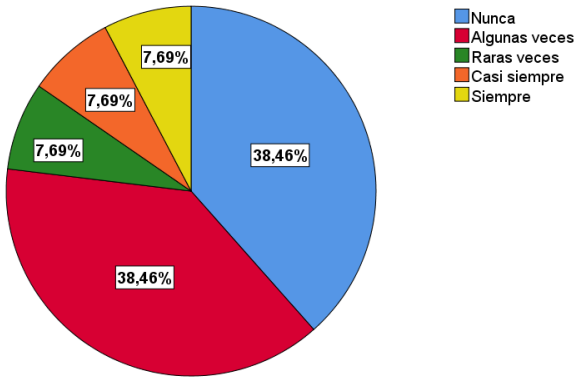
Pregunta 9 ¿Hay control permanente del escritorio y pantalla que buscan reducir el riesgo de ingreso a información confidencial? (Ver tabla 32 y figura 33).

Tabla 32.
Controles de escritorio y pantalla

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	5	38,5	38,5	38,5
	Algunas veces	5	38,5	38,5	76,9
	Raras veces	1	7,7	7,7	84,6
	Casi siempre	1	7,7	7,7	92,3
	Siempre	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 34
Controles de escritorio y pantalla



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Las respuestas proporcionadas indican que existe una distribución variada en las prácticas de control permanente del escritorio y la pantalla para reducir el riesgo de ingreso a información confidencial. 38,5% Un porcentaje significativo indicó que nunca. Un número igual de encuestados señaló que algunas veces, lo que podría indicar que existen esfuerzos intermitentes, pero no de manera consistente. Un pequeño porcentaje de 7,7% respondió raras veces, otro grupo que casi siempre y siempre. De modo que, se puede señalar que hay margen para mejorar, con la posibilidad de implementar medidas más consistentes y efectivas. Finalmente, un 62,5% de los participantes reconoce que, si hay este tipo de actividades, frente un 38;5% que no lo considera así.

Pregunta 10 ¿Los dispositivos usados fuera de la empresa se protegen? (Ver tabla 33 y figura 34).

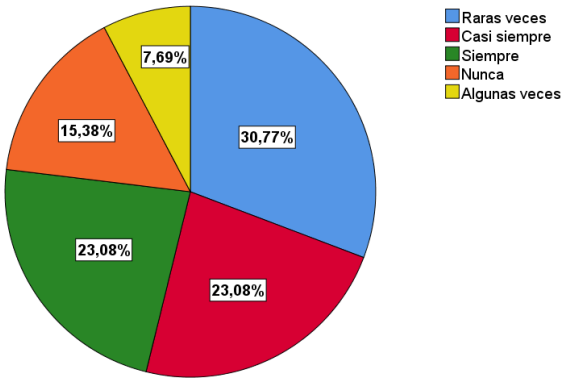
Tabla 33.
Protección de equipos fuera de la empresa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Raras veces	4	30,8	30,8	30,8
	Casi siempre	3	23,1	23,1	53,8
	Siempre	3	23,1	23,1	76,9
	Nunca	2	15,4	15,4	92,3
	Algunas veces	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 35

Protección de equipos fuera de la empresa



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

La interpretación de las respuestas indica que hay diversidad en las prácticas de protección de dispositivos utilizados fuera de la empresa, 30,8% respondió raras veces. 23,1% casi siempre y siempre. 15,7% nunca y 7,7% algunas veces. Las respuestas destacan la variabilidad, con un espacio para mejorar la conciencia y la implementación de medidas de seguridad en este contexto. Finalmente 84,6% de los empleados reconoce que si se protegen los equipos. Frente un 15,5% que no lo considera así.

Pregunta 11 ¿Se ejecutan revisiones de los equipos a fin de eliminar softwares sospechosos? (Ver tabla 34 y figura 35).

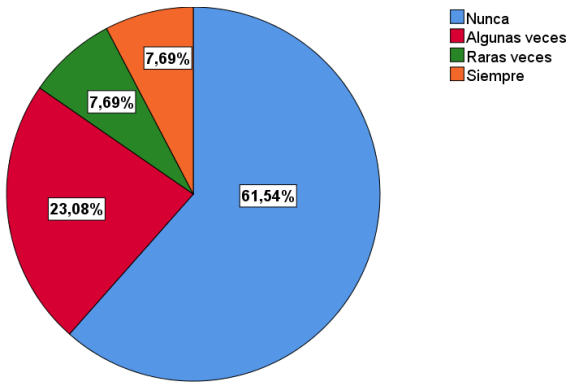
Tabla 34.

Revisiones para eliminar softwares sospechosos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	8	61,5	61,5	61,5
	Algunas veces	3	23,1	23,1	84,6
	Raras veces	1	7,7	7,7	92,3
	Siempre	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 36
Revisiones para eliminar softwares sospechosos



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Las respuestas facilitadas ante la pregunta si se ejecutan revisiones de los equipos a fin de eliminar softwares sospechosos, fueron las siguientes 61.5% de los participantes indicaron que nunca. Se interpreta de varias formas, como por ejemplo confíen en las medidas de seguridad existentes o que no consideren que la amenaza sea significativa en sus entornos. 23,1% seleccionó algunas veces lo que sugiere que hay una conciencia de la necesidad de revisar los sistemas, pero no de manera constante. Una porción de 7,7% indicó que se realiza raramente, esto podría deberse a restricciones de recursos, falta de procedimientos establecidos o una percepción de que el riesgo es mínimo. 7.7% afirmó que siempre, lo que denota una alta responsabilidad en torno a la ciberseguridad, políticas organizativas estrictas o experiencias previas con incidentes de este tipo. Finalmente se puede señalar que 38,5% de los empleados si está atento a este tipo de revisiones, mientras que 61,5% lo desconoce o no lo aplica.

Variable Control tecnológico

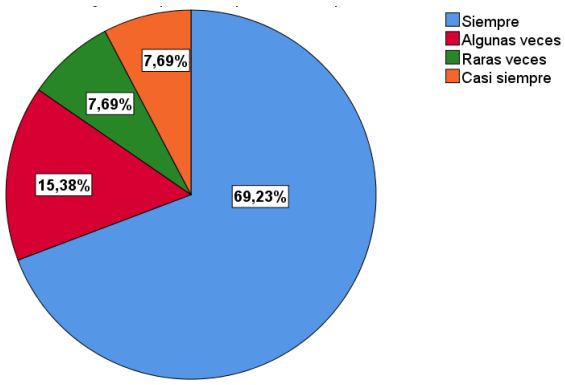
Pregunta 12 ¿Se han implementado procedimientos para autenticación? (Ver tabla 35 y figura 36).

Tabla 35.
Procedimientos de autenticación

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Siempre	9	69,2	69,2	69,2
	Algunas veces	2	15,4	15,4	84,6
	Raras veces	1	7,7	7,7	92,3
	Casi siempre	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 37
Procedimientos de autenticación



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si se han implementado procedimientos para autenticación 69.2& de los participantes indicaron que siempre. Esto sugiere solidez hacia la seguridad en términos de garantizar que los usuarios se autentiquen, lo cual es fundamental para proteger sistemas y datos.15,4% afirmó que algunas veces, lo que podría deberse a diversas razones, como falta de recursos, limitaciones técnicas o una percepción de menor riesgo. 7,7% respondió que raras veces, lo que pasa a ser un área de mejora ya que es esencial para prevenir accesos no autorizados. 7,7% señaló que casi siempre, lo que evidencia un enfoque consistente, aunque no absoluto. Finalmente 100% de los empleados reconoce que si se lleva a cabo este procedimiento.

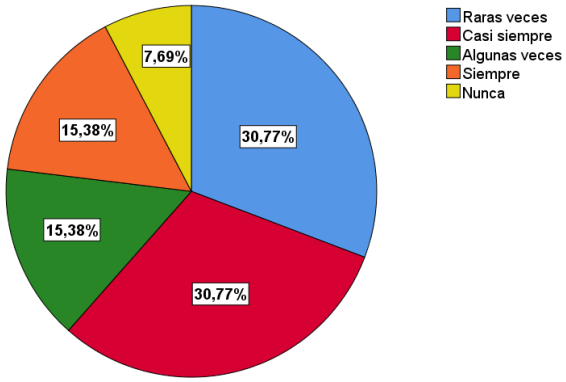
Pregunta 13 ¿Se han implementado controles para evitar fuga de información? (Ver tabla 36 y figura 37).

Tabla 36.
Controles para evitar fuga de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Raras veces	4	30,8	30,8	30,8
	Casi siempre	4	30,8	30,8	61,5
	Algunas veces	2	15,4	15,4	76,9
	Siempre	2	15,4	15,4	92,3
	Nunca	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 38
Controles para evitar fuga de información



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si se han implementado controles para evitar la fuga de información 30, 8% respondió que raras veces. 30,8% señaló que casi siempre lo que resulta alentador y sugiere una atención considerable respecto a este punto. 15,4% manifestó que algunas veces. Esto podría deberse a razones variadas, como percepción de riesgo variable o limitaciones de recursos. El mismo porcentaje indicó que siempre, lo que constituye una señal positiva de un enfoque consistente hacia la seguridad. Una minoría constituida por 7,7% afirmó que nunca se ha llevado tal acción. Finalmente, de acuerdo con los resultados el 92,3% de los empleados reconoce que, si se ejecutan acciones para evitar la fuga de información, aun es evidente que no de manera permanente.

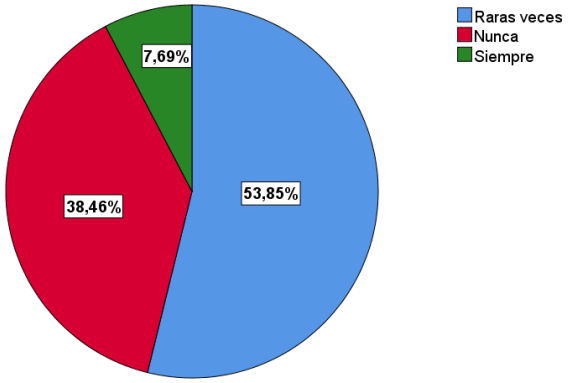
Pregunta 14 ¿Se definen requisitos que deben cumplir los dispositivos móviles controlados por la organización para acceder a sus sistemas? (Ver tabla 37 y figura 38).

Tabla 37.
Controles a dispositivos móviles

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Raras veces	7	53,8	53,8	53,8
	Nunca	5	38,5	38,5	92,3
	Siempre	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 39
Control a dispositivos móviles



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si se definen requisitos que deben cumplir los dispositivos móviles controlados por la organización para acceder a sus sistemas, las respuestas fueron las siguientes 53,8% raras veces lo que indica una falta de prácticas sólidas respecto a este tipo de control. 38,5% respondió que nunca, lo que invita a considerar la necesidad de prevenir los riesgos de seguridad asociados con el uso de estos aparatos en entornos corporativos. Un porcentaje de 7,7% indicó que siempre lo que resulta positivo y sugiere un enfoque estricto y seguro en cuanto al punto ya mencionado. Finalmente, de acuerdo con los resultados se puede mencionar que 61,5% de los empleados reconoce que hay control para equipos móviles, mientras que el 38,5% no lo considera así.

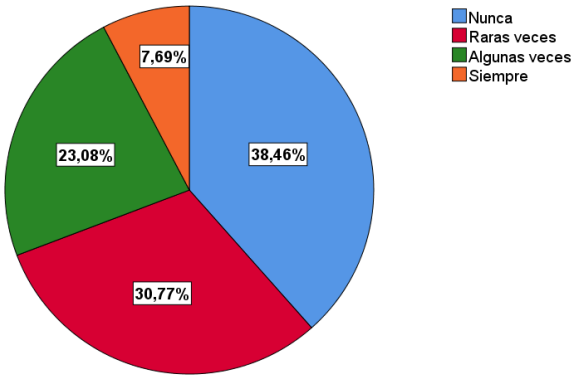
Pregunta 15 ¿Se regula el uso de dispositivos Bring your own device, (BYOD) personales o de terceros para acceder, procesar y transmitir información? (Ver tabla 38 y figura 39).

Tabla 38.
Controles a dispositivos BYOD

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	5	38,5	38,5	38,5
	Raras veces	4	30,8	30,8	69,2
	Algunas veces	3	23,1	23,1	92,3
	Siempre	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 40
Control a dispositivos BYOD



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si se regula el uso de dispositivos BYOD personales o de terceros para acceder, procesar y transmitir información, las respuestas fueron las siguientes 38,5% nunca, lo que plantea la necesidad de ejecutar acciones regulatorias en términos de seguridad y gestión de riesgos. 30,8% raras veces, lo que indica que hay cierta atención a la regulación, pero no de manera consistente. 23,1% algunas veces lo que se asocia a normativa flexible en relación con el uso de este material. 7,7% señaló que siempre se controla, lo que resulta un enfoque estricto y seguro. Finalmente, de acuerdo con los resultados 61,5% de los empleados reconoce que hay regulaciones respecto al tema tratado, frente al 38,5% que no lo considera así.

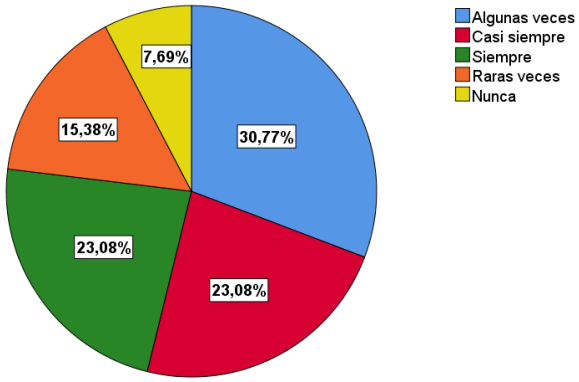
Pregunta 16 ¿Se mantiene respaldo adecuado de la información contenida en los sistemas de información ya sea de forma local o remota? (Ver tabla 39 y figura 40).

Tabla 39.
Respaldo de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Algunas veces	4	30,8	30,8	30,8
	Casi siempre	3	23,1	23,1	53,8
	Siempre	3	23,1	23,1	76,9
	Raras veces	2	15,4	15,4	92,3
	Nunca	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 41
Respaldo de la información



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si se mantiene respaldo adecuado de la información contenida en los sistemas de información ya sea de forma local o remota, las respuestas fueron las siguientes 30,8% algunas veces lo que denota una práctica irregular en términos de copias de seguridad. 23,1% confirmó que casi siempre lo que sugiere que hay ocasiones en las que esto no se realiza de manera consistente. 23,1 manifestó que siempre lo que demuestra una buena acción en torno a esta temática que se está abordando. 15,4% afirmó que raras veces lo que requiere una revisión. 7,7% señaló que nunca al respecto debe mencionarse que la falta de la acción puede tener consecuencias graves en caso de pérdida de datos. Finalmente, se puede señalar que 92,3% de los empleados reconocen que se ejecuta respaldo de la información, rente un 7,7% que no lo considera así.

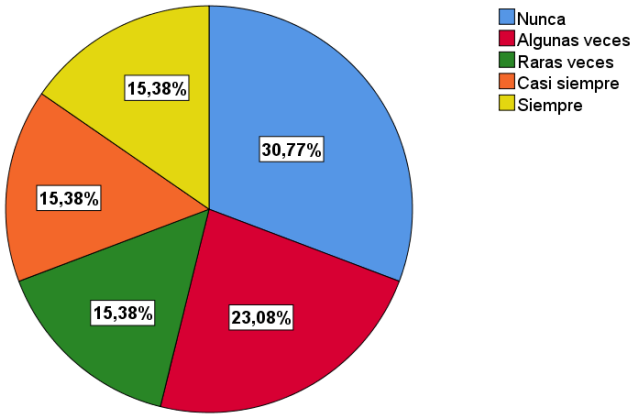
Pregunta 17 ¿Existe autenticación mutua entre los diferentes dispositivos antes de establecer conexión o intercambio de información entre ellos? (Ver tabla 40 y figura 41).

Tabla 40.
Autenticación entre dispositivos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	4	30,8	30,8	30,8
	Algunas veces	3	23,1	23,1	53,8
	Raras veces	2	15,4	15,4	69,2
	Casi siempre	2	15,4	15,4	84,6
	Siempre	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 42
Autenticación entre dispositivos



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si existe autenticación mutua entre los diferentes dispositivos antes de establecer conexión o intercambio de información entre ellos, las respuestas fueron las siguientes 30,8% nunca lo que representa un riesgo de seguridad, ya que esta es una medida importante para garantizar la seguridad en las comunicaciones. 23,1% algunas veces lo que sugiere una práctica inconsistente en términos del tema abordado. 15,4% raras veces lo que resulta similar a la categoría anterior. 15,4% casi siempre que evidencia un enfoque más seguro. Finalmente, se puede mencionar que 60,2% de los empleados reconoce que se realizar estas prácticas de autenticación, frente el 30, 8% que no lo considera así.

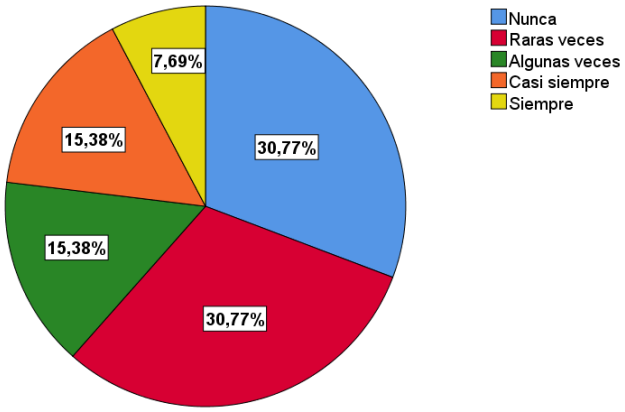
Pregunta 18 ¿Se ejecutan controles periódicos para asegurar que los usuarios tienen autorización para acceder a determinada información al tomar descansos largos en la jornada? (Ver tabla 40 y figura 41).

Tabla 41.
Controles para acceso a la información luego del descanso

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	4	30,8	30,8	30,8
	Raras veces	4	30,8	30,8	61,5
	Algunas veces	2	15,4	15,4	76,9
	Casi siempre	2	15,4	15,4	92,3
	Siempre	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 43
Controles para acceso a la información luego del descanso



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si ejecutan controles periódicos para asegurar que los usuarios tienen autorización para acceder a determinada información al tomar descansos largos en la jornada, las respuestas fueron las siguientes 30,8% nunca. Lo que representa un riesgo de seguridad, ya que esta acción es importante para garantizar que solo los autorizados tengan acceso a la información. Raras veces, 30.8%, lo que sugiere una práctica inconsistente respecto al tema abordado. 15,4% algunas veces, demostrando conciencia de la necesidad de estas acciones. De igual manera un porcentaje similar an indicador anterior respondió que casi siempre, lo que demuestra un enfoque constante hacia la seguridad del acceso. Un 7,7% manifestó que siempre demostrando mayor enfoque y seguridad. Finalmente, en torno a esta interrogante se puede mencionar que 60,2% de los empleados consideran que sui se ejecutan este tipo de acciones, mientras un 30,8% no lo cree así.

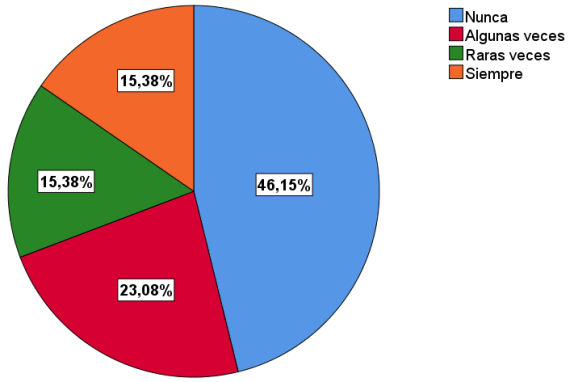
Pregunta 19 ¿La red está segmentada apropiadamente para separar componentes públicos de los privados? (Ver tabla 41 y figura 42).

Tabla 42.
La red segmentada apropiadamente

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	6	46,2	46,2	46,2
	Algunas veces	3	23,1	23,1	69,2
	Raras veces	2	15,4	15,4	84,6
	Siempre	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Figura 44
La red segmentada apropiadamente



Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados (desarrolladores) de Plugthem, S.A.

Análisis e interpretación de los resultados

Al preguntar si la red está segmentada apropiadamente para separar componentes públicos de los privados, las respuestas fueron las siguientes 46,2% nunca, lo que representa un riesgo significativo, ya que la segmentación de la red es una práctica fundamental para controlar el acceso y mitigar riesgos. 23,1% algunas veces lo que sugiere una práctica inconsistente en términos de seguridad de la red. 15,4% raras veces demostrando variabilidad en las buenas prácticas. Otro porcentaje similar respondió que siempre demostrando un enfoque constante hacia el punto abordado.

Resultados del impacto del marco aplicado

En relación con el impacto de la aplicación del marco, es preciso mencionar que este estudio realizó un análisis del impacto generado a partir del establecimiento del

marco de trabajo de ciberseguridad en la ejecución de los procesos de desarrollo de software de la empresa Plugthem S.A. los resultados se presentan en la tabla 43.

Tabla 43.
Impacto del marco de trabajo de ciberseguridad

Indicadores	Valor antes de aplicar el marco	Valor después de aplicar el marco	% Impacto
¿La empresa les ha ofrecido adiestramiento en seguridad informática?	2,61	4,17	**1,56**
¿El teletrabajo permite que ocurra capacitación continua?	4,33	4,61	**0,28**
¿Se tratan temas relacionados con la política de seguridad de la información?	3,56	3,83	**0,28**
¿Se recoge y analiza la información relacionada a amenazas de seguridad?	3,61	6,67	**3,06**
¿Se menciona la existencia de un inventario de activos y los responsables de estos?	4,06	6,67	**2,61**
¿El personal devuelve activos al finalizar la relación laboral?	6,17	6,67	**0,50**
¿La empresa está preparada para la gestión de incidentes de seguridad, incluso hay roles definidos?	4,33	6,67	**2,33**
¿Se usa contraseñas en cada uno de los procesos y clientes que se administran?	2,83	3,61	**0,78**
¿Se realiza control de procesos que logran detectar actividades inusuales?	1,78	3,61	**1,83**
¿Se emplea antivirus en todos los equipos de los empleados?	1,56	3,61	**2,06**
¿Se logra bloquear el acceso a personas no autorizadas mediante cortafuegos?	1,89	3,61	**1,72**
¿Se actualizan de manera constante las listas de acceso al uCXP?	1,89	3,61	**1,72**
¿Se mantiene respaldo adecuado de la información contenida en los sistemas de información ya sea de forma local o remota?	2,44	3,61	**1,17**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a los empleados de Plugthem, S.A.

Interpretación de los datos de la tabla 43

En la tabla se muestran los valores antes y después de aplicar un marco específico en relación con varios indicadores de seguridad informática. Dentro de los puntos que destacan se encuentran el adiestramiento en relación con los procesos de seguridad informática de Plugthem S.A. donde se puede evidenciar un aumento significativo, lo que indica una mejora considerable.

En cuanto a la gestión de amenazas y activos, el impacto fue considerable después de aplicar el marco en áreas como la recopilación y análisis de información relacionada con amenazas de seguridad y la existencia de un inventario de estos. Lo que evidencia una mejora sustancial en la gestión y protección de los activos y la información sensible.

Respecto a la preparación para la gestión de incidentes, hubo un aumento considerable en el valor después de aplicar el marco, lo que sugiere una mejora

significativa en la capacidad de la empresa para manejar y responder a posibles incidentes de seguridad.

En lo relacionado con el uso de herramientas de seguridad, se observan incrementos notables en indicadores como el empleo de antivirus y cortafuegos, lo que señala una mejora fundamental para proteger los sistemas. Lo que permite señalar que la mayoría de los indicadores muestran un impacto positivo después de aplicar el marco de seguridad.

4.2.Discusión

Se procede a presentar la discusión del estudio que permitirá conocer lo que indica la literatura en relación con los resultados obtenidos, lo que se busca es el entendimiento de las de buenas prácticas de ciberseguridad en el teletrabajo para las empresas de desarrollo de software. Este apartado se presenta de acuerdo con las variables que se analizaron.

En relación con las prácticas de ciberseguridad, resulta evidente que no hay un adiestramiento, permanente en el área de seguridad informática, lo que es una oportunidad de mejora para la empresa. En ese sentido se puede mencionar a Adeva y Vera (2020) quienes señalaron que es necesario plantearse este tema como una protección integral fuera de ella. Por otra parte, Khraisat, *et. Al.* (2019) consideraron que los temas relacionados con el punto ya mencionado pasaron a ser fundamentales dentro de las organizaciones. Por esta razón las políticas buscan asegurar acciones consistentes en la protección de procesos y clientes. Esto significa que deben ser fáciles de entender y actualizadas regularmente.

En torno a la instalación de sistemas y medidas de seguridad, es necesario comprender que ante los incumplimientos se requiere establecer una cultura permanente. Por ello resulta esencial abordar esta falta de consistencia y conciencia en la aplicación de las mismas, considerando la importancia crítica de los cortafuegos para proteger la red, de igual forma la gestión de accesos, ya que es fundamental para prevenir posibles riesgos y garantizar un uso adecuado de los recursos. Al respecto, Corrallo, *et al*. (2021) reconoce la importancia y desafíos que afrontan las empresas para garantizar la integridad de la gestión de datos. De manera que, a partir de las actividades de teletrabajo, las organizaciones tienen una oportunidad de mejor, donde la capacitación resulta un elemento clave (Experian, 2015).

En lo que respecta al teletrabajo, se observa variabilidad en la evaluación del desempeño y la elección de espacios para el teletrabajo, lo que indica una transición en las prácticas de evaluación y la necesidad de directrices claras. Además, la percepción de adaptabilidad al cambio y las oportunidades de capacitación varían entre los empleados que trabajan de forma remota, destacando la importancia de promover estrategias que fomenten la flexibilidad y el desarrollo continuo. En torno a ello, Abukari & Bankas (2020) han mencionado el desafío que representa esta modalidad para las organizaciones. Así mismo Borkovich & Skovira (2020) consideran que el principal reto radica en las personas, ya que en muchas ocasiones carecen de conciencia sobre la seguridad, lo que las expone a posibles ciberataques.

Acerca del control organizacional, en la empresa hay una diversidad de percepciones sobre la atención y claridad en las políticas de seguridad de la información, la definición de roles y responsabilidades, el cumplimiento de normas, la recolección y análisis de información sobre amenazas, el control de activos, la gestión de permisos de acceso, la seguridad en la nube, la preparación para gestionar incidentes de seguridad, y auditorías.

Esta variedad subraya la necesidad de mejorar la consistencia y la efectividad en la implementación y seguimiento de prácticas de seguridad de la información en la organización. En tal sentido, Un elemento importante dentro de las prácticas de ciberseguridad lo constituye el adiestramiento del personal que no son otra cosa que una serie de capacitaciones organizadas, con un alto sentido pedagógico y tecnológico para garantizar que el personal pueda desarrollar capacidades que le permitan garantizar el cumplimiento de pasos y le fortalezcan habilidades para enfrentar situaciones laborales asociadas a las vulneraciones de la seguridad.

Huaman, (2021) asegura que es prioritaria la capacitación y adiestramiento de los empleados para estar prevenidos ante cualquier ataque. Ya que según Allauca, (2022) este punto constituye uno de los principales problemas que presentan las empresas. Esto se debe a que hay una notable deficiencia de personal con el conocimiento respecto a el tema.

La organización se beneficiaría de una revisión completa y fortalecimiento de sus manejos y prácticas de seguridad desde la incorporación hasta la finalización de la relación laboral. Por ello, se debe reforzar específicamente el control físico, implementar mejoras continuas y fomentar una cultura de seguridad informática en la empresa para abordar de manera efectiva los desafíos presentes y futuros en este ámbito. Dentro de los

hallazgos, se detectó la necesidad de fortalecer los controles de acceso a las instalaciones mediante la implementación de sistemas como tarjetas de acceso y cámaras de seguridad. Al respecto Abukari & Bankas (2020) señalaron que los documentos que se generan ayudan a mejorar las medidas de seguridad existentes, estos contienen las políticas a aplicar. De igual manera Bukley et al. (2014) enfatiza la importancia de darlos a conocer. Por su parte, Aldawood, & Skinner, (2019) consideran necesario que se implementen acciones para garantizar la ciberseguridad.

Por consiguiente, también es necesario implementar medidas consistentes para el control de escritorios y pantallas, el uso de pantallas de privacidad y la promoción de hábitos seguros entre los empleados. Esto reducirá el riesgo de acceso no autorizado a información confidencial y fortalecerá la seguridad en este aspecto.

Finalmente, el control tecnológico demuestra que la mayoría de los participantes están enfocados en implementar procedimientos de autenticación, regulación del uso de dispositivos BYOD, pero existe variabilidad en la consistencia de estas prácticas. A pesar de los esfuerzos para evitar la fuga de información, hay espacio para mejoras, especialmente entre aquellos que afirman haber implementado estos controles, aunque no de manera periódica.

CAPITULO V
PROPUESTA

Para el diseño del marco de trabajo requiere considerar los resultados obtenidos una vez que se aplicó la encuesta a los trabajadores de la empresa Plugthem S.A. Además, se considera que el modelo debe ser integral y adaptable a las necesidades específicas de Plugthem S.A., tomando como base las normativas ISO 27002 y NIST SP 800-46 para establecer controles, procedimientos y políticas que garanticen un entorno de teletrabajo seguro y protegido contra ciberataques. En ese sentido, se procede a presentar la tabla 44 contentiva de los datos de esta.

De modo que, se justifica el diseño de este marco de trabajo a partir de lo ya evidenciado y se sustenta con lo expuesto por Tjirare & Shava (2017) que mencionaron lo beneficiosos que puede resultar para las organizaciones implementar normas que coadyuven al desarrollo, protección de la información, organización y activos de la empresa. De igual manera, Souppaya & Scarfone (2016) manifestaron que la normativa NIST proporciona consideraciones de seguridad, para el desarrollo de trabajo remoto y BYOD.

Tabla 44.

Datos del marco

Título: Marco de trabajo de buenas prácticas de ciberseguridad en el teletrabajo para empresas de desarrollo de software, basado en los controles de la norma ISO 27002:2022 y la NIST SP 800-46
Objetivos General: Desarrollar marco de trabajo de buenas prácticas de ciberseguridad en el teletrabajo para empresas de desarrollo de software, basado en los controles de la norma ISO 27002:2022 y la NIST SP 800-46 **Específicos:** • Capacitar a los trabajadores de Plugthem S.A sobre las mejores prácticas de ciberseguridad, basándose en los estándares ISO 27002 y NIST SP 800-46. • Proteger información e integridad de los sistemas de la empresa de desarrollo de software • Garantizar mejoras en las políticas de seguridad de la empresa Plugthem S.A.
Responsable: Directivos de la empresa Plugthem S.A. y Richard Esparza
Tiempo de implementación: 1 mes
1- **Contenido a desarrollar:** de acuerdo con controles establecido en ISO 27002, (2022) y el NIST (2018).
Nombre: Concientización, educación y entrenamiento en seguridad de la información/Aprovechamiento de teletrabajo para capacitaciones. Adiestramiento en seguridad informática
Descripción: Todo el personal de la organización debe recibir capacitación en materia de seguridad sobre los elementos relevantes para el adecuado desempeño de sus funciones.
Tipo de Control: Preventivo
Propiedades de Seguridad de la información: Confidencialidad, Integridad Disponibilidad
Dominios de Ciberseguridad: Gobernanza y ecosistema
Medio de Validación: el empleado comprende que puede tener un mejor aprovechamiento de las capacitaciones durante la modalidad de teletrabajo. Se valida mediante la asistencia al ciclo de capacitación.

2- **Contenido a desarrollar:** Tratamiento de información relacionado con la política de seguridad de la información.
Nombre: Concientización, educación y entrenamiento en seguridad de la información/Aprovechamiento de teletrabajo para capacitaciones.
Descripción: Política de datos, devolución de activos, Código de ética. Arquitectura de la plataforma.
Tipo de Control: Preventivo
Propiedades de Seguridad de la información: Confidencialidad, Integridad Disponibilidad
Dominios de Ciberseguridad: Gobernanza y ecosistema
Medio de Validación: el empleado demuestra conocimiento de la política de datos de la empresa y los diferentes documentos que integran el marco metodológico relacionado con protección de datos y protección a ciber ataques. Se valida mediante prueba de dominio.
3- **Contenido a desarrollar:** Responsabilidades al cambio o término de relación laboral.
Nombre: Concientización, educación y entrenamiento en seguridad de la información/Aprovechamiento de teletrabajo para capacitaciones.
Descripción: Devolución de activos, Arquitectura de la plataforma. Se deben establecer y comunicar las responsabilidades que se mantendrán al término o cambio de la relación laboral con la organización
Tipo de Control: Preventivo
Propiedades de Seguridad de la información: Confidencialidad, Integridad Disponibilidad
Dominios de Ciberseguridad: Gobernanza y ecosistema
Medio de Validación: el empleado demuestra conocimiento en cómo se ejecuta el manejo de los activos al finalizar la relación laboral.
4- Contenido a desarrollar: Uso de contraseñas en los diferentes clientes. Actualización de las listas de acceso al uCXP
Nombre: Gestión de cuentas
Descripción: Garantiza una adecuada gestión de autenticación de uno o varios factores para los usuarios por medio de contraseñas, certificados digitales o algún tipo de token. Involucra a todo el proceso que se debe seguir para garantizar un acceso remoto seguro, va desde la documentación de requisitos de acceso hasta la encriptación de todas las conexiones. Funcionamiento de las cuentas de los clientes.
Tipo de Control: Preventivo
Propiedades de Seguridad de la información: Confidencialidad, Integridad Disponibilidad
Dominios de Ciberseguridad: Gobernanza
Medio de Validación: el empleado demuestra conocimiento en cómo se ejecuta el manejo de las contraseñas de los clientes, así como el acceso.
5- **Contenido a desarrollar:** Información relacionada a amenazas de seguridad y su tratamiento. Control de procesos que logran detectar actividades inusuales
Nombre: Concientización, educación y entrenamiento en seguridad de la información/ Reporte de eventos de seguridad de la información
Descripción: La organización debe proveer mecanismos para que personal pueda reportar eventos de seguridad observados a través de canales apropiados.
Tipo de Control: Detectivo
Propiedades de Seguridad de la información: Confidencialidad, Integridad Disponibilidad
Dominios de Ciberseguridad: Dominio y defensa
Medio de Validación: el empleado demuestra conocimiento en cómo se ejecuta acciones para garantizar la seguridad.
6- **Contenido a desarrollar:** Importancia del uso de antivirus en todos los equipos. Bloqueo de acceso a personas no autorizadas mediante cortafuegos
Nombre: Concientización, educación y entrenamiento en seguridad de la información/Trabajo remoto
Descripción: Es necesario implementar todas las medidas necesarias para proteger la información que es accedida, procesada y almacenada fuera de la organización.
Tipo de Control: Preventivo
Propiedades de Seguridad de la información: Confidencialidad, Integridad Disponibilidad
Dominios de Ciberseguridad: Protección
Medio de Validación: el empleado demuestra conocimiento en cómo se ejecuta el manejo de los activos al finalizar la relación laboral.

7- **Contenido a desarrollar:** Respaldo de la información contenida en los sistemas de información.
Nombre: Concientización, educación y entrenamiento en seguridad de la información/Respaldos
Descripción: Se debe mantener un respaldo adecuado de la información contenida en los sistemas de información ya sea de forma local o remota.
Tipo de Control: Preventivo
Propiedades de Seguridad de la información: Confidencialidad, Integridad Disponibilidad
Dominios de Ciberseguridad: Protección
Medio de Validación: el empleado demuestra conocimiento en cómo se ejecuta el respaldo de la información. Reportes de eventos de seguridad de la información

Elaboración propia (2023).

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

De acuerdo con los resultados obtenidos, se procede a presentar las conclusiones de esta investigación. En lo relacionado con el establecimiento de un marco de trabajo de buenas prácticas de ciberseguridad en el teletrabajo para las empresas de desarrollo de software, a través de la síntesis de resultados de un estudio exploratorio, se pudo concretar a partir de los hallazgos obtenidos, que permitieron demostrar la necesidad de esta implementación en la empresa Plugthem S.A.

Para identificar las prácticas de ciberseguridad utilizadas por las empresas que operan bajo la modalidad de teletrabajo, se realizó una revisión de las prácticas de ciberseguridad en el teletrabajo, basado en los controles establecidos en la norma ISO 27002:2022 y la NIST SP 800-46, que permitió conocer que actualmente existen algunas deficiencias en las empresas ecuatorianas en cuanto esta actividad. En lo que respecta a Plugthem S.A. se pudo detectar la falta de adiestramiento permanente en el área de seguridad informática. Además de oportunidades de mejora en torno a la instalación de sistemas y medidas de seguridad, se evidencia una transición en las prácticas de evaluación y la necesidad de directrices claras.

Por lo antes expuesto fue necesario diseñar un marco de trabajo con los mecanismos y procedimientos de ciberseguridad en el teletrabajo apropiados para las empresas de desarrollo de software basada en los controles establecidos en la norma ISO 27002:2022 y la NIST SP 800-46.

Posteriormente se evaluó el impacto del marco de trabajo de ciberseguridad en la ejecución de los procesos de desarrollo de software de la empresa Plugthem S.A. y se obtuvo una mejora notable en relación con la implementación de algunas medidas de ciberseguridad, así como el conocimiento de las políticas y directrices para garantizar la protección de los datos.

Luego de realizar la evaluación del impacto del marco de trabajo de ciberseguridad en la ejecución de los procesos de desarrollo de software de la empresa Plugthem S.A. se pudo obtener una mejora notable en relación a la implementación de algunas medidas de ciberseguridad, así como el conocimiento de las políticas y directrices para garantizar la protección de los datos.

Recomendaciones

Se requiere revisión permanente de las prácticas de ciberseguridad que utiliza la empresa y que están basadas en los controles ISO 27002:2022 y la NIST SP 800-46, esto con la finalidad de promover estrategias que fomenten la flexibilidad y el desarrollo continuo.

De igual forma, es necesario fortalecer los controles de acceso a las instalaciones mediante la implementación de sistemas como tarjetas de acceso y cámaras de seguridad. Ya que esto garantiza un adecuado control de las personas que ingresan o salen de la empresa.

Es relevante, ejecutar adiestramientos de manera permanente con la finalidad de lograr la transición completa de las prácticas de evaluación, establecer e informar directrices de una manera permanente y clara. Por esta razón se requiere monitorear nuevamente el marco de trabajo con los mecanismos y procedimientos de ciberseguridad en el teletrabajo apropiados para las empresas de desarrollo de software.

También se recomienda evaluar el impacto de las diferentes acciones planteadas en el marco de trabajo de ciberseguridad en la ejecución de los procesos de desarrollo de software de la empresa Plugthem S.A. dado que esta práctica permitirá garantizar que se aplica la normativa correspondiente.

REFERENCIAS

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (17 de Julio de 2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity volume 2*.

Abdullah, A., Hamad, R., Abdulrahman, M., Moala, H., & Elkhediri, S. (2019). CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS).* Riyadh: IEEE. doi:10.1109/CAIS.2019.8769560

Abukari, A., & Bankas, E. (2020). Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond. *11*(4), 1401-1407. https://www.researchgate.net/publication/341098664_Some_Cyber_Security_Hygienic_Protocols_For_Teleworkers_In_Covid-19_Pandemic_Period_And_Beyond

Adeva, A., & Vera, J. M. (2020). Teletrabajo seguro, el catalizador digital de la transformación socioeconómica. *SIC: Revista Ciberseguridad, seguridad de la información y privacidad, 29*(140), 62-63. https://revistasic.es/revista-sic/sic-140/especial-sic/

Aldawood, H., & Skinner, G. (2019). An Academic Review of Current Industrial and Commercial Cyber Security Social Engineering Solutions. *2019 the 3rd International Conference on Cryptography, Security and Privacy* (págs. 110-115). Kuala Lumpur: IJSER.

Aldawood, H., & Skinner, G. (2019). An Academic Review of Current Industrial and Commercial Cyber Security Social Engineering Solutions. *2019 the 3rd International Conference on Cryptography, Security and Privacy* (págs. 110-115). Kuala Lumpur: IJSER. doi:https://dl.acm.org/doi/proceedings/10.1145/3309074

Allauca, E. (2022). *Propuesta de mejores prácticas de ciberseguridad para la comunicación en redes en clientes corporativos.* Repositorio PUCE. https://repositorio.pucesa.edu.ec/bitstream/123456789/3779/1/78213.pdf

Alvarado, M. (2021). *Analysis for the adoption of security standards to improve the management of securities in Public Organizations.* https://dspace.ups.edu.ec/bitstream/123456789/19760/1/UPS-GT003120.pdf

Asamblea General. (2016). Código Orgánico de la Economía Social de los Conocimientos, creatividad e innovación. Suplemento. Registro Ofi cial Nº 899. Quito, Pichinca, Ecuador. https://www.gob.ec/sites/default/files/regulations/2019-02/Documento_C%C3%B3digo-Org%C3%A1nico-Econom%C3%ADa-Social-Conocimientos-Creatividad-Innovaci%C3%B3n.pdf

Asamblea General. (2022). Reglamento de Teletrabajo del Ministerio del Trabajo. Registro Oficial 318. Quito, Pichincha, Ecuador. https://www.trabajo.gob.ec/wp-content/uploads/2022/12/MDT-2022-237-ACUERDO-MINISTERIAL-TELETRABAJO-SECTOR-PRIVADO-23-12-22.pdf?x42051

Asamblea Nacional. (2015). Ley Orgánica de Telecomunicaciones. Suplemento. Registroi Oficial 899. Quito, Pichincha, Ecuador. https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pd

Bilge, L., Han, Y., & Dell'Amico, M. (2017). RiskTeller: Predicting the Risk of Cyber Incidents. *CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (págs. 1299-1311). Dallas: Association for Computing Machinery. doi:https://dl.acm.org/doi/10.1145/3133956.3134022

Borkovich, D., & Skovira, R. (2020). Working from home: cybersecurity in the age of COVID-19. *Issues in Information Systems, 24*(4), 234-246. https://iacis.org/iis/2020/4_iis_2020_234-246.pdf

Buckley, O., Nurse, J., Legg, P., Goldsmith, M., & Creese, S. (2014). Reflecting on the ability of enterprise security policy to address accidental insider threat. *2014 Workshop on Socio-Technical Aspects in Security and Trust.* Vienna: IEEE. https://research-portal.uea.ac.uk/en/publications/understanding-insider-threat-a-framework-for-characterising-attac

Bustamante, F., Fuertes, W., Tulkeredis, T., & Ron, M. (2018). Situational Status of Global Cybersecurity and Cyber Defense According to Global Indicators. Adaptation of a Model for Ecuador. *MICRADS 2018* (págs. 12-26). Salinas: Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-319-78605-6_2

CCN-CERT. (2020). *CCN-CERT BP/18 Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia.* España: CCN. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cem-malaga.es/portalcem/novedades/2020/CCN-CERT_BP-18%20Recomendaciones%20para%20Teletrabajo.pdf

CISA. (11 de Marzo de 2022). *Telework guidance and resources*. Telework guidance and resources: https://www.cisa.gov/telework

Corallo, A., Lazoi, M., Lezzi, M., & Pontrandolfo, P. (16 de Junio de 2021). Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level. *IEEE Transactions on Engineering Management, 70*(11), págs. 1-21. https://ieeexplore.ieee.org/document/9457098

CSIRT CELEC EP. (5 de Enero de 2022). *Consejos de ciberseguridad para el teletrabajo*. https://csirt.celec.gob.ec/en/contenidos/guias-y-consejos/175-consejos-de-ciberseguridad-para-el-teletrabajo

Delgado, S. (29 de Mayo de 2023). *La modalidad de teletrabajo en Ecuador.* Actuaria: https://actuaria.com.ec/es/la-modalidad-de-teletrabajo-en-ecuador/

Experian. (2015). *Data Breach Industry Forecast.* Experian. https://www.experian.com/data-breach/2023-data-breach-industry-forecast

Figueroa Suárez, J., Rodríguez Andrade, R., Bone Obando, C., & Saltos Gómez, J. (2018). La seguridad informática y la seguridad de la información. *Polo del conocimiento, 2*(12), págs. 145-155. doi:10.23857/pc.v2i12.420

Gayo, M. R. (2021). Ciberseguridad en el trabajo en movilidad y a distancia (Teletrabajo). *Derecho Social y Empresa*(14), 125-146. https://dialnet.unirioja.es/servlet/articulo?codigo=7976457

Gómez, J. C., & Becerra, A. (2020). El acceso remoto orientado al teletrabajo, un reto para el CISO. *SIC: Revista Ciberseguridad, seguridad de la información y privacidad, 29*(140), 76-77. https://dialnet.unirioja.es/servlet/articulo?codigo=7848954

González, P. (14 de Marzo de 2023). *Centeniales prefieren el trabajo híbrido y la flexibilidad horaria.* https://www.primicias.ec/noticias/economia/teletrabajo-centennials-salario-horario-ecuador/#:~:text=En%20Ecuador%20hay%2013.644%20empresas,28%20de%20febrero%20de%202023.

Google Maps. (30 de julio de 2023). *Plugthem*. https://www.google.com/maps/place/Plugthem/@-0.2946855,-78.4524264,15z/data=!4m2!3m1!1s0x0:0xef6d3f954636fab0?sa=X&ved=2ahUKEwiOlp7swuqBAxU1m2oFHR3aCXgQ_BJ6BAg8EAA&ved=2ahUKEwiOlp7swuqBAxU1m2oFHR3aCXgQ_BJ6BAhMEAg

Hernández, R., & Mendoza, C. (2018). *Metodología de la Investigación* (6° ed.). McGRAW-HILL. http://repositorio.uasb.edu.bo:8080/handle/54000/1292

Hijji, M., & Alam, G. (2021). A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. *Journals & Magazines, 9*, 7152-7169. doi:10.1109/ACCESS.2020.3048839.

Huaman, J. (2021). *Análisis de las capacidades en ciberseguridad y ciberdefensa y telemática del ejército de Lima, 2020.* Repositorio de la ESE. http://repositorio.esge.edu.pe/bitstream/handle/20.500.14141/257/Huaman%20Baltazar%2c%20Jorge%20Luis.pdf?sequence=1&isAllowed=y

Incibe. (25 de Julio de 2019). *La formación como elemento imprescindible en ciberseguridad.* La formación como elemento imprescindible en ciberseguridad: https://www.incibe.es/protege-tu-empresa/blog/formacion-elemento-imprescindible-ciberseguridad

INCIBE. (25 de Julio de 2019). *La formación como elemento imprescindible en ciberseguridad.* La formación como elemento imprescindible en ciberseguridad: https://www.incibe.es/protege-tu-empresa/blog/formacion-elemento-imprescindible-ciberseguridad

Incibe. (2020). *Ciberseguridad en el teletrabajo: Una guía de aproximación para el empresario.* España: INCIBE. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf

ISECM. (2023). *Teleworking, Cybersecurity and COVID-19: A Practical Guide to Maintaining Healthy Digital Hygiene.* https://insecm.ca/teleworking/

ISO. (15 de julio de 2023). *https://normaiso27001.es/*. https://normaiso27001.es/

ISO 27000. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.* https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en

Joyanes, L. (2017). Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0). *Cuadernos de estrategia*, 19-64. Dialnet.

Khan, M., Gide, E., Chaudhry, G., & Hasan, J. (2022). A Cybersecurity Evaluation Model (CSEM) for Indian SMEs Working in a Virtual Team Environment. *2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE).* Gold Coast: IEEE. https://ieeexplore.ieee.org/document/10089355

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Electronics* , *8*(11), 1-18. doi:https://doi.org/10.3390/electronics8111210

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (Abril de 2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *45*, 13-24. doi:10.1016/j.ijinfomgt.2018.10.017

Longras, A., Pereira, T., Carneiro, P., & Pinto, P. (2018). On the Track of ISO/IEC 27001:2013 Implementation Difficulties in Portuguese Organizations. *2018 International Conference on Intelligent Systems (IS)* (págs. 886-890). Funchal: IEEE. https://ieeexplore.ieee.org/document/8710558

López, J. R., Rodríguez, M., Gamboa, N., Ramirez, S., & Cobo, M. (2019). The last five years of Big Data Research in Economics, Econometrics and Finance:

Identification and conceptual analysis. *Procedia Computer Science, 162*, págs. 729-736. doi:https://doi.org/10.1016/j.procs.2019.12.044

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. *2023 International Conference On Cyber Management And Engineering (CyMaEn)*. Bangkok: IEEE.

Marin Diaz, A., Trujillo Casañola, Y., & Buedo Hidalgo, D. (2018). Marco de Trabajo para gestionar actividades de calidad. *Revista Cubana de Ciencias Informáticas, 12*(2), 74-88. http://scielo.sld.cu/pdf/rcci/v12n2/rcci06218.pdf

Marotta, A., & Madnick, S. (2021). Tackling Cybersecurity Regulatory Challenges: A Proposed Research Framework. *19th Workshop on e-Business: The Role of e-Business during the Time of Grand Challenges* (págs. 12-24). Springer.

Marotta, A., & Madnick, S. (2021). Tackling Cybersecurity Regulatory Challenges: A Proposed Research Framework. *19th Workshop on e-Business: The Role of e-Business during the Time of Grand Challenges* (págs. 12-24). Springer. doi:https://doi.org/10.1007/978-3-030-79454-5_2

Martínez, G. (3 de Enero de 2020). *Metodología y Marco de trabajo: la gran duda existencial*. https://www.linkedin.com/pulse/metodolog%C3%ADa-y-marco-de-trabajo-la-gran-duda-gustavo-mart%C3%ADnez-v%C3%A1zquez/?originalSubdomain=es

Medina, C., Casas, M., & Faz, A. (2020). The cyber security in the age of telework: A descriptive research framework through science mapping. *2020 International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy (ICDABI)*. Sakheer: IEEE. doi:10.1109/ICDABI51230.2020.9325633

Ministerio del Trabajo del Ecuador. (Diciembre de 2022). *MDT-2022-237*. https://www.trabajo.gob.ec/wp-content/uploads/2022/12/MDT-2022-237-ACUERDO-MINISTERIAL-TELETRABAJO-SECTOR-PRIVADO-23-12-22.pdf?x42051

MINTEL. (2019). Acuerdo-Ministerial-No.-025-2019-EGSI-version-2.0. Registro Oficial 228. Quito, Pichincha, Ecuador. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/01/Registro-Oficial-Acuerdo-Ministerial-No.-025-2019-EGSI-version-2.0.pdf

MINTEL. (2021). *ACUERDO MINISTERIAL 006-2021*. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

MINTEL. (5 de Agosto de 2022). *Boletín Oficial N° 61*. https://www.telecomunicaciones.gob.ec/por-primera-vez-ecuador-cuenta-con-su-estrategia-nacional-de-ciberseguridad/

Nakhodchi, S., & Dehghantanha, A. (2020). A Bibliometric Analysis on the Application of Deep Learning in Cybersecurity. *Security of Cyber-Physical Systems*(11), 203-221. https://scholar.google.com.ec/scholar?q=A+Bibliometric+Analysis+on+the+Application+of+Deep+Learning+in+Cybersecurity&hl=es&as_sdt=0&as_vis=1&oi=scholart

NIST. (16 de Abril de 2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST. (21 de Mayo de 2018). *NIST Special Publication 800-series General Information*. Information Technology Laboratory: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

Niubox. (9 de Noviembre de 2021). *Ecuador: Políticas en el teletrabajo y seguridad de la información*. https://niubox.legal/teletrabajo-y-ciberseguridad/

NQA. (2013). *ISO 27001:2013 Guía de implantación para la seguridad de la información.* NQA. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Okutan, A., Werner, G., Yang, S. J., & McConky, K. (2018). Forecasting cyberattacks with incomplete, imbalanced, and insignificant data. *Cybersecurity volume 1*(15), págs. 1-16. doi: https://doi.org/10.1186/s42400-018-0016-5

Pereyra, L. (2022). *Metodología de la investigación* (1° ed.). Klik. Retrieved from https://books.google.com.ec/books?hl=es&lr=&id=6e-KEAAAQBAJ&oi=fnd&pg=PP1&dq=investigaci%C3%B3n+no+experimental+pereyra&ots=WGMR_PHCjp&sig=wJkD1Aj41R8xkQyTZXbCwa4plv8&redir_esc=y#v=onepage&q=investigaci%C3%B3n%20no%20experimental%20pereyra&f=false

Rianafirin, K., & Kurniawan, M. (2017). Design network security infrastructure cabling using network development life cycle methodology and ISO/IEC 27000 series in Yayasan Kesehatan (Yakes) Telkom Bandung. *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT).* Kuta Bali: IEEE. https://ieeexplore.ieee.org/document/8320681

Rodríguez, J., & Reguant, M. (2020). Calcular la fiabilidad de un cuestionario o escala mediante el SPSS: el coeficiente alfa de Cronbach. *Reire Revista d'Innovació i Recerca en Educació, 13*(2), 1-13. https://revistes.ub.edu/index.php/REIRE/article/view/reire2020.13.230048/31484

Ron, M., Rivera, O., Fuertes, W., Toulkeridis, T., & Díaz, J. (2019). Cybersecurity Baseline, An Exploration, Which Permits to Delineate National Cybersecurity

Strategy in Ecuador. *ICITS 2019* (págs. 847-857). Quito: Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-11890-7_79

Ron, M., Rivera, O., Fuertes, W., Toulkeridis, T., & Díaz, J. (2019). Cybersecurity Baseline, An Exploration, Which Permits to Delineate National Cybersecurity Strategy in Ecuador. *ICITS 2019* (págs. 847-857). Quito: Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-11890-7_79

Silva, P. (Mayo de 2022). *Mecanismos de ciberseguridad en dispositivos de teletrabajo para una institución financiera.* https://repositorio.pucesa.edu.ec/bitstream/123456789/3647/1/77934.pdf

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (4 de Marzo de 2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Esmerald Insigth, 22*(1), 42-75. https://www.researchgate.net/publication/263387685_Variables_influencing_information_security_policy_compliance_A_systematic_review_of_quantitative_studies

Soriano, M. (2014). *Seguridad en redes y seguridad de la información.* Innovative Methodology for Promising VET Areas: https://psm.fei.stuba.sk/pages/47/Seguridad_de_Red_e_Informacion.pdf

Souppaya, M., & Scarfone, K. (29 de Julio de 2016). *SP 800-46 Rev. 2 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*. NIST: https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

Sulistyowati, D., Suryanto, Y., & Handayani, F. (18 de Diciembre de 2020). Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *International Journal on Informatics Visualization*, págs. 225-230.

Superintendencia de Bancos. (2 de Diciembre de 2021). *Norma de Riesgo Operativo de la CNSB.* https://asobanca.org.ec/wp-content/uploads/2021/12/Res.-SB-2021-2126-Reforma-Norma-de-Riesgo-Operativo-de-la-CNSB.pdf

Teletrabajo flexible y seguro: principales tecnologías y enfoques. (2020). *SIC: Revista Ciberseguridad, seguridad de la información y privacidad*, 66-67.

Tjirare, D., & Shava, F. (2017). A gap analysis of the ISO/IEC 27000 standard implementation in Namibia. *2017 IST-Africa Week Conference (IST-Africa).* Windhoek: IEEE. ttps://www.researchgate.net/publication/320968094_A_gap_analysis_of_the_ISOIEC_27000_standard_implementation_in_Namibia

Tosca, C. (2022). Teletrabajo en el modelo híbrido: alternativa para las organizaciones. *34*(2), 260-266. doi:https://doi.org/10.33975/riuq.vol34n2.934

Ukwen, D. O., & Karabatak, M. (2021). Review of NLP-based Systems in Digital Forensics and Cybersecurity. *2021 9th International Symposium on Digital Forensics and Security (ISDFS).* Elazig: IEEE.

UTN. (23 de julio de 2023). *Vicerrectorado de investigación*. https://www.utn.edu.ec/direccion/#1678470247794-cf300289-335c

Vilcacundo, G. (6 de Octubre de 2021). Propuesta de políticas de Ciberseguridad para el Teletrabajo. Caso de estudio Rectorado ESPOCH. *Domino De Las Ciencias, 7*(6), 63-82. doi:http://dx.doi.org/10.23857/dc.v7i6.2315

Villacís, R. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador. *Revista tecnológica de ciencia y educación Edwars Deming, 6*(1), 50-62. https://revista-edwardsdeming.com/index.php/es/article/view/88/158

Yubin Wang, J., & Xiaoxue, Y. (2018). Information Security Protection in Software Testing. *2018 14th International Conference on Computational Intelligence and Security (CIS)* (págs. 449-452). Hangzhou: IEEE. https://ieeexplore.ieee.org/document/8564344

ANEXOS

Anexo 1. Operacionalización De Variables

TEMA	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.				
INTERROGANTE	¿Cómo se pueden implementar buenas prácticas de ciberseguridad en el teletrabajo para las empresas de desarrollo de software?				
OBJETIVO	Establecer un marco de trabajo de buenas prácticas de ciberseguridad en el teletrabajo para las empresas de desarrollo de software, a través de la síntesis de resultados de un estudio exploratorio.				
INTERROGANTES ESPECÍFICAS	**OBJETIVOS ESPECÍFICOS**	**VARIABLES**	**DIMENSIONES**	**REACTIVOS**	**Instrumento**
¿Cuáles son las prácticas de ciberseguridad utilizadas por las empresas que operan bajo la modalidad de teletrabajo?	Identificar las prácticas de ciberseguridad utilizadas por las empresas que operan bajo la modalidad de teletrabajo.	Prácticas de ciberseguridad	Adiestramiento de personal	1-La empresa le ha ofrecido capacitación acerca de seguridad informática.	Todo el personal
			Reducción de vulnerabilidades	2- Se usa contraseñas en cada uno de los procesos y clientes que se administran. 3-Se cifra o encripta información de manera constante. 4-Se realiza control de procesos, que logran detectar actividades inusuales.	Director de TI/ director de Investigación/ equipo de tecnología.
			Instalación de sistemas y medidas de seguridad	5-Se emplea antivirus en todos los equipos de los empleados. 6-Se logra bloquear el acceso a personas no autorizadas mediante cortafuegos. 7-Se actualizan de manera constante las listas de acceso al uCXP.	
			Sentido común	8- Abre correos y archivos desconocidos en su PC 9-Usa redes de WIFI en todo lugar.	Todo el personal
		Teletrabajo	Resultados	10-El trabajo que se ejecuta se mide por resultados y no por horas laboradas.	
			Lugar	11-Las actividades de teletrabajo se pueden ejecutar desde cualquier espacio.	
			Adaptación	12-El teletrabajo desarrollado permite adaptarse a cambios	
			Horarios	13-Hay flexibilidad de horarios al desarrollar el teletrabajo.	

			Formación	14- el teletrabajo permite que ocurra capacitación continua.	
¿Cómo se puede establecer un marco de trabajo con los mecanismos y procedimientos de ciberseguridad en el teletrabajo apropiados para las empresas de desarrollo de software basada en los controles establecidos en la norma ISO 27002:2022 y la NIST SP 800-46?	Diseñar un marco de trabajo con los mecanismos y procedimientos de ciberseguridad en el teletrabajo apropiados para las empresas de desarrollo de software basada en los controles establecidos en la norma ISO 27002:2022 y la NIST SP 800-46.	Controles establecidos en la norma ISO 27002:2022 y la NIST SP 800-46.	Control organizacional	15- Se tratan temas relacionados con la política de seguridad de la información.	
				16- Los roles de seguridad de la información y Responsabilidades se encuentran claramente definidas con todos los clientes y empleados.	
				17-El personal se rige de acuerdo con la política de seguridad definida.	
				18- Se recoge y analiza la información relacionada a amenazas de seguridad.	
				19- Se menciona la existencia de un inventario de activos y los responsables de estos.	
				20- Usa las normas o reglas para el uso adecuado de activos de información.	
				21- El personal devuelve activos al finalizar relación laboral.	
				22-Se gestionan de manera adecuada permisos de accesos y las actualizaciones necesarias.	
				23-Estan establecidos los procesos de acceso, uso y remoción de la información en la nube.	
				24-La empresa está preparada para la gestión de incidentes de seguridad, incluso hay roles definidos.	
				25-Se revisa constantemente que se cumplan las políticas de seguridad.	
			Control de personas	26-Ante un ingreso se establecen responsabilidades en materia de seguridad que se mantienen hasta que finaliza la relación laboral	Director de TI/ director de Investigación/ equipo de tecnología. Recursos Humanos
				27-Existen mecanismos que permiten reportar eventos de seguridad a través de canales apropiados.	
			Control físico	28- Existen controles físicos para el acceso a las instalaciones.	

				29- Hay control permanente del escritorio y pantalla que buscan reducir el riesgo de ingreso a información confidencial.	
				30-Los dispositivos usados fuera de la empresa se protegen.	
				31-Se ejecutan revisiones de los equipos a fin de eliminar softwares sospechosos.	
			Control tecnológico	32-Se han implementado procedimientos para autenticación.	
				33-Se han implementado controles para evitar fuga de información.	
				34-La empresa vela por que se dirija, monitoree y se revisen las actividades que realizan terceros.	
				35- Se definen requisitos que deben cumplir los dispositivos móviles controlados por la organización para acceder a sus sistemas.	
				36- Se regula el uso de dispositivos BYOD personales o de terceros para acceder, procesar y transmitir información.	
¿Cómo se puede conocer el impacto del marco de trabajo de ciberseguridad en la ejecución de los procesos de desarrollo de software de la empresa Plugthem S.A.?	Evaluar el impacto del marco de trabajo de ciberseguridad en la ejecución de los procesos de desarrollo de software de la empresa Plugthem S.A.			37-Se mantiene respaldo adecuado de la información contenida en los sistemas de información ya sea de forma local o remota.	
				38-Existe autenticación mutua entre los diferentes dispositivos antes de establecer conexión o intercambio de información entre ellos.	
				39- Se ejecutan controles periódicos para asegurar que los usuarios tienen autorización para acceder a determinada información al tomar descansos largos en la jornada.	
				40- La red está segmentada apropiadamente para separar componentes públicos de los privados.	

Elaboración propia (2023).

Anexo 2. Validación del Instrumento

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTEFACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDADINFORMÁTICA

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 27002:2022Y LA NIST SP 800-46.

Validación de instrumento

AUTOR: Ing. Richard Sebastián Esparza

EchaniqueDIRECTOR: MSc.

Pedro Granda Gudiño

IBARRA - ECUADOR

2023

Ibarra, 11 de Octubre de 2023

MSc. Mauricio Rea.

De mis consideraciones:

Conocedor de su alta capacidad profesional me permito solicitarle, muy comedidamente, su valiosa colaboración en la validación de los instrumentos a utilizar en la recolección de datos sobre el tema:

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 27002:2022Y LA NIST SP 800-46.

Mucho agradeceré seguir las instrucciones que se detallan en la matriz de validación.

Aprovecho la oportunidad para reiterarle mi más distinguida consideración.

Atentamente

Ing. Richard Sebastián Esparza

EchaniqueC.I. 1723266407

VALIDACIÓN DE LA ENCUESTA POR EXPERTO

A continuación, se presenta la matriz de operacionalización y los instrumentos que se emplearán para la recolección de los datos. Esta matriz fue diseñada de acuerdo con el planteamiento del problema y variables que se consideraron para la investigación, que se encuentran vinculados con los objetivos general y específicos, en ella además se reflejan las variables de estudio, dimensiones y los reactivos. Posteriormente, se presenta el instrumento a emplear consistentes en un cuestionario para aplicar la técnica de la encuesta. Al final, se encuentra el instrumento que permitirá la validación, por parte del tutor como experto en el tema.

Operacionalización De Variables

TEMA	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.				
INTERROGANTE	¿Cómo se pueden implementar buenas prácticas de ciberseguridad en el teletrabajo para las empresas de desarrollo de software?				
OBJETIVO	Establecer un marco de trabajo de buenas prácticas de ciberseguridad en el teletrabajo para las empresas de desarrollo de software, a través de la síntesis de resultados de un estudio exploratorio.				
HIPÓTESIS	$H_{1:}$Las empresas de desarrollo de software que aplican controles establecidos en la norma ISO 27002:2022 Y LA NIST SP 800-46 tienen mayor ciberseguridad. H_0:Las empresas de desarrollo de software que aplican controles establecidos en la norma ISO 27002:2022 Y LA NIST SP 800-46 no tienen mayor ciberseguridad.				
INTERROGANTES ESPECÍFICAS	**OBJETIVOS ESPECÍFICOS**	**VARIABLES**	**DIMENSIONES**	**REACTIVOS**	**Instrumento**
¿Cuáles son las prácticas de ciberseguridad utilizadas por las empresas que operan bajo la modalidad de teletrabajo?	Identificar las prácticas de ciberseguridad utilizadas por las empresas que operan bajo la modalidad de teletrabajo.	Prácticas de ciberseguridad	Adiestramiento de personal	1-La empresa le ha ofrecido capacitación acerca de seguridad informática.	Todo el personal
			Reducción de vulnerabilidades	2- Se usa contraseñas en cada uno de los procesos y clientes que se administran. 3-Se cifra o encripta información de manera constante. 4-Se realiza control de procesos, que logran detectar actividades inusuales.	Director de TI/ Director de Investigación/ equipo de tecnología.
			Instalación de sistemas y medidas de seguridad	5-Se emplea antivirus en todos los equipos de los empleados. 6-Se logra bloquear el acceso a personas no autorizadas mediante cortafuegos. 7-Se actualizan de manera constante las listas de acceso al uCXP.	
			Sentido común	8- Abre correos y archivos desconocidos en su PC 9-Usa redes de WIFI en todo lugar.	Todo el personal
		Teletrabajo	Resultados	10-El trabajo que se ejecuta se mide por resultados y no por horas laboradas.	
			Lugar	11-Las actividades de teletrabajo se pueden ejecutar desde cualquier espacio.	
			Adaptación	12-El teletrabajo desarrollado permite adaptarse a cambios	

			Horarios	13-Hay flexibilidad de horarios al desarrollar el teletrabajo.	
			Formación	14- El teletrabajo permite que ocurra capacitación continua.	
¿Cómo se puede establecer un marco de trabajo con los mecanismos y procedimientos de ciberseguridad en el teletrabajo apropiados para las empresas de desarrollo de software basada en los controles establecidos en la norma ISO 27002:2022 y la NIST SP 800-46?	Diseñar un marco de trabajo con los mecanismos y procedimientos de ciberseguridad en el teletrabajo apropiados para las empresas de desarrollo de software basada en los controles establecidos en la norma ISO 27002:2022 y la NIST SP 800-46.	Controles establecidos en la norma ISO 27002:2022 y la NIST SP 800-46.	Control organizacional	15- Se tratan temas relacionados con la política de seguridad de la información.	
				16- Los roles de seguridad de la información y Responsabilidades se encuentran claramente definidas con todos los clientes y empleados.	
				17-El personal se rige de acuerdo con la política de seguridad definida.	
				18- Se recoge y analiza la información relacionada a amenazas de seguridad.	
				19- Se menciona la existencia de un inventario de activos y los responsables de estos.	
				20- Usa las normas o reglas para el uso adecuado de activos de información.	
				21- El personal devuelve activos al finalizar relación laboral.	
				22-Se gestionan de manera adecuada permisos de accesos y las actualizaciones necesarias.	
				23-Estan establecidos los procesos de acceso, uso y remoción de la información en la nube.	
				24-La empresa está preparada para la gestión de incidentes de seguridad, incluso hay roles definidos.	
				25-Se revisa constantemente que se cumplan las políticas de seguridad.	
			Control de personas	26-Ante un ingreso se establecen responsabilidades en materia de seguridad que se mantienen hasta que finaliza la relación laboral	Director de TI/ Director de Investigación/ equipo de tecnología.
				27-Existen mecanismos que permiten reportar eventos de seguridad a través de canales apropiados.	
			Control físico	28- Existen controles físicos para el acceso a las instalaciones.	

				29- Hay control permanente del escritorio y pantalla que buscan reducir el riesgo de ingreso a información confidencial.	Recursos Humanos
				30-Los dispositivos usados fuera de la empresa se protegen.	
				31-Se ejecutan revisiones de los equipos a fin de eliminar softwares sospechosos.	
			Control tecnológico	32-Se han implementado procedimientos para autenticación.	
				33-Se han implementado controles para evitar fuga de información.	
				34-La empresa vela por que se dirija, monitoree y se revisen las actividades que realizan terceros.	
				35- Se definen requisitos que deben cumplir los dispositivos móviles controlados por la organización para acceder a sus sistemas.	
				36- Se regula el uso de dispositivos BYOD personales o de terceros para acceder, procesar y transmitir información.	
¿Cómo se puede conocer el impacto del marco de trabajo de ciberseguridad en la ejecución de los procesos de desarrollo de software de la empresa Plugthem S.A.?	Evaluar el impacto del marco de trabajo de ciberseguridad en la ejecución de los procesos de desarrollo de software de la empresa Plugthem S.A.			37-Se mantiene respaldo adecuado de la información contenida en los sistemas de información ya sea de forma local o remota.	
				38-Existe autenticación mutua entre los diferentes dispositivos antes de establecer conexión o intercambio de información entre ellos.	
				39- Se ejecutan controles periódicos para asegurar que los usuarios tienen autorización para acceder a determinada información al tomar descansos largos en la jornada.	
				40- La red está segmentada apropiadamente para separar componentes públicos de los privados.	

Elaboración propia (2023).

Escala: siempre, casi siempre, algunas veces, raras veces, nunca

Investigación: 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.

Técnica Encuesta. Instrumento: Cuestionario

Instrumento para ser llenado por todo el personal de la empresa:

Instrucciones marque con x la (s) respuesta (s) que usted considere de cada pregunta.

DIMENSIONES	REACTIVOS	Siempre	Casi siempre	Algunas veces	Raras veces	Nunca
Adiestramiento de personal	1-La empresa le ha ofrecido adiestramiento acerca de seguridad informática.					
Sentido común	8- Abre correos y archivos desconocidos en su PC 9-Usa redes de WIFI en todo lugar.					
Resultados	10-El trabajo que se ejecuta se mide por resultados y no por horas laboradas.					
Lugar	11-Las actividades de teletrabajo se pueden ejecutar desde cualquier espacio.					
Adaptación	12-El teletrabajo desarrollado permite adaptarse a cambios					
Horarios	13-Hay flexibilidad de horarios al desarrollar el teletrabajo.					
Formación	14- el teletrabajo permite que ocurra capacitación continua.					
Control organizacional	15- Se tratan temas relacionados con la política de seguridad de la información.					
	16- Los roles de seguridad de la información y Responsabilidades se encuentran claramente definidas con todos los clientes y empleados.					
	17-El personal se rige de acuerdo con la política de seguridad definida.					
	18- Se recoge y analiza la información relacionada a amenazas de seguridad.					
	19- Se menciona la existencia de un inventario de activos y los responsables de estos.					

	20- Usa las normas o reglas para el uso adecuado de activos de información.					
	21- El personal devuelve activos al finalizar relación laboral.					
	22-Se gestionan de manera adecuada permisos de accesos y las actualizaciones necesarias.					
	23-Estan establecidos los procesos de acceso, uso y remoción de la información en la nube.					
	24-La empresa está preparada para la gestión de incidentes de seguridad, incluso hay roles definidos.					
	25-Se revisa constantemente que secumplan las políticas de seguridad.					

Elaboración propia (2023).

Investigación: MARCO DE TRABAJO DE BUENAS PRÁCTICAS DE CIBERSEGURIDAD EN EL TELETRABAJO PARA LAS EMPRESAS DE DESARROLLO DE SOFTWARE BASADO EN LOS CONTROLES ESTABLECIDOSEN LA NORMA ISO 27002:2022 Y LA NIST SP 800-46.

Técnica Encuesta. Instrumento: Cuestionario

Instrumento para ser llenado por Director de TI/ Director de Investigación/ equipo de tecnología. Recursos Humanos.

Instrucciones marque con x la (s) respuesta (s) que usted considere de cada pregunta.

DIMENSIONES	**REACTIVOS**	**Siempre**	**Casi siempre**	**Algunas veces**	**Raras veces**	**Nunca**
Reducción de vulnerabilidades	2- Se usa contraseñas en cada uno de los procesos y clientes que se administran.					
	3-Se cifra o encripta información de manera constante.					
	4-Se realiza control de procesos, que logran detectar actividades inusuales					
Instalación de sistemas y medidas de seguridad	5-Se emplea antivirus en todos los equipos de los empleados.					
	6-Se logra bloquear el acceso a personas no autorizadas mediante cortafuegos.					
	7-Se actualizan de manera constante las listas de acceso al uCXP.					
Control de personas	26-Ante un ingreso se establecen responsabilidades en materia de seguridad que se mantienen hasta que finaliza la relación laboral					
	27-Existen mecanismos que permiten reportar eventos de seguridad a través de canales apropiados.					
Control físico	28- Existen controles físicos para el acceso a las instalaciones.					
	29- Hay control permanente del escritorio y pantalla que buscan reducir el riesgo de ingreso a información confidencial.					
	30-Los dispositivos usados fuera de la empresa se protegen.					
	31-Se ejecutan revisiones de los equipos a fin de eliminar softwares sospechosos.					

Control tecnológico	32-Se han implementado procedimientos para autenticación.					
	33-Se han implementado controles para evitar fuga de información.					
	34-La empresa vela por que se dirija, monitoree y se revisen las actividades que realizan terceros.					
	35- Se definen requisitos que deben cumplir los dispositivos móviles controlados por la organización para acceder a sus sistemas.					
	36- Se regula el uso de dispositivos BYOD personales o de terceros para acceder, procesar y transmitir información.					
	37-Se mantiene respaldo adecuadode la información contenida en los sistemas de información ya sea de forma local o remota.					
	38-Existe autenticación mutua entre los diferentes dispositivos antes de establecer conexión o intercambio de información entre ellos.					
	39- Se ejecutan controles periódicos para asegurar que los usuarios tienen autorización para acceder a determinada información al tomar descansos largos en la jornada.					
	40- La red está segmentada apropiadamente para separar componentes públicos de los privados.					

Elaboración propia (2023).

Instrumento de validación

INSTRUCCIONES

1. El instrumento debe ser llenado por el o la experto (a) en el área.
2. Leer detenidamente cada ítem
3. En los espacios redacción, pertinencia, coherencia colocar la letra según sea su criterio, siguiendo la leyenda que se presenta

Bien	Regular	Deficiente
B	R	D

4. Utilizar el espacio de observación si lo considera necesario.
5. Llenar observaciones generales de ser necesario.
6. Llenar los datos que se solicitan al final del instrumento.

REACTIVOS	REDACCIÓN	PERTINENCIA	COHERENCIA	OBSERVACIÓN
1-La empresa le ha ofrecido adiestramiento acerca de seguridad informática.	R	B	B	Sugiero utilizar "capacitación"
2- Se usan contraseñas en cada uno de los procesos y clientes que se administran.	B	B	B	
3-Se cifra o encripta información de manera constante.	B	B	B	
4-Se realiza control de procesos, que logran detectar actividades inusuales.	B	B	B	
5-Se emplea antivirus en todos los equipos de los empleados.	B	B	B	
6-Se logra bloquear el acceso a personas no autorizadas mediante cortafuegos.	B	B	B	
7-Se actualizan de manera constante las listas de acceso al uCXP.	B	B	B	Colocar significado de las siglas o el nombre más amplio del producto.
8- Abre correos y archivos desconocidos en su PC	B	B	B	
9-Usa redes de WIFI en todo lugar.	B	B	B	
10-El trabajo que se ejecuta se mide por resultados y no por horas laboradas.	R	R	R	¿Esta pregunta cómo la relacionamos con el tema de ciberseguridad en teletrabajo? Sugiero cambiar la redacción para direccionar a la búsqueda de

				una información más específica.
11-Las actividades de teletrabajo se pueden ejecutar desde cualquier espacio.	B	B	B	
12-El teletrabajo desarrollado permite adaptarse a cambios	B	B	B	
13-Hay flexibilidad de horarios al desarrollar el teletrabajo.	R	R	R	Igual observación que el reactivo 10.
14- El teletrabajo permite que ocurra capacitación continua.	B	B	B	
15- Se tratan temas relacionados con la política de seguridad de la información.	B	B	B	
16- Los roles de seguridad de la información y Responsabilidades se encuentran claramente definidas con todos los clientes y empleados.	B	B	B	
17-El personal se rige de acuerdo con la política de seguridad definida.	B	B	B	
18- Se recoge y analiza la información relacionada a amenazas de seguridad.	B	B	B	
19- Se menciona la existencia de un inventario de activos y los responsables de estos.	B	B	B	
20- Usa las normas o reglas para el uso adecuado de activos de información.	B	B	B	
21- El personal devuelve activos al finalizar relación laboral.	B	B	B	
22-Se gestionan de manera adecuada permisos de accesos y las actualizaciones necesarias.	B	B	B	
23-Estan establecidos los procesos de acceso, uso y remoción de la información en la nube.	B	B	B	
24-La empresa está preparada para la gestión de incidentes de seguridad, incluso hay roles definidos.	B	B	B	
25-Se revisa constantemente que se cumplan las políticas de seguridad.	B	B	B	
26-Ante un ingreso se establecen responsabilidades en materia de seguridad que se mantienen hasta que finaliza la relación laboral	B	B	B	
27-Existen mecanismos que permiten reportar eventos de seguridad a través de canales apropiados.	B	B	B	
28- Existen controles físicos para el acceso a las instalaciones.	B	B	B	
29- Hay control permanente del escritorio y pantalla que buscan reducir el riesgo de ingreso a información confidencial.	B	B	B	
30-Los dispositivos usados fuera de la empresa se protegen.	B	B	B	

31-Se ejecutan revisiones de los equipos a fin de eliminar softwares sospechosos.	B	B	B	Poner software sospechoso
32-Se han implementado procedimientos para autenticación.	B	B	B	
33-Se han implementado controles para evitar fuga de información.	B	B	B	
34-La empresa vela por que se dirija, monitoree y se revisen las actividades que realizan terceros.	B	B	B	
35- Se definen requisitos que deben cumplir los dispositivos móviles controlados por la organización para acceder a sus sistemas.	B	B	B	
36- Se regula el uso de dispositivos BYOD personales o de terceros para acceder, procesar y transmitir información.	B	B	B	Colocar también el significado de las siglas.
37-Se mantiene respaldo adecuado de la información contenida en los sistemas de información ya sea de forma local o remota.	B	B	B	
38-Existe autenticación mutua entre los diferentes dispositivos antes de establecer conexión o intercambio de información entre ellos.	B	B	B	
39- Se ejecutan controles periódicos para asegurar que los usuarios tienen autorización para acceder a determinada información al tomar descansos largos en la jornada.	B	B	B	
40- La red está segmentada apropiadamente para separar componentes públicos de los privados.	B	B	B	

Elaboración propia (2023).

OBSERVACIONES GENERALES	
El instrumento en general tiene una buena estructura y cumple con aportar información relacionada a los objetivos planteados. Sugiero que considere (consultando a su director) la adición de unos reactivos en relación a la gestión de la continuidad de los servicios que permiten (o van a permitir) el teletrabajo.	
DATOS DEL VALIDADOR	
NOMBRE	XAVIER MAURICIO REA PEÑAFIEL – CI: 1002485744
TÍTULOS	Ingeniero en Sistemas Computacionales, Magíster en Gerencia Informática.
ÁREA DE DESEMPEÑO	Arquitectura de software
FIRMA	 Firmado electrónicamente por: **XAVIER MAURICIO REA PEÑAFIEL**
FECHA	19 de octubre de 2023