UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Marco de trabajo de seguridad de información basado en la ISO/IEC 27001:2013 para el control de acceso de los usuarios en empresas de teletrabajo

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES:

Paredes Cóndor, Julio César (ORCID: 0000-0001-9407-0402)

Voto Bernales Villalobos, Carlos Andrés (ORCID: 0000-0002-7122-8155)

ASESOR:

Mg. Saboya Ríos Nemias (ORCID: 0000-0002-7166-2197)

LÍNEA DE INVESTIGACIÓN:

Auditoría y seguridad de la información

LIMA – PERÚ

2021

Dedicatoria

A nuestro Dios Todo Poderoso que nos permitió avanzar hasta este momento. A nuestras familias por su constante apoyo y motivación.

Agradecimiento

Expresamos nuestro agradecimiento a la Universidad César Vallejo, por el apoyo brindado; a nuestros maestros por sus conocimientos brindados en nuestra formación y a nuestro asesor, el Mg Nemias Saboya Rios, por su dedicación en el desarrollo de la presente investigación.

También a nuestros padres por su amor y paciencia, a nuestros amigos por sus constantes ánimos al apoyarnos en nuestra formación profesional. A todos, gracias.

Índice de contenidos

Índice de Tablas

Índice gráficos y figuras

Resumen

El presente informe de tesis que fue desarrollado en el año 2021, tuvo como finalidad, la creación de un marco de trabajo alineado a la metodología ISO/IEC 27001:2013 para el control de accesos de la seguridad de información de empresas orientadas a teletrabajo, todo ello bajo el enfoque de investigación experimental con tipo pre experimental, el cual surgió debido a la situación actual de salud que afrontó el mundo, lo que llevó a muchas empresas, a migrar a una modalidad de trabajo remoto.

Los resultados obtenidos de los 30 registros del informe de tesis reflejaron que hubo una disminución en el porcentaje total de accesos no autorizados a la información de un 65.4% a un 37.5%, asimismo, el porcentaje total de información modificada sin autorización disminuyó de un 40.1% a 18.1% y finalmente, el porcentaje total de interrupciones a la accesibilidad a la información disminuyó de 65.40% a 37.1%

Con lo dicho previamente se concluyó que el marco de trabajo de seguridad de información basado en la ISO/IEC 27001:2013 para el control de acceso de los usuarios influye significativamente en la seguridad de información en empresas de teletrabajo

Palabras clave: marco de trabajo, seguridad de la información, ISO/IEC

27001:2013, confidencialidad, integridad, disponibilidad.

Abstract

The purpose of this thesis report, which was developed in 2021, was to create a framework aligned to the ISO/IEC 27001:2013 methodology for information security Access control of telework oriented companies, all this under the pre-experimental type of experimental research approach, which arose due to the current health situation facing the worls, which led many companies to migrate to a remote work modality.

The results obtained from the 30 records of the tesis report reflected that there was a decrease in the total percentage of unauthorized Access to information from 65.4% to 37.5%, likewise, the totalpercentage of information modified without authorization decreased from 40.1% to 18.1% and finally, the total percentage of interruptions to information accessibility decreased from 65.4% to 37.1%.

With the aforementioned, it was concluded that the information security framework based on ISO/IEC 27001:2013 for user Access control significantly influences information security in teleworking companies.

Keywords: framework, information security, ISO/IEC 27001:2013, confidentiality, integrity, availability.

I. INTRODUCCIÓN

La seguridad de la información a través de los años hasta la actualidad ha ido ocupando un mayor grado de importancia en las compañías, debido a los ataques informáticos que han ido evolucionando y aumentando durante los últimos años, poniendo en riesgo la información de las empresas. Actualmente, utilizar un sistema de antivirus, ya no es suficiente para mantener protegidos los activos de cada empresa y estos cada día son más vulnerables (Morales, Toapanta y Toasa 2020), de esta manera, durante los últimos años, debido a la integración de la tecnología digital y la migración de la información a un medio virtual, ha ocasionado que las empresas se vean en la necesidad de aumentar sus sistemas de seguridad para proteger dichos activos, lo cual se convierte en un verdadero reto para ellas.

La información es el principal activo dentro de cualquier compañía, ya que es parte fundamental de la toma de decisiones para las partes interesadas (Mariño y Alfonso 2019). Por ello, el área de Tecnología de la información es responsable de derivar y almacenar dicha información en un ambiente seguro, en este caso, en los servidores correspondientes, protegiendo correctamente las bases de datos, ante cualquier hurto y manipulación de personal no autorizado (Patiño, Caicedo y Guaña 2019). Según DPA International gran parte de los dispositivos que permiten el control de acceso, se encuentran relacionados y monitoreados a través de un servidor y un software personalizado del fabricante, la comunicación entre un dispositivo y el servidor debe ser cifrado para que con ello, el agente de amenaza no tenga la capacidad de recoger datos de los usuarios que permitan infiltrarse en el servidor, aunque el atacante puede usurpar el lugar del servidor y forzar ciertas actualizaciones que le permitan añadir nuevos usuarios que puedan alterar la seguridad del dispositivo(Souza, Arima y Belda 2020). La infraestructura de una empresa puede ser monitoreada constantemente, pero ello no garantiza que los riesgos sean menores, ya que siempre dependerá de los procesos que se manejen Se debe tener en cuenta que existen situaciones complejas en las cuales puede existir un ingreso no autorizado o el robo de identidad a un personal de la empresa, el cual permitiría que se logre acceder a información comprometedora para la empresa, por lo cual tener un control de accesos de los usuarios minimizaría el riesgo de este tipo de situaciones (Romero et al. 2018)

Para garantizar que los índices de seguridad sean aceptables para la información que tiene la empresa, es necesario realizar un plan de tratamiento de riesgos, el cual se deberá aprobar por la alta gerencia (Valencia y Orozco 2017). Una gran mayoría de autores se mantienen efectuando una gran cantidad de conjuntos de varias teorías/técnicas como lo son un SGSI, marcos de trabajo, metodologías para realizar procesos, entre otras para examinar, las transgresiones de los protocolos de seguridad instaurados previamente, en los sistemas de información, a causa, de un error humano. También debemos recordar, que el conocimiento se genera a través de nuevos estudios, los cuales podrían desembocar en teorías inéditas, las cuales si se combinan con otras previas, generaría otro tipo de teoría, y así de manera sucesiva e infinita (Bayona y Altamarino 2017). Hasta la actualidad se siguen planteando y realizando investigaciones, evaluando los riesgos que se presentan en las empresas y seguir manteniendo segura la información; y tratar de que dicho margen de riesgo se mantenga en lo más mínimo posible.

Los planes de mejora, aseguran las dimensiones de accesibilidad, integridad y disponibilidad; frente a algún factor existente de riesgo (Andrade y Chavez 2018).

Debido a la pandemia actual que acontece en el mundo, el teletrabajo ha surgido como una solución para continuar con muchas labores, pero ya que la gran mayoría de empresas aún no están preparadas para dicho método de trabajo, la cantidad de ataques ha aumentado día con día, pero no directamente a las empresas, sino a los usuarios, ya que los atacantes, deducen que en los hogares de los trabajadores no existirá la suficiente seguridad, por lo cual ellos podrán infiltrarse y a partir de ahí llegar a información sensible de la empresa (García 2021) .

Los sistemas de prevención contra ataques cibernéticos, actualmente se han convertido en algo más complejo de manejar debido al teletrabajo, ya que ahora los equipos y la red utilizada para manejar la información, ya no solo está centralizada dentro de la empresa, sino que ahora se extiende hasta los hogares de los trabajadores, donde no se tiene un control correcto de los equipos que utilizan (Christiansen 2020). Los ataques de ransomware han optado por utilizar los mecanismos aplicados en los protocolos de escritorio remoto, aprovechando que los usuarios utilizan contraseñas débiles, dichos ataques mediante este método, han incrementado a lo largo del año 2020 hasta la actualidad (Sierra 2021).

En el Perú, utilizando el estándar ISO/IEC 27001:2013 se detectó, que ello contribuyó de manera positiva en la seguridad de información dentro de una entidad de finanzas, al aplicarlo en conjunto a un plan de gestión obteniendo un resultado favorable de un 96.81% a 99.93% en las dimensiones de seguridad, tales como disponibilidad, confidencialidad e integridad de la información (Aguinaga 2021)

De acuerdo con las problemáticas expuestas anteriormente el estudio planteó el siguiente problema general ¿De qué manera un marco de trabajo de seguridad de información para el control de acceso de usuarios utilizando la ISO/IEC 27001:2013 tiene influencia en instituciones orientado al teletrabajo?

Por ello se toma en cuenta los siguientes problemas específicos ¿En qué medida afecta gestionar la norma ISO/IEC 27001:2013 en la confidencialidad para la seguridad de información en instituciones orientadas a teletrabajo?

¿En qué medida afecta la norma ISO/IEC 27001:2013 en la integridad para la seguridad de información en instituciones orientadas a teletrabajo?

¿En qué medida mejora la disponibilidad la norma ISO/IEC 27001:2013 para la seguridad de información en instituciones orientadas a teletrabajo?

El presente informe de tesis se justifica de modo metodológico, ya que, recomienda a la empresa desarrollar un marco de trabajo utilizando la norma ISO/IEC 27001:2013, la cual es una norma a nivel internacional orientado a garantizar la seguridad, que los datos e información se mantengan íntegros y que se encuentren bajo un marco de máxima confidencialidad, mejorando el control de acceso de sus usuarios y garantizar su integridad (International Organization for Standardization 2013). La justificación práctica emerge por la obligación de monitorizar el control de acceso de sus usuarios y más aún hoy en día, que el teletrabajo incrementó de manera considerable, debido a la pandemia global; requiriendo un mayor control debido a que las herramientas ahora se manejan de manera externa a la empresa, por lo cual, un marco de trabajo bajo el estándar ISO/IEC 27001:2013 defiende, protege y gestiona el conjunto de datos como uno de los recursos con mayor importancia en la empresa (Gómez 2018). La justificación teórica se realiza con el propósito de aportar mucho más en el conocimiento existente, acerca de un marco de trabajo de seguridad de información bajo la ISO/IEC 27001:2013, ya que su

propuesta mejorará la seguridad de información y el nivel de desempeño dentro de la empresa (Ocaña y López 2019).

.

Luego de lo mencionado previamente, se definió como objetivo general: Determinar la influencia de un marco de trabajo de seguridad de información para el control de acceso basado en la norma ISO/IEC 27001:2013 en empresas de teletrabajo y como objetivos específicos.

Determinar la mejora desarrollando un marco de trabajo de seguridad de la información basado en la norma ISO/IEC 27001:2013 en la confidencialidad de información en empresas de teletrabajo. Determinar la mejora desarrollando un marco de trabajo de seguridad de la información basado en la norma ISO/IEC 27001:2013 en la integridad de la información en empresas de teletrabajo. Determinar la mejora desarrollando un marco de trabajo de seguridad de la información basado en la norma ISO/IEC 27001:2013 en la disponibilidad de la información en empresas de teletrabajo.

Se planteó la siguiente hipótesis general: El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO/IEC 27001:2013 mejora la seguridad de información en el control de acceso de los usuarios en las instituciones orientadas a teletrabajo.

De la misma manera las hipótesis específicas: El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO/IEC 27001:2013 mejora la confidencialidad de información en los controles de acceso de usuarios en instituciones orientadas a teletrabajo. El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO/IEC 27001:2013 mejora la integridad de información en los controles de acceso de usuarios en instituciones orientadas a teletrabajo. El desarrollo de un marco de trabajo de seguridad de información utilizando la norma ISO/IEC 27001:2013 mejora la disponibilidad de información en los controles de acceso de usuarios en instituciones orientadas a teletrabajo.

II. MARCO TEÓRICO

En el siguiente párrafo, se detalla los antecedentes internacionales y locales para el respaldo de esta investigación.

(Šikman, Latinović y Paspalj 2019) en su artículo científico del año 2019, tuvieron como objetivo general, reconocer los beneficios que conlleva la ejecución del estándar ISO/IEC 27001 en la protección de los recursos informáticos de una institución, lo cual llevo a la conclusión que el estándar ISO/IEC 27001:2013 detalla la manera en que debe dirigirse la seguridad de información en una determinada organización o empresa, lo cual es respaldado por el innumerable número de instituciones que la han llevado a cabo, certificándose.

(Patiño, Caicedo y Guaña 2019) el objetivo de su artículo científico del 2019, fue determinar y encontrar las vulnerabilidades y ejecutar una valoración de sus controles de seguridad, orientados a la eficiencia, con respecto al acceso a los sistemas y aplicativos de la institución, ello fue aplicado en dos empresas, cuyos nombres no fueron revelados por un tema de confidencialidad. Se concluyó que, en ambas empresas, se debe poner en práctica un método formal, para que puedan registrar y eliminar los permisos, que deberá tener cada usuario, con respecto al área a la que pertenece, ya que el nivel de madurez de sus controles de acceso era bajo.

(Palma 2019) El objetivo general de su tesis del año 2019, fue esquematizar un protocolo de seguridad para el control de acceso hacia la infraestructura de red, dicho protocolo tomaría referencia del estándar ISO/IEC 27002:2013. Para ello, se realizaría el análisis de la mayoría de los controles, que posee dicho estándar, lo cual ayudaría a reforzar la seguridad de la confidencialidad, disponibilidad e integridad de la información. Dicho estudio logro subsanar las amenazas que se pudieran presentar dentro de la red del hospital potenciando el nivel de servicio y la constancia del mismo, lo cual llevaría a prevenir cualquier inconveniente con las dimensiones de la información propuestas.

(Ruíz, Estrada y Sánchez 2020): El objetivo de su artículo del 2020, fue realizar el análisis, desarrollo y en base a ello, proponer un patrón adecuado para gestionar la calidad de mantener la información segura, teniendo de guía el estándar ISO/IEC 27001:2013, aplicándolo en establecimientos educativos, ello permitirá identificar con mayor facilidad, los riesgos que podrían irrumpir en la seguridad de establecimientos de Educación superior. Mediante dicho artículo se logró determinar una notable mejora luego de aplicar las buenas prácticas recomendadas con respecto a la seguridad de la información.

(Baca et al. 2020) en su artículo del 2020, su objetivo fue realizar el análisis en base a los efectos que produce la implementación del estándar ISO/IEC 27001 en una compañía peruana. Luego de dicha implementación, se detectó que la disponibilidad, integridad y confidencialidad de la información, fue afecta en gran medida.

(Sasavilca 2017) en su tesis, el objetivo que plantearon fue analizar cuál sería el efecto de utilizar los estándares de la ISO/IEC 27001 dentro del ámbito de un Centro De Atención Telefónica, como Atento en el Perú, en lo que respecta a la seguridad de la información, durante el año 2017. Se concluyó que el nivel de información manipulada sin autorización se redujo hasta en un 97%.

(Arias 2020) en su tesis del 2020 en Perú. Plantearon como objetivo general describir los pasos necesarios que se requieren para implementar el estándar ISO/IEC 27001 en el área de T.I, de la compañía Esvicac, ubicada en Callao, Perú. La conclusión que se obtuvo fue que los procesos que manejaba la empresa en dicho momento mejoraron notablemente, lo cual permitió que los servicios se mantuvieran estables y ello, mejoró la experiencia de los clientes con respecto a los servicios que la compañía brindaba.
En más de 40 países, en una amplia variedad de organizaciones, para exponer las los procesos más efectivos para salvaguardar y proteger la información, constatando que una empresa tiene seguro dicho activo, un sistema que tome como base a la ISO/IEC 27001:2013 proporcionara un enfoque sistemático, para garantizar la seguridad de la integridad, confidencialidad y disponibilidad de la

información corporativa, estos controles bajo la ISO/IEC 27001:2013 se basan en identificar y combatir la gama entera de los posibles riesgos que podrían acontecer a los principales activos de la compañía (Calder 2017).

Según la página oficial (International Organization for Standardization 2013), la ISO/IEC 27001:2013 es un estándar perteneciente a la familia ISO/IEC 27000, el cual proporciona los principales requerimientos que serán necesarios para poder implementar un correcto sistema, para la gestión de la seguridad de la información. (SGSI). Utilizarla permite que las organizaciones o empresas de cualquier tamaño, puedan gestionar cualquier tipo de seguridad dentro de sus activos, tales como información de empleados, datos bancarios, la integridad de la propia empresa o información que haya sido entregada y confiada a la organización, por terceras partes. Esta norma se realizó de manera genérica, lo cual permite que sea aplicable en cualquier tipo de institución, sin importar el rubro o la cantidad de información que manejen.

Dentro de la norma ISO/IEC 27001:2013 existe el Anexo A, donde se describen los controles de seguridad que serán necesarios durante la implementación.

Entre la versión de 2005 y la del 2013, se descartaron una cantidad reducida de requisitos, tales como las acciones preventivas y el requisito para documentar ciertos procedimientos, los cuales se enumeran en la siguiente Tabla 1:

Tabla 1. *ISO 27001/2005-2013 y su evolución*

<table>
<tr><td>ISO/IEC 27001:2005</td><td colspan="2">ISO/IEC 27001:2013</td></tr>
<tr><td colspan="2">NÚMERO DE CONTROLES</td><td>Observaciones</td></tr>
<tr><td rowspan="3">133</td><td rowspan="3">114</td><td>94 permanecieron</td></tr>
<tr><td>39 fueron eliminados</td></tr>
<tr><td>20 fueron agregados</td></tr>
<tr><td colspan="3">DOMINIOS DE SEGURIDAD</td></tr>
<tr><td>11</td><td>14</td><td>3 dominios agregados</td></tr>
<tr><td colspan="3">REQUISITOS DE GESTIÓN</td></tr>
<tr><td>102</td><td>130</td><td>18 REQ-GEST nuevos</td></tr>
</table>

Fuente: ISO/IEC 27001:2013

A continuación, en la Figura 1, se presentan los dominios de la ISO/IEC 27001:2013 presentes en el Anexo A.

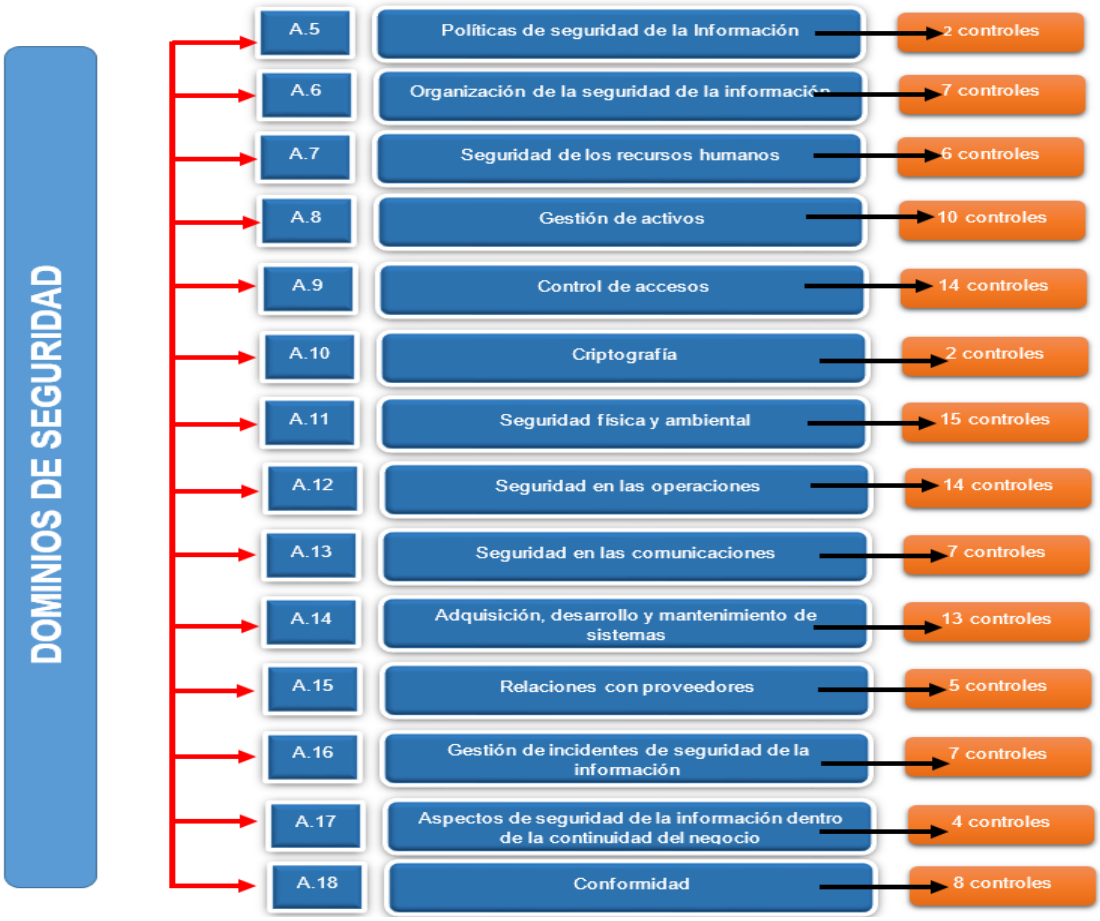


Figura 1. Dominios de la ISO/IEC 27001:2013

Para el presente informe de tesis se tomó los dominios A6 y A9, el dominio A6 denominado Estructura de la seguridad de la información, el cual posee 7 controles, donde podemos encontrar el Anexo A.6.2.2 que está enfocado al teletrabajo o trabajo remoto, tal cual se puede apreciar en la siguiente tabla N° 2:

Tabla 2. *Dominio A.6.2 - descripción*

A.6.2 Dispositivos móviles y teletrabajo
Finalidad: Asegurar la seguridad del trabajo remoto y la utilización de equipos móviles

A.6.2.1	Política para dispositivos móviles	**Control** Deberá plantearse medidas de seguridad de respaldo y políticas de seguridad para manejar los peligros latentes al utilizarse equipos móviles
A.6.2.2	Teletrabajo	**Control** Se debe poner en práctica medidas de seguridad de respaldo y políticas con el fin de mantener la información segura y que no sea afectada de ninguna forma, evitando así interrupciones en el acceso, en almacenamiento o registro de la información.

Fuente: ISO/IEC 27001:2013

Con respecto al Dominio 9, denominado controles de acceso, que posee 14 controles, se tomó el anexo A.9.1.1 y el anexo A.9.1.2 el cual habla sobre las políticas de control de acceso y el acceso a los servicios de red, que se puede apreciar en la siguiente Tabla N° 3:

Tabla 3. *Dominio A.9.1 - descripción*

A.9.1 Requisitos del negocio para control de acceso		
Objetivo: Restringir la entrada a los recursos de procesamiento de la información		
A.9.1.1	Política de control de acceso	Control Se instaura, se realiza la documentación y se procede con la revisión de la política para el control de acceso, que toma como referencia la seguridad de información y los requerimientos de la institución.

A.9.1.2	Acceso a las redes y a los servicios de red	Control El acceso a las redes y sus servicios, deben ser de uso exclusivo a los usuarios que hayan obtenido la autorización por parte de la empresa.

Fuente: ISO/IEC 27001:2013

Una vez que fueron definido los anexos de referencia para el informe de tesis, según la (International Organization for Standardization 2013) propone un sistema de gestión de la seguridad de la información con las siguientes fases para que pueda ser completado exitosamente, el cual ha sido adaptado en la siguiente Figura 2:

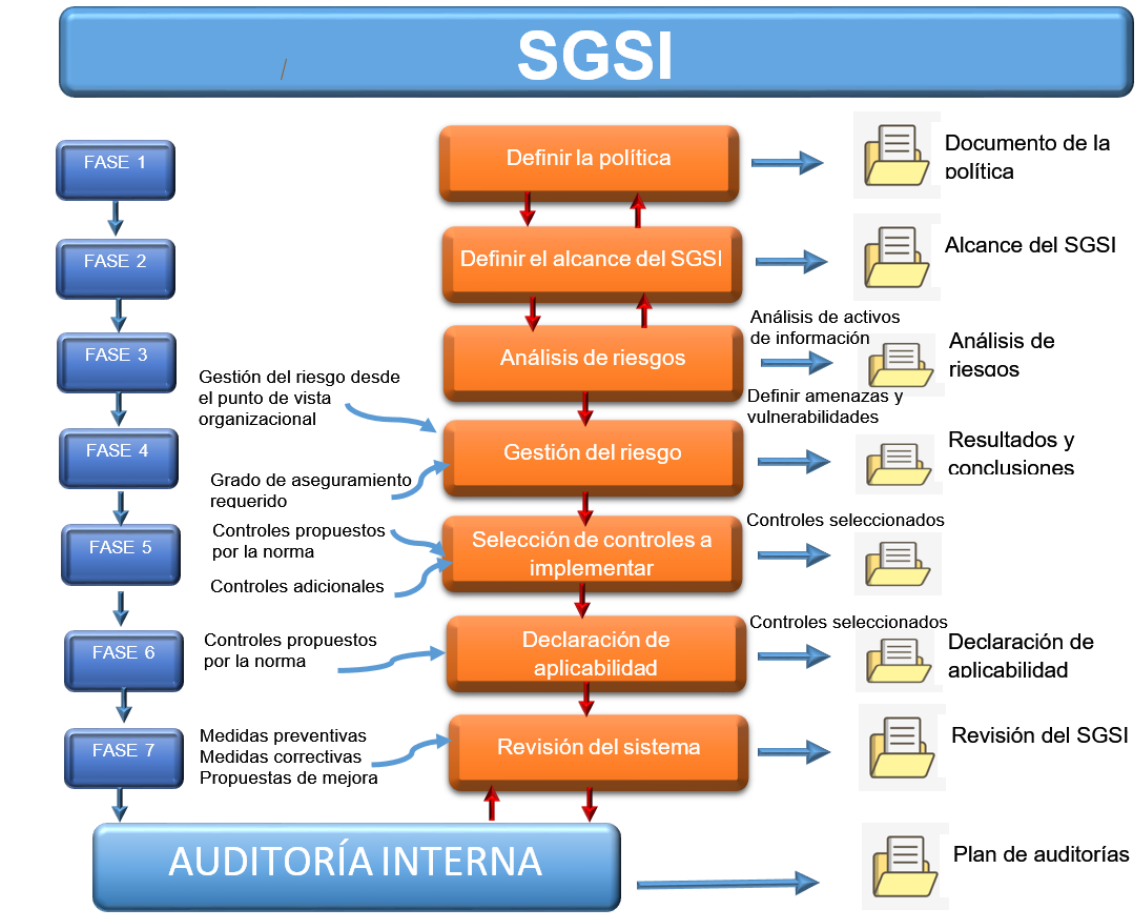


Figura 2. Fases para la implementación de un SGSI según ISO/IEC 27001:2013

Para este informe de tesis se denomina al marco de trabajo como un conjunto de conceptos, criterios y prácticas enfocados a un problema determinado (Pressman 2015). Y un marco de trabajo de seguridad de información, nos permite estructurar las bases necesarias para ordenar las partes de un proceso, en donde se incluyen, las reglas a tenerse en consideración, las actividades que se realizan y la metodología que se aplica dentro de cualquier evento posible, sin tomar en cuenta lo complejo que pueda ser o su tamaño. (MELLON 2010).

Esta investigación desarrollara el presente marco de trabajo aplicando un conjunto de estándares que se encuentra asociados al estándar ISO 27000, la cual es la fuente de donde deriva la ISO/IEC 27001:2013, la cual abarca un grupo de determinados buenos procedimientos a realizarse para que el sistema de gestión de seguridad de la información pueda establecer de manera adecuada, implementarse y llevar el mantenimiento adecuado para su mejora continua. (International Organization for Standardization 2013), utilizando principalmente la norma ISO/IEC 27001:2013, que proporciona un enfoque sistemático para garantizar de manera adecuada la integridad, disponibilidad y confidencialidad de la información corporativa (Alan (Calder 2017), y se tomara en cuenta un pequeño porcentaje de la ISO 27002 la cual determina las instrucciones necesarias y la base principal, que permite la preparación, implementación, mantenimiento y la mejora en el tratamiento de la seguridad de la información, en otras palabras, el objetivo de dicha norma, se basa en proporcionar una guía para orientar a nivel general, en base a lo que se pueda permitir dentro de una correcta administración de la seguridad de información (Ortiz y Valencia 2017), Lo que diferencia principalmente a la norma 27001 y 27002, es que la 27001 se centra en cómo identificar los riesgos de manera continua, mientras que la 27002, es un conjunto de buenas prácticas, organizadas en una guía, donde se describen los objetivos a tenerse en cuenta a nivel de administración y control, lo cual, las empresas deben seguir en lo mayor posible para mantener una buena administración de su seguridad. (Vern 2017).

Un control de accesos enfocado a la seguridad de la información, limita o brinda accesos privilegiados a un área con determinados usuarios o solo a uno.

Para lo cual, se requerirá de un proceso para identificar a dicho usuario, a través de diversos medios de lectura y en otros sistemas, se permite que accedan a todo lo que necesiten, únicamente identificándose exitosamente con el usuario que le hayan proporcionado, pero ello, no sería lo adecuado, para este tipo de casos, se necesita un control más complejo y avanzado.

Un sistema de autenticación (usuario y clave) no es suficiente, tiene que existir un filtro que catalogue los permisos dependiendo el área y el usuario que tiene el personal de la empresa, dichos permisos pueden tomarse de manera jerárquica, tomando como ejemplo la estructura de la compañía. (Mora 2016).

(GESTIÓN 2018), la importancia de esta radica en que los las áreas que manejan tecnología se ven repletas de nuevos controles de acceso, en cortos períodos de tiempo, debido al incremento de posibles peligros que pueden involucrar información de la compañía, que aumentan día con día y más aún con la situación actual, donde gran parte del personal trabaja de manera remota, desde su casa.

Este tipo de situaciones, requiere que la seguridad a nivel de hardware y software, sea más robusta y sofisticada.

Los controles de acceso, pueden estar implementados en sistemas autónomos o sistemas de acceso en red.

Sistemas autónomos: Dicho sistemas son simples y no están interconectados entre ellos. Su función se basa en mantener el control de los accesos de un lugar o varios. Pero al tratarse de un sistema tan simple, no guarda ningún tipo de registro, de las incidencias que ocurran.

Sistemas de acceso en red: Dichos sistemas, son los más utilizados, por lo cual, son bastante complejos. Están interconectados a una central o computador, el cual se encarga de brindar los permisos a los usuarios para acceder a la red basado en su rol en la empresa y permite llevar un control de quienes acceden a la red durante todo el día.

El ABC del Teletrabajo

Colombia desarrollo el “Libro Blanco: el ABC del Teletrabajo en Colombia”, el cual a través de su investigación pretende brindar una guía de ayuda, para las empresa u organizaciones privadas o públicas del país que deseen adoptar la modalidad de

teletrabajo, donde se incluyen guías completas desde los puntos de vista tecnológicos, jurídicos y organizacionales, los cuales están basados en las leyes actuales del país, los resultados vistos a nivel nacional y la forma en cómo se desarrollan estás prácticas a nivel internacional.

Teniendo como objetivo este libro blanco aprovechar el avance en tecnología que se da día a día, así como en las tecnologías de información y comunicaciones.

Buscará siempre aportar innovando en procesos a nivel organizacional tanto a nivel nacional como internacional para que de esta manera se genere un aumento en cuanto a productividad, protegiendo el medio ambiente con calidad de vida en los empleados integrándose de una manera correcta y eficaz en el ámbito de bienes y servicios a nivel internacional.

Modalidades de teletrabajo

Trabajo remoto propio: enfocado en las personas que trabajan de manera independientes

Trabajo remoto adicional: enfocado en personal contratado en una empresa que intercala entre trabajo presencial y remoto durante la semana utilizando las TIC para cumplir con la seguridad de la empresa.

Trabajo remoto móvil: enfocado al personal que mediante su equipo móvil realizar su trabajo. Debido a la condición de su modalidad de trabajo, tienen permitido estar fuera de la oficina constantemente, ya que no tienen un lugar exacto para realizar sus funciones.

Figura 3. El antes y ahora del teletrabajo del Libro Blanco del Teletrabajo en Colombia

En el Perú la empresa Repsol desarrollo también un libro blanco de teletrabajo, donde se especificaban los recursos técnicos necesarios para que la empresa pueda implementar satisfactoriamente la modalidad de teletrabajo sin comprometer a la empresa, ni al empleado.

La modalidad de teletrabajo en Repsol, fue separada en diferentes fases para garantizar el éxito de esta, ello comenzó en el año 2008 con una prueba piloto en las instalaciones que tenían en Madrid y Buenos Aires, donde 131 trabajadores de la empresa de diferentes perfiles, se ofrecieron voluntariamente para formar parte del piloto (40 trabajadores en Argentina y 91 trabajadores en España).

Dentro del marco técnico, se tenía como requisitos que el trabajador cumpliera con determinados aspectos de salud y seguridad en el lugar donde realizaba sus labores, para ello se acerca un personal capacitado enviado por la empresa para que pueda evaluar el domicilio del trabajador.

Se realizaron entrevistas, donde los resultados mostraron que 8 de cada 10 trabajadores que pasaron a la modalidad de teletrabajo, consideraban que habían optimizado sus tareas, lo cual llevó a incrementar su rendimiento en sus áreas respectivas. Y 9 trabajadores de 10, indicaron que su motivación había aumentado. Ellos comentan, que con la modalidad de teletrabajo adquirieron mayores beneficios en el ámbito económico al ahorrar tiempo y dinero en pasajes hacia el establecimiento, en el ámbito emocional, ya que se sentían más tranquilos y se podían concentrar más al estar en un entorno más cálido como lo eran sus hogares y en el ámbito personal, es que disponían de mayor tiempo para dedicarle a sus familias y a ellos mismos.

La modalidad de teletrabajo ha permitido que la empresa Repsol mejorara su reputación desde la perspectiva de otros países, ya que mostraban a la empresa como un lugar agradable para trabajar y con una visión innovadora, adaptándose a las nuevas tecnologías, lo cual atrae nuevos talentos a la empresa.

Beneficios del teletrabajo

- Permite la reducción del presupuesto invertido en la empresa e incrementa el nivel de trabajo por parte del trabajo al encontrarse en un entorno más conocido por ellos, como lo son sus hogares.
- Promueve el trabajo en equipo y permite que la calidad de vida de los empleados mejore gradualmente.
- Permite que exista mayor inclusión social.
- Reduce el índice de contaminación ambiental y el tráfico en transporte público y privado.
- Promueve la implementación y manejo de nuevas tecnologías

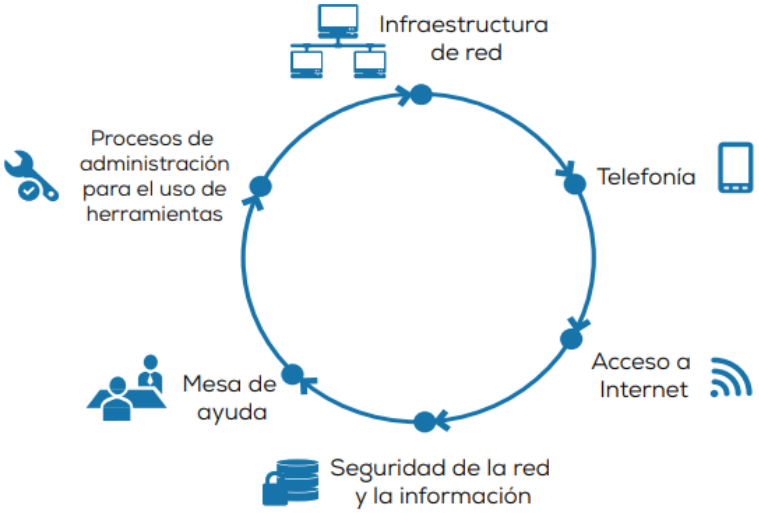


Figura 4. Componentes de teletrabajo que indican en el Libro Blanco de Teletrabajo en Colombia

Se realizó una revisión a nivel nacional e internacional, de modelos que se implementaron, con lo cual se propuso etapas que enmarcaran un proceso para una gestión en el cambio organizacional, donde se buscó la estructura adecuada y que las personas que formaran parte del proyecto, fueron previamente capacitadas para que aplicación del proyecto sea exitoso.

Dimensiones.

- Confidencialidad
- Integridad
- Disponibilidad

A continuación, se presentan algunos conceptos de dichas dimensiones:

Según (Bonilla 2019), define confidencialidad como aquella dimensión la cual debe dar garantía que la información y recursos, solo puedan ser manipulados y accedidos por el personal autorizado.

Con respecto a la integridad, (Godoy 2014) indica que, esta dimensión se basa en la búsqueda de que los datos se mantengan intactos y que no se realicen modificaciones sin la autorización correspondiente.

La dimensión de disponibilidad, según (Camacho 2008) se basa en asegurar a los usuarios que tengan los permisos necesarios, que la información y los recursos relacionados a esta, podrán ser accedidos en cualquier momento, que sea requerido. El presente informe de tesis, en base a sus dimensiones planteadas, para desarrollar un marco de trabajo para la seguridad de información presenta los siguientes indicadores medidas a escala proporcional, que posee intervalos entre niveles de la variable siendo cero un atributo natural (Guerra y Ramos 2020)

Indicadores

- Porcentaje total de accesos a la información sin autorización.
- Porcentaje total de Información modificada sin autorización.
- Porcentaje total de accesibilidad a la información.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Para este proyecto se usó la investigación cuantitativa aplicada. Según (Rasinger 2020), este procedimiento se compone de información que puede ser de una u otra forma cuantificable, pudiendo transformar los datos cuantitativos en información y gráficos; para que así se puedan procesar mediante procesos de estadística.

Para (Carrasco 2017) la definición de un diseño pre experimental consiste en realizar a un único grupo el diagnostico correspondiente, en el cual se tendrá dos momentos, previo a la ejecución del marco del marco de trabajo y posterior a la ejecución obteniendo diferentes resultados en ambas situaciones, donde se compararán los resultados obtenidos.

Su grafico es el siguiente:

$$G \quad O_1 \; X \; O_2$$

En el cual:

G: Grupo de experimento

O1: Preliminarmente a la medición de la variable dependiente ()X: soluciona la variable independiente

O2: Subsiguiente a la medición de la variable dependiente ()

Se aplica un pretest (antes de implantar; O1) a un determinado grupo de elementos (G), tratamiento posterior (Control de accesos; X), finalizando con el postest (luego de instaurar; O2)

3.2. Variables y operacionalización

Variable independiente: Marco de trabajo de seguridad de la información
Se brinda mayor detalle de la variable independiente, sus dimensiones e indicadores en el Anexo 10.

Variable dependiente: Control de accesos de seguridad la información
Se brinda mayor detalle de la variable independiente, sus dimensiones e indicadores en el Anexo 4.

Definición operacional

Variable independiente: Marco de trabajo de seguridad de la información. Ver detalle en Anexo 10.

Identificar posibles riesgos de seguridad para sus activos de información, protegiendo de estos riesgos mediante el desarrollo y la implementación de salvaguardias, permitiendo recuperarse de estas incidencias mediante la restauración de los activos socavados (Calder 2017)

Variable dependiente: Control de accesos de seguridad la información trata los ingresos en base a ciertos parámetros de seguridad que se establecieron previamente. Dichos parámetros o controles, que se diferencian entre accesos autorizados y no autorizados, son vitales en gran medida para los sistemas de seguridad («Suministro E Instalacin De Sistema De Control De Accesos Presencia Y Cctv, Mantenimiento Preventivo (spain-bilbao: Access Control System)» 2020)

En la siguiente Tabla N° 4, se describe a mayor detalle los indicadores del Control de accesos de seguridad la información:

Tabla 4. *Indicadores de Control de acceso de seguridad de información*

DIMENSIÓN	INDICADOR	DESCRIPCIÓN	TÉCNICA	INSTRUMENTO	UNIDAD DE MEDIDA	FÓRMULA
Confidencialidad	Porcentaje total de accesos no autorizados a la información	Para (Rodríguez 2015) es el porcentaje de información que es accedida por usuarios no autorizados previamente por una falla de seguridad o falta de controles.	FICHAJE	FICHA DE REGISTRO	PORCENTAJE	
Integridad	Porcentaje total de información	Para (Taboada y Cotos 2015) es el porcentaje de información perdida o alterada de manera intencional	FICHAJE	FICHA DE REGISTRO	PORCENTAJE	
Disponibilidad	Porcentaje total de accesibilidad a la información	Para (Molina 2016) el porcentaje de accesibilidad a la información es la disponibilidad de un ambiente metropolitano, servicios, construcciones o medios informativos para lograr el acceso correcto en buenas condiciones, con respecto a la autonomía, seguridad y comodidad.	FICHAJE	FICHA DE REGISTRO	PORCENTAJE	

Fuente: Elaboración propia

3.3. Población, muestra y muestreo, unidad de análisis

Para Sánchez (2018) se define población a las personas u objetos agrupados que sirven en una investigación para poder recolectar datos, siendo esta analizada, dando inicio a la investigación

Para esta investigación se contó con un periodo de 30 días donde se realizó un total de 30 registros para lograr los objetivos propuestos de la implementación del marco de trabajo encomendados por la empresa, analizando el estado en el cual se encontraba cada área.

Muestra

La muestra es el fragmento de la totalidad de un estudio de un objeto, producto o fenómeno que representa de manera simplificada aquellos resultados que se obtuvieron (Hernández-Lalinde Mgtr et al. 2019).

Esta muestra se aplicó al promedio del total de registros bajo el periodo de 30 días, se midió con un test los niveles de seguridad y estándares que se aplicaron con el marco de trabajo específicamente a la información para mantenerla segura día a día en la empresa en el control de acceso de usuarios

3.4. Técnicas e instrumentos de recolección de datos:

En la siguiente tabla 5 se brindan detalles de las técnicas e instrumentos que se utilizaron:

Tabla 5. *Técnicas e instrumentos utilizados.*

TÉCNICA	INSTRUMENTO	FUENTE	INFORMANTE
Observación	**Ficha de observación.** Esta ficha de observación se utilizó en el momento de llenar la información en base a las incidencias que se presentaron en torno a cada uno de nuestros indicadores, esto se aplicó diariamente durante cada mes, donde se obtuvo al final, un porcentaje total utilizando la formula indicada en cada ficha.	Información de la gerencia	Gerente
TÉCNICA	INSTRUMENTO	FUENTE	INFORMANTE
Encuesta	**Cuestionario de Marco de trabajo.** Esta encuesta fue respondida marcando una x dentro del casillero, indicando el grado que se tiene respecto al concepto que se expresa en cada ítem de acuerdo a una escala, esta escala contó con 5 puntos de acuerdo al grado de aprobación o desaprobación de cada afirmación: • 5 – Totalmente de acuerdo. • 4 – De acuerdo. • 3 – Ni de acuerdo, ni en desacuerdo. • 2 – En desacuerdo. • 1 – Totalmente en desacuerdo Luego de esto se aplicó el método indicado en el documento para de esta manera obtener el nivel por cada indicador planteado.	Información de los empleados	Empleado

Fuente: Elaboración propia

Procedimiento automatizado para detectar modificaciones no autorizadas

Para poder detectar el usuario y momento en el que se realiza alguna modificación a algún archivo, se deberá habilitar una unidad exacta donde será almacenada toda la información/archivos que se requieran utilizar, dividido por áreas.

Para ello podremos usar programas como File Access Monitor, el cual es un software gratuito que permite ello, el cual proporciona una lista completa, centralizada y ordenable de eventos de acceso (o intentos de acceso) a las rutas que se ha seleccionado.

Donde cada registro detalla lo siguiente:

- Ruta de archivo.
- Tipo de acceso (lectura, escritura, eliminación, cambio de nombre, ejecución, propiedad, permisos, atributos de escritura).
- Tipo de objeto (archivo, carpeta).
- Estado (concedido / denegado).
- Fecha y hora de acceso.
- Usuario.
- Dominio.
- Dirección IP origen.
- Nombre de la máquina (Hostname).

3.5. Procedimientos

En la siguiente Figura 5, se detallan los procesos que se realizaron para la construcción del informe de tesis:

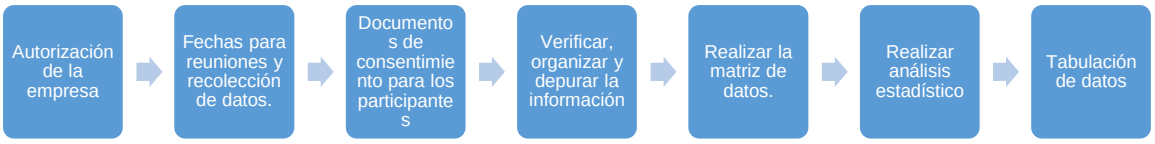


Figura 5. Procesos para la aplicación del informe de tesis

Para el presente informe de tesis, se contó con la autorización por parte de la empresa mediante un documento, que nos brindó el permiso para desarrollar la investigación, dicho documento está en el Anexo N° 1.

Se pactaron reuniones, en fechas determinadas, donde nos reunimos con los usuarios y se les brindó también a ellos, un documento donde ellos confirmaron su consentimiento para participar en los procesos que se requieran dentro de la investigación, dicho documento está en el Anexo N° 2.

Una vez se obtuvo la información de los usuarios y se aplicó nuestras fichas y cuestionarios, las cuales se encuentran en el Anexo 6, se procedió con la verificación de dicha información, se organizó mediante cuadros y se fue depurando la información para lograr la construcción de nuestra matriz de datos. Cuando se obtuvo todo ello correctamente, procedimos a realizar el análisis estadístico correspondiente y se fue tabulando los datos obtenidos.

Para la extracción y el conteo de nuestros indicadores, se tomó las incidencias reportadas vía Service Desk como se muestra en la figura 6 que manejaba la empresa, donde llegaban todas las incidencias que ocurrían durante el día en la empresa, de las cuales se fueron seleccionando las que estuvieran relacionadas a nuestros indicadores y ordenando en tablas para luego realizar el conteo correspondiente.

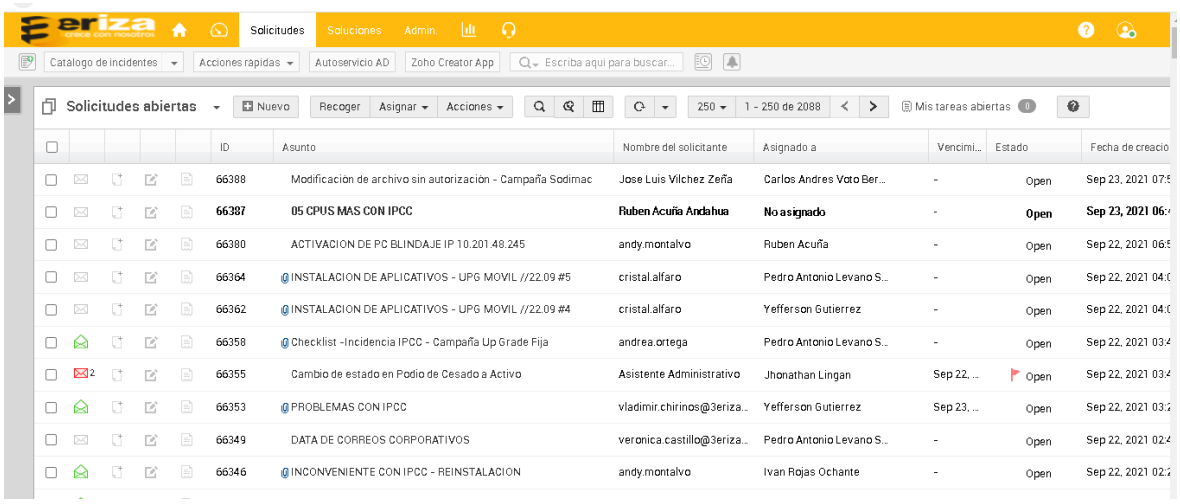


Figura 6. Service Desk de Área de TI de 3eriza

El método de recepción de una incidencia en Service Desk, se daba de la siguiente manera:

- Usuario presentaba una incidencia y lo reportaba con su supervisor a cargo
- Supervisor a cargo, mediante el correo institucional de la empresa enviaba un correo a servicedesk@3eriza.pe
- Una vez enviado el correo, el supervisor recibía un correo de respuesta, donde se le indicaba su número de ticket de atención, como se puede apreciar en la Figura 7.

Figura 7. Creación del ticket de atención en el Service Desk.

3.6. Método de análisis de datos

Según (Cohen, Nestor 2019), indican que los investigadores utilizarán determinadas técnicas, las cuales son necesarias para obtener la información debida, por lo cual se deberá seguir determinados procesos de manera sucesiva,

donde se medirán los resultados que darán solución al problema planteado en el análisis del informe de tesis.

El método de análisis de datos que se utilizó para la presente investigación fue de método estadístico descriptivo, comparativo, el cual se vio reflejado a través de diversas tablas de frecuencia, análisis de tendencia central (media y desviación estándar) y gráficos correspondientes.

Adicional a ello, se utilizaron análisis estadísticos inferenciales no paramétricos, para muestras independientes, luego de que se realizó y fueron comprobados los supuestos de normalidad, se utilizó la prueba estadística de U Man de Whitney. Dichos análisis permitieron que las hipótesis de investigación pudieran ser contrastadas, las cuales, fueron evaluadas con un 95% de confianza y 5% de error.

Hipótesis de Investigación 1

Hipótesis Estadística (HE1):

El desarrollo de un marco de trabajo de seguridad de información usando la ISO 27001 mejora la confidencialidad de información en los controles de acceso de usuarios en instituciones orientadas a teletrabajo.

Indicador 1: Porcentaje total de accesos a la información sin autorización

$PTDIF_a$: Porcentaje total de accesos a la información sin autorización antes de usar marco de trabajo de seguridad de información

$PTDIF_d$: Porcentaje total de accesos a la información sin autorización después de usar marco de trabajo de seguridad de información

Hipótesis Estadística 1:

Hipótesis Nula (H0):

El desarrollo de un marco de trabajo de seguridad de información usando la ISO 27001 no mejora la confidencialidad de información en los controles de acceso de usuarios en instituciones orientadas a teletrabajo.

H0: PTDIFa ≥ PTDIFd

Hipótesis Alternativa (Ha):

El desarrollo de un marco de trabajo de seguridad de información usando la ISO 27001 mejora la confidencialidad de información en los controles de acceso de usuarios en instituciones orientadas a teletrabajo.

Ha: PTDIFa < PTDIFd

Se llegó a concluir que este indicador usando un marco de trabajo de seguridad de información basado en la ISO 27001 es mejor que el indicador sin el uso de uno.

Hipótesis de Investigación 2

Hipótesis Específico (HE2)

El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 mejora la integridad de información en los controles de acceso de los usuarios en instituciones orientadas a teletrabajo

Indicador 2: Porcentaje total de información modificada sin autorización

$PTIM_a$: Porcentaje total de información modificada sin autorización antes de usar un marco de trabajo de seguridad de información

$PTIM_d$: Porcentaje total de información modificada sin autorización después de usar un marco de trabajo de seguridad de información

Estadística 2: Hipótesis Nula (H0):

El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 no mejora la integridad de información en los controles de acceso de los usuarios en instituciones orientadas a teletrabajo

$H0: PTIM_a \geq PTIM_d$

Hipótesis Alternativa (Ha):

El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 mejora la integridad de información en los controles de acceso de los usuarios en instituciones orientadas a teletrabajo

$$\mathbf{Ha: PTIM_a < PTIM_d}$$

Se llegó a concluir que este indicador usando un marco de trabajo de seguridad de información basado en la ISO 27001 es mucho mejor que el indicador sin el uso de uno.

Hipótesis de Investigación 3

Hipótesis Específico (HE3)

El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 mejora la disponibilidad de información en los controles de acceso de los usuarios en instituciones orientadas a teletrabajo

Indicador 3: Porcentaje total de accesibilidad a la información

$PTAI_a$: Porcentaje total de accesibilidad a la información antes de usar un marco de trabajo de seguridad de información

$PTAI_d$: Porcentaje total de accesibilidad a la información después de usar un marco de trabajo de seguridad de información

Estadística 3: Hipótesis Nula (H0):

El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 no mejora la disponibilidad de información en los controles de acceso de los usuarios en instituciones orientadas a teletrabajo

$$\mathbf{H0: PTAI_a \geq PTAI_d}$$

Hipótesis Alternativa (Ha):

El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 mejora la disponibilidad de información en los controles de acceso de los usuarios en instituciones orientadas a teletrabajo

$$\mathbf{Ha: PTAI_a < PTAI_d}$$

Se llegó a concluir que este indicador usando un marco de trabajo de seguridad de información basado en la ISO 27001 es mucho mejor que el indicador sin el uso de uno.

3.7. Aspectos éticos

El Colegio de Ingenieros del Perú, indica que los ingenieros deben servir a la sociedad, contribuyendo al bienestar humano, donde su principal objetivo será la seguridad y el correcto uso de los recursos otorgados para el desempeño de sus tareas profesionales.

También debe tomarse en cuenta, que los investigadores debieron informar desde el principio de la investigación, todos los detalles correspondientes al informe de tesis que se realizó, a los participantes que estuvieron involucrados.
El investigador tiene la obligación de proteger el bienestar y la dignidad de los involucrados.

Se toma en cuenta que según el artículo 427 del Código Penal, este informe de tesis es de auditoría de los investigadores y no se está utilizando o adulterando un proyecto de otra persona; y tomando crédito de dicha investigación.

Se tomaron referencias de diferentes autores para poder avalar determinados puntos dentro de la investigación, donde se realizó la cita correspondiente, siguiente los estándares de la ISO 690, la cual permite que los autores puedan tener el crédito correspondiente por su trabajo realizado.

IV. RESULTADOS

Descripción

La presente investigación se efectuó en dos partes para poder concluir la afirmación o el rechazo de la hipótesis planteada, teniendo en cuenta el diseño Pre-Experimental. Como primera parte del estudio se efectuó el Pre-Test, consistiendo en utilizar una evaluación en los indicadores previamente determinados antes de la ejecución del marco de trabajo propuesto. Posteriormente, como segunda parte del estudio se efectuó el Post-Test, consistiendo en utilizar una evaluación a los indicadores seleccionados en la investigación luego de haber ejecutado el marco de trabajo propuesto. Estas dos partes en conjunto permitieron que se pueda realizar una comparativa de los resultados que se obtuvo en todas las fases y así comprobar si existe una mejora o no.

El análisis de los datos conseguidos mediante los instrumentos que ayudan a la recolección de información se dio con la herramienta IBM SPSS Statistics 26, teniendo como finalidad realizar las respectivas pruebas de normalidad, sabiendo el número de la población y a su vez concluir si se aceptaba o rechazaban las hipótesis.

Análisis descriptivo

Se realizó para esta investigación la ejecución de un marco de trabajo de seguridad de información con la finalidad de evaluar la confidencialidad, integridad y disponibilidad de la información, para esto se realizó un Pre-Test para identificar la situación originaria de cada dimensión previamente mencionado. Posteriormente, se efectuó la ejecución del marco de trabajo de seguridad de información basado en la ISO 27001:2013 y se recopilo información acerca de la confidencialidad, integridad y disponibilidad mediante un Post-Test. Estos resultados que se obtuvieron de estas comparativas se pueden visualizar en las siguientes tablas:

En la tabla 6 se puede visualizar los resultados conseguidos en el indicador porcentaje total de accesos no autorizados a la información. Consiguió un valor del 65,44% en el Pre-test, en tanto se consiguió un valor de 37,53% en el Post-Test (Ver figura 8), reflejando así la gran diferencia del antes y el después a la hora de implementar el marco de trabajo de seguridad de información. Por otro lado, como mínimo resultado se obtuvo un 37.5% antes y de un 12,1% después. Además, se obtuvo una variabilidad del 8.63 antes y 1.55 después.

Tabla 6. *Porcentaje total de accesos a la información sin autorización*

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
PRETEST	30	3,75	8,00	6,5446	,86352
POSTEST	30	1,21	8,33	3,7532	1,55365
N válido (por lista)	30				

Fuente: Elaboración propia

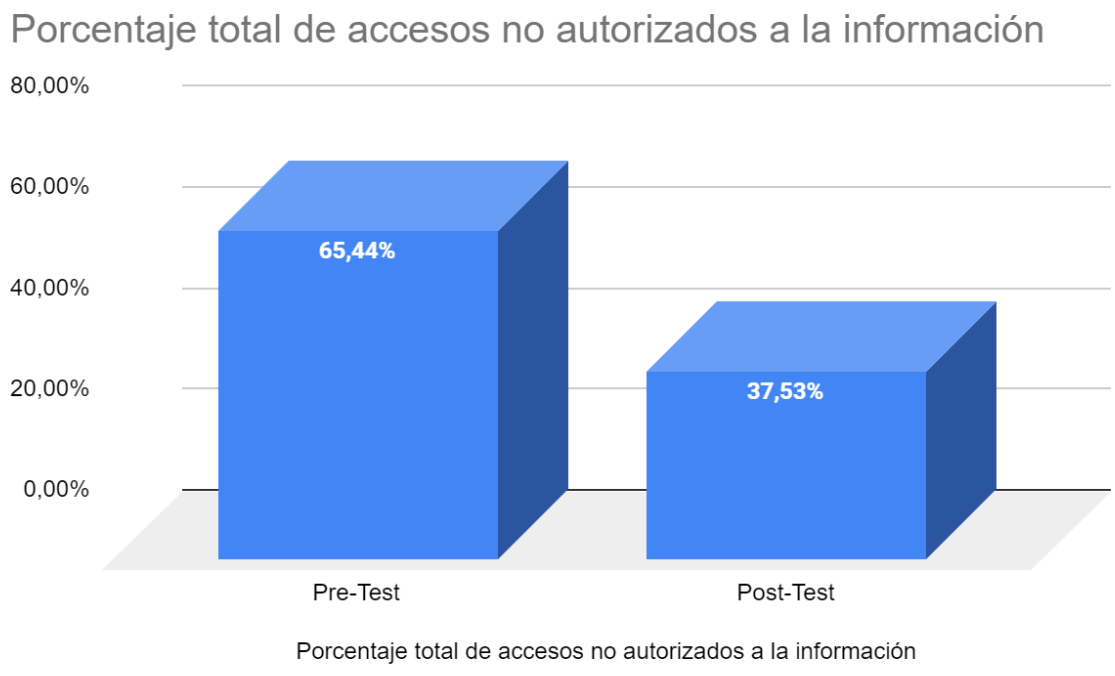


Figura 8. *Porcentaje total de accesos a la información sin autorización*

Asimismo, en la Tabla 7, se evidencia que los resultados conseguidos en el indicador porcentaje total de información modificada sin autorización. Como resultados se obtuvieron que se alcanzó un porcentaje de 40,07% en el Pre-Test en tanto se alcanzó un porcentaje de 18,12% en el Post-Test (Ver figura N°7), evidenciando con claridad las diferencias entre el antes de implementar el marco de trabajo de seguridad de información y después. Así mismo, se consiguió el valor de la variabilidad antes de 1.98 y después de 1.79.

Tabla 7. *Porcentaje total de información modificada sin autorización*

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
PRETEST	30	1,00	8,33	4,0071	1,98998
POSTEST	30	,00	8,33	1,8121	1,79521
N válido (por lista)	30				

Fuente: Elaboración propia

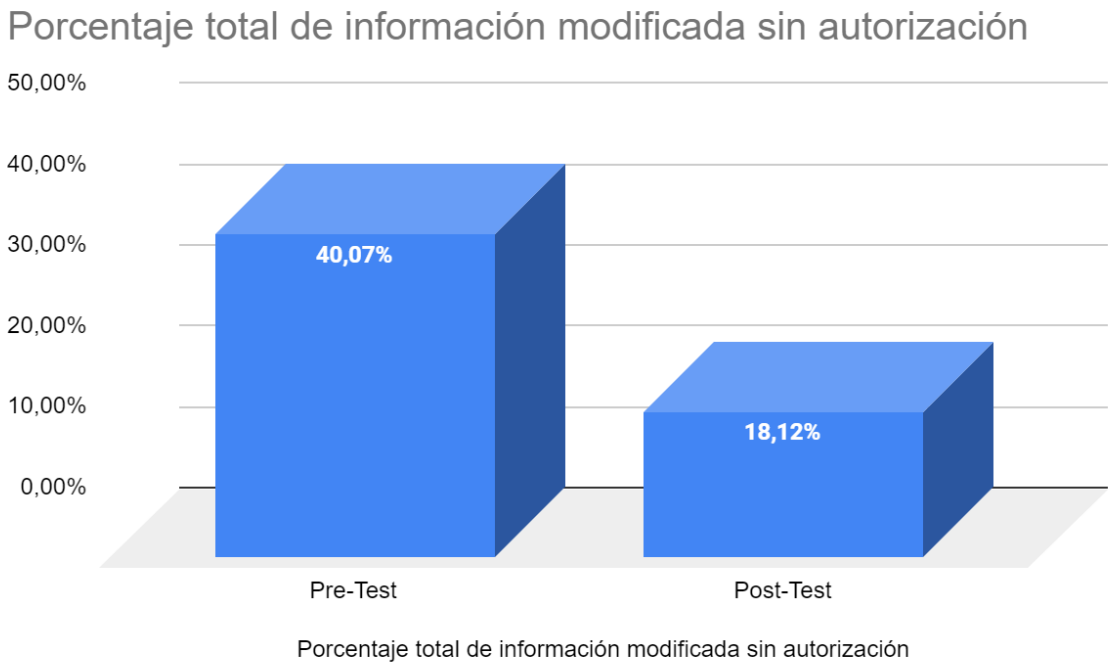


Figura 9. *Porcentaje total de información modificada sin autorización*

Asimismo, en la tabla 8, se evidencia que los resultados obtenidos en el indicador porcentaje total de accesibilidad a la información. Como resultados se obtuvieron

que se alcanzó un porcentaje de 65,43% en el Pre-Test en tanto se alcanzó un porcentaje de 37.10% en el Post-Test (Ver figura 10), evidenciando con claridad las diferencias entre el antes de implementar el marco de trabajo de seguridad de información y después. Así mismo, se consiguió el valor de la variabilidad antes de 0.9 y después de 1.6.

Tabla 8. *Porcentaje total de accesibilidad a la información*

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
PRETEST	30	3,75	8,33	6,5431	,90285
POSTEST	30	1,00	6,88	3,7197	1,68317
N válido (por lista)	30				

Fuente: Elaboración propia

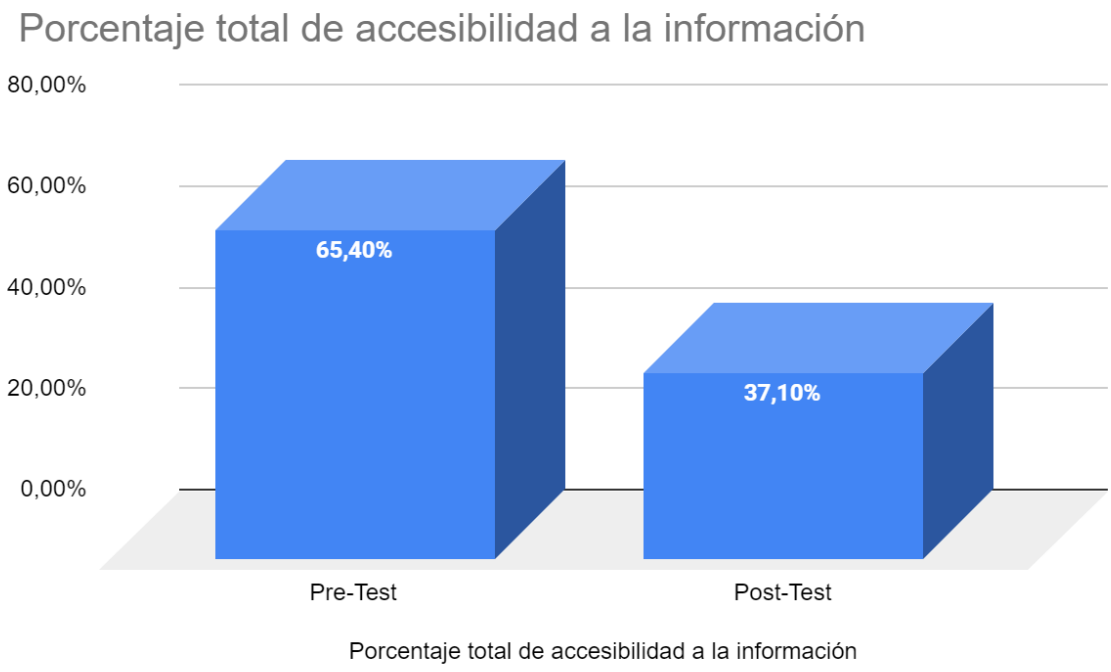


Figura 10. *Porcentaje total de accesibilidad a la información*

Análisis Inferencial

Se efectuó la prueba de normalidad con el método de Shapiro-Wilk debido a que la población que se seleccionó es de 30 fichas de registro, siendo inferior al mínimo que es 50, en fundamento según comenta Romero (2016). Por ende, se hizo la aplicación del IBM SPSS STATISTICS 26, Considerando un 95% en el nivel de confianza. A su vez, si el nivel de significancia es mayor a 0.05 entonces los resultados son normales; y si el nivel de significancia tiende a ser menor que 0.05 por ende los datos obtenidos no son normales (p. 112)[55].

Mientras que en la tabla 9, Se visualizan los resultados conseguidos del indicador porcentaje total de accesos no autorizados a la información.

Teniendo un 0.03 en el nivel de significancia de en el Pre-test, siendo menor que 0.05, esto quiere decir que los datos no son normales. Así mismo, teniendo 0.24 en el nivel de significancia del Post-test, siendo superior a 0.05, resultando que los datos obtenidos son normales. Por lo tanto, los datos obtenidos no pueden ser distribuidos normalmente.

Tabla 9. Prueba Shapiro-Wilk - indicador Porcentaje total de accesos a la información sin autorización

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PRETEST	,159	30	,052	,923	30	,031
POSTEST	,111	30	,200*	,956	30	,245

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia

A su vez, de la Figura 11 se visualiza que se consiguió una media de 65.4 en el pre-test y 0.86 de desviación estándar.

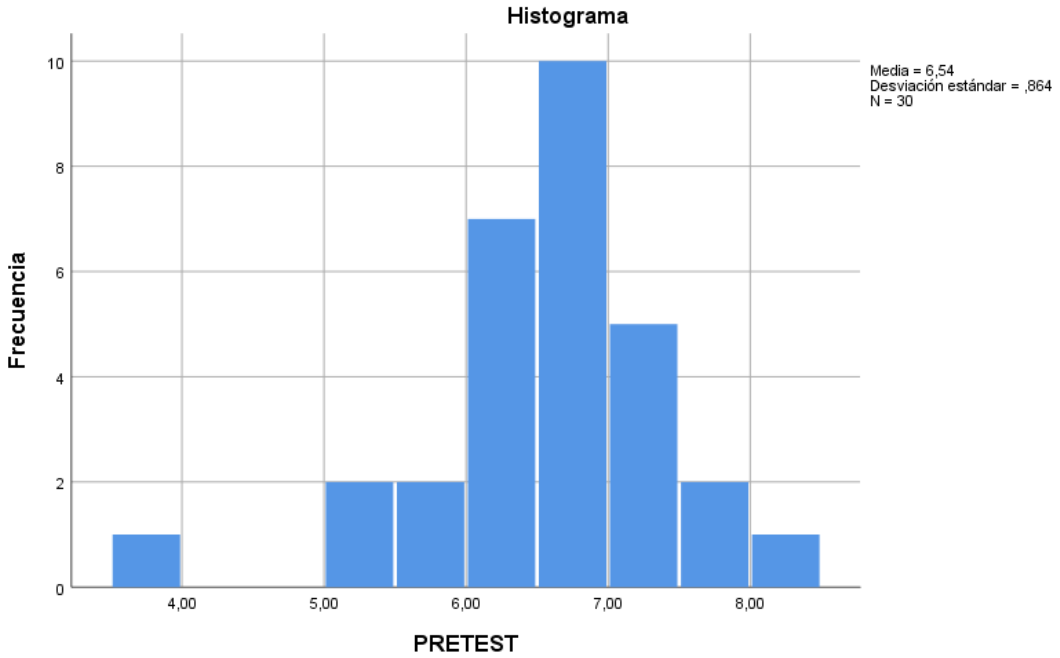


Figura 11. *Prueba de normalidad del Porcentaje total de accesos a la información sin autorización*

En la Figura 12 asimismo se puede visualizar que se obtiene una media de 37,5 en el Post-Test y 1,5 de desviación estándar.

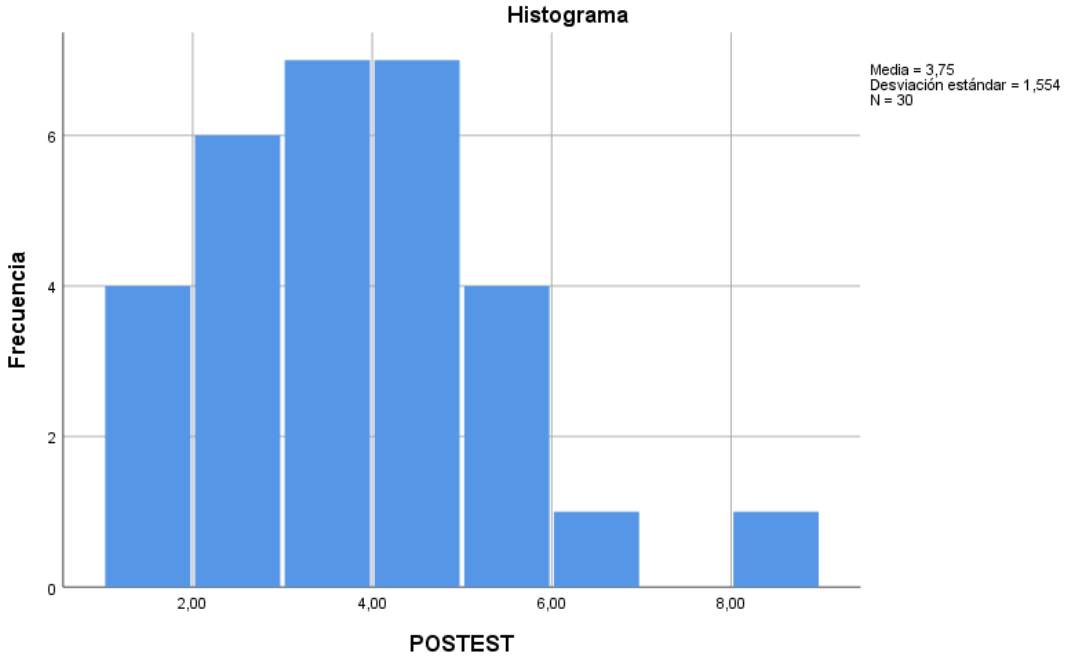


Figura 12. *Prueba de normalidad del Porcentaje total de accesos a la información sin autorización*

Por consiguiente, en vista de que las Figuras N°8 y N°9 se evidencia que hubo una mejora en el porcentaje total de accesos no autorizados a la información de 65,4 hasta 37,5. De la misma forma, se efectuó la prueba de rangos de Wilcoxon para poder aceptar o rechazar las hipótesis planteadas debido a que los datos obtenidos no se distribuyen de una forma normal.

Además, De la Tabla 10 se reflejan los resultados en el indicador porcentaje total de información modificada sin autorización. Durante el pre-test el nivel de significancia alcanzó un valor de 0,1, siendo este superior a 0.05, resultando sus datos normales. Mientras que el nivel de significancia en el post-test alcanzó un valor de 0.00, siendo este inferior a 0.05. Por lo tanto, los datos obtenidos no pueden ser distribuidos normalmente.

Tabla 10. *Prueba de Shapiro-Wilk – Porcentaje total de información modificada sin autorización*

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PRETEST	,135	30	,173	,952	30	,186
POSTEST	,156	30	,059	,826	30	,000

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia

De la misma manera, en la Figura 13, se visualiza que se consiguió una media de 40,1 en el pre-test con 1,9 de desviación estándar.

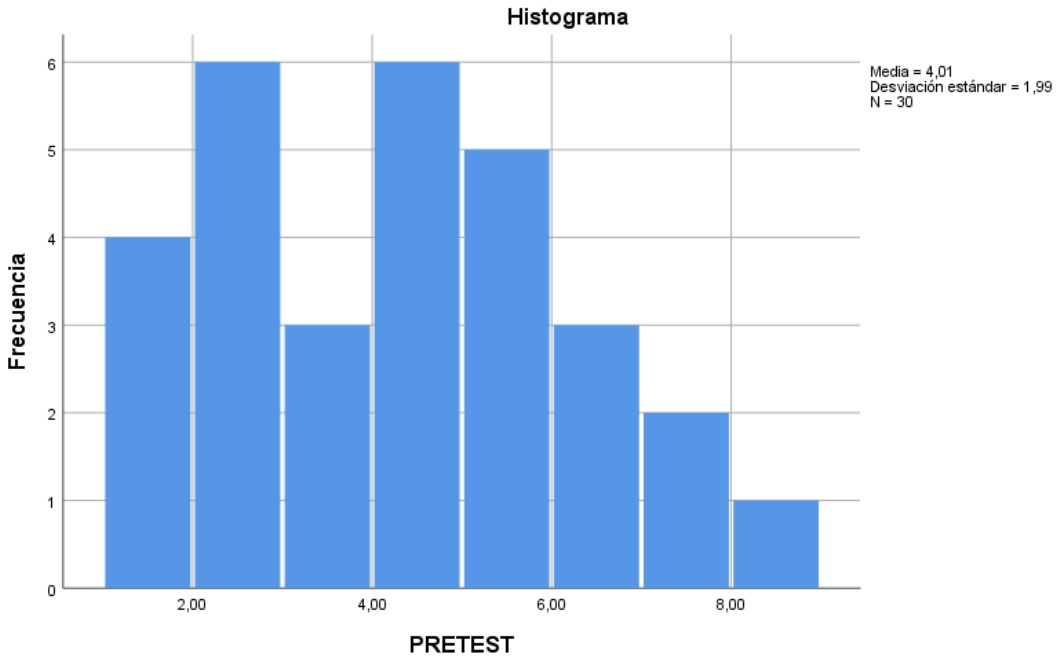


Figura 13. Prueba de normalidad del Porcentaje total de información modificada sin autorización

Igualmente, de la Figura 14 se visualiza que se tuvo 18,1 como media en el post-test y 1,7 de desviación estándar.

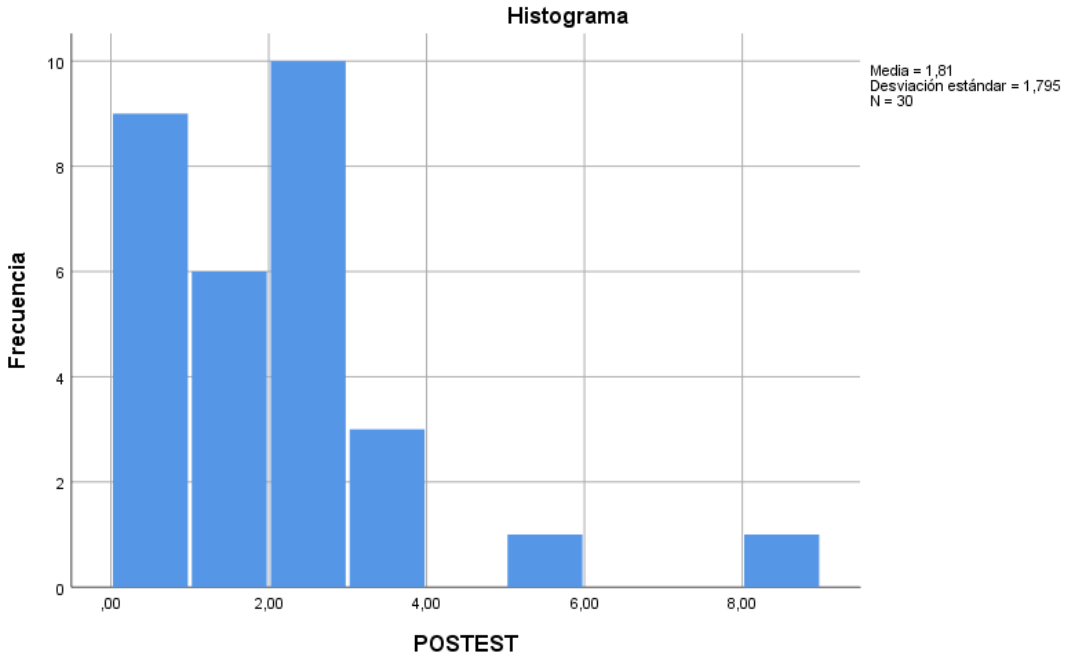


Figura 14. *Prueba de normalidad del Porcentaje total de información modificada sin autorización*

Por ende, teniendo en consideración las Figuras N°10 y N°11, se puede visualizar una mejoría en el porcentaje total de información modificada sin autorización de 40,1 a 18,1. De igual forma, se efectuó la prueba de rangos de Wilcoxon para que las hipótesis planteadas puedan ser aceptadas o rechazadas dado que los datos obtenidos no se pueden distribuir de una forma normal.

Además, De la Tabla 11 se reflejan los resultados en el indicador porcentaje total de accesibilidad a la información. Durante el pre-test el nivel de significancia alcanzó un valor de 0.2, siendo este superior a 0.05, resultando sus datos normales. Mientras que el nivel de significancia en el post-test alcanzó un valor de 0.2, igualmente siendo este superior a 0.05. Por lo tanto, los datos obtenidos si pueden ser distribuidos normalmente.

Tabla 11. *Prueba de Shapiro-Wilk – Porcentaje total de accesibilidad a la información*

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PRETEST	,149	30	,086	,941	30	,099
POSTEST	,131	30	,200*	,953	30	,207

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia

De la misma manera, en la Figura 15, se visualiza que se consiguió una media de 65,4 en el pre-test con 0.9 de desviación estándar.

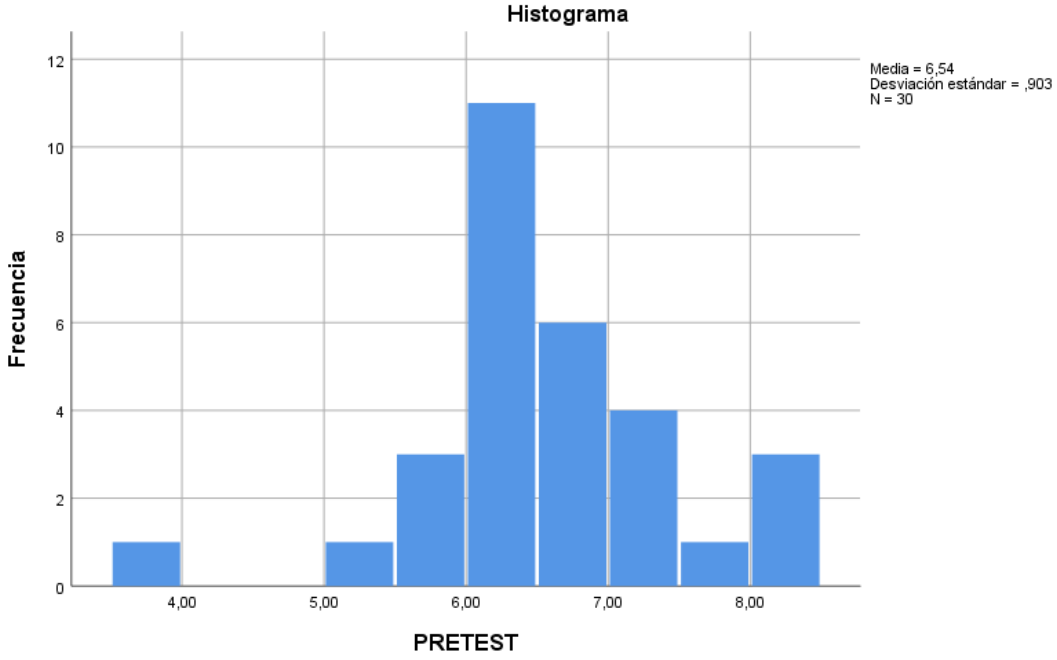


Figura 15. Prueba de normalidad del Porcentaje total de accesibilidad a la información

Igualmente, de la Figura 16 se visualiza que se tuvo 37.2 como media en el post-test y 1,6 de desviación estándar.

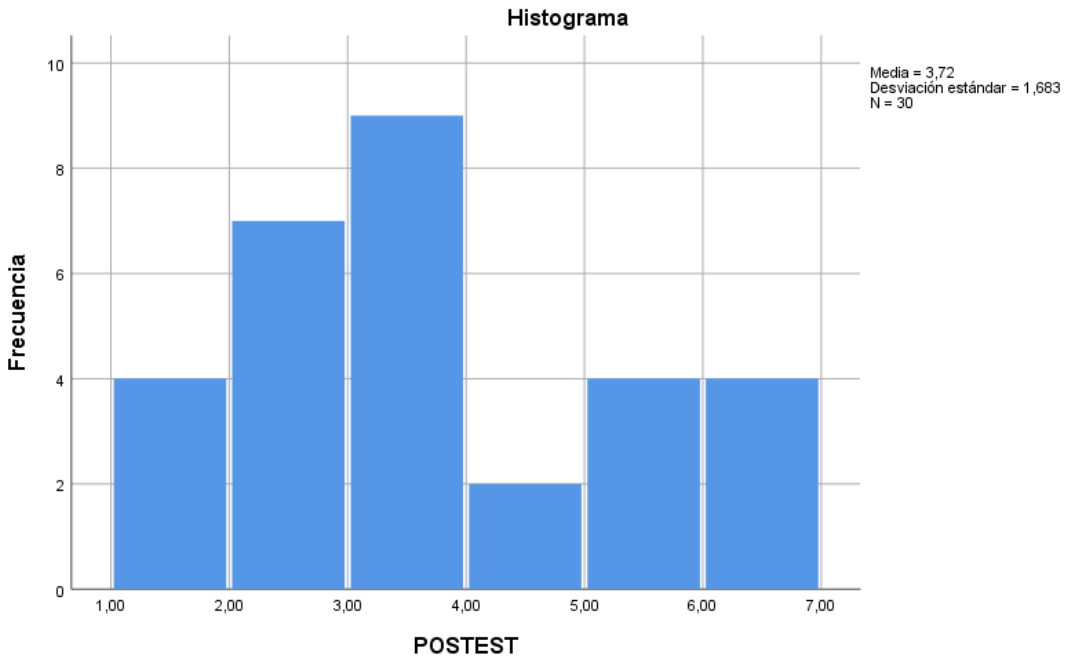


Figura 16. *Prueba de normalidad del Porcentaje total de accesibilidad a la información*

Por ende, teniendo en consideración las Figuras 15 y 16, se puede visualizar una mejora en el porcentaje total de accesibilidad de información de 65,4 a 37,2. De igual forma, se efectuó la prueba de rangos de T-Student para que las hipótesis planteadas puedan ser aceptadas o rechazadas dado que los datos obtenidos si se distribuyen de una forma normal.

Prueba de Hipótesis 1

Hipótesis específica 1: El desarrollo de un marco de trabajo de seguridad de información usando la ISO 27001 mejora la confidencialidad de información en los controles de acceso de usuarios en instituciones orientadas a teletrabajo.

Indicador: Porcentaje total de accesos no autorizados a la información.

Hipótesis estadísticas

Definición de variables:

$PTDIF_a$: Porcentaje total de accesos a la información sin autorización antes de usar marco de trabajo de seguridad de información

$PTDIF_d$: Porcentaje total de accesos a la información sin autorización después de usar marco de trabajo de seguridad de información

H_o: El desarrollo de un marco de trabajo de seguridad de información usando la ISO 27001 no mejora la confidencialidad de información en los controles de acceso de usuarios en instituciones orientadas a teletrabajo.

H_O: PTDIFa ≥ PTDIFd

H_a: El desarrollo de un marco de trabajo de seguridad de información usando la ISO 27001 mejora la confidencialidad de información en los controles de acceso de usuarios en instituciones orientadas a teletrabajo.

Ha: PTDIFa < PTDIFd

Para comprobar si es aceptada o rechazada la hipótesis planteada se utilizó la prueba de rangos Wilcoxon ya que los datos del indicador no son normales. Los resultados se presentan en las siguientes Tablas 12 y 13

Tabla 12. *Prueba Wilcoxon - indicador Porcentaje total de accesos a la información sin autorización*

Rangos

		N	Rango promedio	Suma de rangos
POSTEST - PRETEST	Rangos negativos	28[a]	16,11	451,00
	Rangos positivos	2[b]	7,00	14,00
	Empates	0[c]		
	Total	30		

a. POSTEST < PRETEST

b. POSTEST > PRETEST

c. POSTEST = PRETEST

Fuente: Elaboración propia**.**

Tabla 13. *Estadísticos de prueba*[a]

	POSTEST - PRETEST
Z	-4,494[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Fuente: Elaboración propia

De las anteriores Tablas 12 y 13, conforme a la comparativa de los promedios se puede evidenciar que ocurrió un aumento en Z, con relación al porcentaje total de accesos a la información sin autorización utilizando el marco de trabajo de seguridad de información al 95% de confianza.

De la anterior Tabla N°13, se visualiza que el nivel de significancia es 0.000, valor que se empleó para poder realizar la comparación en la tabla Shapiro-Wilk con el valor de referencia (ver anexo N°14)

Como muestra tomada fue de 30 por parte del indicador del porcentaje total de accesos no autorizados a la información, consiguientemente, fue 0.91 en el punto de comparación.

La Tabla N°11 presenta 0.000 en el nivel de significancia, siendo este inferior a 0.91 (ver anexo N°14), de la misma forma es inferior a 0.05 en el nivel de significancia (Ramírez y Polack, 2020, p. 200)[56]. Por consiguiente, la hipótesis nula fue rechazada y la alterna fue aceptada, debido a que el el marco de trabajo de seguridad de información usando la ISO 27001 mejora la confidencialidad de información en los controles de acceso de usuarios en instituciones orientadas a teletrabajo.

Prueba de Hipótesis 2

Hipótesis específica 2: El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 mejora la integridad de información en los controles de acceso de los usuarios en instituciones orientadas a teletrabajo

Indicador: Porcentaje total de información modificada sin autorización

Hipótesis estadísticas

Definición de variables:

$PTIM_a$: Porcentaje total de información modificada sin autorización antes de usar un marco de trabajo de seguridad de información

$PTIM_d$: Porcentaje total de información modificada sin autorización después de usar un marco de trabajo de seguridad de información

H_o: El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 no mejora la integridad de información en los controles de acceso de los usuarios en instituciones orientadas a teletrabajo

$$\mathbf{H0: PTIM_a \geq PTIM_d}$$

H_a: El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 mejora la integridad de información en los controles de acceso de los usuarios en instituciones orientadas a teletrabajo

$$\mathbf{Ha: PTIM_a < PTIM_d}$$

Para comprobar si es aceptada o rechazada la hipótesis planteada se efectuó la prueba de rangos Wilcoxon ya que los datos del indicador no son normales. Estos resultados son presentados en las Tablas 14 y 15

Tabla 14. *Prueba Wilcoxon - indicador* Porcentaje total de información modificada sin autorización.

Rangos

		N	Rango promedio	Suma de rangos
POSTEST - PRETEST	Rangos negativos	22[a]	12,50	275,00
	Rangos positivos	1[b]	1,00	1,00
	Empates	7[c]		
	Total	30		

a. POSTEST < PRETEST

b. POSTEST > PRETEST

c. POSTEST = PRETEST

Fuente: Elaboración propia.

Tabla 15. *Estadísticos de prueba*[a]

	POSTEST - PRETEST
Z	-4,172[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

Fuente: Elaboración propia

En las Tablas 14 y 15, conforme a la comparativa de los promedios se puede evidenciar que ocurrió una mejora en Z, aplicando el marco de trabajo de seguridad de información al 95% de confianza con relación al porcentaje total de información modificada sin autorización

De la Tabla 15, se visualiza que el nivel de significancia es 0.00, valor que se utilizó para realizar la comparación en la tabla Shapiro-Wilk con el valor de referencia.

Como muestra tomada fue 24 por parte del indicador del porcentaje total de información modificada sin autorización, consiguientemente, fue 0.91 en el punto de comparación.

La Tabla 15 presenta que el nivel de significancia es de 0.00, siendo este inferior a 0.91, de la misma forma es inferior a 0.05 en el nivel de significancia (Ramírez y

Polack, 2020, p. 200)[56]. Por consiguiente, la hipótesis nula fue rechazada y la alterna fue aceptada, debido a que el marco de trabajo de seguridad de información utilizando la ISO 27001 mejoro la integridad de información en los controles de acceso de los usuarios en instituciones orientadas a teletrabajo

Prueba de Hipótesis 3

Hipótesis específica 3: El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 mejora la disponibilidad de información en los controles de acceso de los usuarios en instituciones orientadas a teletrabajo

Indicador: Porcentaje total de accesibilidad a la información

Hipótesis estadísticas

Definición de variables:

$PTAI_a$: Porcentaje total de accesibilidad a la información antes de usar un marco de trabajo de seguridad de información

$PTAI_d$: Porcentaje total de accesibilidad a la información después de usar un marco de trabajo de seguridad de información

H_o: El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 no mejora la disponibilidad de información en los controles de acceso de los usuarios en instituciones orientadas a teletrabajo

$$\mathbf{H0: PTAI_a \geq PTAI_d}$$

H_a: El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 mejora la disponibilidad de información en los controles de acceso de los usuarios en instituciones orientadas a teletrabajo

$$\mathbf{Ha: PTAI_a < PTAI_d}$$

Para comprobar si es aceptada o rechazada la hipótesis planteada se efectuó la prueba de T de Student ya que los datos del indicador son normales. Estos resultados son presentados en la Tabla 16.

Tabla 16. *Prueba de muestras relacionadas Porcentaje total de accesibilidad a la información*

Prueba de muestras emparejadas

			Diferencias emparejadas						Sig. (bilateral)
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	
Par 1	PRETEST - POSTEST	2,8234 0	2,01477	,36784	2,07107	3,57573	7,676	29	,000

Fuente: Elaboración propia.

En la tabla 16 se puede visualizar que en la prueba T-Student del indicador porcentaje total de accesibilidad a la información se obtuvo un valor de 7,67 en **t**, siendo este un valor mayor que la región de aceptación. Por consiguiente, la hipótesis nula fue rechazada y la alterna fue aceptada, debido a que el marco de trabajo de seguridad de información utilizando la ISO 27001 mejora la disponibilidad de información en los controles de acceso de los usuarios en instituciones orientadas a teletrabajo

V. DISCUSIÓN

La presente investigación consiguió como resultado que el marco de trabajo de seguridad de información basado en la ISO 27001 disminuyo el porcentaje total de accesos a la información sin autorización en la empresa Terceriza E.I.R.L de un 65,4% a un 37,5%, equivalente a una disminución del 27.9%. Por consiguiente, el marco de trabajo mejoro el nivel de confidencialidad dentro de la empresa Terceriza E.I.R.L.

De la misma forma Aguinaga Quispe, Will, en su tesis titulada “Sistema de gestión alineado a la norma ISO/IEC 27001:2013 para la seguridad de información de una institución financiera, Chachapoyas Amazonas, 2021.”, obtuvo como resultados que el sistema de gestión incrementó el nivel de confidencialidad de un 75.52% a un 87.36%.

Asimismo, el resultado obtenido en el indicador porcentaje total de información modificada sin autorización indica que el marco de trabajo de seguridad de información basado en la ISO disminuyo en la empresa Terceriza E.I.R.L de un 40.1% a un 18.1%, equivalente a una disminución de un 22%, por consiguiente, el marco de trabajo mejoro el nivel de integridad dentro de la empresa Terceriza E.I.R.L.

De la misma forma Aguinaga Quispe, Will, en su tesis titulada “Sistema de gestión alineado a la norma ISO/IEC 27001:2013 para la seguridad de información de una institución financiera, Chachapoyas Amazonas, 2021.”, obtuvo como resultados que el sistema de gestión incremento el nivel de integridad de un 50.83% a un 72.36%.

Asimismo, el resultado obtenido en el indicador porcentaje total de accesibilidad a la información indica que el marco de trabajo de seguridad de información basado en la ISO disminuyo en la empresa Terceriza E.I.R.L de un 65,4% a un 37,1%, equivalente a una disminución de un 28.3%. Por consiguiente, el marco de trabajo

mejoro el nivel de disponibilidad de la información dentro de la empresa Terceriza E.I.R.L

De la misma forma Aguinaga Quispe, Will, en su tesis titulada “Sistema de gestión alineado a la norma ISO/IEC 27001:2013 para la seguridad de información de una institución financiera, Chachapoyas Amazonas, 2021.”, obtuvo como resultados que el sistema de gestión incremento el nivel de disponibilidad de un 96.81% a un 99.93%.

Esto quiere decir que los resultados conseguidos en este estudio demuestran que la aplicación de un marco de trabajo mejora el nivel de confidencialidad, integridad y disponibilidad de información; a su vez, mejoran los procesos internos de la organización. Esto se confirma debido a que el marco de trabajo de seguridad de información disminuyo el porcentaje total de acceso no autorizados a la información en 27.9%, el porcentaje total de información modificada sin autorización en 18.1% y el porcentaje de disponibilidad de información en 28.3%

En conclusión, se llega a que el marco de trabajo de seguridad de información basado en la ISO 27001:2013, mejoro el control de acceso de usuarios dentro de la empresa Terceriza E.I.R.L

VI. CONCLUSIONES

Este proyecto de investigación tiene como conclusiones lo siguiente:

PRIMERO: Se concluye que el marco de trabajo de seguridad de información basado en la ISO 27001:2013 disminuyó el porcentaje total de accesos a la información sin autorización en un 27,9%. En un principio teniendo 65.4% y después un 37.5%. Por lo tanto, se puede afirmar que el marco de trabajo disminuyó el porcentaje total de accesos a la información sin autorización en la empresa Terceriza E.I.R.L

SEGUNDO: Se concluye que el marco de trabajo de seguridad de información basado en la ISO 27001:2013 disminuyó el porcentaje total de información modificada sin autorización en un 22%. En un principio teniendo 40.1% y después un 18.1%. Por lo tanto, se puede afirmar que el marco de trabajo disminuyó el porcentaje total información modificada sin autorización en la empresa Terceriza E.I.R.L

TERCERO: Se concluye que el marco de trabajo de seguridad de información basado en la ISO 27001:2013 disminuyó el porcentaje total de accesos interrumpidos a la información en un 28,3%. En un principio teniendo 65.4% y después un 37.1%. Por lo tanto, se puede afirmar que el marco de trabajo disminuyó el porcentaje total de accesos interrumpidos a la información en la empresa Terceriza E.I.R.L

CUARTO: Se concluye que la implementación de un marco de trabajo de seguridad de información usando la ISO 27001 mejoró el control de acceso de usuarios en la empresa Terceriza E.I.R.L

VII. RECOMENDACIONES

Al término de la presente investigación se recomienda lo siguiente:

- Se recomienda llevar un seguimiento a los reportes de los trabajadores para la mejor toma de decisiones y poder cumplir los objetivos establecidos en la organización.
- Se recomienda que a futuro puedan utilizar un sistema de Active Directory de contar con los recursos suficientes para la mejora en el sistema de seguridad para los usuarios y así las políticas de seguridad sean más fáciles de configurar.
- Se recomienda que, para futuras aplicaciones del marco de trabajo, se tome un rango mayor de tiempo con respecto al Pos-test, de mínimo 2 meses a más, para que, con ello, se pueda realizar una estadística de moda y obtener mayores resultados estadísticos.
- Se recomienda para una futura aplicación utilizar otros controles de acceso o tomar otra normativa similar a la ISO 27001 o también usar más controles de la ISO 27002.

REFERENCIAS

AGUINAGA, Q., 2021. *Sistema de gestión alineado a la norma ISO/IEC 27001:2013 para la seguridad de la información en una institución financiera, Chachapoyas-Amazonas, 2021.* S.l.: UNIVERSIDAD CESAR VALLEJO.

ANDRADE, J. y CHAVEZ, C., 2018. *Generación de un plan para la gestión integral de seguridad de la información basado en el marco de la norma ISO 27001 y las mejores prácticas de seguridad de la norma iso 27002 para la compañía international Gym Ecuaintergym S.A. de la ciudad de Guayaqui* [en línea]. S.l.: Universidad de Guayaquil. Disponible en: http://repositorio.ug.edu.ec/handle/redug/32606.

ARIAS, E., 2020. *Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac, Callao* [en línea]. S.l.: Universidad Cesar Vallejo. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/47276/Arias_QES-SD.pdf?sequence=1&isAllowed=y.

BACA, L.S.R., DE LA VEGA, C.F.C.P., CORREDOR, C.M. y DIAZ, M.A.A., 2020. Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana TT - Application of ISO 27001 and its influence on the information security of a Peruvian private company. En: Copyright - © 2020. This work is published under https://creativecommons.org/licenses/by-nc-nd/4.0/ (the “License”). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License.Última actualización - 2020-12-10, *Propositos y Representaciones* [en línea], vol. 8, no. 3, pp. 1-11. ISSN 23077999. DOI http://dx.doi.org/10.20511/pyr2020.v8n3.786. Disponible en: https://www.proquest.com/scholarly-journals/aplicación-de-iso-27001-y-su-influencia-en-la/docview/2468684801/se-2?accountid=37408.

BAYONA, S. y ALTAMARINO, J., 2017. Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. *Revista Ibérica de Sistemas e Tecnologias de Información* [en línea], pp. 134. Disponible en: http://www.scielo.mec.pt/pdf/rist/n25/n25a09.pdf.

BONILLA, E., 2019. *PROPUESTA DE MEJORAMIENTO CONTINÚO DE LA*

SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR [en línea]. S.l.: UNIVERSIDAD SANTO TOMÁS. Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/20824/2019erikabonilla.pdf?sequence=15.

CALDER, A., 2017. *ISO27001/ISO27002: una Guía de Bolsillo* [en línea]. Estados Unidos: s.n. ISBN 9781849289177. Disponible en: https://www.proquest.com/docview/2133079960/$N?accountid=37408.

CAMACHO, R., 2008. *DISEÑO E IMPLANTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PROTECCIÓN DE LOS ACTIVOS INFORMÁTICOS DE LA UNIVERSIDAD CENTRAL DE VENEZUELA*. S.l.: UNIVERSIDAD CENTRAL DE VENEZUELA.

CARRASCO, S., 2017. *METODOLOGÍA DE LA INVESTIGACIÓN CIENTIFICA*. LIMA - PERÚ: s.n.

CHRISTIANSEN, A., 2020. Ciberseguridad y teletrabajo: los nuevos riesgos de la oficina remota. , pp. 16.

COHEN, NESTOR, G.G., 2019. *METODOLOGÍA DE LA INVESTIGACIÓN, ¿PARA QUÉ?* BUENOS AIRES - ARGENTINA: s.n. ISBN 9789877231908.

DEMING, W.E., 1986. *Out of the Crisis*. S.l.: MIT Press. Cambridge.

GARCÍA, M., 2021. El teletrabajo, los dispositivos móviles y cloud, los tres vectores que hay que proteger en la era post-covid. , pp. 16.

GESTIÓN, T.S.C.Y., 2018. TD SISTEMAS CONTROL Y GESTIÓN. [en línea]. Disponible en: https://www.tdsistemas.com/.

GODOY, R., 2014. SEGURIDAD DE LA INFORMACIÓN. *REVISTA DE LA SEGUNDA COHORTE DEL DOCTORADO EN SEGURIDAD ESTRATÉGICA GUATEMALA, 2014*, pp. 308.

GÓMEZ, P.O., 2018. La justificación de la abducción en el contexto del debate sobre el realismo científico: una aproximación argumentativa TT - The Justification of Abduction in the Context of the Debate over Scientific Realism: an Argumentative Approach. En: Copyright - © 2018. This work is published under https://creativecommons.org/licenses/by-nc-nd/3.0/es/ (the “License”). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License.Personas - Toulmin, StephenÚltima

actualización - 2020-12-10SubjectsTermNotLitGenreText - Toulmin, Stephen, *Artefactos* [en línea], vol. 7, no. 2, pp. 35-57. DOI http://dx.doi.org/10.l4201/art2018723557. Disponible en: https://www.proquest.com/scholarly-journals/la-justificación-de-abducción-en-el-contexto-del/docview/2172570076/se-2?accountid=37408.

GUERRA, R. y RAMOS, F., 2020. *Introducción a los Métodos Estadísticos* [en línea]. Cuba: Editorial Universitaria. ISBN 9789591643476. Disponible en: https://books.google.com.pe/books?id=-RH8DwAAQBAJ&pg=PT7&dq=escala+proporcional&hl=es-419&sa=X&ved=2ahUKEwijoamK8-vwAhUFIrkGHVQRC5wQ6AEwA3oECAcQAg#v=twopage&q&f=false.

HERNÁNDEZ-LALINDE MGTR, J., ESPINOSA-CASTRO, J.-F., CHACÍN MGTR, M., CARRILLO-SIERRA MGTR, S.-M. y ÁLVAREZ MGTR, D.G., 2019. Plan de muestreo para el estudio de obesidad, sobrepeso y variables biopsicosociales en niños y adolescentes escolarizados de Cúcuta, Colombia TT - Sampling plan for the study of obesity, overweight and biopsychosocial variables in children and adolescen. En: Copyright - Copyright Sociedad Latinoamericana de Hipertension 2019Última actualización - 2020-03-04SubjectsTermNotLitGenreText - Cucuta Colombia, *Archivos Venezolanos de Farmacologia y Terapéutica* [en línea], vol. 38, no. 5, pp. 615-621. ISSN 07980264. Disponible en: https://www.proquest.com/scholarly-journals/plan-de-muestreo-para-el-estudio-obesidad/docview/2354381544/se-2?accountid=37408.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013. *ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements* [en línea]. 2013. Suiza: s.n. Disponible en: https://www.iso.org/standard/54534.html.

MARIÑO, S. y ALFONSO, P., 2019. Evidencias de Accesibilidad Web en la generación de sitios. Propuesta de un método. [en línea], pp. 60. Disponible en: https://teyet-revista.info.unlp.edu.ar/TEyET/article/view/1133/955.

MELLON, U.C., 2010. *MEJORA DE LOS PROCESOS PARA EL DESARROLLO DE MEJORES PRODUCTOS Y SERVICIOS* [en línea]. Pensilvania - Estados Unidos: s.n. Disponible en:

https://resources.sei.cmu.edu/asset_files/WhitePaper/2010_019_001_28782.pdf.

MOLINA, L., 2016. *ACCESIBILIDAD DE LA INFORMACION Y LA COMUNICACION*. ESPAÑA: s.n. ISBN 9788416109159.

MORA, A., 2016. *GESTIÓN DE LA PREVENCIÓN. CONTROL DE ACCESOS* [en línea]. S.l.: UNIVERSIDAD POLITECNICA DE CARTAGENA. Disponible en: https://repositorio.upct.es/bitstream/handle/10317/5636/tfm-mor-ges.pdf?sequence=3.

MORALES, F., TOAPANTA, S. y TOASA, R.M., 2020. Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información TT - Implementation of a perimeter security system as an information security strategy. En: Copyright - © 2020. This work is published under https://creativecommons.org/licenses/by-nc-nd/4.0/ (the "License"). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License.Última actualización - 2021-03-26SubjectsTermNotLitGenreText - Ecuador, *Revista Ibérica de Sistemas e Tecnologias de Informação* [en línea], no. E27, pp. 553-565. ISSN 16469895. Disponible en: https://www.proquest.com/scholarly-journals/implementación-de-un-sistema-seguridad-perimetral/docview/2385756526/se-2?accountid=37408.

NUÑEZ, W. y CHACÓN, E., 2017. *DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA SEREXCEL SERVICIOS FUNERARIOS* [en línea]. S.l.: UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS. Disponible en: https://repository.udistrital.edu.co/bitstream/handle/11349/8323/edinson andres chacon umaña - william andres nuñez vergara 2017.pdf?sequence=1&isallowed=y.

OCAÑA, A.O. y LÓPEZ, M.I.A., 2019. Hacer decolonial: desobedecer a la metodología de investigación * TT - Decolonial doing: disobey the research methodology Fazer decolonial: desobedecer a metodologia de pesquisa. En: Copyright - © 2019. This work is published under https://creativecommons.org/licenses/by-sa/4.0/ (the "License"). Notwithstanding the ProQuest Terms and Conditions, you may use this content

in accordance with the terms of the License.Última actualización - 2019-06-14SubjectsTermNotLitGenreText - Argentina, *Hallazgos* [en línea], vol. 16, no. 31, pp. 147-166. ISSN 17943841. DOI http://dx.doi.org/10.15332/s1794-3841.2019.0031.06. Disponible en: https://www.proquest.com/scholarly-journals/hacer-decolonial-desobedecer-la-metodología-de/docview/2239547925/se-2?accountid=37408.

ORTIZ, L. y VALENCIA, F., 2017. Gestión de riesgos en eTOM. Un análisis comparativo con los estándares de riesgo corporativo. *Revista LOGOS CIENCIA Y TECNOLOGÍA* [en línea], pp. 17. Disponible en: https://revistalogos.policia.edu.co:8443/index.php/rlct/article/view/334/pdf.

PALMA, M., 2019. *DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO27002:2013 PARA EL CONTROL DE ACCESO A LA INFRAESTRUCTURA DE RED DE AXXIS HOSPITAL* [en línea]. S.l.: UNIVERSIDAD INTERNACIONAL SEK SER MEJORES. Disponible en: https://repositorio.uisek.edu.ec/bitstream/123456789/3647/1/PALMA AGAMA MARÍA FERNANDA.pdf.

PATIÑO, S., CAICEDO, A. y GUAÑA, E.R., 2019. Modelo de evaluación del Dominio Control de Acceso de la norma ISO 27002 aplicado al proceso de Gestión de Bases de Datos. En: Copyright - © 2019. This work is published under https://creativecommons.org/licenses/by-nc-nd/4.0 (the “License”). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License.Última actualización - 2021-03-26, *Revista Ibérica de Sistemas e Tecnologias de Informação* [en línea], no. E22, pp. 230-241. ISSN 16469895. Disponible en: https://www.proquest.com/scholarly-journals/modelo-de-evaluación-del-dominio-control-acceso/docview/2317841707/se-2?accountid=37408.

PRESSMAN, R., 2015. *Software Engineering: A Practitioner’s Approach* [en línea]. septima. Estados Unidos: s.n. ISBN 978-0-07-337597-7. Disponible en: https://whyphi.staff.telkomuniversity.ac.id/files/2016/01/ebook-pressman-sw-engineering.pdf.

RASINGER, S., 2020. *LA INVESTIGACIÓN CUANTITATIVA EN LINGÜÍSTICA* [en línea]. Cambridge: s.n. ISBN 9788446046455. Disponible en:

https://books.google.com.pe/books?id=0h4EEAAAQBAJ&printsec=frontcover&dq=investigación+cuantitativa&hl=es-419&sa=X&redir_esc=y#v=onepage&q=investigación cuantitativa&f=false.

RODRIGUEZ, A., 2015. *Secreto industrial y confidencialidad*. S.l.: LAWGIC.

ROMERO, M., FIGUEROA, G., VERA, D., ÁLAVA, J., PÁRRALES, G., ÁLAVA, C., MURILLO, Á. y CASTILLO, M., 2018. *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES* [en línea]. Primera. Alicante-España: s.n. ISBN 978-84-949306-1-4. Disponible en: https://books.google.com.pe/books?id=5Z9yDwAAQBAJ&printsec=frontcover&dq=seguridad+de+información+de+control+de+accesos&hl=es-419&sa=X&ved=2ahUKEwiG2aLq0sXwAhVIK7kGHeLcBscQ6AEwAnoECAMQAg#v=onepage&q=seguridad de información de control de accesos&f=false.

RUÍZ, J., ESTRADA, C. y SÁNCHEZ, M., 2020. PROPUESTA DE UN MODELO DE UN SISTEMA DE GESTIÓN DE CALIDAD EN SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA INSTITUCIONES EDUCATIVAS. *Revista de investgación latinoamericana en competitividad organizacional* [en línea], no. 2659-5494, pp. 26. Disponible en: https://www.eumed.net/rev/rilco/05/gestion-instituciones.html.

SASAVILCA, J., 2017. *Implementación de la norma ISO 27001 en la Gestión de la Seguridad de la Información en la empresa Atento del Perú 2017* [en línea]. S.l.: UNIVERSIDAD CESAR VALLEJO. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/39329/Salsavilca_RJC..pdf?sequence=1&isAllowed=y.

SIERRA, G., 2021. Ransomware: cómo es la nueva guerra global de secuestro de datos que aterroriza a países y empresas de la que hablarán Biden y Putin. *INFOBAE*. RUSIA, junio 2021. pp. 10.

ŠIKMAN, L., LATINOVIĆ, T. y PASPALJ, D., 2019. ISO 27001 - INFORMATION SYSTEMS SECURITY, DEVELOPMENT, TRENDS, TECHNICAL AND ECONOMIC CHALLENGES. En: Copyright - © 2019. This work is published under NOCC (the “License”). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License.Última actualización - 2020-01-24, *Annals of the Faculty of Engineering Hunedoara* [en línea], vol. 17, no. 4, pp. 45-48. ISSN 15842665.

Disponible en: https://www.proquest.com/scholarly-journals/iso-27001-information-systems-security/docview/2344260662/se-2?accountid=37408.

SOUZA, J.G.S., ARIMA, C.H. y BELDA, F.R., 2020. Information security treatment analysis on a federal public education institution TT - Análise de tratamento da segurança da informação de uma instituição de ensino público federal. Análisis del tratamiento de seguridad de la información de una instituci. En: Copyright - © 2020. This work is published under http://creativecommons.org/licenses/by-nc-sa/4.0/ (the “License”). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License.Última actualización - 2020-08-20, *Revista Ibero-Americana de Estudos em Educação* [en línea], vol. 15, no. 3, pp. 1309-1321. ISSN 24468606. DOI http://dx.doi.org/10.21723/riaee.v15i3.13584. Disponible en: https://www.proquest.com/scholarly-journals/information-security-treatment-analysis-on/docview/2435511297/se-2?accountid=37408.

Suministro E Instalacin De Sistema De Control De Accesos Presencia Y Cctv, Mantenimiento Preventivo (spain-bilbao: Access Control System). En: Copyright - © 2021 Al Bawaba (Albawaba.com) Provided by SyndiGate Media Inc. (Syndigate.info).Última actualización - 2021-01-08SubjectsTermNotLitGenreText - Spain, *MENA Report* [en línea], 2020. Disponible en: https://www.proquest.com/trade-journals/suministro-e-instalacin-de-sistema-control/docview/2468091633/se-2?accountid=37408.

TABOADA, J. y COTOS, J., 2015. *SISTEMAS DE INFORMACIÓN MEDIOAMBIENTAL* [en línea]. ESPAÑA: s.n. ISBN 84-9745-056-6. Disponible en: https://books.google.com.pe/books?id=FEBhY2xmmT8C&pg=PA27&dq=integridad+de+información&hl=es-419&sa=X&ved=2ahUKEwjJlry_7NLxAhUzqpUCHTkZD_AQ6wEwAHoECAcQAQ#v=onepage&q=integridad de información&f=false.

VALENCIA, F. y OROZCO, M., 2017. Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas e Tecnologias de Información*, pp. 88.

VERN, A., 2017. *G2700 Giac Certified Iso-27000 Specialist: Questions and*

Answers. Estados Unidos: s.n. ISBN CreateSpace Independent Publishing Platform.

ANEXOS

ANEXO 1: AUTORIZACIÓN DE LA EMPRESA

Lima, 15 de mayo del 2021

Por medio de la presente, yo Carlos Barreto Rodríguez, identificado con DNI 10802820, siendo el jefe del área de T.I de la empresa 3eriza, con razón social RUC TERCERIZA S.R.L y RUC 20521074745, ubicada en Surquillo, Calle Los Halcones 102, doy autorización a los estudiantes Julio César Paredes Cóndor y Carlos Voto Bernales Villalobos, para que puedan realizar su investigación dentro de la empresa, brindándole los accesos que requerirán, siempre y cuando ello no afecte la integridad de la empresa.

Firma del jefe del área de TI

ANEXO 2: DECLARACIÓN DE IMPLEMENTACIÓN DEL MARCO DE TRABAJO

Lima, 10 de diciembre del 2021

CONSTANCIA DE IMPLEMENTACIÓN DEL MARCO DE TRABAJO

TÍTULO: Marco de trabajo de seguridad de información basado en la ISO/IEC 27001:2013 para el control de acceso de los usuarios en empresas de teletrabajo

INVESTIGADOR / IMPLEMENTADOR:

- Paredes Cóndor, Julio César
- Voto Bernales Villalobos, Carlos Andrés

EMPRESA: TERCERIZA S.R.L

Por medio de la presente, yo **CARLOS BARRETO RODRÍGUEZ** con N° de **DNI 10802820** representante de la empresa del área de TI de **TERCERIZA PERU S.R.L** CON RUC 20521074745 manifiesto el cumplimiento de la implementación del marco de trabajo que nuestros colaboradores han venido desarrollando durante estos 8 meses de investigación hasta la implementación del mismo, el cual ha beneficiado en muchos aspectos en nuestra seguridad de la información para el personal que trabaja de manera remota, por ende le agradecemos el esfuerzo y dedicación para el cumplimientodel proyecto planteado.

Se expide la constancia para los fines que el crea conveniente.

Carlos Barreto Rodríguez
DNI: 10802820

ANEXO 3: Matriz de consistencia

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES E INDICADORES	METODOS Y TECNICAS DE INVESTIGACION
PROBLEMA GENERAL ¿De qué manera un marco de trabajo de seguridad de información para el control de acceso de usuarios tiene influencia en instituciones orientadas a teletrabajo? **PROBLEMAS ESPECIFICOS** 1. ¿En qué medida afecta gestionar la norma ISO 27001 en la confidencialidad para la seguridad de información en instituciones orientadas a teletrabajo? 2. ¿En qué medida afecta la norma ISO 27001 en la integridad para la seguridad de información en instituciones orientadas a teletrabajo? 3. ¿En qué medida mejora la disponibilidad para la seguridad de información en instituciones orientadas a teletrabajo?	**OBJETIVO GENERAL** Determinar la influencia de un marco de trabajo de seguridad de información para el control de acceso basado en la ISO 27001 en empresas de teletrabajo y como objetivos específicos. **OBJETIVOS ESPECIFICOS** 4. Determinar la mejora desarrollando un marco de trabajo de seguridad de la información basado en la ISO 27001 en la confidencialidad de información en empresas de teletrabajo. 5. Determinar la mejora desarrollando un marco de trabajo de seguridad de la información basado en la ISO 27001 en la integridad de la información en empresas de teletrabajo. 6. Determinar la mejora desarrollando un marco de trabajo de seguridad de la información basado en la ISO 27001 en la disponibilidad de la información en empresas de teletrabajo.	**HIPÓTESIS GENERAL** El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 mejora la seguridad de información en el control de acceso de los usuarios en las instituciones orientadas a teletrabajo. **HIPÓTESIS ESPECIFICOS** **H1:** El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 mejora la confidencialidad de información en los controles de acceso de usuarios en instituciones orientadas a teletrabajo. **H2:** El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 mejora la integridad de información en los controles de acceso de usuarios en instituciones orientadas a teletrabajo. **H3:** El desarrollo de un marco de trabajo de seguridad de información utilizando la ISO 27001 mejora la disponibilidad de información en los controles de acceso de usuarios en instituciones orientadas a teletrabajo.	**VARIABLE DEPENDIENTE**: **Control de accesos de seguridad de la información** **D1. Confidencialidad** Indicadores: 1. Porcentaje total de accesos a la información sin autorización Indicadores: **D2. Integridad** 2. Porcentaje total de Información modificada sin autorización **D3. Disponibilidad** Indicadores: 1. Porcentaje total de accesibilidad a la información	**Métodos:** **Tipo:** Cuantitativo **Nivel:** Explicativo - tecnológico **Diseño:** experimental de tipo pre-experimental Grupo | Antes | Intervención | Después GE: | 0_1 | X | 0_2 GE: Trabajadores a nivel usuario de la empresa O1: Aplicación de instrumentos en función de los indicadores antes del marco de trabajo de seguridad de la información X: Aplicación del marco de trabajo de seguridad de información O2: Aplicación de instrumentos en función de los indicadores después de la ejecución del marco de trabajo de seguridad de información **Técnicas:** • **De muestreo** No probabilística • **De recolección de datos** ▪ **Encuesta** por cuestionario de satisfacción ▪ **Observación** por: - ficha de observación en función de los resultados del sistema ▪ Hojas de control de calidad del producto

ANEXO 4: Matriz de Operacionalización de la variable dependiente

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	INSTRUMENTOS DE MEDICIÓN	ESCALA
Control de acceso de seguridad de información	Un control de acceso de seguridad de información restringe o permite el acceso de un usuario o grupo de usuarios a un área específica validando la identificación por medio de diferentes tipos de lectura y en algunos sistemas se otorga acceso completo después de la autenticación exitosa del usuario, pero la mayoría de los sistemas requieren un control más sofisticado y complejo, además del mecanismo de autenticación como una contraseña, el control de acceso se refiere a cómo se estructuran las autorizaciones, en algunos casos, la autorización puede reflejar la estructura de la organización (Arantxa Mora Pérez, 2016)	trata las entradas, salidas o presencia de personas, objetos o vehículos en un recinto, de acuerdo con unos criterios establecidos con anterioridad. Este control, o diferenciación entre personal o material autorizado y no autorizado, es vital para la mayoría de los Sistemas de Seguridad. (PUEDE HABER)	Confidencialidad	Porcentaje total de accesos a la información sin autorización	Ficha de observación	Razón
			Integridad	Porcentaje total de Información modificada sin autorización		
			Disponibilidad	Porcentaje promedio de accesibilidad a la información		

ANEXO 5: Instrumento para la validez de la propuesta de ingeniería – Variable independiente

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	INSTRUMENTOS DE MEDICIÓN
Marco de trabajo de seguridad de la información	Un marco de trabajo de seguridad de información es una visión general amplia o esquema de elementos interconectados, que define un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular (Press, 2015)	Identificar posibles riesgos de seguridad para sus activos de información, protegiendo de estos riesgos mediante el desarrollo y la implementación de salvaguardias, permitiendo recuperarse de estas incidencias mediante la restauración de los activos socavados (Alan Calder, 2018)	Satisfacción	Nivel de satisfacción del usuario	Cuestionario de percepción.
			Eficacia	Nivel de desempeño dentro de la empresa	
			Confiabilidad	Nivel de incidencias dentro de la empresa	

ANEXO 6: INSTRUMENTOS – FICHAS DE REGISTRO

FICHA DE REGISTRO				
INVESTIGADOR	Paredes Condor Julio cesar	Voto Bernales Villalobos Carlos Andrés	**TIPO DE PRUEBA**	Pre-Test
EMPRESA	TERCERIZA PERÚ S.R.L			
DIRECCIÓN	Cal. los Halcones Nro. 102 Surquillo			
FECHA DE INICIO	01/10/2021	**FECHA FINAL**		30/10/2021
VARIABLE	**INDICADOR**	**MEDIDA**	**FÓRMULA**	
Control de acceso de seguridad de información	Porcentaje total de accesos no autorizados a la información	Porcentaje	PTANI = TDISA/TAIDG *100 PTANI: Porcentaje total de accesos no autorizados a la información TDISA: Total del día de accesos sin autorización TAIDG: Total de accesos del día en general	
N° de día	FECHA	TDISA	TAIDG	PTANI
1	01/10/2021	25	35	71.43
2	02/10/2021	12	15	80.00
3	03/10/2021	15	28	53.57
4	04/10/2021	10	18	55.56
5	05/10/2021	13	19	68.42
6	06/10/2021	9	13	69.23
7	07/10/2021	10	15	66.67
8	08/10/2021	28	36	77.78
9	09/10/2021	10	16	62.50
10	10/10/2021	11	15	73.33
11	11/10/2021	6	16	37.50
12	12/10/2021	31	45	68.89
13	13/10/2021	19	28	67.86
14	14/10/2021	24	38	63.16
15	15/10/2021	18	29	62.07
16	16/10/2021	8	13	61.54
17	17/10/2021	9	18	50.00
18	18/10/2021	10	15	66.67
19	19/10/2021	10	15	66.67
20	20/10/2021	33	45	73.33
21	21/10/2021	18	29	62.07
22	22/10/2021	16	25	64.00
23	23/10/2021	9	16	56.25
24	24/10/2021	9	12	75.00
25	25/10/2021	19	30	63.33
26	26/10/2021	27	39	69.23
27	27/10/2021	15	23	65.22
28	28/10/2021	18	26	69.23
29	29/10/2021	30	42	71.43
30	30/10/2021	10	14	71.43
TOTAL				65.45

FICHA DE REGISTRO				
INVESTIGADOR	Paredes Condor Julio cesar Voto Bernales Villalobos Carlos Andrés		**TIPO DE PRUEBA**	Post-Test
EMPRESA	TERCERIZA PERÚ S.R.L			
DIRECCIÓN	Cal. los Halcones Nro. 102 Surquillo			
FECHA DE INICIO	01/11/2021	FECHA FINAL		30/11/2021
VARIABLE	**INDICADOR**	**MEDIDA**	**FÓRMULA**	
Control de acceso de seguridad de información	Porcentaje total de accesos no autorizados a la información	PORCENTAJE	PTANI = TDISA/TAIDG *100 PTANI: Porcentaje total de accesos no autorizados a la información TDISA: Total del día de accesos sin autorización TAIDG: Total de accesos del día en general	
N° de día	FECHA	TDISA	TAIDG	PTANI
1	01/11/2021	10	30	33.33
2	02/11/2021	8	25	32.00
3	03/11/2021	10	32	31.25
4	04/11/2021	5	20	25.00
5	05/11/2021	8	18	44.44
6	06/11/2021	4	33	12.12
7	07/11/2021	6	24	25.00
8	08/11/2021	10	24	41.67
9	09/11/2021	10	29	34.48
10	10/11/2021	15	33	45.45
11	11/11/2021	4	15	26.67
12	12/11/2021	8	29	27.59
13	13/11/2021	9	31	29.03
14	14/11/2021	8	41	19.51
15	15/11/2021	1	26	3.85
16	16/11/2021	1	19	5.26
17	17/11/2021	11	27	40.74
18	18/11/2021	9	21	42.86
19	19/11/2021	13	29	44.83
20	20/11/2021	3	17	17.65
21	21/11/2021	9	16	56.25
22	22/11/2021	9	14	64.29
23	23/11/2021	1	12	8.33
24	24/11/2021	12	38	31.58
25	25/11/2021	1	18	5.56
26	26/11/2021	1	30	3.33
27	27/11/2021	10	35	28.57
28	28/11/2021	2	15	13.33
29	29/11/2021	14	26	53.85
30	30/11/2021	7	17	41.18
TOTAL				29.63

FICHA DE REGISTRO				
INVESTIGADOR	Paredes Condor Julio cesar	Voto Bernales Villalobos Carlos Andrés	TIPO DE PRUEBA	Pre-Test
EMPRESA	TERCERIZA PERÚ S.R.L			
DIRECCIÓN	Cal. los Halcones Nro. 102 Surquillo			
FECHA DE INICIO	01/10/2021	**FECHA FINAL**		30/10/2021
VARIABLE	**INDICADOR**	**MEDIDA**	**FÓRMULA**	
Control de acceso de seguridad de información	Porcentaje total de información modificada sin autorización	Porcentaje	PTIMSA = TDIMSA/TDIMG *100 PTIMSA: Porcentaje total de información modificada sin autorización TDIMSA: Total del día de información modificada sin autorización TDIMG: Total del día de información modificada en general	
N° de día	FECHA	TDIMSA	TDIMG	PTIMSA
1	01/10/2021	5	10	50.00
2	02/10/2021	5	7	71.43
3	03/10/2021	1	4	25.00
4	04/10/2021	1	12	8.33
5	05/10/2021	2	5	40.00
6	06/10/2021	1	4	25.00
7	07/10/2021	3	10	30.00
8	08/10/2021	1	9	11.11
9	09/10/2021	2	11	18.18
10	10/10/2021	4	6	66.67
11	11/10/2021	6	9	66.67
12	12/10/2021	1	1	100.00
13	13/10/2021	2	5	40.00
14	14/10/2021	1	5	20.00
15	15/10/2021	2	8	25.00
16	16/10/2021	1	4	25.00
17	17/10/2021	2	5	40.00
18	18/10/2021	3	6	50.00
19	19/10/2021	2	3	66.67
20	20/10/2021	2	2	100.00
21	21/10/2021	2	5	40.00
22	22/10/2021	5	7	71.43
23	23/10/2021	2	5	40.00
24	24/10/2021	1	5	20.00
25	25/10/2021	4	8	50.00
26	26/10/2021	1	3	33.33
27	27/10/2021	2	4	50.00
28	28/10/2021	2	4	50.00
29	29/10/2021	1	3	33.33
30	30/10/2021	2	5	40.00
TOTAL				43.57

FICHA DE REGISTRO				
INVESTIGADOR	Paredes Condor Julio cesar	Voto Bernales Villalobos Carlos Andrés	TIPO DE PRUEBA	Post-Test
EMPRESA	TERCERIZA PERÚ S.R.L			
DIRECCIÓN	Cal. los Halcones Nro. 102 Surquillo			
FECHA DE INICIO	01/11/2021	**FECHA FINAL**		30/11/2021
VARIABLE	**INDICADOR**	**MEDIDA**	**FÓRMULA**	
Control de acceso de seguridad de información	Porcentaje total de información modificada sin autorización	Porcentaje	PTIMSA = TDIMSA/TDIMG *100 PTIMSA: Porcentaje total de información modificada sin autorización TDIMSA: Total del día de información modificada sin autorización TDIMG: Total del día de información modificada en general	
N° de día	FECHA	TDIMSA	TDIMG	PTIMSA
1	01/11/2021	2	10	20.00
2	02/11/2021	1	7	14.29
3	03/11/2021	2	6	33.33
4	04/11/2021	1	12	8.33
5	05/11/2021	0	5	0.00
6	06/11/2021	1	7	14.29
7	07/11/2021	1	10	10.00
8	08/11/2021	1	9	11.11
9	09/11/2021	2	11	18.18
10	10/11/2021	1	6	16.67
11	11/11/2021	2	9	22.22
12	12/11/2021	0	1	0.00
13	13/11/2021	0	5	0.00
14	14/11/2021	1	5	20.00
15	15/11/2021	2	8	25.00
16	16/11/2021	1	4	25.00
17	17/11/2021	0	5	0.00
18	18/11/2021	2	6	33.33
19	19/11/2021	1	3	33.33
20	20/11/2021	0	5	0.00
21	21/11/2021	1	5	20.00
22	22/11/2021	2	7	28.57
23	23/11/2021	1	5	20.00
24	24/11/2021	0	3	0.00
25	25/11/2021	1	5	20.00
26	26/11/2021	0	3	0.00
27	27/11/2021	1	4	25.00
28	28/11/2021	2	4	50.00
29	29/11/2021	0	4	0.00
30	30/11/2021	0	5	0.00
TOTAL				15.62

FICHA DE REGISTRO				
INVESTIGADOR	Paredes Condor Julio cesar	Voto Bernales Villalobos Carlos Andrés	TIPO DE PRUEBA	Pre-Test
EMPRESA	TERCERIZA PERÚ S.R.L			
DIRECCIÓN	Cal. los Halcones Nro. 102 Surquillo			
FECHA DE INICIO	01/10/2021	**FECHA FINAL**		30/10/2021
VARIABLE	**INDICADOR**	**MEDIDA**	**FÓRMULA**	
Control de acceso de seguridad de información	Porcentaje total de accesibilidad a la información	Porcentaje	PTACI = TSAII/TSAIG * 100 PTACI: Porcentaje total de accesibilidad a la información TSAII: Total de solicitudes de acceso a la información interrumpidas TSAIG: Total de solicitudes de acceso a la información general	
N° de día	FECHA	TSAII	TSAIG	PTACI
1	01/10/2021	20	24	83.33
2	02/10/2021	12	15	80.00
3	03/10/2021	15	28	53.57
4	04/10/2021	11	18	61.11
5	05/10/2021	11	17	64.71
6	06/10/2021	11	18	61.11
7	07/10/2021	10	14	71.43
8	08/10/2021	28	36	77.78
9	09/10/2021	10	16	62.50
10	10/10/2021	11	17	64.71
11	11/10/2021	6	16	37.50
12	12/10/2021	31	42	73.81
13	13/10/2021	19	28	67.86
14	14/10/2021	24	38	63.16
15	15/10/2021	18	29	62.07
16	16/10/2021	8	13	61.54
17	17/10/2021	11	20	55.00
18	18/10/2021	8	13	61.54
19	19/10/2021	10	15	66.67
20	20/10/2021	35	49	71.43
21	21/10/2021	16	27	59.26
22	22/10/2021	16	25	64.00
23	23/10/2021	11	18	61.11
24	24/10/2021	8	10	80.00
25	25/10/2021	21	32	65.63
26	26/10/2021	25	37	67.57
27	27/10/2021	17	25	68.00
28	28/10/2021	16	24	66.67
29	29/10/2021	32	44	72.73
30	30/10/2021	8	14	57.14
TOTAL				65.43

FICHA DE REGISTRO				
INVESTIGADOR	Paredes Condor Julio cesar	Voto Bernales Villalobos Carlos Andrés	TIPO DE PRUEBA	Post-Test
EMPRESA	TERCERIZA PERÚ S.R.L			
DIRECCIÓN	Cal. los Halcones Nro. 102 Surquillo			
FECHA DE INICIO	01/11/2021	**FECHA FINAL**		30/11/2021
VARIABLE	**INDICADOR**	**MEDIDA**	**FÓRMULA**	
Control de acceso de seguridad de información	Porcentaje total de accesibilidad a la información	Porcentaje	PTACI = TSAII/TSAIG * 100 PTACI: Porcentaje total de accesibilidad a la información TSAII: Total de solicitudes de acceso a la información interrumpidas TSAIG: Total de solicitudes de acceso a la información general	
N° de día	FECHA	TSAII	TSAIG	PTACI
1	01/11/2021	8	28	28.57
2	02/11/2021	10	27	37.04
3	03/11/2021	8	30	26.67
4	04/11/2021	7	22	31.82
5	05/11/2021	10	20	50.00
6	06/11/2021	2	31	6.45
7	07/11/2021	8	28	28.57
8	08/11/2021	8	22	36.36
9	09/11/2021	12	31	38.71
10	10/11/2021	17	29	58.62
11	11/11/2021	6	16	37.50
12	12/11/2021	6	27	22.22
13	13/11/2021	11	33	33.33
14	14/11/2021	6	39	15.38
15	15/11/2021	3	28	10.71
16	16/11/2021	1	17	5.88
17	17/11/2021	13	29	44.83
18	18/11/2021	7	19	36.84
19	19/11/2021	13	29	44.83
20	20/11/2021	5	19	26.32
21	21/11/2021	7	14	50.00
22	22/11/2021	11	16	68.75
23	23/11/2021	2	9	22.22
24	24/11/2021	14	41	34.15
25	25/11/2021	1	16	6.25
26	26/11/2021	3	30	10.00
27	27/11/2021	4	35	11.43
28	28/11/2021	1	15	6.67
29	29/11/2021	8	26	30.77
30	30/11/2021	5	18	27.78
TOTAL				29.62

ANEXO 7: INSTRUMENTOS DE VALIDEZ

INSTRUMENTO DE VALIDEZ DE CONTENIDO DE LA PROPUESTA DE INGENIERÍA.

Apellidos y Nombres del Experto:

Titulo y/o Grado Académico:
Doctor ( ) Magister (X) Ingeniero (X) Licenciado ( ) Otro ( )
Fecha: /06/2021

TESIS: Marco de trabajo de seguridad de información basado en la ISO/IEC 27001 para el control de acceso de los usuarios en empresas de teletrabajo

Autores: Paredes Cóndor, Julio César – Voto Bernales Villalobos, Carlos Andrés

ESCALA DE EVALUACIÓN
MUY MALO (1) MALO (2) REGULAR (3) BUENO (4) EXCELENTE (5)

Mediante la evaluación de expertos usted tiene la facultad de calificar el instrumento para validar la propuesta tecnológica utilizando la tabla de validación del instrumento. Esta tabla presenta escalas del 1 al 5 con su respectivo indicador de evaluación, se exhorta calificar de acuerdo a lo que Ud. considera como experto. Y proceda a realizar la sumatorias de los valores para establecer su validación

Cuestionario de marco de trabajo

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACIÓN				
		1	2	3	4	5
1. CLARIDAD	El cuestionario es formulado con lenguaje apropiado.					
2. OBJETIVIDAD	Permite cumplir con la medición del indicador					
3. ACTUALIDAD	Esta organizado, considerando las dimensiones e indicadores					
4. SUFICIENCIA	Las preguntas por dimensión se consideran suficientes					
5. INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					
6. CONSISTENCIA	Está basado en aspectos teóricos y científicos actuales.					
7. COHERENCIA	Las preguntas están relacionadas al indicador.					
8. METODOLOGÍA	Responde al propósito de evaluación del producto tecnológico para investigación.					
9. PERTENENCIA	El instrumento es adecuado al tipo de usuario al cual será aplicado.					
	TOTAL					

III. PUNTAJE TOTAL

	Sugerencias	

IV. OPCIÓN DE APLICABILIDAD

( ) [34 -45] El instrumento puede ser aplicado, tal como está elaborado
( ) [22 -33] El instrumento debe ser mejorado antes de ser aplicado
( ) [9 -21] El instrumento debe replanteado en su totalidad

FIRMA DEL EXPERTO _____

Es adecuado el avance, la ciencia y tecnología.
Existe una organización lógica.
Comprende los aspectos de cantidad y calidad.

Cuestionario de Marco de trabajo de seguridad de la información

INVESTIGADORES: PAREDES CONDOR JULIO CESAR
VOTO BERNALES VILLALOBOS CARLOS ANDRES

EMPRESA:

PERSONA ENTREVISTADA:

DEPARTAMENTO EN QUE LABORA:

CARGO:

Esta encuesta debe ser respondida marcando con una X un casillero dentro de la escala, indicando el grado de acuerdo que tienes respecto al concepto que se expresa en cada ítem. La escala tiene cinco puntos de acuerdo al grado de aprobación o desaprobación de cada afirmación:

- 5 – Totalmente de acuerdo.
- 4 – De acuerdo.
- 3 – Ni de acuerdo, ni en desacuerdo.
- 2 – En desacuerdo.
- 1 – Totalmente en desacuerdo

VARIABLE: MARCO DE TRABAJO DE SEGURIDAD DE INFORMACIÓN							
DIMENSIONES	INDICADORES						
	Nivel de satisfacción del usuario		1	2	3	4	5
Satisfacción	1	El marco de trabajo de seguridad de información me resulta fácil de usar					
	2	Necesitaría ayuda de un experto para usar el marco de trabajo.					
	3	Las buenas prácticas del marco de trabajo están correctamente enfocadas al área donde laboro.					
	4	Percibí que varias funciones del marco de trabajo estaban integradas en base a las metas del área donde laboro					

	5	Pienso que la mayoría de personal de TI podrían aprender a emplear el marco de trabajo.					
	6	El marco de trabajo me resulta rápido y sencillo al ponerlo en práctica.					
	7	Necesité de poco tiempo para aprender varias cosas, antes de utilizar el marco de trabajo.					
Eficacia	Nivel de desempeño dentro de la empresa						
	8	El Marco de trabajo de seguridad de información cumple las exceptivas del área donde laboro.					
	9	Las buenas prácticas establecidas fueron adaptables a las necesidades del área donde laboro.					
	10	Las buenas prácticas del marco de trabajo permitieron una reducción de las incidencias de seguridad en el área donde laboro.					
	11	La comunicación y retroalimentación entre las áreas mejoraron en base a sus necesidades.					
	12	El marco de trabajo logró disminuir las incidencias con respecto a la manipulación de información sin autorización entre las áreas.					
	Nivel de incidencias dentro de la empresa						
Confiabilidad	13	Se logró una disminución de las incidencias por acceso a la información					
	14	El marco de trabajo permite detectar en menor tiempo los casos por acceso a información sin autorización.					
	15	Se logró disminuir los accesos no autorizados a la información					

NIVEL DE SATISFACCION

Para poder determinar el nivel de satisfacción, se tomó el total de preguntas (7) y se multiplicó por el valor máximo de este (5), y así definimos el valor máximo que podría tomarse en nuestra escala. Para definir el valor mínimo, solo tomamos el valor máximo de una pregunta (5).

Luego de ello, definimos los rangos para la cantidad de escalas que usaremos. En este caso solo se tomarán 3 escalas.

Satisfecho – Ni satisfecho, Ni insatisfecho - Insatisfecho

Una vez definido que se usarán 3 escalas, procedemos a restar el Valor máximo (35) y el valor mínimo (5), con dicho resultado, se procederá a dividir entre el número de escalas (3), dicho valor será utilizado para definir el rango de valores que se tomarán entre escalas (3) que definimos.

Una vez obtenido el rango, se procede a ir definiendo los valores que tendrá cada escala. Comenzando con la escala “Insatisfecho”, donde se toma el valor mínimo (5) y se le suma el rango obtenido previamente. Luego se repite ello, con las otras 2 escalas restantes.

5 – 15 = Nivel insatisfecho
16 – 25 = Nivel ni satisfecho ni insatisfecho(neutro)
26 -35 = Nivel satisfecho

NIVEL DE DESEMPEÑO

Para poder determinar el nivel de desempeño, se tomó el total de preguntas (5) y se multiplicó por el valor máximo de este (5), y así definimos el valor máximo que podría tomarse en nuestra escala. Para definir el valor mínimo, solo tomamos el valor máximo de una pregunta (5).

Luego de ello, definimos los rangos para la cantidad de escalas que usaremos. En este caso solo se tomarán 3 escalas.

Satisfecho – Ni satisfecho, Ni insatisfecho - Insatisfecho

Una vez definido que se usarán 3 escalas, procedemos a restar el Valor máximo (25) y el valor mínimo (5), con dicho resultado, se procederá a dividir entre el número de escalas (3), dicho valor será utilizado para definir el rango de valores que se tomarán entre escalas (3) que definimos.

Una vez obtenido el rango, se procede a ir definiendo los valores que tendrá cada escala. Comenzando con la escala “Insatisfecho”, donde se toma el valor mínimo (5) y se le suma el rango obtenido previamente. Luego se repite ello, con las otras 2 escalas restantes.

5 – 12 = Nivel insatisfecho
13 – 19 = Nivel ni satisfecho ni insatisfecho(neutro)
20 - 25 = Nivel satisfecho

NIVEL DE INCIDENCIAS

Para poder determinar el nivel de desempeño, se tomó el total de preguntas (3) y se multiplicó por el valor máximo de este (5), y así definimos el valor máximo que podría tomarse en nuestra escala. Para definir el valor mínimo, solo tomamos el valor máximo de una pregunta (5).

Luego de ello, definimos los rangos para la cantidad de escalas que usaremos. En este caso solo se tomarán 3 escalas.

Satisfecho – Ni satisfecho, Ni insatisfecho - Insatisfecho

Una vez definido que se usarán 3 escalas, procedemos a restar el Valor máximo (15) y el valor mínimo (5), con dicho resultado, se procederá a dividir entre el número de escalas (3), dicho valor será utilizado para definir el rango de valores que se tomarán entre escalas (3) que definimos.

Una vez obtenido el rango, se procede a ir definiendo los valores que tendrá cada escala. Comenzando con la escala “Insatisfecho”, donde se toma el valor mínimo (5) y se le suma el rango obtenido previamente. Luego se repite ello, con las otras 2 escalas restantes.

5 – 8 = Nivel insatisfecho

9 – 12 = Nivel ni satisfecho ni insatisfecho(neutro)

23 - 15 = Nivel satisfecho

ANEXO 8: Validación de juicio de expertos

Validador: Chapoñán Camarena, Rudy

INSTRUMENTO DE VALIDEZ DE CONTENIDO DE LA PROPUESTA DE INGENIERÍA.

Apellidos y Nombres del Experto:	Chapoñan Camarena Rudy
Titulo y/o Grado Académico:	Maestría en Gestión De Tecnologías De Información

Doctor ( ) Magister (X) Ingeniero (X) Licenciado ( ) Otro ( )

Fecha: /06/2021

TESIS: Marco de trabajo de seguridad de información basado en la ISO/IEC 27001 para el control de acceso de los usuarios en empresas de teletrabajo

Autores: Paredes Cóndor, Julio César – Voto Bernales Villalobos, Carlos Andrés

ESCALA DE EVALUACIÓN

MUY MALO (1) MALO (2) REGULAR (3) BUENO (4) EXCELENTE (5)

Mediante la evaluación de expertos usted tiene la facultad de calificar el instrumento para validar la propuesta tecnológica utilizando la tabla de validación del instrumento. Esta tabla presenta escalas del 1 al 5 con su respectivo indicador de evaluación, se exhorta calificar de acuerdo a lo que Ud. considera como experto. Y proceda a realizar la sumatorias de los valores para establecer su validación

Cuestionario de marco de trabajo

II. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**1**	**2**	**3**	**4**	**5**
1. CLARIDAD	El cuestionario es formulado con lenguaje apropiado.				x	
2. OBJETIVIDAD	Permite cumplir con la medición del indicador				x	
3. ACTUALIDAD	Esta organizado, considerando las dimensiones e indicadores				x	
4. SUFICIENCIA	Las preguntas por dimensión se consideran suficientes				x	
5. INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				x	
6. CONSISTENCIA	Está basado en aspectos teóricos y científicos actuales.				x	
7. COHERENCIA	Las preguntas están relacionadas al indicador.				x	
8. METODOLOGÍA	Responde al propósito de evaluación del producto tecnológico para investigación.				x	
9. PERTENENCIA	El instrumento es adecuado al tipo de usuario al cual será aplicado.				x	
	TOTAL				36	

III. PUNTAJE TOTAL

36	Sugerencias	

IV. OPCIÓN DE APLICABILIDAD

(x) [34 -45] El instrumento puede ser aplicado, tal como está elaborado
( ) [22 -33] El instrumento debe ser mejorado antes de ser aplicado
( ) [9 -21] El instrumento debe replanteado en su totalidad

FIRMA DEL EXPERTO

UNIVERSIDAD CÉSAR VALLEJO

INSTRUMENTO DE VALIDACIÓN DE EXPERTOS POR INDICADOR: Porcentaje total de Divulgación de información sin autorización

I. DATOS GENERALES

Apellidos y Nombres del Experto: Chapoñan Camarena Rudy
Título y/o Grado Académico: **Magister en Gestión de Tecnologías de Información**

Doctor () **Magister (x)** **Ingeniero ()** **Licenciado ()** **Otro ()**.....

Universidad que labora:
Fecha:

TESIS: Marco de trabajo de seguridad de información basado en la ISO/IEC 27001 para el control de acceso de los usuarios en empresas de teletrabajo

Autores: Paredes Condor, Julio Cesar; Voto Bernales Villalobos, Carlos Andres

Deficiente (0-20%) **Regular (21-50%)** **Bueno (51-70%)** **Muy Bueno (71-80%)** **Excelente (81-100%)**

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	La ficha de observación es formulada con lenguaje apropiado.				75%	
OBJETIVIDAD	Está expresado en conducta observable.				75%	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				75%	
ORGANIZACION	Existe una organización lógica.				75%	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				75%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				75%	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				75%	
COHERENCIA	En los datos respecto al indicador.				75%	
METODOLOGÍA	Responde al propósito de investigación.				75%	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				75%	
	TOTAL				75%	

III. PROMEDIO DE VALIDACIÓN

IV. OPCION DE APLICABILIDAD

() El instrumento puede ser aplicado, tal como está elaborado El instrumento debe ser mejorado antes de ser
() aplicado

FIRMA DEL EXPERTO

UNIVERSIDAD CÉSAR VALLEJO

INSTRUMENTO DE VALIDACION DE EXPERTOS POR INDICADOR: Porcentaje total de información modificada sin autorización

I. DATOS GENERALES

Apellidos y Nombres del Experto: **Chapoñan Camarena Rudy**

Título y/o Grado Académico: **Magister en Gestión de Tecnologías de Información**

Doctor () **Magister (x)** **Ingeniero ( )** **Licenciado ( )** **Otro ( )**.....

Universidad que labora:

Fecha:

TESIS: Marco de trabajo de seguridad de información basado en la ISO/IEC 27001 para el control de acceso de los usuarios en empresas de teletrabajo

Autores: Paredes Condor, Julio Cesar; Voto Bernales Villalobos, Carlos Andrés

Deficiente (0-20%) **Regular (21-50%)** **Bueno (51-70%)** **Muy Bueno (71-80%)** **Excelente (81-100%)**

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				75%	
OBJETIVIDAD	Esta expresado en conducta observable.				75%	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				75%	
ORGANIZACION	Existe una organización lógica.				75%	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				75%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				75%	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				75%	
COHERENCIA	En los datos respecto al indicador.				75%	
METODOLOGÍA	Responde al propósito de investigación.				75%	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				75%	
	TOTAL				75%	

III. PROMEDIO DE VALIDACION

IV. OPCION DE APLICABILIDAD

(x) El instrumento puede ser aplicado, tal como está elaborado El instrumento debe ser mejorado antes de ser

() aplicado

FIRMA DEL EXPERTO

UNIVERSIDAD CÉSAR VALLEJO

INSTRUMENTO DE VALIDACION DE EXPERTOS POR INDICADOR: Porcentaje total de accesibilidad de información

I. DATOS GENERALES

Apellidos y Nombres del Experto:	**Chapoñan Camarena Rudy**
Título y/o Grado Académico:	**Magister en Gestión de Tecnologías de**

Doctor () **Magister (x)** **Ingeniero ()** **Licenciado ( )** **Otro ( )**.....

Universidad que labora:	
Fecha:	

TESIS: Marco de trabajo de seguridad de información basado en la ISO/IEC 27001 para el control de acceso de los usuarios en empresas de teletrabajo

Autores: Paredes Condor, Julio Cesar; Voto Bernales Villalobos, Carlos Andrés

Deficiente (0-20%) **Regular (21-50%)** **Bueno (51-70%)** **Muy Bueno (71-80%)** **Excelente (81-100%)**

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				75%	
OBJETIVIDAD	Esta expresado en conducta observable.				75%	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				75%	
ORGANIZACION	Existe una organización lógica.				75%	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				75%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				75%	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				75%	
COHERENCIA	En los datos respecto al indicador.				75%	
METODOLOGÍA	Responde al propósito de investigación.				75%	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				75%	
	TOTAL					75%

III. PROMEDIO DE VALIDACIÓN

IV. OPCION DE APLICABILIDAD

(x) El instrumento puede ser aplicado, tal como está elaborado El instrumento debe ser mejorado antes de ser
() aplicado

FIRMA DEL EXPERTO

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR EXPERTOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	INDICADOR: 1. Promedio total de Divulgación de información sin autorización	Si	No	Si	No	Si	No	
1	$PTDIF = \frac{TDISA}{TID} * 100$	x		x		x		
	INDICADOR: 2. Promedio total de Información modificada sin autorización	Si	No	Si	No	Si	No	
2	$PTIM = \frac{TIMSA}{TIM} * 100$	x		x		x		
	INDICADOR: 3. Promedio total de accesibilidad a la información							
3	$PTACI = \frac{TSAII}{TSAI} * 100$	x		x		x		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Chapoñan Camarena Rudy **DNI:** 09635313

Especialidad del validador: Magister en Gestión de Tecnologías de Información

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

de junio del 2021

Firma del Experto Informante.

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR EXPERTOS

Nº	Competencias digitales instrumentales	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Ítems/reactivos/enunciado	SI	NO	SI	NO	SI	NO	
1	El marco de trabajo de seguridad de información me resulta fácil de usar	x		x		x		
2	Necesitaría ayuda de un experto para usar el marco de trabajo.	x		x		x		
3	Las buenas prácticas del marco de trabajo están correctamente enfocadas al área donde laboro.	x		x		x		
4	Percibí que varias funciones del marco de trabajo estaban integradas en base a las metas del área donde laboro	x		x		x		
5	Pienso que la mayoría de personal de TI podrían aprender a emplear el marco de trabajo.	x		x		x		
6	El marco de trabajo me resulta rápido y sencillo al ponerlo en práctica.	x		x		x		
7	Necesité de poco tiempo para aprender varias cosas, antes de utilizar el marco de trabajo.	x		x		x		
8	El Marco de trabajo de seguridad de información	x		x		x		

	cumple las exceptivas del área donde laboro.							
9	Las buenas prácticas establecidas fueron adaptables a las necesidades del área donde laboro.	x		x		x		
10	Las buenas prácticas del marco de trabajo permitieron una reducción de las incidencias de seguridad en el área donde laboro.	x		x		x		
11	La comunicación y retroalimentación entre las áreas mejoraron en base a sus necesidades.	x		x		x		
12	El marco de trabajo logró disminuir las incidencias con respecto a la manipulación de información sin autorización entre las áreas.	x		x		x		
13	Se logró una disminución de las incidencias por acceso a la información	x		x		x		
14	El marco de trabajo permite detectar en menor tiempo los casos por acceso a información sin autorización.	x		x		x		
15	Se logró disminuir los accesos no autorizados a la información	x		x		x		

UNIVERSIDAD CÉSAR VALLEJO

Observaciones (precisar si hay suficiencia): ____

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Chapoñan Camarena Rudy **DNI:** 09635313

Especialidad del validador: Magister en Gestión de Tecnologías de Información

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

de junio del 2021

Firma del Experto Informante.

Validador: Daza Vergaray, Alfredo

INSTRUMENTO DE VALIDEZ DE CONTENIDO DE LA PROPUESTA DE INGENIERÍA.

Apellidos y Nombres del Experto:	Daza Vergaray Alfredo
Titulo y/o Grado Académico:	Dr sistemas

Doctor (x) Magister ( ) Ingeniero ( ) Licenciado ( ) Otro ( )

Fecha: /06/2021

TESIS: Marco de trabajo de seguridad de información basado en la ISO/IEC 27001 para el control de acceso de los usuarios en empresas de teletrabajo

Autores: Paredes Cóndor, Julio César – Voto Bernales Villalobos, Carlos Andrés

ESCALA DE EVALUACIÓN

MUY MALO (1) MALO (2) REGULAR (3) BUENO (4) EXCELENTE (5)

Mediante la evaluación de expertos usted tiene la facultad de calificar el instrumento para validar la propuesta tecnológica utilizando la tabla de validación del instrumento. Esta tabla presenta escalas del 1 al 5 con su respectivo indicador de evaluación, se exhorta calificar de acuerdo a lo que Ud. considera como experto. Y proceda a realizar la sumatorias de los valores para establecer su validación

Cuestionario de marco de trabajo

II. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	1	2	3	4	5
1. CLARIDAD	El cuestionario es formulado con lenguaje apropiado.				4	
2. OBJETIVIDAD	Permite cumplir con la medición del indicador				4	
3. ACTUALIDAD	Esta organizado, considerando las dimensiones e indicadores				4	
4. SUFICIENCIA	Las preguntas por dimensión se consideran suficientes				4	
5. INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				4	
6. CONSISTENCIA	Está basado en aspectos teóricos y científicos actuales.				4	
7. COHERENCIA	Las preguntas están relacionadas al indicador.				4	
8. METODOLOGÌA	Responde al propósito de evaluación del producto tecnológico para investigación.				4	
9. PERTENENCIA	El instrumento es adecuado al tipo de usuario al cual será aplicado.				4	
	TOTAL					

III. PUNTAJE TOTAL

	Sugerencias	

IV. OPCIÓN DE APLICABILIDAD

( ) [34 -45] El instrumento puede ser aplicado, tal como está elaborado
( ) [22 -33] El instrumento debe ser mejorado antes de ser aplicado
( ) [9 -21] El instrumento debe replanteado en su totalidad

FIRMA DEL EXPERTO

Es adecuado el avance, la ciencia y tecnología.
Existe una organización lógica.
Comprende los aspectos de cantidad y calidad.

UNIVERSIDAD CÉSAR VALLEJO

INSTRUMENTO DE VALIDACIÓN DE EXPERTOS POR INDICADOR: Porcentaje total de Divulgación de información sin autorización

I. DATOS GENERALES

Apellidos y Nombres del Experto:	daza Vergaray Alfredo
Título y/o Grado Académico:	Dr sistemas

Doctor (x) Magister ( ) Ingeniero ( ) Licenciado ( ) Otro ( ) .....

Universidad que labora:	
Fecha:	

TESIS: Marco de trabajo de seguridad de información basado en la ISO/IEC 27001 para el control de acceso de los usuarios en empresas de teletrabajo

Autores: Paredes Cóndor, Julio Cesar; Voto Bernales Villalobos, Carlos Andrés

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%) Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

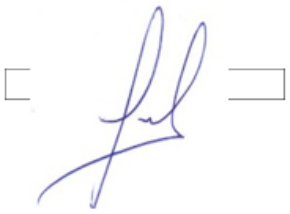
		VALORACION				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	La ficha de observacion es formulada con lenguaje apropiado.				80	
OBJETIVIDAD	Esta expresado en conducta observable.				80	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				80	
ORGANIZACION	Existe una organizacion logica.				80	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				80	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				80	
COHERENCIA	En los datos respecto al indicador.				80	
METODOLOGIA	Responde al proposito de investigacion.				80	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				80	
	TOTAL				80	

III. PROMEDIO DE VALIDACIÓN

IV. OPCION DE APLICABILIDAD

( ) El instrumento puede ser aplicado, tal como está elaborado El instrumento debe ser mejorado antes de ser
( ) aplicado

FIRMA DEL EXPERTO



UNIVERSIDAD CÉSAR VALLEJO

INSTRUMENTO DE VALIDACIÓN DE EXPERTOS POR INDICADOR: Porcentaje total de información modificada sin autorización

I. DATOS GENERALES

Apellidos y Nombres del Experto: daza Vergaray Alfredo

Título y/o Grado Académico: Dr sistemas

Doctor (x) Magister ( ) Ingeniero ( ) Licenciado ( ) Otro ( ).....

Universidad que labora:

Fecha:

TESIS: Marco de trabajo de seguridad de información basado en la ISO/IEC 27001 para el control de acceso de los usuarios en empresas de teletrabajo

Autores: Paredes Cóndor, Julio Cesar; Voto Bernales Villalobos, Carlos Andrés

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno(71-80%) Excelente(81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

I. ASPECTOS DE VALIDACIÓN

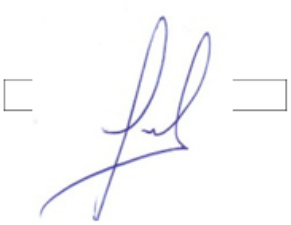
		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				80	
OBJETIVIDAD	Esta expresado en conducta observable.				80	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				80	
ORGANIZACION	Existe una organizacion logica.				80	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				80	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80	
CONSISTENCIA	Esta basado en aspectos teóricos y científicos.				80	
COHERENCIA	En los datos respecto al indicador.				80	
METODOLOGIA	Responde al proposito de investigacion.				80	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				80	
	TOTAL					

II. PROMEDIO DE VALIDACIÓN

III. OPCION DE APLICABILIDAD

(x) El instrumento puede ser aplicado, tal como está elaborado El instrumento debe ser mejorado antes de ser
( ) aplicado

FIRMA DEL EXPERTO



UNIVERSIDAD CÉSAR VALLEJO

INSTRUMENTO DE VALIDACIÓN DE EXPERTOS POR INDICADOR: Porcentaje total de accesibilidad de información

I. DATOS GENERALES

Apellidos y Nombres del Experto:	daza Vergaray Alfredo
Título y/o Grado Académico:	Dr sistemas

Doctor (x) Magister ( ) Ingeniero ( ) Licenciado ( ) Otro ( ).....

Universidad que labora:	
Fecha:	

TESIS: Marco de trabajo de seguridad de información basado en la ISO/IEC 27001 para el control de acceso de los usuarios en empresas de teletrabajo

Autores: Paredes Cóndor, Julio Cesar; Voto Bernales Villalobos, Carlos Andrés

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

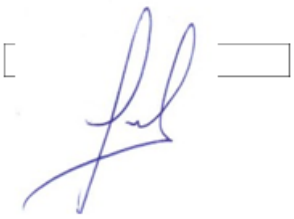
		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				80	
OBJETIVIDAD	Esta expresado en conducta observable.				80	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				80	
ORGANIZACIÓN	Existe una organizacion logica.				80	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				80	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80	
CONSISTENCIA	Esta basado en aspectos teóricos y científicos.				80	
COHERENCIA	En los datos respecto al indicador.				80	
METODOLOGÍA	Responde al proposito de investigacion.				80	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				80	
	TOTAL					

III. PROMEDIO DE VALIDACIÓN

IV. OPCION DE APLICABILIDAD

(x) El instrumento puede ser aplicado, tal como está elaborado El instrumento debe ser mejorado antes de ser
( ) aplicado

FIRMA DEL EXPERTO



UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR EXPERTOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	INDICADOR: 1. Porcentaje total de Divulgación de información sin autorización	SI	No	SI	No	SI	No	
1	$PTDIF = \frac{TDISA}{TID} * 100$	x		x		x		
	INDICADOR: 2. Porcentaje total de información modificada sin autorización	SI	No	SI	No	SI	No	
2	$PTIM = \frac{TIMSA}{TIM} * 100$	x		x		x		
	INDICADOR: 3. Porcentaje total de accesibilidad a la información							
3	$PTACI = \frac{TSAII}{TSAI} * 100$	x		x		x		

Observaciones (precisar si hay suficiencia): ...

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir []** **No aplicable []**

Apellidos y nombres del juez validador. **DNI:** 40466240

Especialidad del validador: **Dr Sistemas**

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

de junio del 2021

Firma del Experto Informante.

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR EXPERTOS

Nº	Competencias digitales instrumentales	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Ítems/reactivos/enunciado	SI	NO	SI	NO	SI	NO	
1	El marco de trabajo de seguridad de información me resulta fácil de usar	x		x		x		
2	Necesitaría ayuda de un experto para usar el marco de trabajo.	x		x		x		
3	Las buenas prácticas del marco de trabajo están correctamente enfocadas al área donde laboro.	x		x		x		
4	Percibí que varias funciones del marco de trabajo estaban integradas en base a las metas del área donde laboro	x		x		x		
5	Pienso que la mayoría de personal de TI podrían aprender a emplear el marco de trabajo.	x		x		x		
6	El marco de trabajo me resulta rápido y sencillo al ponerlo en práctica.	x		x		x		
7	Necesité de poco tiempo para aprender varias cosas, antes de utilizar el marco de trabajo.	x		x		x		
8	El Marco de trabajo de seguridad de información	x		x		x		

UNIVERSIDAD CÉSAR VALLEJO

	cumple las exceptivas del área donde laboro.							
9	Las buenas prácticas establecidas fueron adaptables a las necesidades del área donde laboro.	x		x		x		
10	Las buenas prácticas del marco de trabajo permitieron una reducción de las incidencias de seguridad en el área donde laboro.	x		x		x		
11	La comunicación y retroalimentación entre las áreas mejoraron en base a sus necesidades.	x		x		x		
12	El marco de trabajo logró disminuir las incidencias con respecto a la manipulación de información sin autorización entre las áreas.	x		x		x		
13	Se logró una disminución de las incidencias por acceso a la información	x		x		x		
14	El marco de trabajo permite detectar en menor tiempo los casos por acceso a información sin autorización.	x		x		x		
15	Se logró disminuir los accesos no autorizados a la información	x		x		x		

UNIVERSIDAD CÉSAR VALLEJO

Observaciones (precisar si hay suficiencia): ...

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Chapoñan Camarena Rudy **DNI:** 09635313

Especialidad del validador: Magister en Gestión de Tecnologías de Información

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

de junio del 2021

Firma del Experto Informante.

Validador: Sabora Ríos, Némias

Cuestionario de Marco de trabajo de seguridad de la información

INVESTIGADORES: PAREDES CONDOR JULIO CESAR
VOTO BERNALES VILLALOBOS CARLOS ANDRES

EMPRESA:

PERSONA ENTREVISTADA:

DEPARTAMENTO EN QUE LABORA:

CARGO:

Esta encuesta debe ser respondida marcando con una X un casillero dentro de la escala, indicando el grado de acuerdo que tienes respecto al concepto que se expresa en cada ítem. La escala tiene cinco puntos de acuerdo al grado de aprobación o desaprobación de cada afirmación:

- 5 – Totalmente de acuerdo.
- 4 – De acuerdo.
- 3 – Ni de acuerdo, ni en desacuerdo.
- 2 – En desacuerdo.
- 1 – Totalmente en desacuerdo

VARIABLE: MARCO DE TRABAJO DE SEGURIDAD DE INFORMACIÓN								
DIMENSIONES	INDICADORES							
Satisfacción		Nivel de satisfacción del usuario	1	2	3	4	5
	1	El marco de trabajo de seguridad de información me resultó fácil de usar					x
	2	Necesitaría la ayuda de un experto para usar el marco de trabajo de seguridad de información					x
	3	Las buenas prácticas del marco de trabajo de seguridad de información están bien integradas					x
	4	Percibí que varias funciones del marco de trabajo de seguridad de información estaban ausentes o no integradas					x

	5	Pienso que la mayoría de personal de TI podrían aprender a emplear el marco de trabajo de seguridad de información					x
	6	El marco de trabajo de seguridad de información me resulta pesado y complicado al usar					x
	7	Necesité detenerme para aprender varias cosas antes de poder avanzar usando el marco de trabajo de seguridad de información					x
Eficacia		Nivel de desempeño dentro de la empresa					
	8	El Marco de trabajo de seguridad de información cumplió con lo descrito al inicio del proyecto					x
	9	Las buenas prácticas establecidas fueron adaptables a las necesidades del área					x
	10	Las buenas prácticas permitieron una mejora en la seguridad de información de la empresa					x
	11	Hubo una constante comunicación y retroalimentación en base a las necesidades del área					x
	12	Se logró disminuir las modificaciones sin autorización a la información de la empresa					x
		Nivel de incidencias dentro de la empresa					
Confiabilidad	13	Se logró una disminución de las incidencias por acceso a la información					x
	14	El marco de trabajo permite detectar con mayor facilidad los casos por acceso a información					x
	15	Se logró detectar la principal razón de los accesos no autorizados a la información					x

UNIVERSIDAD CÉSAR VALLEJO

INSTRUMENTO DE VALIDACIÓN DE EXPERTOS POR INDICADOR: Porcentaje total de Divulgación de información sin autorización

I. DATOS GENERALES

Apellidos y Nombres del Experto:	**Saboya Ríos, Nemias**
Título y/o Grado Académico:	Mgtr. Ing. De Sistemas

Doctor ( ) **Magister (x)** **Ingeniero (x)** **Licenciado ( )** **Otro ( )**.....

Universidad que labora:	
Fecha:	16/07/21

TESIS: Marco de trabajo de seguridad de información basado en la ISO/IEC 27001 para el control de acceso de los usuarios en empresas de teletrabajo

Autores: Paredes Condor, Julio Cesar; Voto Bernales Villalobos, Carlos Andres

Deficiente (0-20%) **Regular (21-50%)** **Bueno (51-70%)** **Muy Bueno (71-80%)** **Excelente (81-100%)**

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0%-100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	La ficha de observación es formulada con lenguaje apropiado.				X	
OBJETIVIDAD	Está expresado en conducta observable.				X	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				X	
ORGANIZACION	Existe una organización lógica.				X	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				X	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				X	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				X	
COHERENCIA	En los datos respecto al indicador.				X	
METODOLOGÍA	Responde al propósito de investigación.				X	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				X	
	TOTAL				80	

III. PROMEDIO DE VALIDACIÓN

IV. OPCIÓN DE APLICABILIDAD

( ) El instrumento puede ser aplicado, tal como está elaborado El instrumento debe ser mejorado antes de ser
( ) aplicado

FIRMA DEL EXPERTO

UNIVERSIDAD CÉSAR VALLEJO

INSTRUMENTO DE VALIDACION DE EXPERTOS POR INDICADOR: Porcentaje total de información modificada sin autorización

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Saboya Ríos, Nemias
Título y/o Grado Académico:	Mgtr. Ing. De Sistemas

Doctor ( ) Magister (X) Ingeniero (X) Licenciado ( ) Otro ( ).....

Universidad que labora:	
Fecha:	

TESIS: Marco de trabajo de seguridad de información basado en la ISO/IEC 27001 para el control de acceso de los usuarios en empresas de teletrabajo

Autores: Paredes Condor, Julio Cesar; Voto Bernales Villalobos, Carlos Andres

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				X	
OBJETIVIDAD	Esta expresado en conducta observable.				X	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				X	
ORGANIZACION	Existe una organización lógica.				X	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				X	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				X	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				X	
COHERENCIA	En los datos respecto al indicador.				X	
METODOLOGÍA	Responde al propósito de investigación.				X	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				X	
	TOTAL				80	

III. PROMEDIO DE VALIDACION

IV. OPCIÓN DE APLICABILIDAD

( ) El instrumento puede ser aplicado, tal como está elaborado El instrumento debe ser mejorado antes de ser _____

( ) aplicado

FIRMA DEL EXPERTO

UNIVERSIDAD CÉSAR VALLEJO

INSTRUMENTO DE VALIDACION DE EXPERTOS POR INDICADOR: Porcentaje total de accesibilidad de información

I. DATOS GENERALES

Apellidos y Nombres del Experto:	Saboya Ríos, Nemias
Título y/o Grado Académico:	Mgtr. Ing. De Sistemas

Doctor () **Magister (X)** **Ingeniero (X)** **Licenciado ( )** **Otro ( )**.....

Universidad que labora:	
Fecha:	

TESIS: Marco de trabajo de seguridad de información basado en la ISO/IEC 27001 para el control de acceso de los usuarios en empresas de teletrabajo

Autores: Paredes Condor, Julio Cesar; Voto Bernales Villalobos, Carlos Andres

Deficiente (0-20%) **Regular (21-50%)** **Bueno (51-70%)** **Muy Bueno (71-80%)** **Excelente (81-100%)**

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucradas mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

		VALORACIÓN				
INDICADOR	**CRITERIO**	**0-20%**	**21-50%**	**51-70%**	**71-80%**	**81-100%**
CLARIDAD	Es formulado con lenguaje apropiado.				X	
OBJETIVIDAD	Esta expresado en conducta observable.				X	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				X	
ORGANIZACION	Existe una organización lógica.				X	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				X	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				X	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				X	
COHERENCIA	En los datos respecto al indicador.				X	
METODOLOGÍA	Responde al propósito de investigación.				X	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				X	
	TOTAL				80	

III. PROMEDIO DE VALIDACIÓN

IV. OPCIÓN DE APLICABILIDAD

( ) El instrumento puede ser aplicado, tal como está elaborado El instrumento debe ser mejorado antes de ser
( ) aplicado

FIRMA DEL EXPERTO

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR EXPERTOS

Nº	Competencias digitales instrumentales	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Ítems/reactivos/enunciado	SI	NO	SI	NO	SI	NO	
1	El marco de trabajo de seguridad de información me resultó fácil de usar	x		x		x		
2	Necesitaría la ayuda de un experto para usar el marco de trabajo de seguridad de información	x		x		x		
3	Las buenas prácticas del marco de trabajo de seguridad de información están bien integradas	x		x		x		
4	Percibí que varias funciones del marco de trabajo de seguridad de información estaban ausentes o no integradas	x		x		x		
5	Pienso que la mayoría de personal de TI podrían aprender a emplear el marco de trabajo de seguridad de información	x		x		x		
6	El marco de trabajo de seguridad de información me resulta pesado y complicado al usar	x		x		x		
7	Necesité detenerme para aprender varias cosas antes de poder avanzar usando el	x		x		x		

UNIVERSIDAD CÉSAR VALLEJO

	marco de trabajo de seguridad de información							
8	El Marco de trabajo de seguridad de información cumplió con lo descrito al inicio del proyecto	x		x		x		
9	Las buenas prácticas establecidas fueron adaptables a las necesidades del área	x		x		x		
10	Las buenas prácticas permitieron una mejora en la seguridad de información de la empresa	x		x		x		
11	Hubo una constante comunicación y retroalimentación en base a las necesidades del área	x		x		x		
12	Se logró disminuir las modificaciones sin autorización a la información de la empresa	x		x		x		
13	Se logró una disminución de las incidencias por acceso a la información	x		x		x		
14	El marco de trabajo permite detectar con mayor facilidad los casos por acceso a información	x		x		x		
15	Se logró detectar la principal razón de los accesos no autorizados a la información	x		x		x		

UNIVERSIDAD CÉSAR VALLEJO

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Saboya Ríos, Nemias

Especialidad del validador: Mgtr. Ing. De Sistemas

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

16 de julio del 2021

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante.

UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO POR EXPERTOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	INDICADOR: 1. Promedio total de Divulgación de información sin autorización	Si	No	Si	No	Si	No	
1	$PTDIF = \frac{TDISA}{TID} * 100$	X		X		X		
	INDICADOR: 2. Promedio total de Información modificada sin autorización	Si	No	Si	No	Si	No	
2	$PTIM = \frac{TIMSA}{TIM} * 100$	X						
	INDICADOR: 3. Promedio total de accesibilidad a la información	Si	No	Si	No	Si	No	
3	$PTACI = \frac{TSAII}{TSAI} * 100$	X		X		X		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Saboya Ríos, Nemias

Especialidad del validador: Mgtr. Ing. De Sistemas

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

16 de julio del 2021

Firma del Experto Informante.

ANEXO 9: Recibo Digital Turnitin

turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	JULIO CESAR PAREDES CONDOR
Título del ejercicio:	Turnitin
Título de la entrega:	Turnitin_Marco_de_Trabajodocx.docx
Nombre del archivo:	Turnitin_Marco_de_Trabajodocx.docx
Tamaño del archivo:	941.11K
Total páginas:	53
Total de palabras:	10,481
Total de caracteres:	56,149
Fecha de entrega:	18-dic.-2021 06:30p. m. (UTC-0500)
Identificador de la entre...	1733504648

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Título de trabajo de investigación

Marco de trabajo de seguridad de información basado en la ISO/IEC 27001:2013 para el control de acceso de los usuarios en empresas de teletrabajo

TRABAJO DE INVESTIGACIÓN PARA OBTENER EL GRADO ACADÉMICO DE BACHILLER EN INGENIERÍA DE SISTEMAS

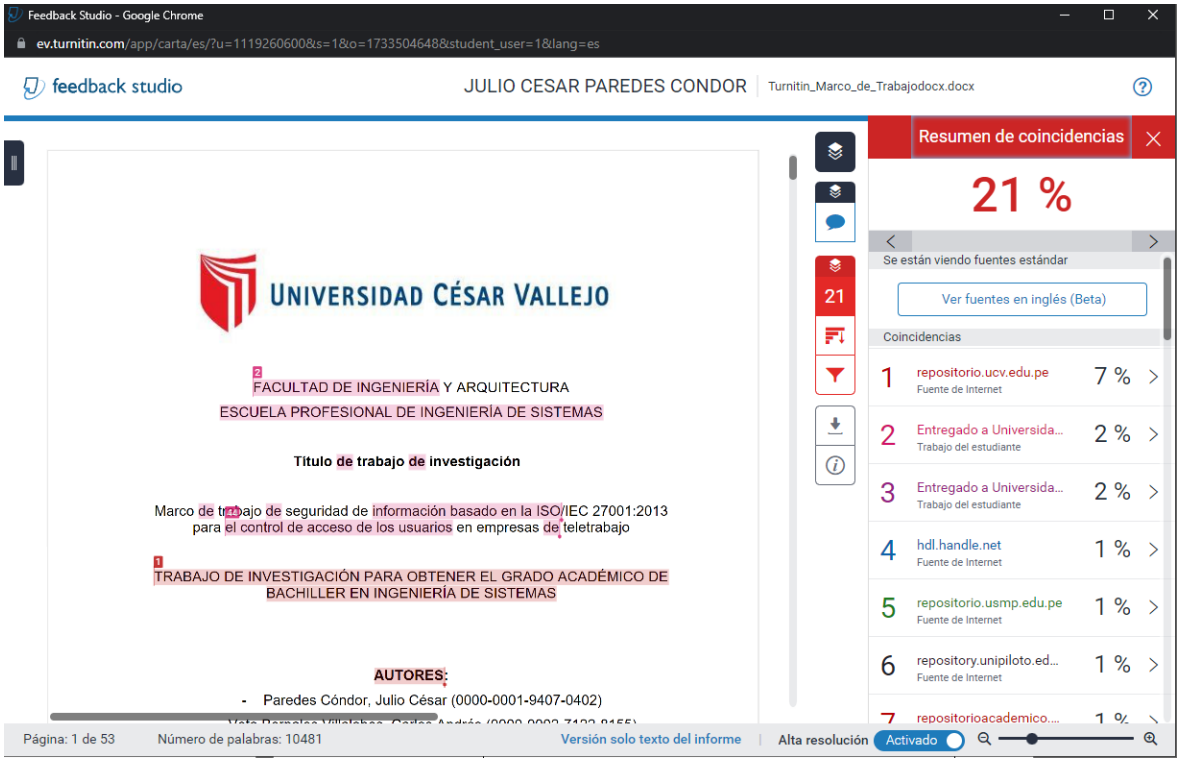
AUTOR(ES):
- Paredes Cóndor, Julio César (0000-0001-9407-6482)
- Yoto Bernales Wilsabes, Carlos Andrés (0000-0002-7122-8155)

ASESOR:
Mg. Saboya Rios Nerissa (000-0002-7180-2197)

LÍNEA DE INVESTIGACIÓN
Auditoría y seguridad de la información

Lima – PERÚ
2021

ANEXO 10: Porcentaje en Turnitin



Anexo 11: Marco de Trabajo

Objetivo

a. Seleccionar controles de la ISO/IEC 27001:2013 a aplicarse en base a la necesidad de la organización.

b. Establecer formatos de confidencialidad. Checklist, aprobación y comunicación de los efectos de controles, políticas, procedimientos, niveles de riesgos, roles y responsabilidades al recurso humano del nivel operativo de una empresa de teletrabajo.

Alcance

La propuesta será limitada a la protección de los activos lógicos de información que están dentro de cualquier empresa de teletrabajo. Esta investigación se adapta a la necesidad de la empresa, en la cual se identificaron vulnerabilidades y amenazas, que se controlarán con el marco de trabajo, basándose en la norma internacional ISO/IEC 27001:2013

Usuarios

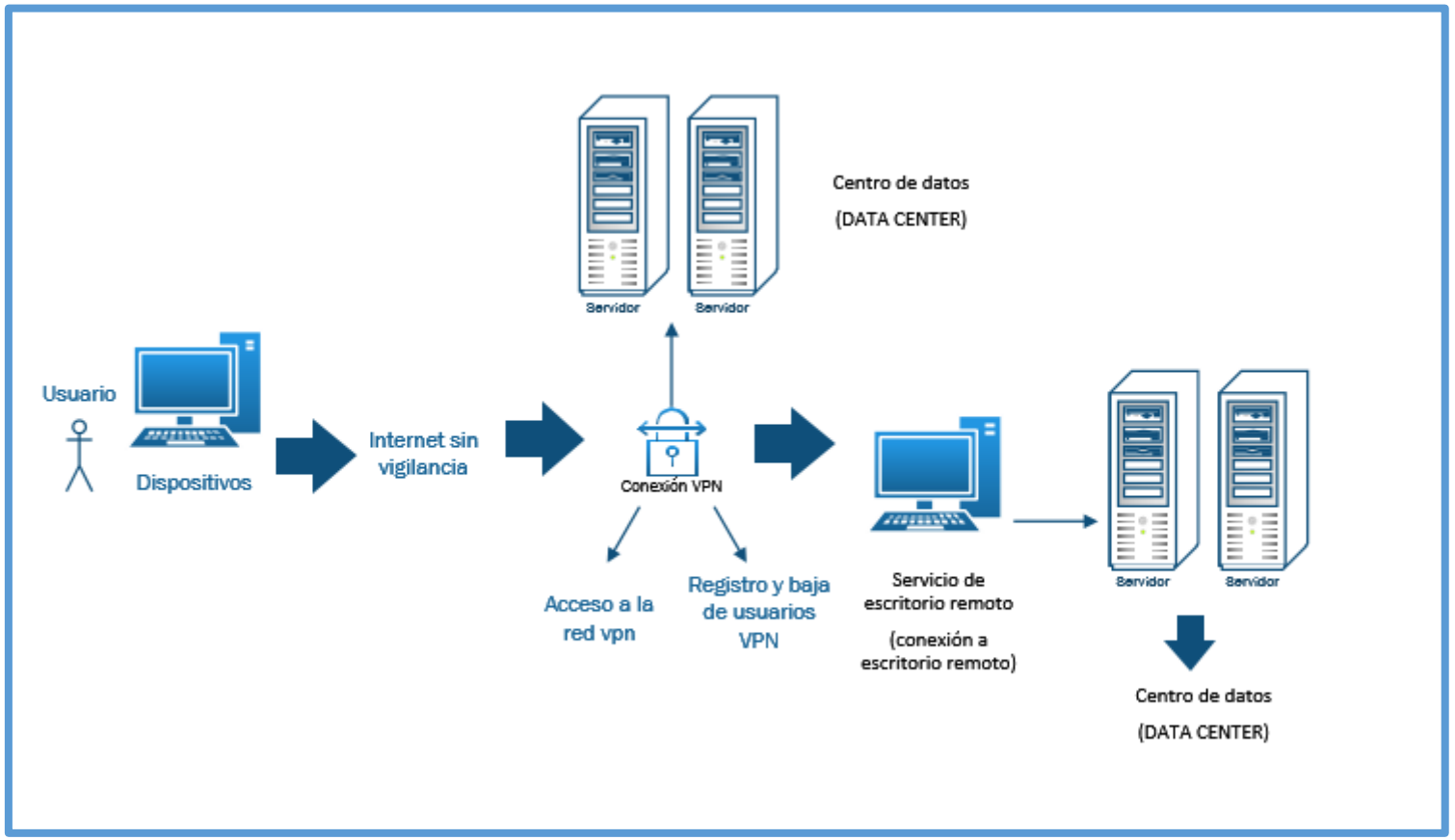
MIEMBROS DE ALTA DIRECCION
ROL
Gerente de agencia
Recursos humanos
Jefe de soporte de TI
Usuarios y trabajadores de la empresa

EQUIPO DEL PROYECTO SGSI
Usuarios de la empresa
Oficial de seguridad de la información (jefe de soporte de TI)

Documentos de referencia

2. Libro Blanco del teletrabajo en Colombia
3. ISO/IEC 27001: 2013
4. NTP/ISO 27001:2014
5. Ley de protección de datos personales

Anexo 12: Arquitectura de la empresa de Teletrabajo antes del marco de trabajo



En al anexo 12 se muestra la estructura que tenía la empresa antes de aplicar el Marco de trabajo.

Debido a la urgencia que tuvieron varias empresas por la situación mundial de salud (Covid 19), se vieron obligados a migrar a la modalidad de trabajo para poder mantener la empresa a flote, por lo cual no todos estaban preparados para realizar este cambio, tanto a nivel de plataforma y estructura de seguridad.

El proceso que estuvo realizando para la conexión de manera remota era el siguiente:

Conexión a VPN y escritorio remoto:

El área de TI, mediante un servidor, instaló y configuró una VPN, que permitía el acceso de manera remota a escritorios remotos configurados, a personal de la empresa.

Para ello primero llegaba el requerimiento mediante correo en el ServiceDesk, en dicho correo se indicaba los datos del personal, tales como nombres y apellidos completo, cargo, área en la que iba a laborar.

Con dicha información, el personal del área de TI, le creaba un usuario personalizado y le habilitaba el acceso a una Pc remota, previamente configurada para sus funciones.

El usuario, mediante un dispositivo (PC, Tablet, celular) se conecta a la red privada de la empresa mediante la VPN con el usuario que el área de TI le envió, una vez conectado a la VPN, el personal ya podría hacer uso del escritorio remoto y acceder a la PC de la empresa para comenzar sus funciones.

Como se puede apreciar en el flujo que venía utilizando el área de TI, no existía ningún filtro de seguridad que bloqueara o limitara los accesos del personal una vez se conectaba a la red VPN.

Política de seguridad: documento que describe la forma en como la dirección gestionará la seguridad de la información.

Guía para control de documentos y registros: describir la manera de redactar los documentos, títulos, letras, encabezado y otros detalles que lo conformen.

Identificación de amenazas y vulnerabilidades: se evalúa el nivel de riesgo y se asigna un responsable.

Plan de tratamiento del riesgo: documento que detalla controles de seguridad para cada tipo de riesgo como evidencia de su tratamiento.

Alcance del sistema de seguridad de la información

Naturaleza de la organización

Es una empresa proveedora de soluciones rápidas y eficientes a emprendedores, empresarios y empresas, a través de la ejecución de procesos de soporte y aplicación de tecnología.

Misión

Implementamos soluciones prácticas con resultados tangibles que resuelven los problemas de enfoque, crecimiento, eficiencia y transformación de las empresas, a partir de un equipo humano comprometido y en constante preparación.

Visión

Ser una organización referente en servicio, sabiendo que servimos a clientes, colaboradores y a la sociedad.

Comprensión de las necesidades y expectativas de las partes involucradas

Las partes importantes al SGSI son:

Personal: colaboradores del Call Center Terceriza, a los cuales se le asignan responsabilidades de activos y deben cumplir estricta seguridad de los mismos en la empresa.

Clientes: personas que requieren acceso a información de los empleados.

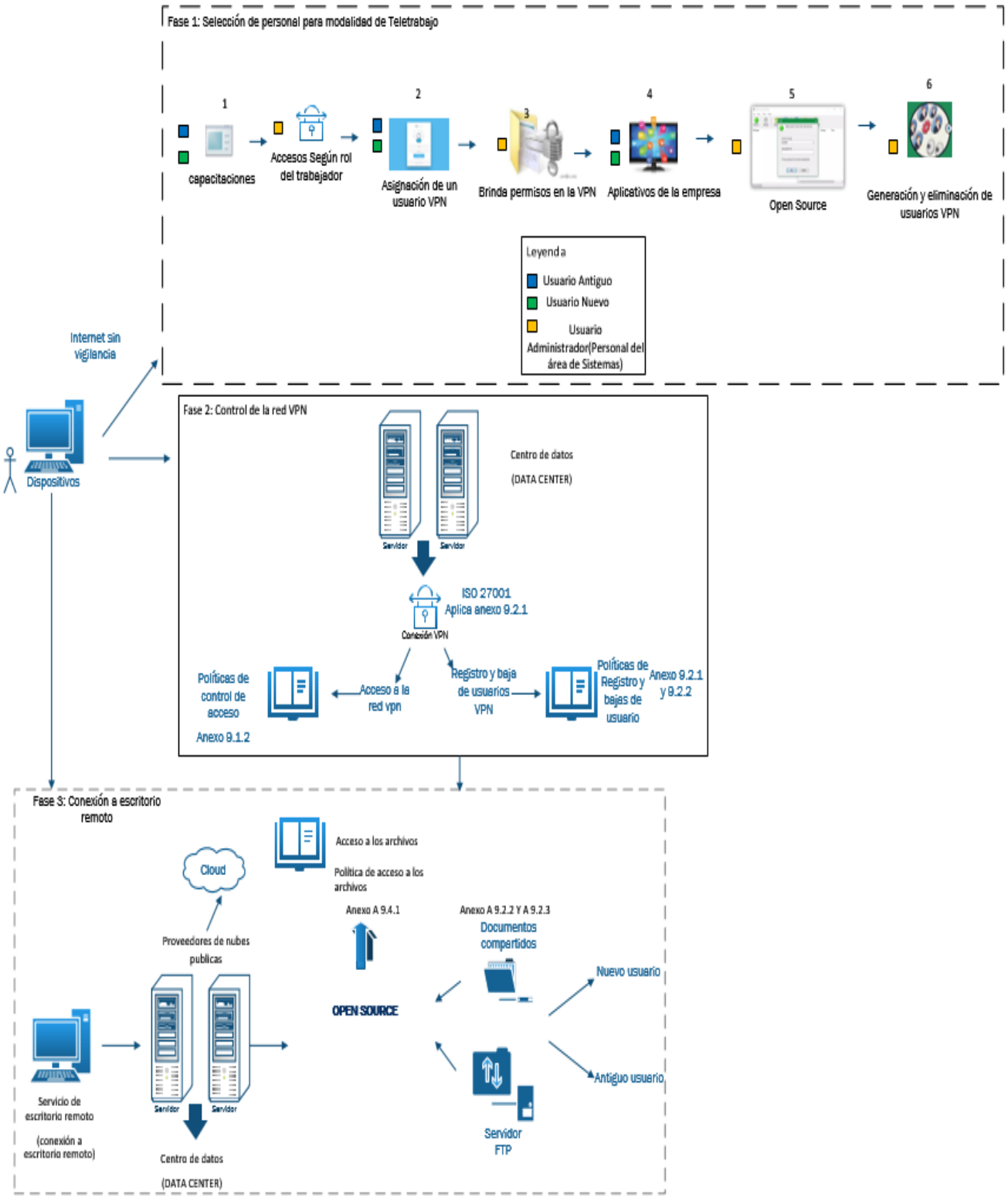
Competidores: con la seguridad de la información se adquiere ventaja competitiva y de imagen institucional.

Inventario de activos lógicos

En esta sección como se aprecia en la Tabla 10, se debe tener un registro de todos los activos lógicos que la empresa utilice en la gestión diaria de su personal.

N°	**Activos de información**
1	Copias dni
2	Copias documento de propiedad
3	Copias separación matrimonial
4	Copias licencia municipal
5	Declaración jurada de servicios
6	Copias carta no adeudo
7	Copias cronograma de créditos
8	Copias voucher de cancelación
9	Contratos de trabajo
10	Boletas de pago
11	Libro de actas
12	Información de empresas (ruc, pdt, vigencia, constitución)
13	Certificados médicos
14	Convenios
15	Cartas poder
16	Numero de cuentas
17	Data de clientes inactivos y vigentes

Anexo 13: Marco de trabajo propuesto



Fase 1: Selección de personal para modalidad de Teletrabajo

Para esta primera fase, la empresa deberá seleccionar al personal que tendrá la posibilidad de trabajar de manera remota.

Para ello, dicho personal deberá contar con ciertos requerimientos básicos para que pueda optar por esta modalidad de trabajo desde casa.

Dichos requerimientos pueden cambiar dependiendo de la empresa y los aplicativos que serán necesarios para el cumplimiento de sus funciones.

Nuevo Ingreso: Los nuevos ingresos que serán contratados directamente para trabajar de manera remota, deberán cumplir primero con determinados requerimientos mínimos a nivel de software y hardware en caso de utilizar una PC propia para realizar sus funciones, adicional a ello de contar con un buen ancho de banda de internet, de ser posible conectado vía cable de red.

Dichos requerimientos se ven en la tabla 11:

Requerimientos mínimos para modalidad de teletrabajo

Hardware	**Software**
- PC con procesador INTEL i3 de 4ta generación o su equivalente en AMD - 6 GB de RAM como mínimo	- Herramientas Office con funciones completas, ya sea de Microsoft o versiones Open Source, tales como Libre Office, WPS Office, etc. - Aplicativo VPN de paga u Open Source como Open VPN(de no tenerlo instalado, el área de TI se encargará de dicho procedimiento)
- **Ancho de Banda de internet:**	10 MBps como mínimo, validados mediante un test de velocidad.

En el caso particular de la empresa donde se desarrolló el proyecto, ellos solicitan los siguientes requerimientos mínimos:

1 Descripción de la Situación

Con la finalidad de mantener una gestión optima con la aplicación IPCC, es necesario cumplir los requisitos planteados por Soporte Claro y Soporte 3eriza

2 Requisito VPN para campañas que utilizan IPCC

En este tipo de conexión la aplicación IPCC y aplicaciones claro utilizan el recurso de la PC del usuario final (Hardware, Software, Internet).

Nombre	Requerimiento de configuración
CPU	• Intel Core i5 Gen 7 @ 2.9 GHz o superior (Recomendado por claro) **Equivalentes:** Ryzen 5-2500x /+ Ryzen 7-2700 /+ Ryzen 9 Todas. A6-7480 /+ A8-5600 /+ A10-5800 /+ • Intel Core i5 Gen 4 @ (1.8, 2.0, 2.3) GHz o superior (Soporte 3eriza) **Equivalentes:** Ryzen 3 2200G /+ Ryzen 5 2400G /+ Ryzen 7 1700x/+ A6-5400 /+ A8-5600 /+ A10-5800K /+
Memoria (RAM)	8 GB o superior (*)
Sistema Operativo	Windows 10 Pro 64bits Versiones **(21h1) Importante para la instalación de IPCC**
Navegador	Internet Explorer 11 32/64 bits
Resolución de pantalla	Ver sección 3.2.7 del documento. **Importante para la grabación de Pantallas** a. 1280 * 720 b. 1278 * 768
Cable de Red	Categoría 6 Certificado (Min) **(Recomendado)**
Velocidad de Internet	20 Mbps o mayor (***) 15 Mbps o mayor (***) (Soporte 3eriza)

3 Requisito VPN para campañas que no utilizan IPCC

En este tipo de conexión las aplicaciones utilizan el recurso de la PC del usuario final (Hardware, Software, Internet). Son campañas que no utilizan IPCC para su gestión.

Nombre	Requerimiento de configuración
CPU	• Intel Core i5 Gen 4 @ (1.8, 2.0, 2.3) GHz o superior **Equivalentes:** Ryzen 3 2200G /+ Ryzen 5 2400G /+ Ryzen 7 1700x/+ A6-5400 /+ A8-5600 /+ A10-5800K /+
Memoria (RAM)	6 GB o superior (*)
Sistema Operativo	Windows 10 Pro 64bits Versiones **(21h1) Ideal** Solo campañas: - Tienda Virtual (Ram: 6GB) - Oncosalud (Ram: 4GB) - Linea Positiva: (Ram: 4GB) - Concar: (Ram: 6 GB) Windows 10 Home 64bits / Windows 10 Pro 64bits
Navegador	Internet Explorer 11 32/64 bits
Resolución de pantalla	No es necesario
Cable de Red	Categoría 6 Certificado (Recomendado)
Velocidad de Internet	15 Mbps o mayor (***)

De contar con estos requerimientos el personal postulante como nuevo ingreso para trabajar de manera remota, deberá pasar por una capacitación donde se les explicará las funciones que deberán cumplir, los aplicativos a utilizar de su gestión diaria, los aplicativos para conectarse a la red de la empresa de manera remota y como conectarse a ellos.

Antiguo usuario: En el caso de tratarse de un personal que ya ha estado trabajando dentro de la empresa, solo deberá contar con los requerimientos mínimos necesarios, solicitarlo mediante su jefe inmediato y tener una breve capacitación del uso de los aplicativos desde casa.

Administrador: Cuando nos referimos al administrador, estamos hablando del personal perteneciente al área de Sistemas de la empresa, el cual se encargará de realizar las instalaciones necesarias, altas de usuarios nuevos, habilitación de permisos, entre demás funciones.

Fase 2: Conexión a la red VPN

Dicha Red VPN, será administrada únicamente por el personal del área de TI, designando a determinado personal denominado Administrador de red, que deberá realizar las configuraciones necesarias para mantener el servidor VPN, ampliar su capacidad de ser requerido y mitigar cualquier tipo de caída de servidor y desconexión de usuarios.

Para el levantamiento de dicha VPN, deberá tenerse en consideración las recomendaciones brindadas en la ISO/IEC 27001:2013 en el Anexo A 9.1.2 donde se detallan las políticas de control de acceso.

Una vez seleccionado el personal que procederá a realizar trabajo desde su domicilio, se le deberá habilitar el usuario VPN para que pueda conectarse a la red de la empresa y así acceder a los aplicativos y archivos; que serán necesarios para su gestión. Dichos usuarios podrán ser creados por personal del área de TI de la empresa.

Registro y baja de usuarios

En este control dentro de la tabla 12 se establece el siguiente proceso donde el personal del área de TI (área de sistemas) deberá realizar el registro de los usuarios nuevos que se requieran en la empresa. Para este proceso se recomienda que previo a la creación del usuario, debe existir una solicitud mediante correo por parte del jefe a cargo del área donde se solicite la creación del usuario, indicando los datos personales del nuevo usuario, cargo y permisos que necesitará para su gestión diaria.

Registro y baja de usuarios VPN

N°	Actividad	Descripción	Encargado
1	Registro, modificacióno baja de usuarios	El encargado del área solicita mediante correo institucional al Servicedesk este requerimiento	
2	Registra solicitud	El oficial deberá registrarla como evidencia de su decisión en la que autoriza o	

		rechaza	Oficial de seguridad de la información
3	Toma de decisión	Si aprueba la solicitud, este debe identificar el tipo de usuario con su permiso correspondiente	
4	Configuración correspondiente	De hacer el registro de un nuevo usuario, se asigna una clave y se conceden los permisos de acuerdo a sus funciones. Para modificar se alteran los permisos y en una baja de usuarios se deben eliminar esos permisos	
5	Comunicación de resultados	Una vez terminado el proceso se debe informar al usuario vía correo institucional	

Fase 3: Conexión a escritorio remoto y red interna de la empresa

Una vez el usuario haya completado los procesos previos y obtenido su usuario VPN correspondiente ya estará habilitado para poder conectarse a la red de la empresa y comenzar con sus labores.

Una vez ya conectado a la VPN de la empresa, el personal podrá conectarse a los aplicativos necesarios para su gestión, ya sea directamente en su PC o utilizando un escritorio remoto previamente configurado por el área de TI para dicho usuario.

Para la creación de una correcta y segura contraseña para el escritorio remoto, se deben seguir los parámetros de la Tabla 13, el personal del área de TI previamente habrá configurado una contraseña simple que se le brindará al jefe a cargo que generó la solicitud mediante correo.

El cual le brindará dicha información al personal nuevo. El personal en su primera conexión recibirá un mensaje donde se le indicará que deberá cambiar su contraseña, la cual debe contar con ciertos parámetros de seguridad.

Políticas de seguridad para contraseñas

Políticas de seguridad para contraseñas
a) Toda contraseña correspondiente a cuentas de usuario final es personal, intransferible y no debe ser compartida con nadie más. b) Las contraseñas establecidas por cada uno de los funcionarios para los diferentes sistemas informáticos serán administrados y gestionados bajo su única responsabilidad. c) El área de TI configurará los sistemas informáticos para que el límite de intentos fallidos al ingresar una contraseña, sea de 5 intentos, luego de lo cual se bloqueará la cuenta de usuario. d) El área de TI configurará el sistema operativo, de forma que éste se bloquee indefinidamente hasta que, por pedido del usuario, solicite el desbloqueo. e) Para generar contraseñas seguras para las cuentas de usuario final, éstas deberán cumplir los siguientes parámetros: - Tener una longitud mínima de 8 caracteres. - Contener Mayúsculas y Minúsculas. - Contener al menos un número y carácter especial (ej: “#*?) f) Los sistemas se configurarán de manera que los usuarios finales, al cambiar de contraseña, no puedan utilizar ninguna de las 3 contraseñas anteriores ingresadas. g) Se prohíbe solicitar y/o entregar contraseñas vía telefónica o por escrito en medios como correo electrónico o papeles. h) Las contraseñas correspondientes a cuentas especiales de administración de infraestructura serán de uso y responsabilidad del área. i) En el caso de que se requiera obtener información del computador de escritorio o portátil, de un funcionario que se encuentre ausente de forma temporal o definitiva, únicamente podrá ser solicitado por el jefe inmediato del área, a través del formulario de obtención de información y dicha persona tomará toda la responsabilidad acerca de dicho dispositivo. j) El área de Soporte a Usuarios, es responsable de obtener la información solicitada en el literal anterior mediante la cuenta de Administrador Local del equipo. k) Todos los equipos de la institución deben tener un usuario de administrador local cuya contraseña será gestionada únicamente por personal del área de TI.

l) Siempre que un funcionario sospeche que la confidencialidad de su contraseña este comprometida, deberá cambiarla inmediatamente o deberá forzar el cambio de clave.

Fase 4: Acceso a la información de la empresa

El usuario accederá a la información mediante el software Soft Perfect File Access Monitor con el usuario que se le habrá creado previamente, donde dependiendo del cargo del usuario, tendrá determinados privilegios, tales como la posibilidad de editar, eliminar o crear.

Para la configuración de accesos a los archivos se tomará como referencia lo indicado en el anexo A 9.4.1 de la ISO/IEC 27001:2013 para la creación de las políticas de seguridad de acceso a la información, los cuales se pueden apreciar en la tabla 14:

Políticas de seguridad de acceso a la información

Políticas de seguridad de acceso a la información – Agregar anexo
a) Se utilizan menús para controlar el acceso a las distintas funciones b) Se oculta las funciones de administración a los usuarios habituales c) Se determinan que datos son accesibles basado en que datos pueden estar disponibles para cada ID de usuario(cargo). d) Se restringe de forma selectiva derechos de lectura / escritura / eliminación / ejecución etc.

Se explican las políticas que deberán tener los activos lógicos que tenga la empresa, donde se especifica que puede hacerse con la información brindada por la empresa y que no debe realizarse con ella.

Política de uso de los activos lógicos

Política de uso de los activos lógicos
a) Los sistemas informáticos solo podrá ser utilizados para los roles que se le serán asignados por la organización, más no para uso personal. b) Se prohíbe la manipulación de las configuraciones realizadas por el personal de TI c) De presentarse alguna incidencia o falla, comunicarse vía correo institucional, describiendo la incidencia y número de contacto, no realizar configuraciones por su cuenta.

Política de uso de los activos de información
a) Cada analista es responsable de la información asignada. b) No se divulgará ni se prestará a terceros, tampoco es de uso personalen actividades de jornada no laboral. c) Almacenar correctamente en los estantes asignados d) Se prohíbe circular información difamatoria ya sea de persona natural o jurídica. e) La copia de algún documento se debe solicitar por correo al analista responsable f) Realizar el arqueo de expedientes los primeros días de cada mes sin excepción. g) En caso de pérdida, comunicar de manera inmediata con gerencia.

Política de control de accesos
a) Definir roles de usuario basado en el área de trabajo donde estarán. b) Definir los permisos necesarios para que cada usuario pueda realizar sus funciones con normalidad c) La clave de seguridad deberá ser renovada cada 15 días y es de uso exclusivo del personal. d) Las claves estarán compuestas de al menos 8 dígitos, los cuales deberá incluir letras, una mayúscula, carácter y número como mínimo e) El personal de TI, es el encargado de configurar las claves de seguridad y su asignación. En caso de que el personal se olvide su contraseña, deberá solicitar un reseteo vía correo institucional. f) Una vez finalizada su gestión diaria el personal deberá bloquear su máquina

Política de control de servicios móviles e informáticos
a) Solo se permite usar la aplicación de WhatsApp y de la organización, cualquier otra aplicación de comunicación o entretenimiento estará denegada. b) Denegar el acceso a redes sociales y juegos por los navegadores c) El wifi y bluetooth estará deshabilitado d) Esta denegado la instalación de programas por los usuarios e) Acceso restringido a descargas de programas f) Todos los programas a utilizar por los usuarios deben estar licenciados

Protección de información de registros
a) Las unidades de almacenamiento para estos registros deben estar correctamente protegidas contra adulteración y el acceso no autorizado b) Los documentos deben estar agrupados por tipo de información c) Cualquier evento como falla y excepciones será derivado al oficial de seguridad de la información. d) Las carpetas con información importante deben estar almacenadas bajo el nombre de analista responsable. e) Los eventos realizados en esta sección serán registrados por el oficial de seguridad de la información.

Acuerdos de transferencia de información
a) el gerente de agencia solo está permitido para la transferencia de información. b) No se revela información de clientes y el estado de su crédito a ningún agente externo a la organización c) Esta denegado el uso de dispositivos de almacenamiento. d) No realizar copias de data de clientes vigentes e inactivos sin autorización e) El uso inapropiado de las cuentas es sancionado de acuerdo a la ley servir N° 30057

Políticas de seguridad de la información basado en la ISO 27001:2013

El priorizar en principio el acceso mínimo con restricciones es el enfoque general para la protección, en lugar de dar acceso libre con derechos de súper usuario sin un resguardo cuidadosamente considerado. Como tales, los usuarios sólo deberían tener acceso a la red y a los servicios de red que necesitan usar o conocer para desarrollar únicamente su trabajo en el área correspondiente, es por ellos que se implementan las siguientes políticas:

ANEXO 9.1.2 acceso a redes y servicios de red
a) El área de TI debe implementar el uso de mecanismos que aseguren la identificación del equipo tanto a nivel lógico y físico. **b)** El administrador de red debe asegurar establecer reglas de identificación de equipos en las redes y debe revisar periódicamente la vigencia de estas. **c)** El área de TI deberá siempre tener actualizado el registro detallado de todas las redes que administra **d)** El área de TI debe definir los niveles de riesgo existente en la contratación del personal externo para el soporte y administración de las redes de la entidad **e)** El área de TI deberá mantener el registro de las fallas reportadas durante el proceso de respaldo y recuperación de la información al igual como de las soluciones que se realizaron **f)** Sólo los usuarios previamente autorizados podrán utilizar los beneficios del Sistema VPN, los que, además, serán los responsables del correcto uso del servicio de acceso remoto **g)** El uso del sistema VPN debe ser controlado utilizando una contraseña de autenticación fuerte, manteniéndola siempre en secreto

h) Las puertas de enlace VPN serán configuradas y administradas por el área de TI de la empresa

i) El concentrador VPN define tiempos de conexión según el perfil del usuario, los cuales son distintos para gerencia, miembros del área de TI y empleados

j) Los usuarios de equipos de cómputo que no son de la empresa, deberán cumplir todas las disposiciones establecidas en las políticas de la empresa y además firmar un acuerdo de confidencialidad de la información.

k) Según el tipo de usuario se definen el máximo de sesiones simultáneas, que podrá generar cada usuario

l) Cuando esté conectado activamente a la red de la empresa, el sistema VPN permitirá el tráfico de acuerdo con el perfil del usuario hacia y desde el equipo de cómputo a través del túnel VPN, el resto del tráfico pasará por la conexión respectiva.

Es preciso implementar un proceso formal de registro y cancelación de registro de usuarios. Un buen proceso para la administración de ID de usuario incluye la posibilidad de asociar ID individuales a personas reales y limitar las ID de acceso compartido, que deben probarse y registrarse, para ello se implementaran las siguientes políticas:

Registro de usuarios y anulación de registros

Anexo 9.2.1 registro de usuarios y anulación de registros
a) El administrador de la red, es el único autorizado en crear usuarios a los equipos de cómputos pertenecientes al inventario de activos de la empresa. **b)** Cuando un usuario recibe una cuenta, debe firmar un documento donde declara conocer las políticas, marcos de referencia y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta **c)** Se deberá llevar un registro de Ids o cuentas de usuario donde se vincula o identifica al usuario **d)** Los ids redundantes nunca pueden ser asignados a otros usuarios **e)** Los ids deben desactivarse automáticamente o de forma inmediata cuando el usuario abandona la organización **f)** Eliminación periódica de usuarios redundantes **g)** Al cancelar un usuario se revocará el id del usuario y los permisos de este **h)** Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.

En la actualidad el teletrabajo es una actividad tremendamente difundida en todo tipo de organizaciones por lo que la seguridad de la Información es un aspecto clave para garantizar la protección de esta actividad. Para aquellas organizaciones que deseen aplicarla, esta norma nos indica una serie de controles a tener en cuenta en el análisis de su aplicación que son las siguientes:

Anexo 6.2.2 teletrabajo

a) Aplicaciones y recursos a los que tiene acceso cada usuario

b) Accesos seguros

c) Configuración de los dispositivos de teletrabajo

d) Cifrado de los soportes de información

e) Definición de la política de almacenamiento en los equipos de trabajo y en la red corporativa

f) Planificación de las copias de seguridad de todos los soportes

g) Uso de conexiones seguras a través de una red privada virtual o VPN

h) Aplicaciones de escritorio remoto siempre a través de una VPN

i) Virtualización de entornos de trabajo

j) Priorizar el uso de dispositivos corporativos

k) Conexión a Internet estable a una velocidad óptima.

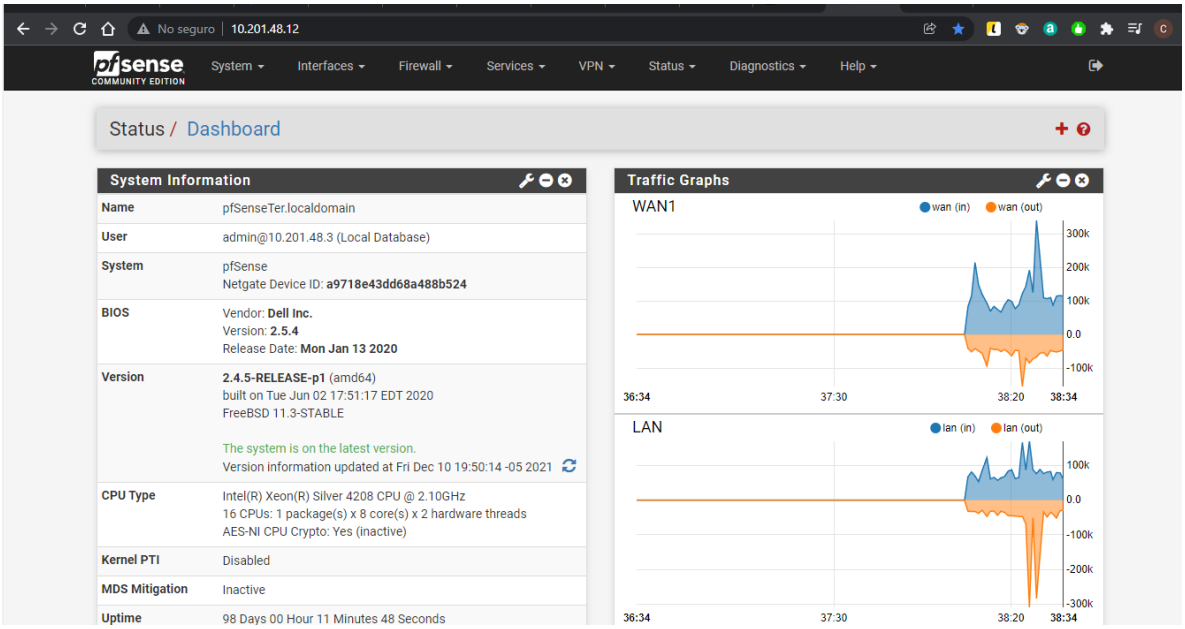
l) Uso de dispositivos personales bajo una política BYOD

m) Concientizar a los empleados antes de empezar a trabajar de manera remota.

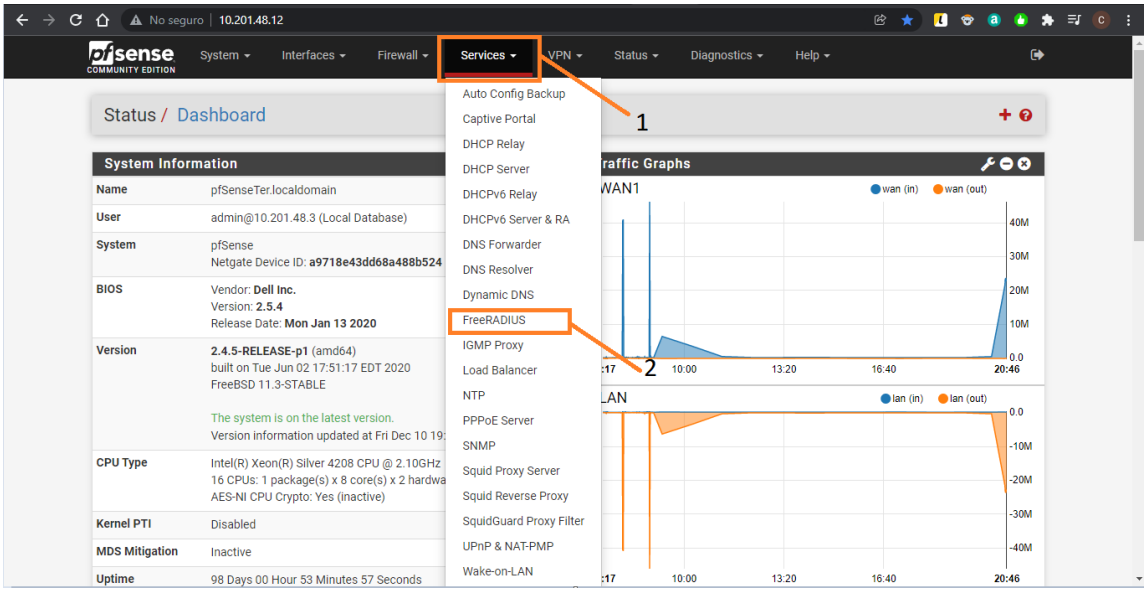
n) Aplicaciones de teleconferencia y colaborativas

ANEXO 13: Creación de usuarios en PFSense para la VPN:

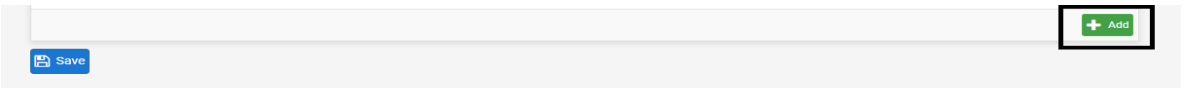
1.- Como primer paso, el personal del área de TI (Soporte de TI) deberá acceder a la ruta del pfsense, ya sea estando de manera presencial o de manera remota, al link http://10.201.48.12/



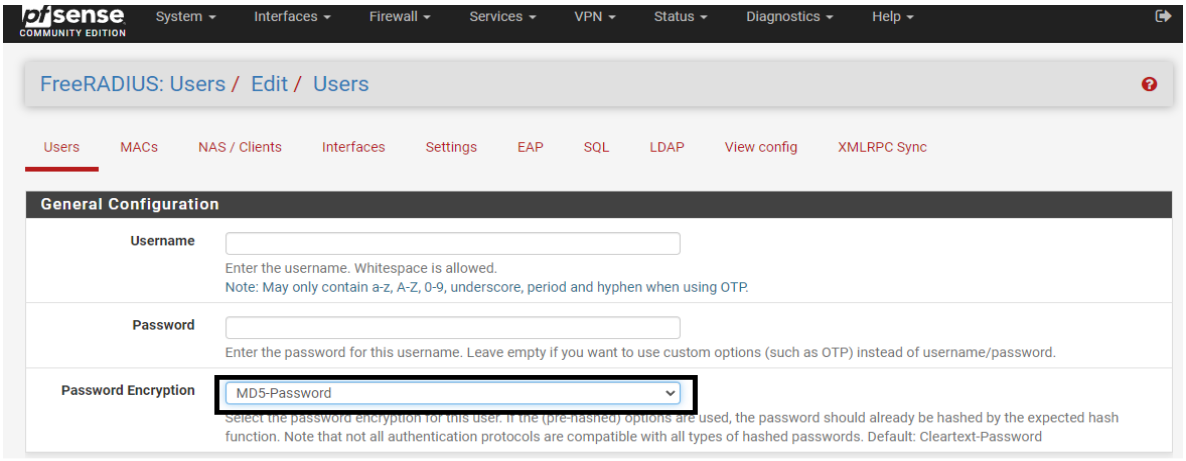
2.- Luego de acceder al link de PfSense, damos clic en la pestaña SERVICES y entre las opciones que sean listadas, escogemos la opción FreeRADIUS



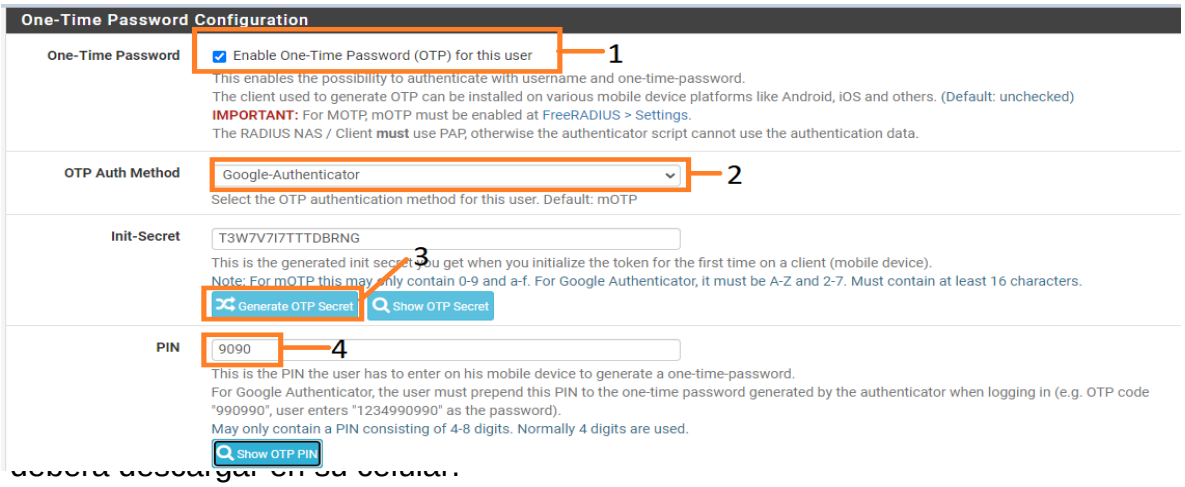
3.- Dentro de la opción FreeRADIUS es donde se realizará la creación del nuevo usuario, deslizándose hasta la parte final de la pantalla y dándole clic en ADD



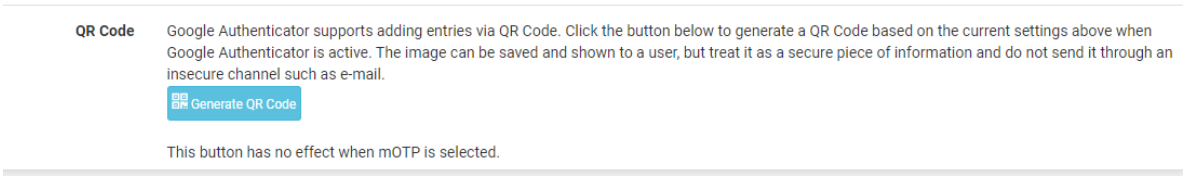
4.- En la primera parte, procederemos a crear el nombre de usuario y activar la encriptación de la contraseña (Password encryption) en MD5-Password



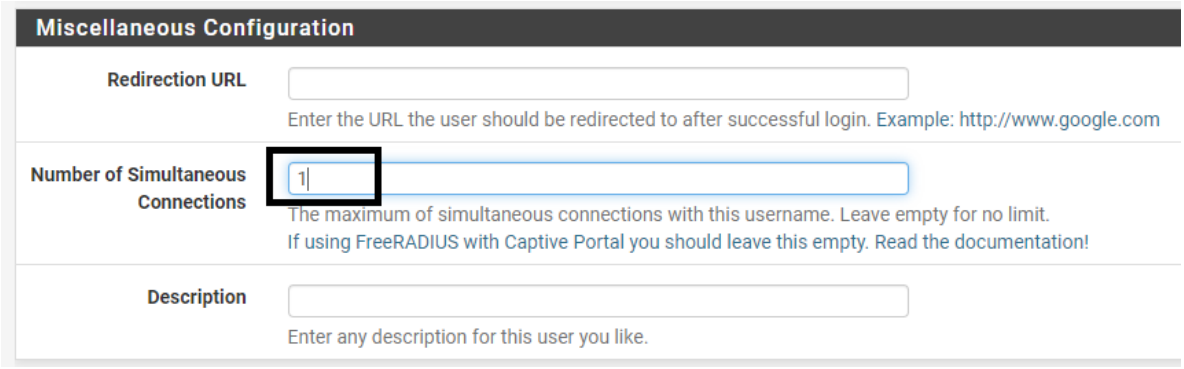
5.- En la sección **One-Time Password Configuration** activamos la casilla “Enable One-Time Password(OTP) for this user”, luego, en la opción “OTP Auth Method” seleccionamos la opción Google-Authenticator. Después de ello, damos clic en “Generate OTP Secret” y en PIN, colocaremos una cantidad de números que serán la base de la contraseña que utilizará el personal junto a la que le provea Google Autenticador



debera descargar en su celular.



7.- Luego de ello, en la sección “Miscellaneous Configuration”, en la casilla “Number of Simultaneous Connections” colocaremos 1, para que solo un usuario pueda conectarse a la vez, con dicho usuario:


Miscellaneous Configuration
Redirection URL
Enter the URL the user should be redirected to after successful login. Example: http://www.google.com
Number of Simultaneous Connections
1
The maximum of simultaneous connections with this username. Leave empty for no limit.
If using FreeRADIUS with Captive Portal you should leave this empty. Read the documentation!
Description
Enter any description for this user you like.

Anexo 14: Manual de Owncloud

Parte 1: Acceso y creación de carpetas.

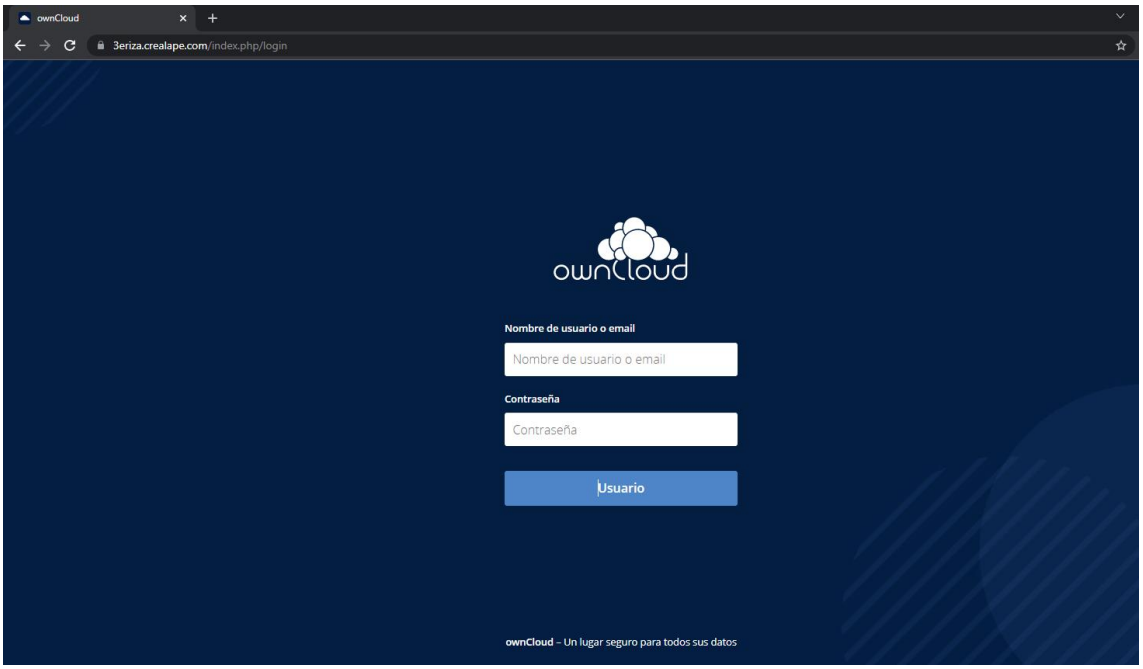
Para el control de accesos a las carpetas y archivos compartidos, se utilizó la el software Open Source conocido como OwnCloud, la cual fue instalada en un dominio público para tener una mayor seguridad a su ingreso.

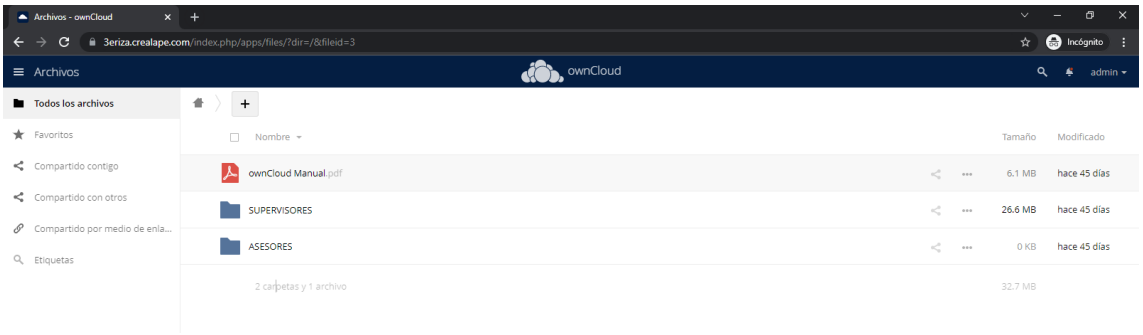
Dentro de esta plataforma es donde el personal de TI, creará las carpetas y usuarios para el accesos a la información de la empresa.

Se diferenciarán por Supervisores y asesores en el caso de la empresa Terceriza S.R.L en la cual se desarrolló el proyecto

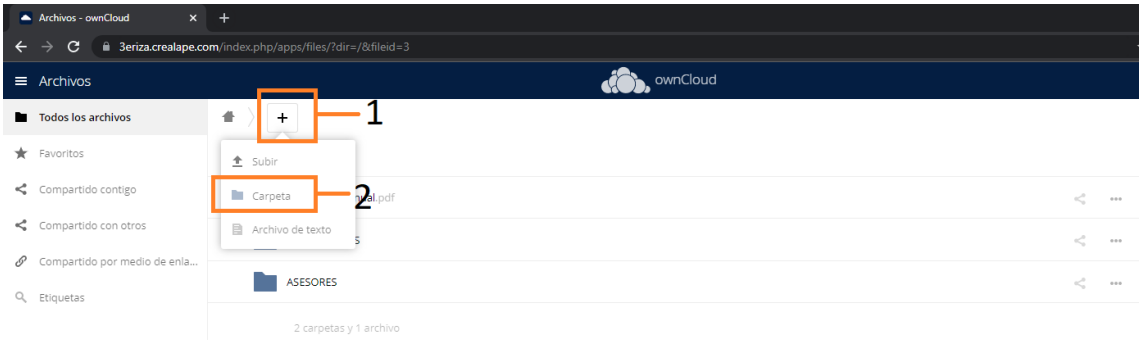
1.- El personal de TI deberá acceder con la cuenta de administrador al acceso de Owncloud:

https://3eriza.crealape.com/index.php/login

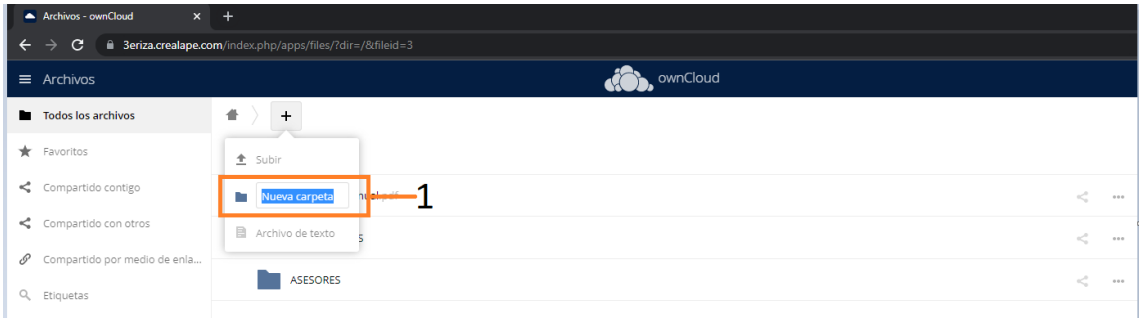




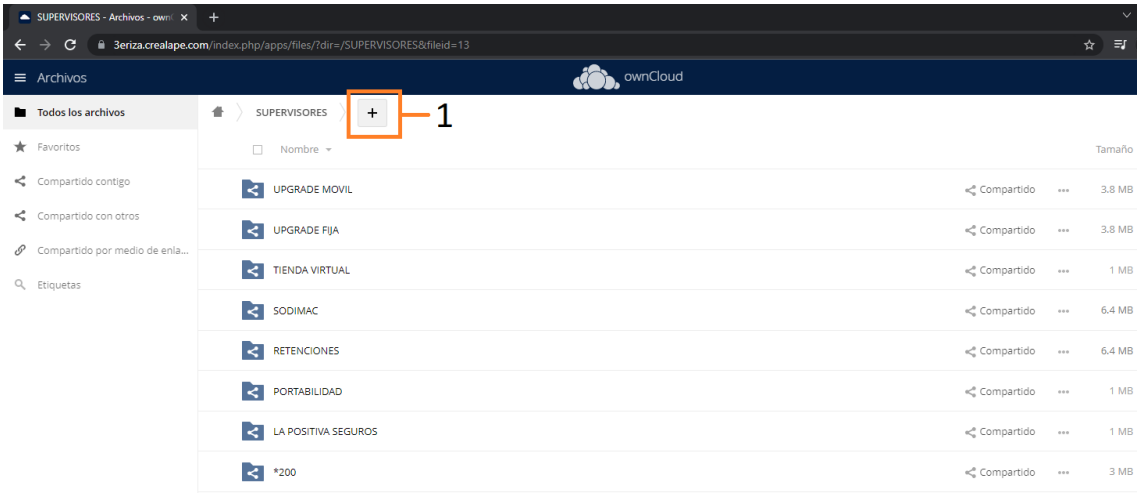
2.- Una vez dentro del portal, se procede a crear las carpetas necesarias para categorizar a los usuarios. Para ello damos clic en el botón “+”(1) y luego aparecerá una lista desplegable, donde escogeremos la opción “carpeta”(2)



3.- Se habilitará una casilla donde deberemos colocar el nombre de la carpeta que se desea crear.

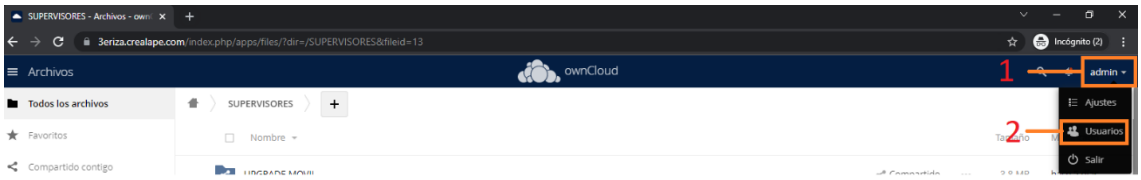


4.- Dentro de la carpeta creada podemos crear subcarpetas para las áreas que se requerirán en la empresa, dando clic en “+”(1).

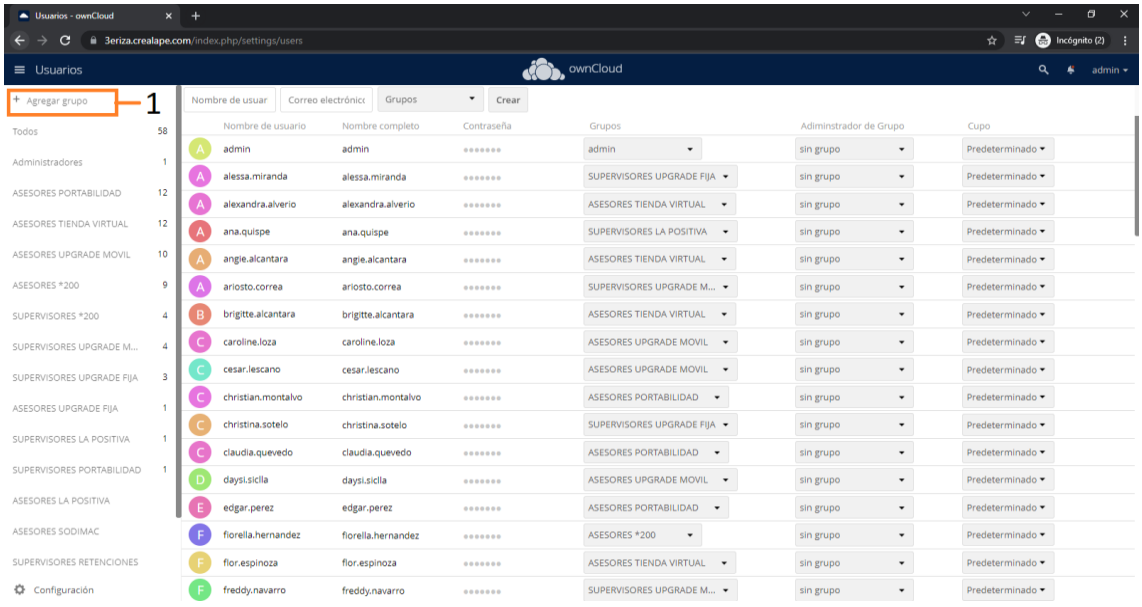


Parte 2: Creación de usuarios

1.- Damos clic en la opción “admin” (1) y luego en la opción Usuario (2):



2.- Creamos un grupo para organizar a los usuarios por áreas y cargo, ya sea Supervisor o Asesor, para ello damos clic en la opción Agregar grupo(1)

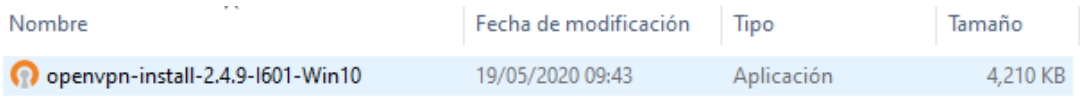


Anexo 15: Manual de Open VPN

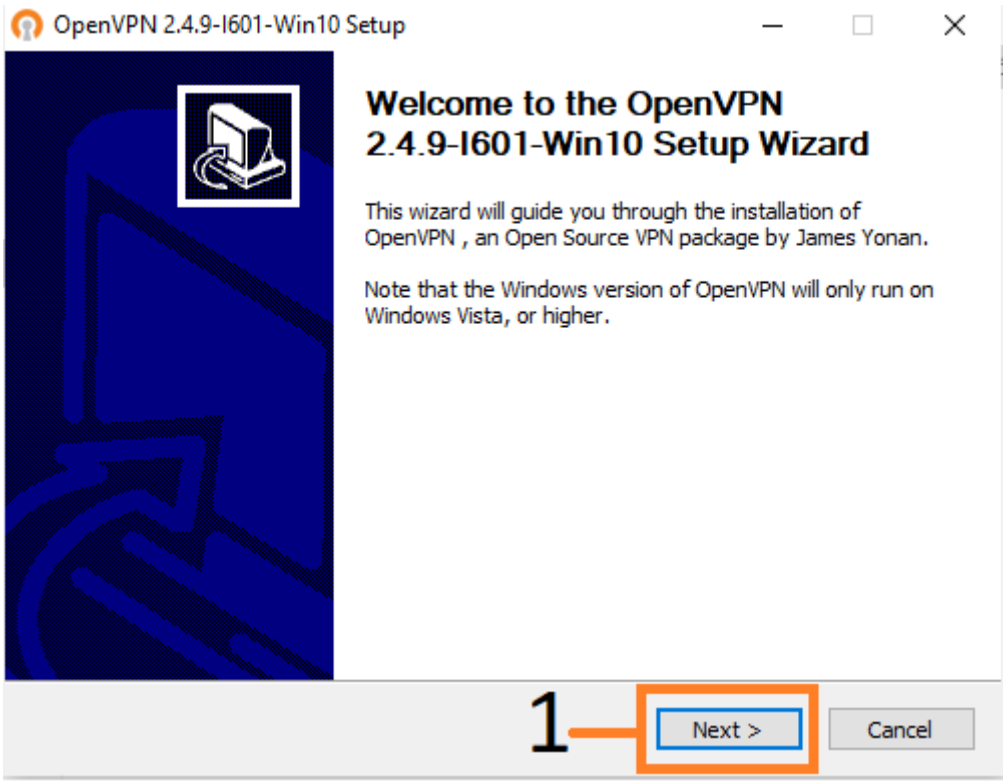
Para poder conectarse a la red interna de la empresa y acceder a los aplicativos y archivos necesarios para la gestión diaria, el personal de TI, deberá instalar en los dispositivos de los usuarios, el programa Open Source OpenVPN GUI.

Parte 1: Instalación de OpenVPN GUI

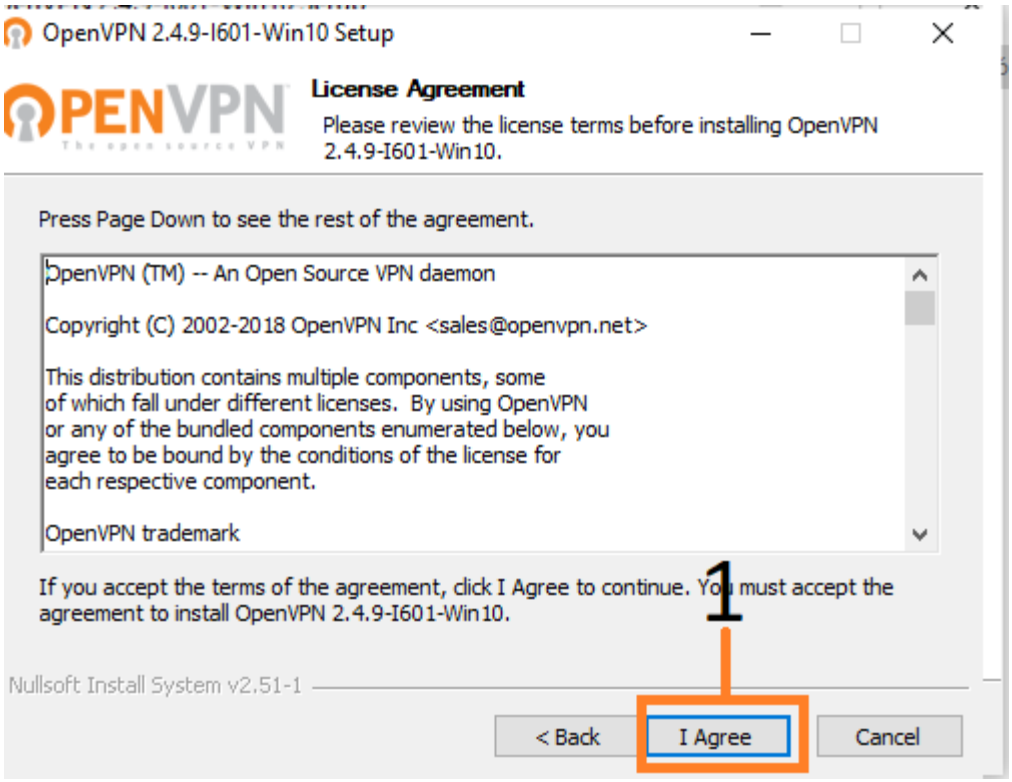
1.- El personal de TI, copiará el archivo ejecutable de instalación para el OpenVPN GUI en el dispositivo del usuario dependiendo la versión de Sistema operativo que tuviera, ya sea Windows 7-8 o Windows 10 y procederá a darle doble clic para que inicie la instalación:



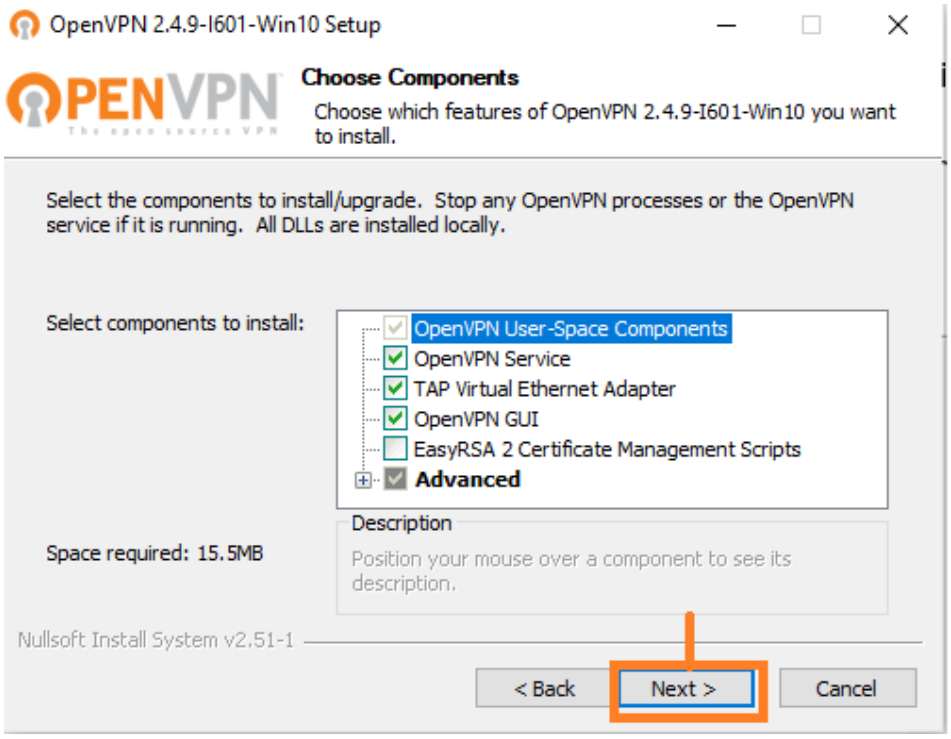
2.- Una vez ejecutada la aplicación deberá dar en “Next”:



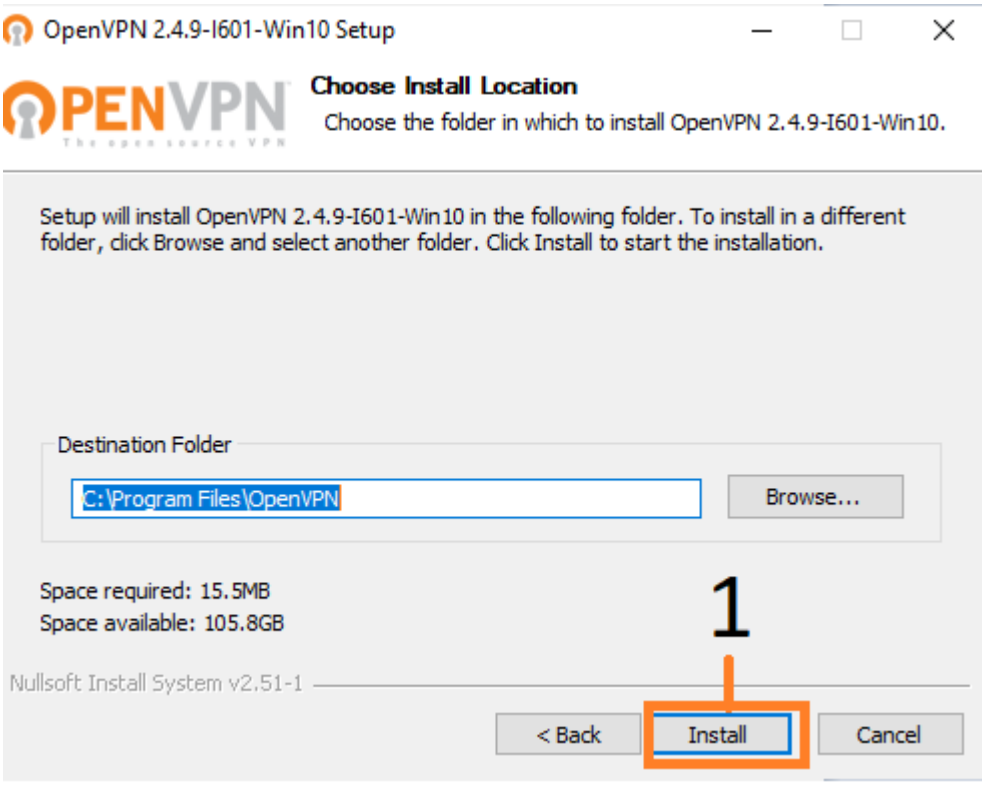
3.- A continuación, deberá aceptar los términos de la licencia dando clic en “I agree”:



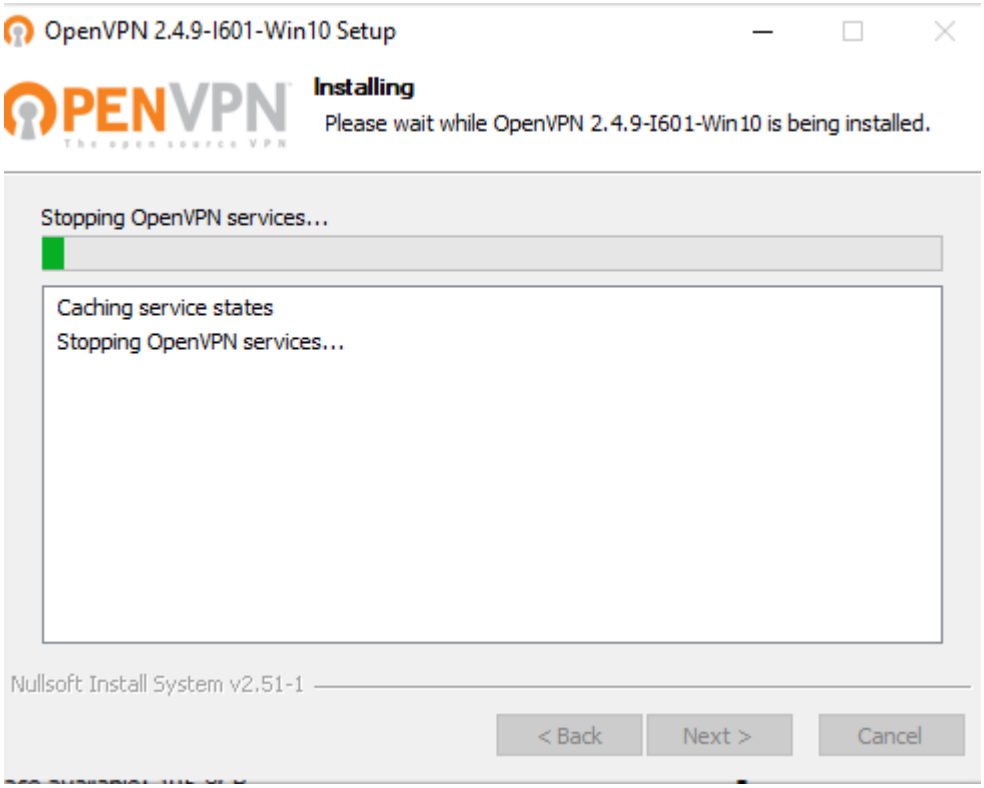
4.- En la siguiente pantalla, se escogerán los componentes de la VPN a instalar, en este caso, los dejamos tal y como aparecen en la imagen y damos clic en “Next”:



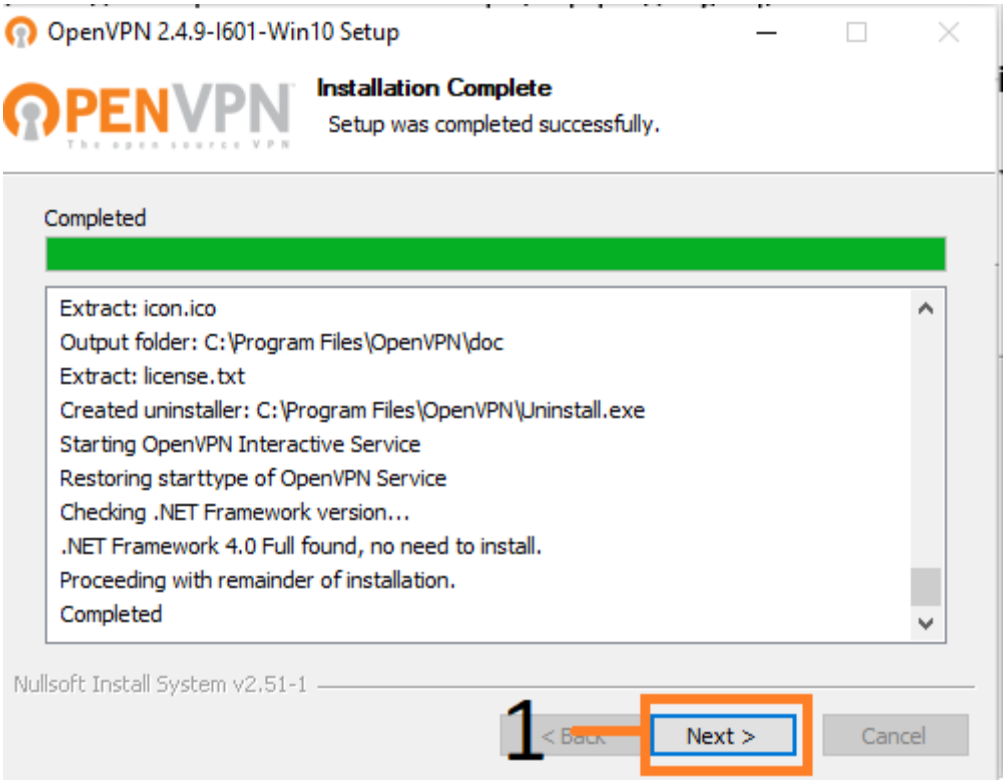
5.- En la ventana siguiente, escogeremos donde se instalará el programa, lo dejaremos por defecto y daremos clic en “Install”:



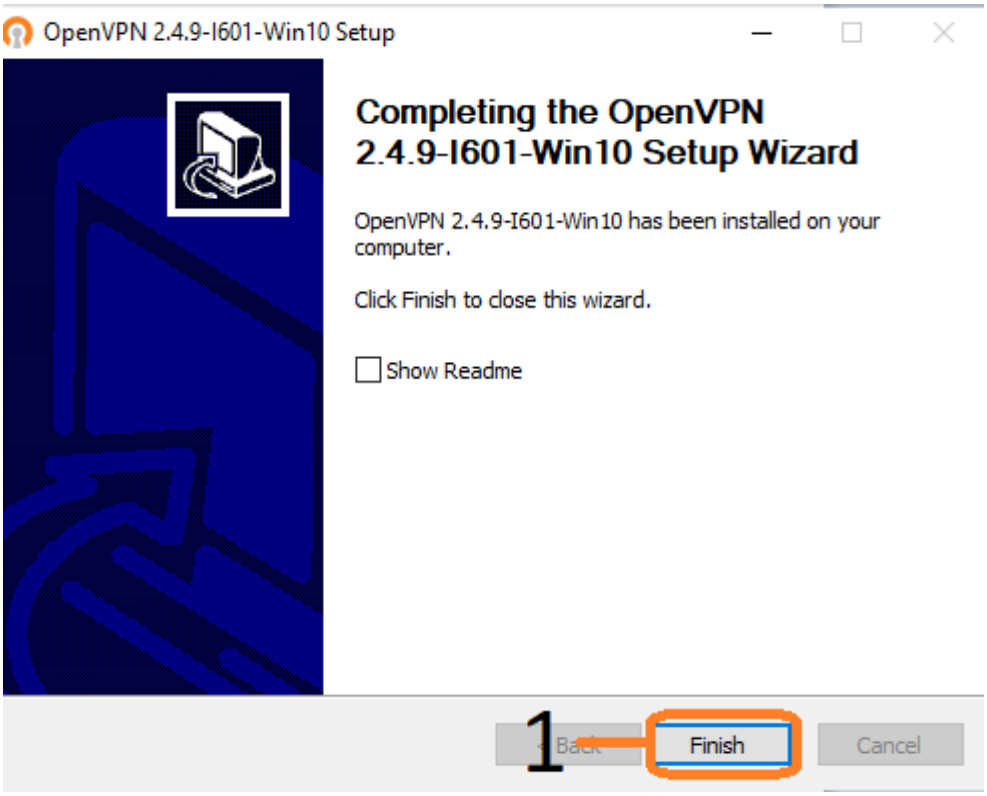
6.- A continuación, solo esperamos que la instalación finalice:



7.- Finalizada la instalación, aparecerá esta ventana donde daremos clic en “Next”:



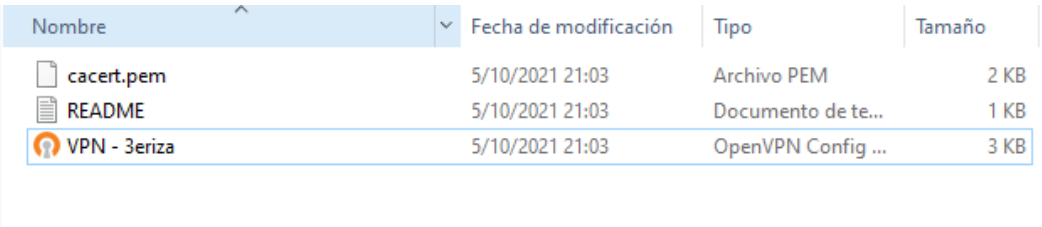
8.- Finalmente, aparecerá esta pantalla donde daremos clic en “Finish” para finalizar el proceso de instalación:



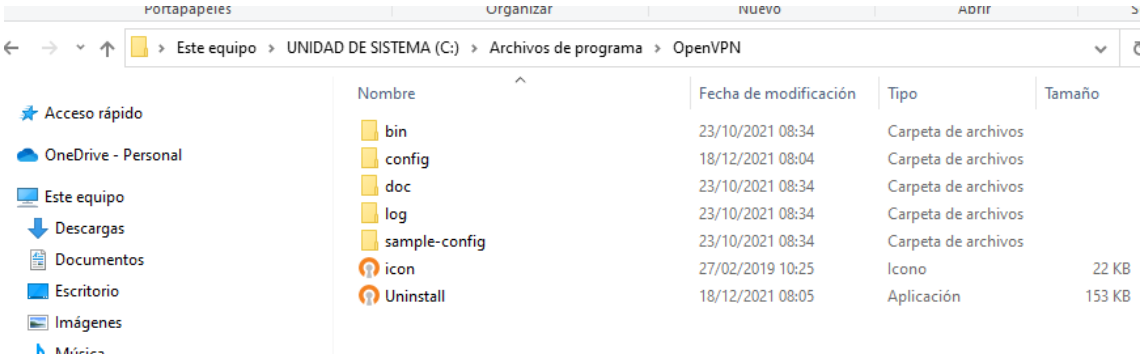
Parte 2: Añadir configuración de PfSense a OpenVPN GUI

Una vez instalado el programa OpenVPN GUI deberemos asignarle la configuración correspondiente para que reconozca las credenciales que creamos previamente en el programa PfSense.

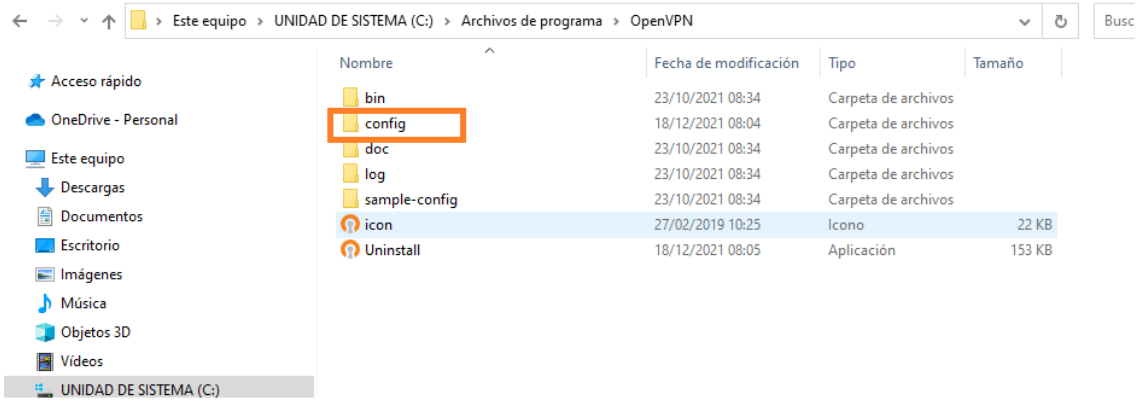
1.- Copiamos el archivo de configuración de PfSense:



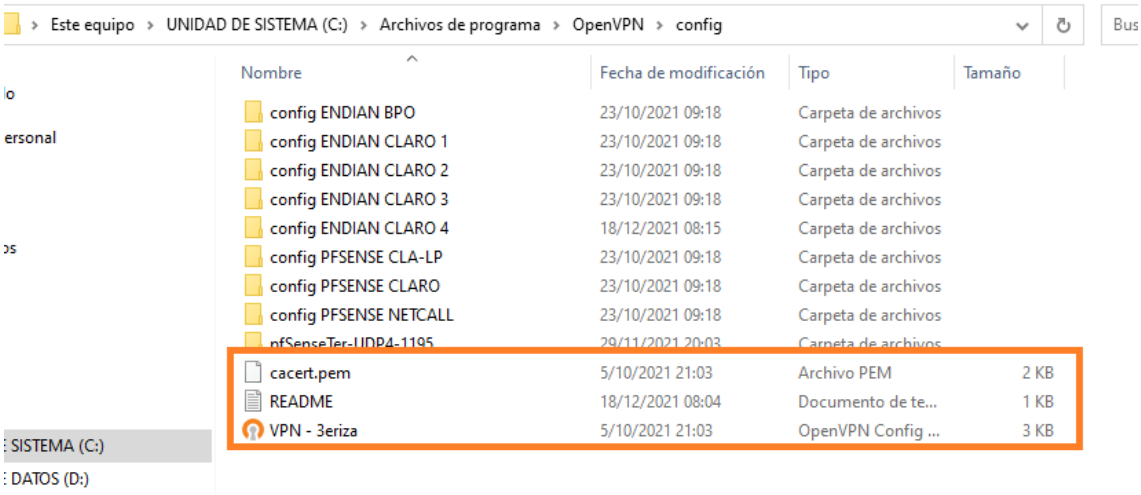
2.- Dichos archivos, deberán ser copiados en la carpeta de instalación de OpenVPN GUI, ubicada en la siguiente ruta C:\Program Files\OpenVPN



3.- Dentro de la ruta de instalación del OpenVPN GUI, accederemos a la carpeta Config:



4.- Dentro de dicha carpeta procederemos a copiar los archivos de PfSense:



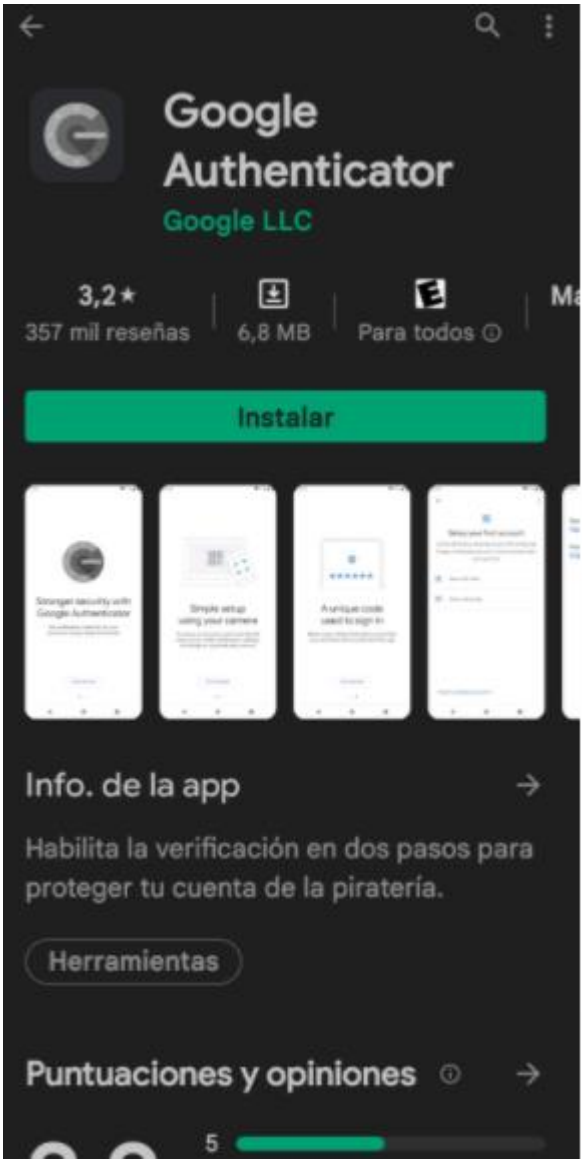
Con ello, ya estaría configurado el OpenVPN GUI para acceder a la red de la empresa.

Parte 3: Conexión a la VPN

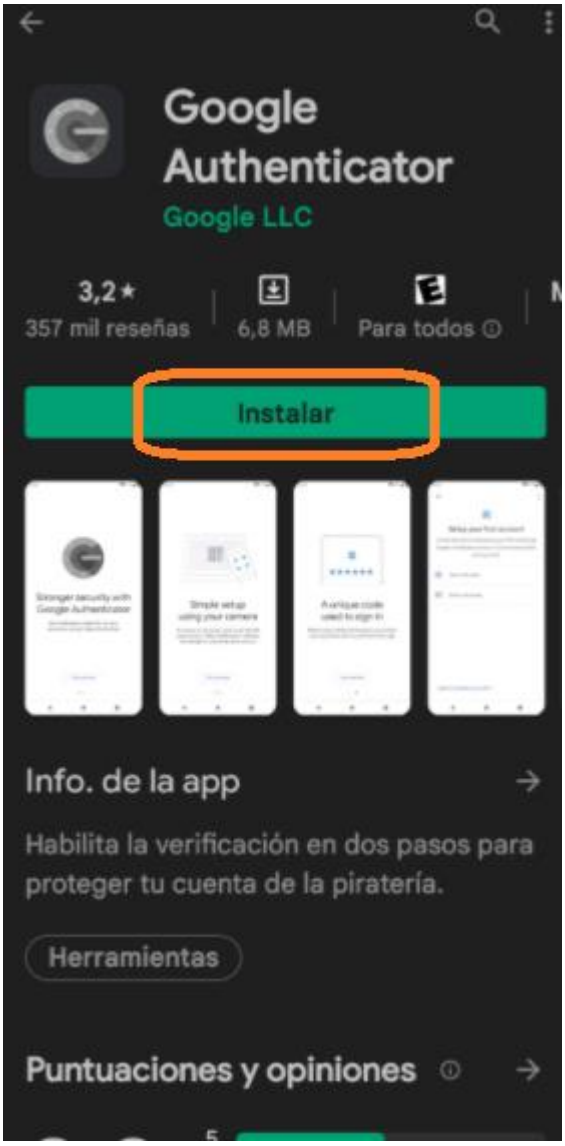
Para proceder con la conexión a la VPN, el personal de TI deberá indicarle al usuario que descargue en su celular previamente la app Google Authenticator, ubicada en la Playstore del dispositivo celular:

Parte 1: Instalar App Google Authenticator

1.- Acceder a Playstore y buscar “Google Authenticator”:



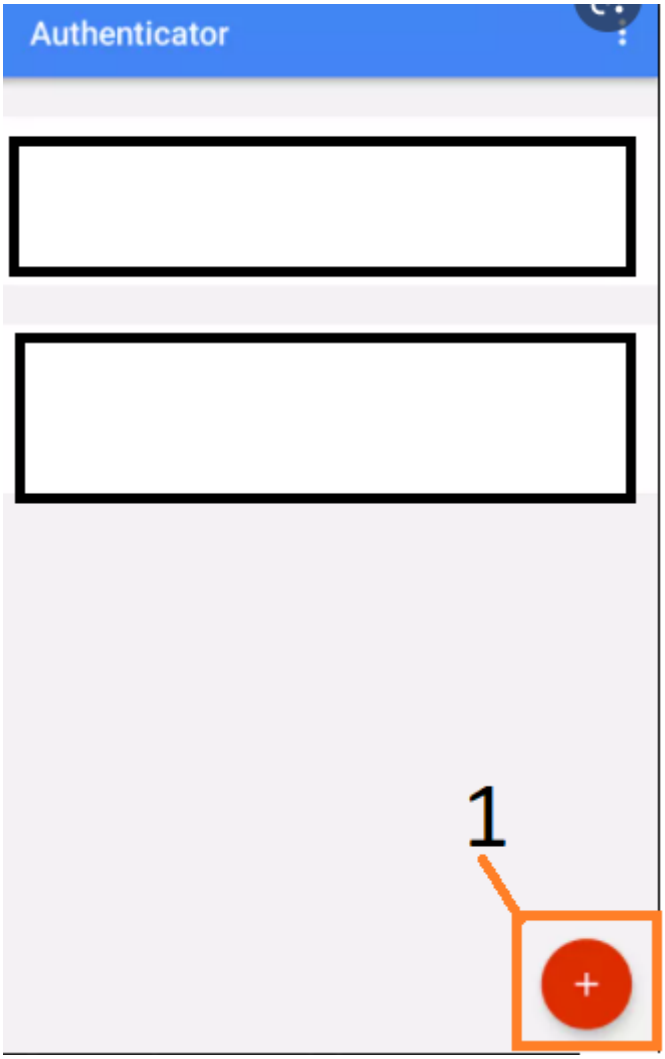
2.- Clic en “Instalar”



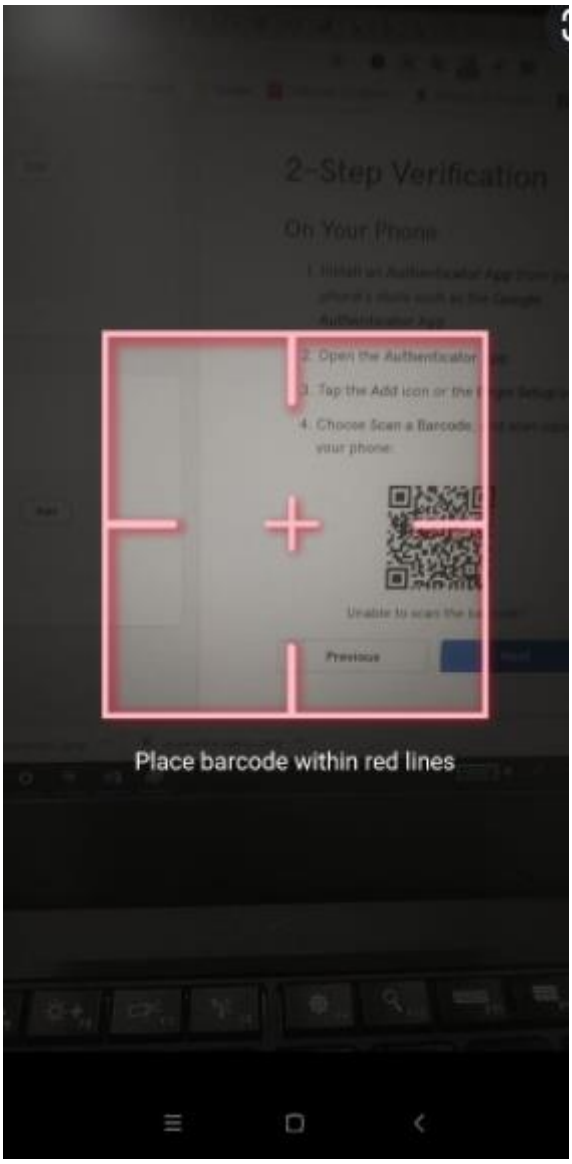
Una vez ya tengamos instalada la aplicación Google Authenticator, solo procedemos a escanear el código QR que se creó en conjunto al usuario para la VPN en el PfSense:

Parte 2: Escanear Código QR

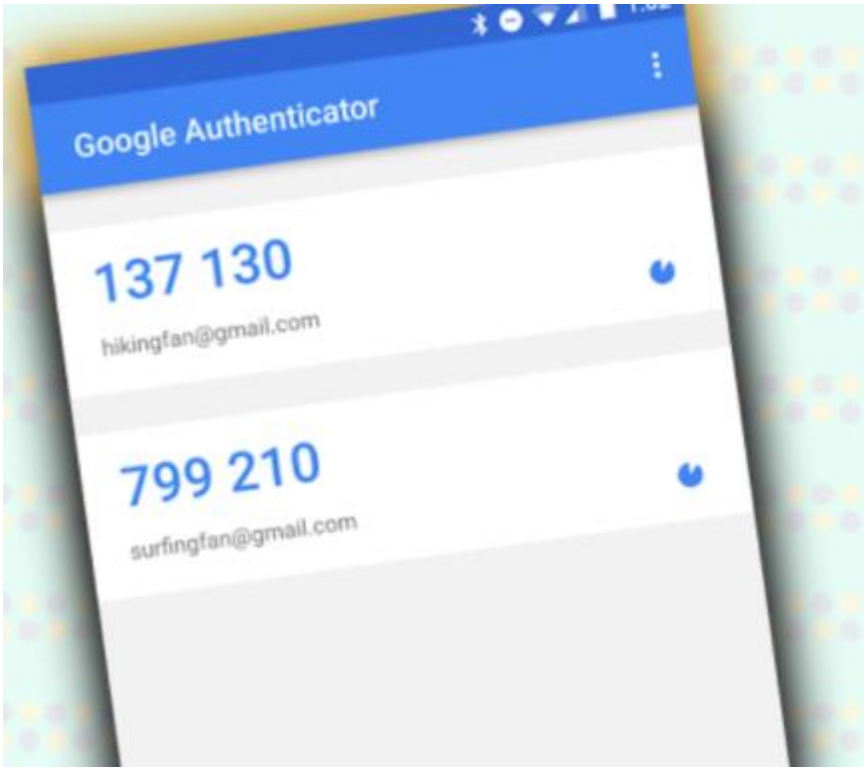
1.- Accedemos al aplicativo Google Authenticator en el celular y damos clic en el símbolo de “+”:



2.- Aparecerá la siguiente pantalla, donde debemos ubicar el cuadro sobre el código QR generado por el personal de TI para el usuario:

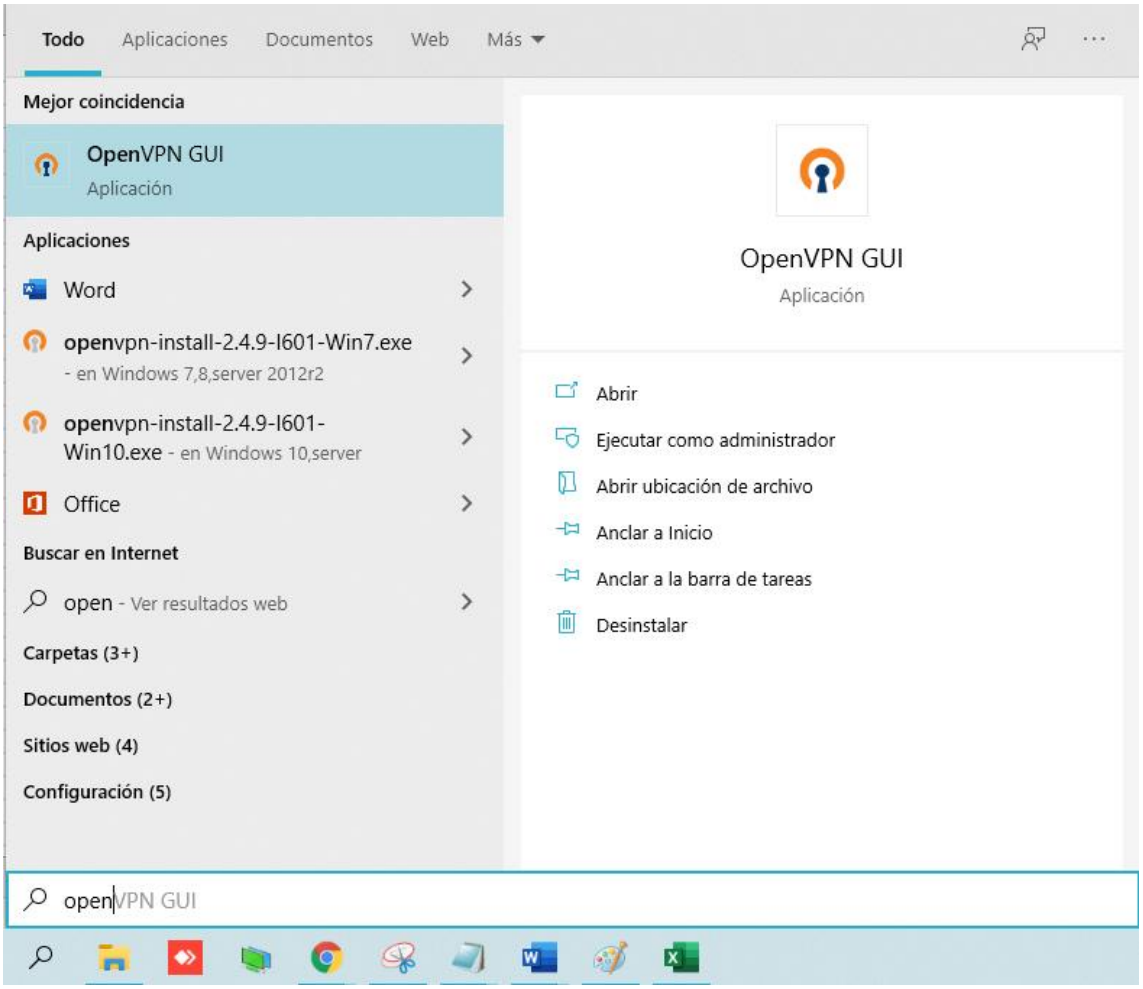


3.- Una vez el código QR fue escaneado por la aplicación Google Authenticator, verificará la siguiente pantalla, donde aparecerá su nombre de usuario que se le creó para la VPN y 6 números que serán su clave secreta dinámica, que deberá colocar luego del número PIN de4 dígitos que le brindará el soporte de TI.



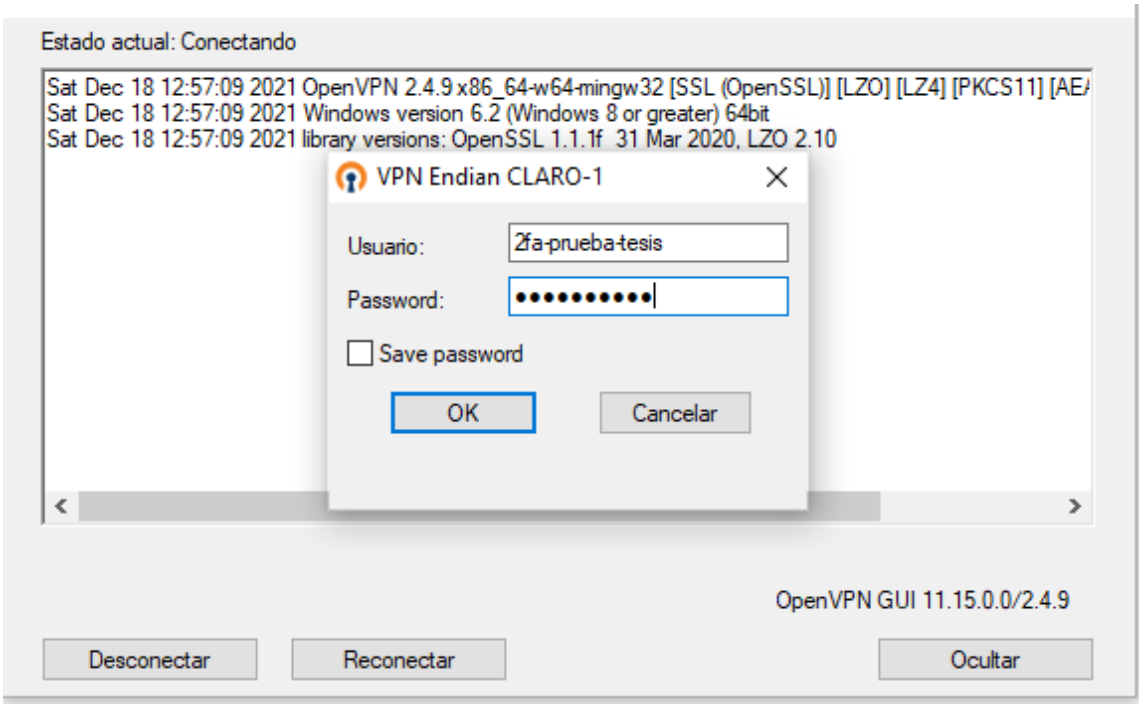
Parte 4: Conexión a la VPN

1.- Deberá abrir el programa Open VPN, ya sea desde el acceso directo en el escritorio o buscándolo en la barra de programas:

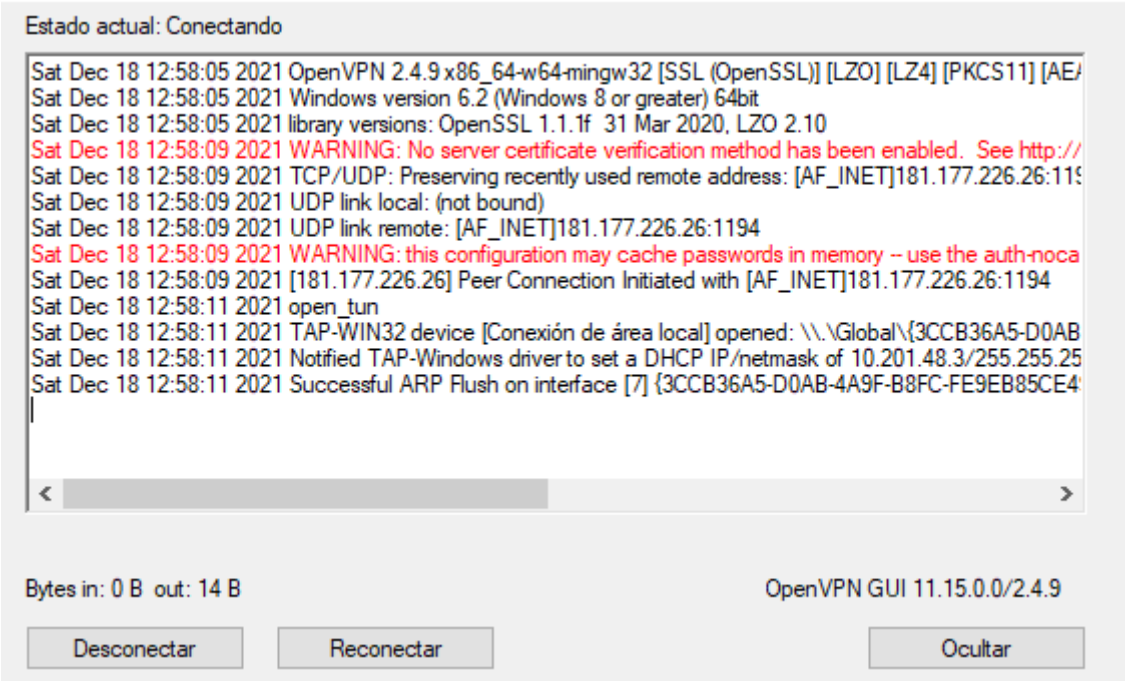


2.- Una vez abierto el programa OpenVPN GUI, en la esquina inferior derecha de la barra de tareas, al lado de la hora, aparecerá el ícono de una pantalla con un candado, dicho símbolo es el ícono del programa OpenVPN GUI, al cual le dará doble clic

3.- Aparecerá la siguiente ventana, donde deberá ingresar los 4 dígitos del PIN proporcionado por el área de TI, sumado a los 6 dígitos que le aparezcan en su aplicación de Google Authenticator:



4.- Una vez ingrese correctamente las credenciales y de clic en “Ok”, comenzará a cargar la conexión como se muestra en la siguiente imagen:



5.- Una vez finalizada la carga, el ícono de la OpenVPN GUI, se tornará de color verde: