Implementación De Políticas De Seguridad En El Sistema De Información De La Empresa Funtraev

Implementation Of Security Policies In The Information System Of The Company Funtraev

Jhon Alexander Penagos Montoya[1]
Kevin Kenny Rentería Gil[2]
Yeferson Ibarguen Mena[3]
Vanessa García Pineda[4]
Frey Castro Ramírez[5]

DOI: *https://doi.org/10.26495/icti.v9i2.2271*

RESUMEN

La seguridad de las organizaciones se ha convertido en un aspecto fundamental en la actualidad. La cantidad de información compartida y el internet de todo generan un gran flujo de datos en la red cada día. Sin embargo, a pesar del avance de las tecnologías de la información y la comunicación, no todas las empresas cuentan con un diseño y parámetros de seguridad debidamente implementados para garantizar la protección de la información que se encuentra disponible en sus equipos. Lo anterior, debido a que algunos equipos y la implementación de parámetros y diferentes factores de seguridad son costosos para las pequeñas y medianas organizaciones y requieren de profesionales expertos para su implementación, gestión y monitoreo. Por lo anterior, el objetivo general de esta investigación fue la implementación de políticas de seguridad informática en la entidad FUNTRAEV que permita establecer parámetros de seguridad de acceso a la información. Para lo anterior se llevó a cabo una metodología estructurada en 4 fases, por medio de la cual es posible el análisis previo de la red, para posteriormente diseñar, implementar y operar las diferentes políticas necesarias para garantizar la seguridad en la red. Como resultado principal, se logró la definición de políticas en la red y la capacitación de los empleados de la organización respecto al uso adecuado de la información en la red. Finalmente, al realizar la distribución de políticas y la capacitación respecto a la importancia de la seguridad en la red los empleados de la organización observaron la mejoría en la red.

PALABRAS CLAVE:
seguridad de la información, políticas de seguridad, red, implementación, control de acceso.

[1] *Ingeniero en sistemas de, Corporación Universitaria Americana, Medellín, Colombia, penagosjhon7667@americana.edu.co*
[2] *Ingeniero en sistemas de, Corporación Universitaria Americana, Medellín, Colombia, kaywen730@gmail.com*
[3] *Ingeniero en sistemas de, Corporación Universitaria Americana, Medellín, Colombia, ibarguenyefersson1474@coruniamericana.edu.co*
[4] *Docente investigadora Facultad de ingenierías, Corporación Universitaria Americana, Medellín, Colombia, vgarcia@americana.edu.co, https://orcid.org/0000-0003-3418-8956*
[5] *Docente Facultad de ingenierías, Corporación Universitaria Americana, Medellín, Colombia, fcastro@coruniamericana.edu.co, https://orcid.org/0000-0003-0142-6006*

ABSTRACT

The security of organizations has become a fundamental aspect today. The amount of information shared and the internet of everything generate a large flow of data on the network every day. However, despite the advancement of information and communication technologies, not all companies have a design and security parameters duly implemented to guarantee the protection of the information that is available on their equipment. This is due to the fact that some equipment and the implementation of parameters and different security factors are expensive for small and medium-sized organizations and require expert professionals for their implementation, management and monitoring. Therefore, the general objective of this research was the implementation of computer security policies in the FUNTRAEV entity that allows the establishment of security parameters for access to information. For the above, the structured in 4 phases methodology was carried out, through which it is possible to previously analyze the network, to later design, implement and operate the different policies necessary to guarantee security in the net. As a main result, the definition of network policies and the training of the organization's employees regarding the proper use of information on the network were achieved. Finally, by carrying out the distribution of policies and training regarding the importance of network security, the employees of the organization observed the improvement in the network.

KEYWORDS: information security, security policies, network, implementation, access control.

1. **Introducción**

La seguridad de la información y seguridad en los sistemas de información, son estrategias utilizadas por las diferentes organizaciones, con el fin de reducir al máximo los riesgos de inseguridad en el tratamiento de la información sensible o de conocimiento de la empresa (Instituto Nacional de Ciberseguridad, 2010). Dichas estrategias han sido llevadas a cabo por las organizaciones debido a que en la actualidad se han detectado diferentes métodos de acceso a la información de manera violenta, donde el caso más común es secuestrar la información y después pedir recompensa para que esta sea devuelta. (Riascos Erazo et al., 2014).

Cuando se decide conformar una empresa o entidad, hay que tener en cuenta los riesgos que se toman en el manejo de la información de usuarios o integrantes de la misma, cuando se deja a un lado la seguridad de la información y los sistemas de información, se corre el riesgo que los datos lleguen a manos ajenas o que sean manipulados por terceros (Bagchi et al., 2020).

Como ejemplo a esta problemática, se encuentra la información publicada por Rivas (2017) con la que se da a conocer datos de las diferentes modalidades utilizadas para vulnerar la seguridad de la información y los sistemas de información, una de estas es que a diario se hackea un aproximado de 30.000 webs, en un mes aproximadamente se crean 6.000 virus, gran porcentaje de los e-mail son spam, las contraseñas no se cambian en grandes periodos de tiempo manejando números o letras continuas, para los dispositivos móviles los ciberdelincuentes son los encargados de crea virus que permiten el secuestro de información, creación de software con errores “bug”. Blaser es el gusano de red más utilizado en la historia, los puertos USB representan uno de los mayores referentes en seguridad.

Este problema no afecta solo las pequeñas y medianas empresas, claro ejemplo el que nos da Rivas (2017) donde nos ilustra cómo la NASA en 21 días, debió mantener sus computadoras apagadas, esto debido a que se generó un ataque a sus sistemas por medio de un hacker, quien de igual forma realizó esta misma práctica con El Pentágono.

Con el fin de mantener la seguridad tanto de los datos como de información de las diferentes empresas u organizaciones, en el transcurrir del tiempo se han implementado diferentes metodologías que han

ayudado en la seguridad y reserva de estos, como también la creación de normas que han permitido el juzgamiento de actividades delictivas que van en contra de la reserva de la información. Uno de los proyectos más relevantes del 2009 fue el proyecto epSOS (Seguridad de la información. Protección de datos) en el que Acevedo et al., (2009) plantean ante los diferentes países que integran la UE (UNIÓN EUROPEA) crear un proyecto de información de historias clínicas, en el cual se utilizaran datos sensibles de los usuarios, con el fin que se pueda compartir entre estos, así el paciente no pertenezca a este país o localidad, para esto proponen la utilización de sistemas de seguridad modernos y que permitan mantener un buen tratamiento de la información.

Con el fin que se dé un adecuado tratamiento a la información Acevedo et al., (2009) plantea una estrategia interesante y novedosa para la época, la cual consiste en la autenticación de los profesionales que estarán a cargo de la extracción y entrega de esta información como también la autorización de extracción de esta por parte del usuario, es por esto que es necesario dar a conocer al personal la normatividad vigente y las consecuencias que esta trae al no cumplimiento de esta.

Ramos & Gabriel (2021) dan a conocer estudios realizados a diferentes empresas en las cuales desconocían la importancia y procedimientos que se deben de realizar para la protección de la información y datos que estas manejan, de igual forma resalta que la empresa N&V ASESORES SAC, no mostró intenciones claras de querer implementar controles de seguridad en sus sistemas de información, esto debido a su desconocimiento en seguridad de datos e información, por esto es que el proyecto es enfocado en la norma ISO/IEC 27001:2014.

El término Seguridad de la información según Soriano (2014) es un concepto que ha sido tomado por diferentes personas de la menara equivocada, porque lo relacionan solo como un mecanismo para eliminar virus y evitar el ingreso de hackers a la red o sistemas de información, concepto que no es acorde a lo que en realidad abarca esta palabra, su significado es mucho más extenso a lo que muchos creen y opinan al momento de indagar sobre este tema.

De acuerdo con la definición propuesta por Soriano (2014) sobre lo que es la seguridad de la información, se puede observar que es un campo de información muy extenso, ya que este nos manifiesta que este concepto aparte de suministrar seguridad en redes y sistemas de información, también necesita de un componente esencial para que este cumpla su objetivo y es los empleados o administradores de las empresas o compañías, quienes deben de fomentar las buenas prácticas para que los datos de la entidad no estén expuestos a ser manipulados por otros.

Soriano (2014) en su libro nos regala un concepto claro de lo que significa “Política de seguridad”, definiéndose de una manera muy clara y con ejemplos que son significativos, ya que lo principal en una empresa u organización es que se cumplan las políticas de seguridad, pero si en esta no se han creado entonces no se estaría cumpliendo con este gran paso, es por esto que lo primero que este nos da a conocer en su ejemplo es que se debe de tener un documento en el que la entidad tenga plasmada las políticas a seguir por los integrantes de la empresa u organización.

Dussan (2006) dice que el 60% de las organizaciones Colombia no cuenta con un protocolo de seguridad informática, esto conlleva a que las organizaciones directa o indirectamente corren el riesgo de ser víctima de pérdida de información o vulnerabilidades informáticas de muchos tipos. Con esto queda demostrado que si somos víctima de un ciberataque no nos ponemos las pilas a montar un programa de seguridad informática en la organización. A veces somos víctimas de los ataques informáticos y no nos damos cuenta y están trabajando por debajo de nuestros sistemas de la organización y antivirus no es garantía para proteger la información en su totalidad solo es para ponernos en alerta. Lo más importante es invertir en el área de sistemas y en especial tener una persona que se encargue solamente de la seguridad.

Villaverde et al., (2021) enseñan que lo importante de toda organización es tener un departamento de sistemas bien constituido y a su vez capacitar a todos los empleados en general que conozcan los tipos de ataques que existe y así los empleados ya tendrán más cuidado a la hora de navegar en la red y de no estar abriendo cualquier archivo. A veces la curiosidad nos lleva a pecar en el área de las TIC y esto lleva a que la organización pierda mucho dinero, entonces debemos de capacitar a nuestros empleados para disminuir los ataques.

Es por esto por lo que se decide llevar a cabo este proyecto en la empresa Fundación de Trabajadores de Empresas Varias (FUNTRAEV). Después de realizar una verificación en la empresa, se identificaron diversos problemas de seguridad de la información y de los sistemas, en los que se destacan: equipos sin contraseñas, puertos USB abiertos, uso de cualquier equipo de la organización sin restricción, etc. En este caso la información de la organización se encuentra expuesta a que cualquier individuo que no pertenezca a la empresa tome información privada de la entidad FUNTRAEV que pueda ser expuesta más adelante y eso genere inconvenientes para la organización, por eso es necesario implementar políticas de seguridad en dicha organización.

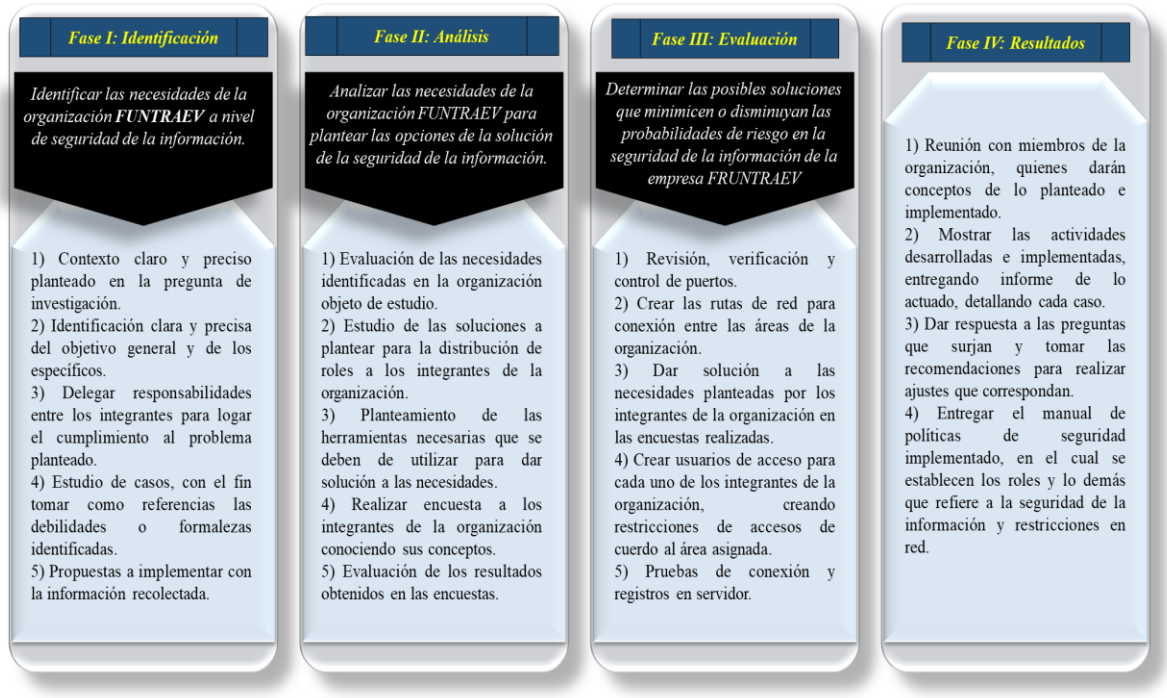
Con la implementación de estas políticas de seguridad, se logrará demostrar las falencias y debilidades que la empresa hasta el momento tenía, y que con la implementación de dichas políticas se pudieron minimizar los riesgos en los que se encontraba la información de la organización. Se realizará un mapeo de puertos y se verifican los permisos desde un servidor, el cual nos permitirá brindar mayor seguridad de la información en las diferentes aplicaciones y archivos de la entidad FUNTRAEV. De igual forma se le daría un orden en la parte de distribución de roles y de red a personal de la empresa, surge entonces la pregunta de investigación; ¿Cómo se puede mejorar la seguridad de la información en la organización FUNTRAEV? De acuerdo con lo anterior, el objetivo general de este trabajo de grado es implementar políticas de seguridad informática en la entidad FUNTRAEV. Para el logro de este objetivo, se han planteado 3 objetivos específicos; el primero busca identificar las necesidades de la organización “FUNTRAEV” a nivel de seguridad de la información, el segundo objetivo específico corresponde al análisis de las debilidades para plantear las opciones de la solución de la seguridad de la información, finalmente, se procede con la determinación de las posibles soluciones que disminuyan las probabilidades de riesgo en la seguridad de la información. Los objetivos presentados anteriormente, permiten direccionar las actividades con el fin de dar cumplimento claro a la problemática propuesta.

Para lo anterior, se llevó a cabo una metodología estructurada, con la cual se desarrollan de manera inicial estrategias que permiten identificar y analizar las debilidades, de la empresa FUNTRAEV, con el fin de determinar sus posibles soluciones, para con esto dar solución al problema identificado.

2. MATERIALES Y MÉTODOS

Como se indicó anteriormente, la metodología utilizada para el desarrollo del proyecto se estructuró en 4 fases de la siguiente manera, la primera fase correspondió a una identificación del problema, la segunda fase a un análisis en el cual se evaluaron e identificaron los factores problema, la tercera fase correspondiente a la evaluación y la cuarta fase correspondiente a la obtención de resultados, como se puede observar en la Figura 1.

Figura 1: Fases de desarrollo del proyecto



Fuente: elaboración propia

FASE I: IDENTIFICACIÓN

Inicialmente, esta fase se realiza con el fin de dar contexto al proyecto y formular todo el marco teórico del mismo, se inicia con la formulación de la pregunta de investigación, donde después de identificarlo y revisarlo, se procede a crear un objetivo general, el cual se logra con el cumplimiento de los objetivos específicos, pero para que esto cumpla con lo requerido y que se ajuste a las necesidades, se da a conocer el equipo de trabajo, para con esto iniciar con la delegación de responsabilidades entre los integrantes.

Cuando cada uno de los integrantes conoce sus responsabilidades y actividades a realizar, se convoca reunión en la que se inicie con el estudio de casos, con el fin tomar como referencia las debilidades o fortalezas identificadas dentro de la organización, ya con esto y teniendo en cuenta que cada uno identificó como le aporta y que debe de adelantar para que estas se ajusten a los requerimientos, se aportan propuestas a implementar con la información recolectada.

FASE II: ANÁLISIS

Mediante un análisis detallado de lo planteado y las verificaciones realizadas en la organización, se procede a evaluar las necesidades identificadas, mediante un reconocimiento de los sistemas de la organización, identificando las áreas con las que esta cuenta, y un sondeo de preguntas de pruebas que da las pautas de observación, con el fin de adecuar criterios que permitan proponer nuevas ideas que se ajusten al estudio de las soluciones a plantear para la distribución de roles a los integrantes de la organización, conociendo las funciones y actividades que cada uno desarrolla, para así establecer que herramientas son necesarias y cumplan con los requisitos necesarios para dar solución a las necesidades.

Después de adelantar la actividad de identificación de necesidades y realizar un consenso detallado, se desarrollan actividades de recolección de información que permiten conocer nuevas ideas o necesidades que mejoren los procesos de la organización, para esto se hacen encuestas a los integrantes de la organización conociendo sus puntos de vistas y recomendaciones, las cuales se deben de llevar a una nueva mesa de trabajo en la que se hace evaluación de los resultados obtenidos en dichas encuestas.

Para tal fin, se tomaron todas las dudas e inquietudes que surgieron en el desarrollo de la recolección de información, la cual sirvió para crear un banco de preguntas que sirvieron para conocer mas a fondo lo que cada integrante de la organización conoce, desconoce o requiere conocer sobre la seguridad informática y lo demás que esta aporta en seguridad de una organización.

Para tal caso se realizó el siguiente cuestionario:

1. ¿Ha escuchado o sabe sobre la seguridad informática?
2. ¿Sabe qué son políticas de seguridad?
3. ¿En su empresa ha recibido capacitación sobre seguridad de la información?
4. ¿Cuántas Capacitaciones ha recibido?
5. ¿Cuenta con usuario y contraseña de acceso a pc o a red de la empresa?
6. ¿Qué tipo de recursos informáticos utiliza?
7. ¿Los equipos poseen algún tipo de protección?
8. ¿Ha tenido algún inconveniente de pérdida de información?
9. ¿Realiza respaldo de seguridad de su información?
10. ¿Le gustaría recibir capacitación sobre seguridad y respaldo de información?

Al compartir el enlace de la encuesta, se recibieron 30 respuestas, obteniendo los siguientes resultados:

- De acuerdo con la pregunta ¿Ha escuchado o sabe sobre la seguridad informática?, se observa que el 80% de los empleados han escuchado temas referentes a la seguridad informática, el 20% lo desconocen totalmente.
- De acuerdo con la pregunta ¿Sabe que son políticas de seguridad? El 83% de los empleados conocen sobre estas, mientras que el 17% lo desconocen totalmente.
- De acuerdo con la pregunta ¿En su empresa ha recibido capacitación sobre seguridad de la información?, se observa que el 27% de los empleados han sido capacitados, el 73% aun no la reciben.
- De acuerdo con la pregunta ¿Cuántas Capacitaciones ha recibido?, se propuso 3 respuestas, donde el 23% han recibido entre 1 y 2 capacitaciones, el 7% más de dos y 70% no ha sido capacitado.

- De acuerdo con la pregunta ¿cuenta con usuario y contraseña de acceso a pc o a red de la empresa?, el 53% acceden mediante este medio, mientras que el 47% lo realizan de manera fácil sin restricciones.
- De acuerdo con la pregunta ¿Qué tipo de Recursos informáticos utiliza?, se dan dos opciones de respuesta en las que el 37% utilizan el Equipo de escritorio y el 63% por medio de equipo de cómputo portátil.
- De acuerdo con la pregunta ¿los equipos poseen algún tipo de protección?, se plantearon 5 opciones de respuestas, de las cuales se podían seleccionar varias, el 17% utilizan antivirus, 23% antivirus y contraseña, el 27% Antivirus, Firewall, Contraseñas, el 17% contraseña, 3% Firewall, contraseña, el 3% Firewall, y no sabe, el 3% no saben y el 7% no utiliza.
- De acuerdo con la pregunta ¿Ha tenido algún inconveniente de pérdida de información?, el 20% han registrado este inconveniente, mientras que el 80% han evitado esta falencia.
- De acuerdo con la pregunta ¿Realiza respaldo de seguridad de su información?, el 83% realiza respaldo de la información, mientras que el 17% no lo realizan, poniendo en riesgo la pérdida de esta.
- De acuerdo con la pregunta ¿le gustaría recibir capacitación sobre seguridad y respaldo de información?, el 60% desean ser capacitados, el 37% tal vez quiera recibir estos conocimientos y el 3% no le interesa.

Después de analizar y tener claro las falencias que se observan en las respuestas obtenidas en las encuestas, se extraen criterios que serán tenidos en cuenta para el desarrollo de dicho proyecto, observando que lo principal es crear la seguridad de acceso a los sistemas, toda vez que el 47% de los encuestados lo realizan de manera fácil, sin ningún tipo de restricción, mostrando con esto que las posibilidades de vulnerabilidad y pérdida de información es muy alta.

De igual forma, aunque el 83% de las personas encuestadas saben o conocen sobre políticas de seguridad, es preocupante que no las apliquen, que aun sabiendo lo importante que son para la compañía, no ayuden a que se mantengan las buenas prácticas y se respeten por quienes la integran, sin embargo, es importante resaltar que el 60% de estos desean recibir capacitación para realizar respaldos de información y seguridad de esta. De esta manera, a nivel general se detectan las siguientes necesidades:

1. Seguridad de acceso a los equipos de cómputo.
2. Las Áreas de trabajo no cuentan con accesos delimitados.
3. Servidor que no cuenta con uso, solo está conectada la impresora e instalado software contable.
4. Falta de almacenamiento para realizar respaldo frecuente de la información.
5. Red WIFI no se encuentra con encriptación.
6. Puertos USB abiertos, permitiendo la extracción de información o instalación de software malicioso.

Aunque la encuesta fue corta, se resalta la efectividad y orientación que esta da al desarrollo del proyecto, toda vez que al conocer las opiniones de quienes a diario se enfrentan a estos riesgos o que han vivido las falencias que registra la organización, es determinante a la hora de tomar decisiones y plantear estrategias.

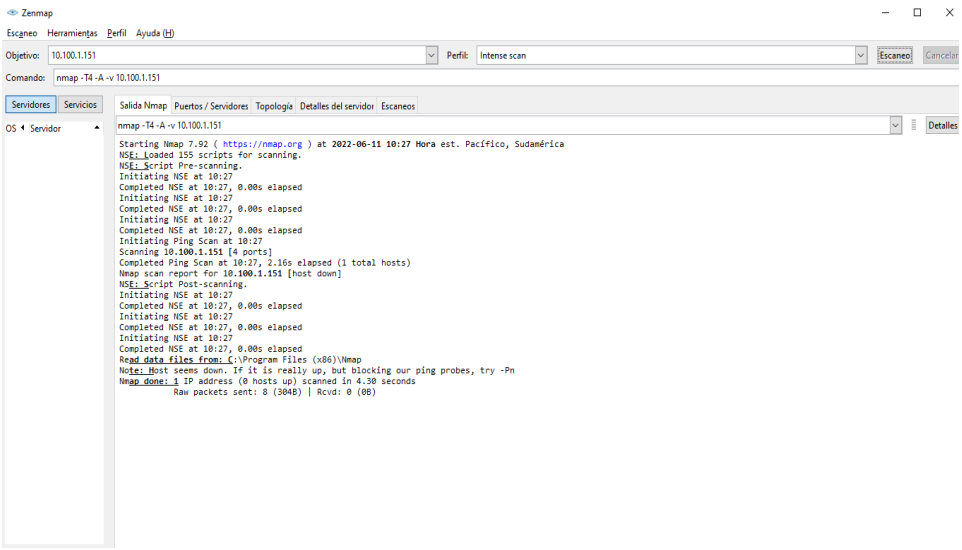
A partir de las respuestas obtenidas en las encuestas, se logró identificar que los principales factores a fortalecer en la organización son, generar una cultura de las buenas prácticas para el cuidado y manejo de información de acuerdo a su nivel de riesgo, acceso de forma segura a los sistemas remotos, aplicar las políticas de seguridad en todos los ámbitos de la seguridad informática, restricción de puertos y distribución de redes para que la información no llegue a zonas no autorizadas o a quien no la requiere.

FASE III: EVALUACIÓN

Después de conocer un poco más de las necesidades, falencias y demás que afectan la seguridad de la información de la empresa FUNTRAEV, se inician las actividades por parte de los integrantes del proyecto quienes, de acuerdo con las responsabilidades asignadas y acordades, se procede con la revisión, verificación y control de puertos, posterior a esto, mediante reunión se verifica lo hallado en dicha actividad y se tomarán las decisiones.

Para el escaneo de puertos de red y saber con exactitud cuáles de estos pueden generar algún nivel de vulnerabilidad, se utilizó Nmap-Zenmap, como se observa en la Figura 2, programa que facilita realizar dicha actividad, como resultado de esto, mediante imágenes se ilustran las actividades y resultados de las mismas. La anterior, es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales (Nmap.Org, 2021).

Figura 2: Uso de Zenmap



Fuente: elaboración propia

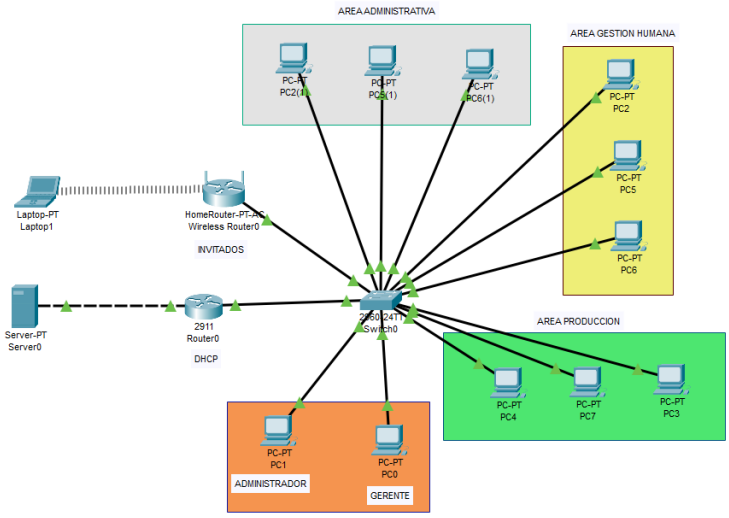
En la Figura 2, se muestra la interfaz de NMAP, la cual cuenta con 4 botones en la barra de herramientas, una barra de Objetivo, Perfil y otra de Comando. cuatro botones de consulta que permiten iniciar la tarea de escáner y un campo donde se reflejan los resultados en este caso de la IP consultada.

IP VERIFICADAS: 10.100.1.151– 10.100.3.8 – 10.100.1.103 – 10.100.1.194 – 10.100.2.248 – 10.100.3.165 – 10.100.3.235 – 10.100.1.138 – 10.100.1.101.

Así mismo, se pudo observar el resultado del escáner de cada IP, con esto ya se verifica que puertos deben de ser tratados y que determinaciones se toman, dejando claro que dicha decisión se toma en reunión coordinada entre los integrantes del grupo y personal de la empresa, ilustrando los riesgos y consecuencias que acarrea el no tratamiento de estos.

A partir del escáner de red y puertos, y después de la reunión de coordinación para la toma de decisiones, en la que se determinaron cuáles puertos deben de ser cerrados y a cuáles dar prioridad. En la Figura 3, se observa cómo se procede a realizar la distribución de áreas y acceso a la red de los integrantes de la organización.

Figura 3: Diagrama de red



Fuente: Elaboración propia

Con la distribución que se realizó por áreas, con previa autorización de quienes representan la organización, se procedió a distribuir los usuarios para cada integrante de la empresa, donde estos deben de grabar la contraseña, la cual contará con los últimos niveles de seguridad como lo es: debe de contener por lo menos una letra mayúscula, minúsculas, números y caracteres, no pueden colocar nombres propios, de igual forma esta contará con un periodo de continuidad, donde cada mes debe de ser cambiada.

Finalizadas estas actividades, se convoca reunión con los miembros de la organización, con el fin de socializar las actividades realizadas, el funcionamiento de las nuevas estrategias y políticas de seguridad de la información implementadas, los beneficios que estas traen tanto para la organización como para los empleados y usuarios.

Con la capacitación de empleados, se procede con las pruebas de conexión, y registros en el servidor, que cada integrante acceda a la red que le corresponda en el área que labora, que no les permita el acceso a otras zonas de la red y que se cumplan las condiciones de seguridad que se establecieron.

FASE IV

Mediante la verificación, reconocimiento de las áreas de trabajo y el componente funcional de la empresa FUNTRAEV, se diseñaron importantes estrategias de seguridad informática, con las cuales se logró dar un entorno más seguro, en el que se minimizaron los riesgos en los que se puede ver afectada la información de la organización, como también el de los empleados y usuarios que desarrollan actividades en la empresa.

Con la verificación y reconocimiento, se procedió con las actividades de mejora, iniciando con la identificación de los componentes con los que cuenta la entidad, entre los que se encuentran, un servidor, un switch, Router, computadores de mesa y portátiles, también las áreas de la organización y las funciones que en esta se cumplen.

Posterior a lo anterior, se procedió con un escaneo detallado de la red, con el fin de identificar esos puertos que nos pueden generar riesgos, de igual forma como se están conectando las áreas y los funcionarios de la empresa, como acceden a los equipos, cómo se comparte la información y donde se está almacenando, con qué frecuencia se hacen las copias de seguridad y en que se realizan.

Ya conociendo todo esto, se realizaron las siguientes actividades así:

- El servidor no se encontró funcionando con los pc de la empresa, por lo que se conectaron todos a este y se realizó la distribución,
- La distribución consistió en dar dirección a los pc hacia el área, a la que pertenece cada funcionario.
- Se escaneo detalladamente la red, cerrando algunos puertos que se encontraban abiertos y no eran utilizados, como también de se dejaron habilitaron los que se requerían.
- Se entregaron los usuario y contraseña a los integrantes de la empresa, generando políticas de seguridad para el manejo de las contraseñas.
- Se denegó el acceso a algunas páginas web en el navegador.
- A todos los pc, se les denegó el acceso a los puertos USB, teniendo en cuenta que es el mayor generador de inseguridad de información.
- Se compartió documento con listado de medidas de seguridad en la seguridad de la información.

3. RESULTADOS

Las actividades de seguridad y restricciones en los sistemas de información se desarrollan mediante CISCO MERAKI (es una de las carteras de negocios de más rápido crecimiento de Cisco y es el líder del mercado en redes administradas en la nube con más de, 250.000 clientes en todo el mundo, 1.5 millones de redes de Meraki conectadas) (Cisco, 2022).

Figura 4: Interfaz de red en Meraki

Fuente: Elaboración propia

En la Figura 4 de la plataforma MERAKI**,** se observa la configuración de IP y los permisos otorgados por parte del administrador al usuario.

Figura 5: Verificación de IP en Meraki

En la Figura 5, correspondiente a la verificación IP Meraki**,** se observa que la IP se encuentra en estado normal, lo que significa que el usuario puede navegar en red, pero con denegación a las políticas de grupo asignado por la organización FUNTRAEV.

Figura 6: Verificación de políticas en Meraki

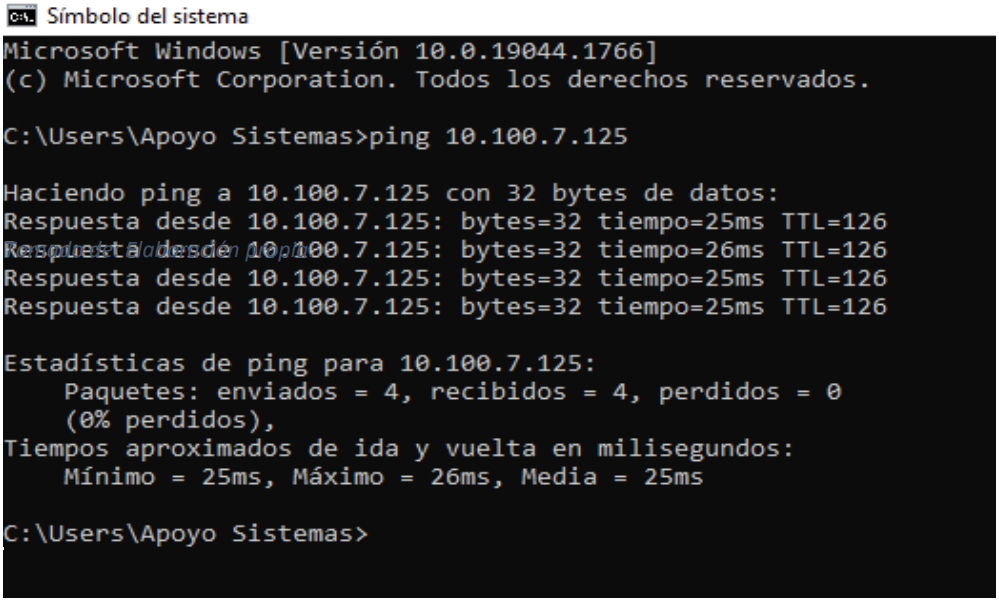
Fuente: elaboración propia

En la Figura 6 de políticas de Grupo Meraki**,** se muestran los tipos de políticas grupales que maneja la empresa FUNTRAEV en las diferentes áreas, como también se observan las políticas que tiene cada área y a su vez las restricciones o reglas aplicadas en cada departamento.

Respecto a la verificación de conexión por áreas entre equipos, mediante la consola de comandos, se realizó verificación de conexión de equipos en la red, donde se buscaba probar la correcta distribución de IP, que cada usuario y área tenga acceso a su entorno laboral sin salirse de los parámetros establecidos.

De la IP 10.100.3.224 perteneciente al área de gestión humana, se realizó PING a la IP 10.100.7.125 perteneciente a esta misma área, la cual arrojo una conexión exitosa como se observa en la Figura 7, PING IP 10.100.3.224 - 10.100.7.125.

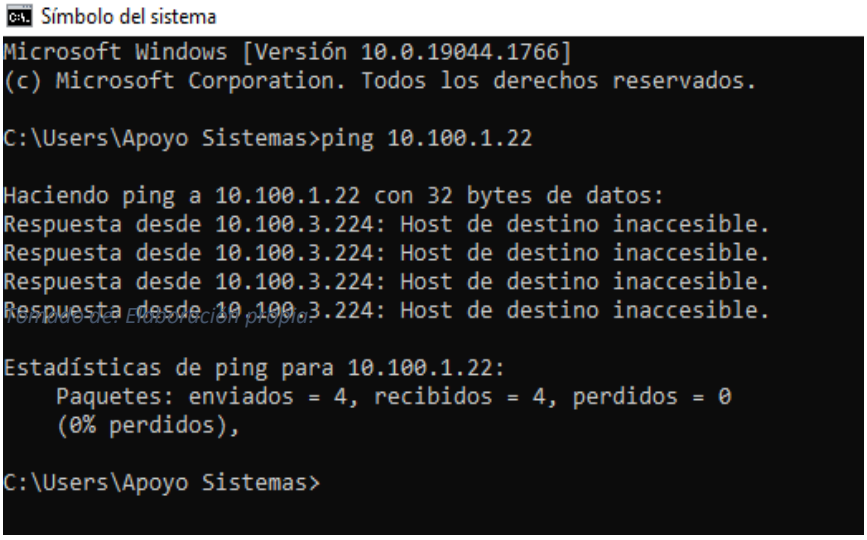
Figura 7: Verificación de conectividad



Fuente: elaboración propia

De la IP 10.100.3.224 perteneciente al área de gestión humana, se realizó PING a la IP 10.100.1.22 perteneciente al área Administrativa, la cual arrojó una conexión no exitosa como se observa en la Figura 8, PING IP 10.100.3.224 - 10.100.1.22.

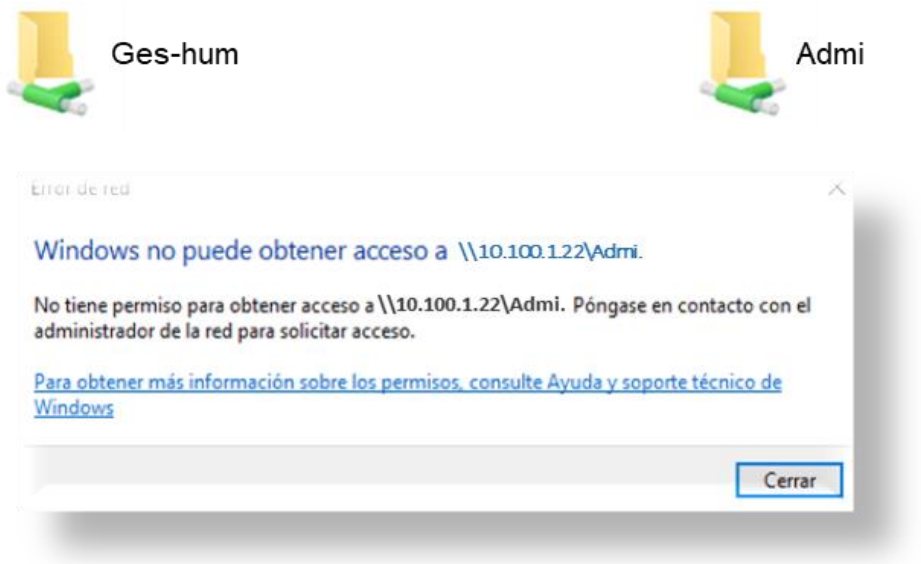
Figura 8: Verificación de no acceso



Fuente: elaboración propia

Este mismo procedimiento se realizó con las IP registradas en la entidad, verificando cada área, donde se estableció que se aplicaron correctamente las políticas de seguridad de la información.

Figura 9: Acceso a carpetas



Fuente: elaboración propia

En la Figura 9, ingreso a carpetas por área, se observa que se intentó ingresar desde un usuario del área de gestión humana a la carpeta del área administrativa, donde se puede evidenciar el cumplimiento a la política de denegación de acceso a los archivos o carpetas de otras áreas de la organización.

Finalmente, a partir de la implementación de estas políticas, se logró redactar el documento oficial "*compromisos con el sistema de gestión de seguridad de la información"*, en el cual cada uno de los integrantes de la empresa FUNTRAEV, se comprometen al cumplimiento de las políticas de seguridad de la información y las buenas prácticas que se deben de mantener en la entidad.

4. DISCUSIÓN

Según lo propuesto por Soriano (2014) dónde nos ilustra de una manera más concreta que el concepto de seguridad de la información debe de tomarse como aquel mecanismo que se debe utilizar para proteger la información y los sistemas del acceso, el uso, la divulgación, modificación o alteración, lectura, inspección, registro y todo aquello que puedo generar pérdida de la información secuestro de esta. Se espera que después de la ejecución de este proyecto y la capacitación de los empleados**,** se pueda brindar una mejora en la seguridad y tratamiento de la información a nivel interno. Adicionalmente, siguiendo lo indicado por Acevedo et al (2009) también que los usuarios externos o internos de la entidad accedan a la información de manera restringida, teniendo en cuenta su rol o cargo, de igual forma que cada área cuente con una sola ruta de acceso y que la información allí almacenada sólo se pueda tratar entre ellos.

5. CONCLUSIONES

A partir de la revisión de literatura, se encontró que existen diferentes factores que pueden afectar la seguridad de la información de las organizaciones. Pero, no todas tienen en cuenta al momento de realizar la implementación de la red de telecomunicaciones, los diferentes aspectos y configuración específica que se debe tener en cuenta de acuerdo con los requerimientos de seguridad de la organización. Esto, dada la importancia que tiene la seguridad de la información tanto para la organización como para empleados y usuarios, desconociendo que un mal manejo de esta generaría inconvenientes internos y penales ante la justicia.

Continuando con las investigación desarrolladas para ampliar el conocimiento de lo que está pasando en el mundo actual con la seguridad de la información, mediante consultas realizadas a personas que tienen o tuvieron a su cargo empresas u organizaciones, manifiestan que conocen la importancia de la seguridad de la información, sin embargo muy pocos la implementan de manera correcta y con los estándares de calidad requeridos, esto por motivos de costos que genera el manejo y control de los sistemas de información que tenga la entidad, adquisición de equipos y demás software necesarios.

Sin embargo y con el fin de conocer otros puntos de vista, se tomaron los conceptos que tienen los empleados de la empresa, quienes tienen acceso directo a la información y son los responsables alimentan las bases de datos con la información de otros usuarios o bienes de la empresa, donde reconocen lo importante que es la implementación de políticas de seguridad y los beneficios que esto trae para su actuar diario.

Se observó que los empleados, aunque no conocían mucho del tema, aplicaban métodos no convencionales, pero que para ellos eran útiles y que les aseguraban la información, cuando se les planteó las metodologías convencionales y como estas ayudan a la conservación y manejo de la información, decidieron buscar capacitaciones en estos temas y que la empresa las implementara para con esto evitar eventualidades en las que se pueda ver en peligro sus datos e información.

Conocidos estos criterios, se desarrolló el presente proyecto, enfocado en dar solución a todas esas falencias que se evidenciaron y que serían de gran aporte para la entidad u organización, cada paso desarrollado era evidenciado por los integrantes de la empresa, donde reconocían el trabajo y como este les permitía estar más seguros al momento de almacenar información.

A partir de la implementación de las políticas de seguridad, la distribución de la red y la capacitación realizada, se evidencio que cada integrante de la empresa, se acopló rápido al cambio y no se vio afectado su proceso laboral, por el contrario, se resaltó la actividad realizada y cómo este proceso de modernización en la empresa ayudó a darle un orden a las áreas y la información.

6. REFERENCIAS

Acevedo, I., Giménez, J., Etreros, J., Muñoz, J., & Vaquerizo, C. (2009, January). Algunas consideraciones sobre seguridad de la información en el proyecto europeo de historia clínica digital (Proyecto EPSOS). *ISSN 1133-7400*, 87–98.

Cisco. (2022). *Meraki*. Obtenido de https://meraki.cisco.com/es-co/

Bagchi, S., Abdelzaher, T. F., Govindan, R., Shenoy, P., Atrey, A., Ghosh, P., & Xu, R. (2020). New Frontiers in IoT: Networking, Systems, Reliability, and Security Challenges. *IEEE Internet of Things Journal*, *7*(12), 11330–11346. https://doi.org/10.1109/JIOT.2020.3007690

Dussan, A. (2006). *Políticas de seguridad informática* (1st ed., Vol. 2). 2006.

Instituto Nacional de Ciberseguridad. (2010). *Colección Protege tu Empresa*.

Nmap.Org. (2021). *Nmap*. Obtenido de https://nmap.org/zenmap/

Ramos, F., & Gabriel, R. (2021). Análisis y diseño de un sistema de gestión de seguridad de la información basado en la norma NTP – ISO/IEC 27001:2014 en la empresa consultora N&V asesores SAC. *Escuela de Ingeniería de Sistemas*.

Riascos Erazo, S. C., Aguilera Castro, A., & Ávila Fajardo, G. P. (2014, May 15). *Seguridad de los sistemas de información en las Pymes de Santiago de Cali (Colombia)*. Riascos, ET AL.

Rivas, G. (2017, March 28). *11 Datos increíbles sobre seguridad digital que te conviene conocer*. Gb Advisors - Tech-Blog. www.gb-advisors.com/es/11-datos-increibles-sobre-seguridad-digital/

Soriano, M. (2014). *Seguridad en redes y seguridad de la información* (Primera edición, Vol. 1).

Villaverde, exicoLuis, Cabrera, J., Parra, J., Olivares, S., Ochoa, A., Mata, W., Ceja, L., & Martinez, R. (2021, December 31). An´alisis de Cultura de Seguridad Inform´atica. *Difusión Científica, Ingeniería y Tecnologías*, 1–9.