UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCION DEL TITULO DE INGENIERA EN SISTEMAS

TEMA

ANALISIS DE LA ESTRUCTURA DE RED DE LA EMPRESA DANICA FRUITS S.A EN LA CIUDAD DE BABA

EGRESADO

DANIELA MARISOL OLVERA MACIAS

TUTOR

ING. CARLOS ALFREDO CEVALLOS

AÑO

2022

RESUMEN

La gestión actual de LAN y WAN permite a las empresas y las organizaciones optimizan el uso de recursos a través de una red centralizada que permite una entrega de información rápida y segura.

El presente estudio busca conocer, analizar y recomendar acciones que vayan direccionadas a solucionar los inconvenientes existentes. Integrando los conocimientos adquiridos para optimizar la infraestructura de red implementada en la empresa Danica Fruits S.A.

Posterior al análisis realizado, se definió la importancia que representa la seguridad, el control y mantenimiento que requiere una red a nivel empresarial. Aplicando estos protocolos se obtendrá un mayor rendimiento y, por ende, existirán menos riesgos para la red de ser intervenidas por ciberdelincuentes.

Palabras claves: LAN, Infraestructura de red, Seguridad, Red, Gestión.

ABSTRACT

Current LAN and WAN management allows companies and organizations to optimize the use of resources through a centralized network that allows fast and secure information delivery.

The present study seeks to know, analyze and recommend actions to solve the existing problems. Integrating the acquired knowledge to optimize the network infrastructure implemented in Danica Fruits S.A. company.

After the analysis, the importance of security, control and maintenance required by a network at enterprise level was defined. By applying these protocols, a higher performance will be obtained and, therefore, there will be less risks for the network to be intervened by cybercriminals.

Keywords: Local Area Network, Network infrastructure, Security, Network, Management

INTRODUCCION

Por lo general, las empresas que utilizan computadoras para satisfacer sus necesidades de información suelen comenzar con unas pocas computadoras y algunos periféricos. Sin embargo, los recursos de hardware y software para la gestión de la información van aumentando paulatinamente. Esta extensión suele estar relacionada con problemas de redundancia en software, datos, hardware, etc. Una red de área local (LAN) permite que varias computadoras y dispositivos periféricos se conecten para que puedan conectarse y compartir recursos.

El presente estudio de caso tiene como propósito analizar la red de información en la empresa Danica Fruits S.A, para posteriormente, brindar sugerencias que permitan las posibles soluciones de mejora en el aspecto estructural interno de la red.

Cabe destacar que la línea que se aplicó al presente trabajo de investigación fue la línea de sistemas de información y comunicación, emprendimiento e innovación, y en la sub línea de investigación que comprende las redes y tecnologías inteligentes de software y hardware.

Para el presente estudio de caso se procedió a utilizar la encuesta como instrumento de recopilar información relevante acerca de la empresa, su gestión y manera de llevar a cabo sus diversas actividades. Sirviendo esta recopilación como base para haber obtenido un criterio acorde a las carencias e ineficiencias presentadas en la red.

DESARROLLO

Normalmente en las empresas se suele manejar las topologías físicas para mantener conectados todos los dispositivos entre sí. Por lo general este de red tiene relación con la configuración de cables, pcs y otros periféricos. La topología física no debería confundirse con la topología lógica, que es el procedimiento usado para pasar información entre estaciones de trabajo.

En redes, el concepto "topología" hace referencia al diseño de los dispositivos conectados en una red. Hay diversos tipos de topología de red. Uno puede pensar en una topología como la manera o composición virtual de una red. Esta manera no corresponde precisamente con el diseño físico real de los dispositivos en la red. Ejemplificando, las pcs en una LAN doméstica tienen la posibilidad de estar dispuestas en círculo en una habitación familiar, sin embargo, podría ser bastante poco posible que esté una topología de anillo real ahí. Se ordenan en los próximos tipos básicos.

- Topología de las estrellas
- Topología de anillo
- Topología de bus
- Topología de árbol
- Topología de malla
- Topología Híbrida

La información que se tratara en esta situación de análisis, es para llevar a cabo los beneficios y desventajas que reflejan a la examinar los peligros informáticos que hay en la empresa y contribuir a que existan mejoras para el mismo, siendo de esta forma una ayuda que se verá reflejada con acontecimientos a futuros, realizando que se vuelva incierta.

- La información que se ejecute en cualquier compañía debería continuamente consumar con las normas establecidas en lo cual es la estabilidad informática.
- La estabilidad informática se debería tener puntos, donde se debería de llevar a cabo, y a su vez se debería de eludir.
- Se debe realizar. Esto es, utilizar sistema de antivirus y conservar una contraseña periódicamente cambiante, conservar un respaldo de la información que se tiene de los usuarios, cifrar archivos importantes.
- Una vez que cubrimos lo que se debe y no se debe hacer, debemos considerar el uso de Wi-Fi abierto, lo que conlleva el riesgo de que se guarde información, lo que lleva a enlaces sospechosos o filtraciones de Wi-Fi.

Seguridad informática

Es brindar estabilidad y seguridad a la información institucional que se manipula por usuarios internos y externos de la Corporación, aplicando mecanismos de estabilidad informática que garanticen la confidencialidad, totalidad y disponibilidad de los sistemas de información. (Duque, Eliecer, Ortiz, Iragorri, & Hoyos, 2017). Es por esto que se debería de precautelar en conservar la información de forma que la organización brinde la confianza, totalidad y sobre todo la seguridad de lo que reposa en ella.

A demás la estabilidad de la información, ayuda que la organización se encuentre preparada para cualquier ataque cibernético y logre atender paulatinamente, lo cual le está sucediendo y darles prioridad a las cosas, como lo sugiere (Empresas, 2018) "El proyecto de estabilidad informática para la compañía va a poder decidir cuál emergencia atender en primera instancia, y de manera constante**"** Esto asegura una acción consciente y prudente en el proceso de toma de decisiones.

En cuanto a la empresa DANICA FRUIT S S.A que se encuentra ubicada en el cantón baba perteneciente a la provincia de Los Ríos, teniendo en cuenta el acuerdo del esquema 166 nos indica "Que, es fundamental adoptar políticas, tácticas, reglas, procesos, métodos, tecnologías y medios necesarios para conservar la estabilidad en la información que se crea y protección en diferentes medios y formatos de las entidades de la Gestión Pública Central, Institucional y que están sujetas a la Funcionalidad Ejecutiva." Es por esto que se debería de utilizar las reglas estipuladas en la administración de estabilidad informática para evadir que exista la vulnerabilidad al instante de retener información y que sean atacados por Hackers. (Castillo Peñaherrera, 2013)

Políticas de Estabilidad de defensa y respaldo a la Información

En esta situación de análisis se aplicaría lo cual es la regla ISO/IEC 27002:2005 – Código para la Práctica de la Administración de la Estabilidad de la Información El cual ayudaría a que la información que está siendo procesada en la Compañía sea protegida evitando perdidas de información. (Especial, 2018).

ISO 27005

Además, se podría ejercer lo cual es la regla ISO 27005: es una guía de sugerencias respecto a cómo abordar la administración de peligros de estabilidad de la información que logren comprometer a las empresas. No especifica ni una metodología de estudio y administración de peligros concreta, sin embargo, incluye ejemplos de probables amenazas, vulnerabilidades e impactos." Se conserva la información segura y se analizaría y se gestionaría los peligros concretos, realizando que se defina la vulnerabilidad del caso y su efecto de lo cual podría ocurrir, si o se toma presente las medidas de prevención. (Información, 2016)

Se puede hacer una estimación de cualquier problema que puede surgir, ejemplo en un incendio en las horas laborables.

- Notificar a las oficinas de Estabilidad de la Información de la Organización.
- Solucionar y restablecer el servicio perjudicado por el incidente gracias a la par de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes.

En la actualidad cada comercio está conectado a Internet y cada red de comercio es parte de Internet. La capacidad para interactuar entre si es una sección clave de este ámbito donde el peligro va siendo creciente. Los ciber-delitos y el ciber-espionaje incrementan los peligros en la fama, en las operaciones, en el rendimiento financiero y en la postura competitiva en el mercado. Se observa en la sociedad de la cual formamos parte un aumento sin antecedente de los peligros debido al creciente nivel de digitalización de la información multimedia donde se ha pasado por diferentes estadios, a partir de la mensajería, al almacenamiento de información, a los sistemas transaccionales, a la incorporación de tecnologías e inclusive a los negocios basados en la total unión de la información.

¿Cómo hacer un estudio de la red de tu empresa?

Hacer un estudio de la red de tu organización posibilita asegurar su buen desempeño y, por consiguiente, contar con el marco correcto para que las aplicaciones empresariales de administración, ventas y comunicación funcionen de forma óptima. Para hacer un estudio profundo y efectivo de la red de una compañía se necesita considerar una secuencia de componentes como la infraestructura de la red, los dispositivos que permanecen conectados, la función de la red y las medidas de ciberseguridad implementadas (ambit, 2020).

¿Por qué hacer un estudio de la red de tu compañía?

Hacer un estudio o una auditoría de la red de una compañía posibilita obtener una perspectiva real del estado de la misma, logrando identificar errores, brechas de estabilidad o infraestructuras obsoletas o con un manejo deficiente. La auditoría de red posibilita conocer el cómo está la red a grado físico y lógico, y hallar qué grupos y cómo se conectan a la red. (ambit, 2020)

¿Cómo hacer un estudio de la red de tu compañía?

Para hacer un estudio de la red se necesita hacer revisiones de estabilidad físicas (orientada a conocer y evaluar el hardware y el cableado) y revisiones lógicas (que poseen como objetivo revisar y evaluar medidas de defensa sobre la información y los procesos).

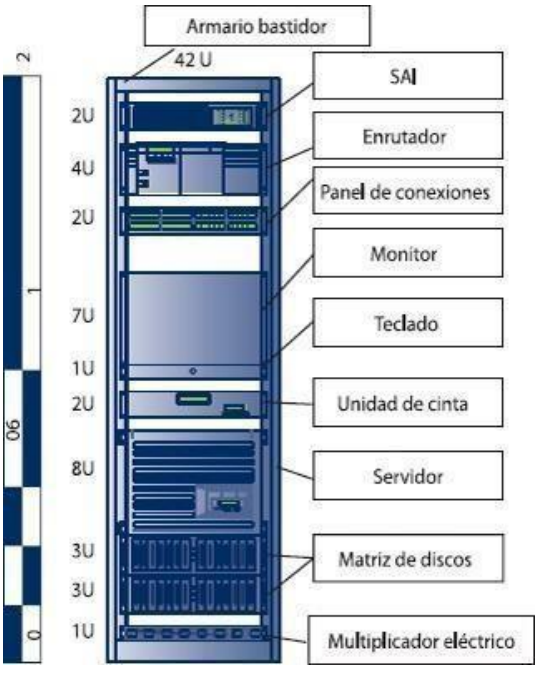
Análisis de la infraestructura

La infraestructura de TI es parte importante, por lo cual se necesita hacer una revisión y comprobación de todos los recursos de hardware que intervienen en la red de la compañía.

Rack

El rack es el soporte, mueble o armario donde se alberga equipamiento informático y comunicación de la organización. En él suele hallarse el servidor, el switch primordial, el patch panel, el router y otros recursos informáticos (a modo de ejemplo, un sistema de ingesta de alimentos ininterrumpida SAI). El rack es una sección importante de la red de la organización puesto que es donde se hallan varios de los dispositivos básicos de la red. Al revisar el estado del rack se debe tener varios componentes presente como la temperatura ambiente (ver si dispone de medidas de refrigeración como ventiladores o viento acondicionado), el aseo (el polvo suele acumularse en los armarios dañando los dispositivos), el estado de los cables de red y su organización (la proporción de cables en un rack podría ser bastante enorme ya que cada una de las conexiones de red irán a él), y la sujeción y repartición de los diversos dispositivos dentro del rack (evitar dispositivos superpuestos, anclaje de dispositivos para eludir vibraciones, etcétera.). (ambit, 2020)

Imagen 1



Fuente: (Online, 2020)

Router

La conexión a internet se hace por medio del router proporcionado por el abastecedor de servicios. Es fundamental revisar que el router dispone de las últimas tecnologías en comunicación para asegurar que la conexión a internet de la organización sea lo más veloz y estable viable. Ciertos de los puntos a evaluar son: si dispone de banda dual para transmisión de datos por diversas frecuencias, estándar WI-Fi 802.11ac, MU-MIMO para lograr proporcionar datos simultáneos a diversos dispositivos, control de ancho de banda (para eludir que cualquier dispositivo conectado acapara el ancho de banda), puertos Gigabit ethernet (velocidades de hasta 1000 Mbps), cifrados de estabilidad modernos y antenas externas que dan más alcance de la señal WI-Fi. (ambit, 2020)

Imagen 2

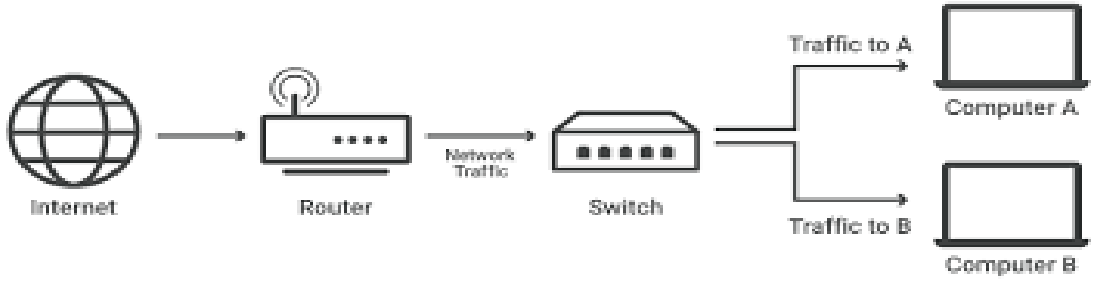
Fuente: (Morelo, 2021)

Switch

El switch posibilita repartir de manera inteligente la información por medio de los diversos dispositivos que se conectan a la red por ethernet. Es fundamental revisar que los switches que use la organización no se encuentren limitando la rapidez de transferencia (es usualhallar switches obsoletos 10/100 que no son capaces de transmitir a 1000 Mbps y permanecen limitando la comunicación de la red empresarial).

En este apartado es fundamental que las conexiones de los cables ethernet al switch, patch panel y en la entrada final se encuentren marcadas, para de esta forma poder detectar cualquier problema fácilmente. En caso de que cualquier punto no se encuentre marcado, debería ser reconocido y proceder a etiquetarlo para minimizar la era de mediación frente a un futuro problema de conectividad.

Imagen 3



Fuente: (cloudflare, 2021)

Puntos de ingreso AP

Los puntos de vista de ingreso se delegan de repartir por las diferentes regiones de la organización la señal Wi-Fi. Para eso, dichos dispositivos se conectan a un punto ethernet de la red y producen una señal Wi-Fi, permitiendo que los dispositivos se conecten a la misma como si se tratase de la señal primordial del router. Es fundamental revisar que los AP (access point) se encuentren localizados en las superiores regiones para lograr cubrir de manera óptima el área de trabajo de la organización. En caso de no estar bien colocados se deberá replantear su localización, aumentar nuevos puntos de vista de ingreso o sustituirlos por modelos con más alcance. (ambit, 2020)

Tipo de cableado

El cableado de la red es determinante para que cada dispositivo tenga una entrada óptima a la misma. En este aspecto se debe verificar que el cable usado sea por lo menos de categoría 5e o 6 (cat 5e o cat 6, o superior) para eludir que limite la función de transferencia delos datos por la red. Si alguno de los cables que se aplican está en mal estado o no cumple conla categoría mínima elemental tendrá que ser sustituido. Otros puntos a verificar en el cableado son los conectores RJ45 de los cables y las rosetas RJ45 de pared. Frecuentemente los inconvenientes de red de cualquier dispositivo de la organización permanecen ocasionados porun conector o roseta estropeado o con cualquier cable suelto. Dichos conectores deteriorados tienen que ser reemplazados por unos nuevos.

Unidad NAS

Si la organización usa un dispositivo NAS para copias de estabilidad e ingreso a la información es fundamental revisar que el mismo cuente con una conexión ethernet idónea y esté conectado a una unidad SAI (para en caso de caída de la red eléctrica tener tiempo de hacer una réplica de seguridad).

Servidor Firewall

Si la organización cuenta con un cortafuego físico se debe comprobar que esté bien situado dentro del rack y que cuente con conexión ethernet Gigabit.

Servidor y pcs

El servidor de la compañía es el que suministra a los diversos dispositivos por medio de la red, como pcs, portátiles e impresoras, la información y las aplicaciones correctas para los diversos procesos. El servidor debería disponer de una buena localización dentro del rack que posibilite entrar al mismo en caso de necesidad, debería contar con conexión a la red Gigabit, estar conectado a una SAI y contar con refrigeración suficiente para que su manejo

sea el óptimo (impidiendo que baje el rendimiento, se apague o se deterioren sus partes internas). Se debe revisar que todas las computadoras que se conectan a la red cuentan con tarjeta ethernet Gigabit para evadir que ningún puesto tenga reducida su rapidez de ingreso a la red. Los deteriorados tienen que ser reemplazados por unos nuevos.

Auditoría de dispositivos

Con la herramienta idónea es viable consultar qué conjuntos se hallan conectados a la red obteniendo información fundamental sobre los mismos. Con esta información se puede producir un informe que contenga todos los datos referentes a los diversos dispositivos que accedan a la red. El informe de auditoría de dispositivos se va a tener información fundamental de los dispositivos como:

- Nombre del dispositivo.
- Dirección MAC del dispositivo.
- Dirección IP a partir de la que se conecta a la red.

Disponiendo de esta información se va a tener una perspectiva real de la red y se van a poder ejercer medidas como delimitar ingreso a la red por la dirección MAC para aumentar las medidas de estabilidad (listas de control de ingreso en routers), o identificar dispositivos no autorizados que permanecen accediendo a la red (por ejemplo, dispositivos móviles particulares o de individuos ajenas a la empresa).

Ancho de banda y alcance de la red inalámbrica

Las redes empresariales recientes contarán con ciertos servicios subcontratados a organizaciones externas proveedoras de servicios. Dichos servicios tienen la posibilidad de ser escritorios remotos, aplicaciones o almacenamiento en la nube y semejantes. Por dicha razón es fundamental que la conexión a internet de los dispositivos conectados a la red empresarial sea el óptimo.

Una de las primeras cosas a verificar va a ser si el router está ofreciendo todo el ancho de banda contratado. Para eso se debe verificar con un equipo conectado de manera directa a un puerto ethernet del router si se alcanza el más alto de Mbps (realizando ejemplificando cualquier examen en línea o con un instrumento específica). Además, es fundamental verificar que todos los dispositivos tienen ingreso al ancho de banda que corresponde, tomando medidas en la situación de que no lleguen a esa rapidez (revisión de cableado, inconvenientes de configuración del dispositivo, etcétera.). (ambit, 2020)

Actualmente la utilización de dispositivos móviles en el trabajo (como tabletas y Smartphones) son usuales por lo cual se necesita que la red Wi-Fi de la organización llegue a todos los sitios de la oficina o del sitio de trabajo. En este aspecto se debe verificar que la entrada a la red por Wi-Fi a partir del router y los puntos de vista de ingreso de las instalaciones de la organización funcionen de manera correcta y abarquen toda la zona disponible. En caso de hallar regiones sin cobertura tienen la posibilidad de tomar medidas correctoras para solucionarlo (instalación de más dispositivos AP, reubicación de AP o cambio de router). (ambit, 2020)

Seguridad de la red

La ciberseguridad pertenece a los aspectos que se debe comprobar al examinar una red empresarial para de esta forma asegurar que no hay vulnerabilidades y minimizar el número de amenazas a las que está expuesta. Se necesita que la revisión técnica de estabilidad tenga presente los protocolos y dispositivos usados para lograr identificar debilidades y corregirlas (incluso llegando a simular ataques a la red para evaluar vulnerabilidades y medidas de seguridad).

Según (Cisco, 2021), el escaneo de puertos es una técnica utilizada por los atacantes para detectar servicios vulnerables, y por lo tanto perpetrar un ataque. Cada máquina conectada a una red de área local (LAN) o Internet ejecuta diferentes servicios escuchando en puertos conocidos y desconocidos.

El escaneo de puertos ayuda a los atacantes a localizar qué puertos aún están disponibles, básicamente, el escaneo de puertos envía un mensaje a cada puerto a la vez. El tipo de respuesta recibida indica si el puerto está escuchando, por lo que se pueden realizar más pruebas para determinar el agotamiento.

Metodología aplicada en este estudio

Es importante resaltar que la línea de investigación aplicada a este estudio es: Sistemas de información y comunicación, emprendimiento e innovación. Y la sub línea corresponde a: Redes y tecnologías inteligentes de software y hardware.

De la misma manera, se utilizó la encuesta como instrumento de recolección de datos, la misma que permitió conocer a detalle las opiniones y por ende obtener información relevante referente a la empresa.

Para el presente trabajo se utilizó el método cuantitativo, el mismo que se basa en la medida de un fenómeno, cuantificada y numéricamente representada por un parámetro estudiado en una población.

Recursos de la empresa

Es preciso destacar los recursos que posee la empresa que ha sido objeto del presente estudio de caso.

Recursos de la empresa Danica Fruits S. A	
Hardware	**Software**
Router	Antivirus
Cableado estructurado	Sistema operativo Windows
impresora	Correo electrónico
Computadora de escritorio	Base de datos

Tabla 1. Recursos de la empresa

Elaborado por: Daniela Olvera Macías

La investigación de la estabilidad de la red debería atender a estándares de estabilidad, marcos de alusión y requisitos que deban ser cumplidos. Ciertos puntos a considerar en la red en relación a estabilidad son:

- Revisión de tipos de contraseñas usadas para identificar si son contraseñas seguras.
- Revisión del programa de custodia como antimalware y cortafuegos por programa, prestando particular atención a si se hallan de manera correcta actualizados a su última versión.
- Uso de dispositivos de estabilidad como detectores de huellas, tarjetas identificadoras u otros sistemas semejantes.
- Revisión de los sistemas de copias de estabilidad local, por red o en la nube y recuperación frente a desastres.
- Disponibilidad de un sistema alternativo de conexión a internet por si la entrada primordial no está disponible (como ingreso alternativo con router 5G).

Al hacer un estudio de la red de tu organización tendrás la posibilidad de tener una perspectiva universal y real de cuál es el estado en el cual está la misma, tanto de infraestructura como de ciberseguridad. Tras un estudio intensivo de la red se van a poder identificar fallos, dispositivos obsoletos, cuellos de botella, vulnerabilidades y otros puntos negativos que tienen la posibilidad de influir al desempeño óptimo de la red empresarial. Con esta información se van a poder ejercer medidas correctoras idóneas para lograr un desempeño eficiente de la red de la organización que posibilite hacer los procesos de comercio de manera dinámica y óptima.

¿Por qué es importante contar con herramientas de ciberseguridad en tu empresa?

- Los datos de la encuesta de CISCO muestran que el delito cibernético es relativamente más rentable que todo el tráfico de drogas del mundo combinado.

- En una red oscura, se puede obtener herramientas profesionales para piratear todo tipo de red.

- La investigación de Netscout muestra que solo se necesitan 5 minutos para piratear un dispositivo IoT desprotegido.

- Según IBM, solo el 38% de las empresas de todo el mundo anunciaron que están equipadas y listas para responder de manera efectiva contra los ataques remotos con gran valor. (InfoSecurity, 2022)

Herramienta

Wireshark

Imagen 4

Fuente: (Darkcrizt, 2020)

Los inconvenientes que este programa es capaz de llegar a abordar van a partir de paquetes caídos, inconvenientes de latencia y hasta actividad maliciosa en su red, ejemplificando, mediante pedidos HTTP. Posibilita examinar la red como si viéramos una placa con un microscopio en un laboratorio por de esta forma decirlo y da herramientas y comandos para filtrar y examinar con más detalles el tráfico de red, acercándose a la causa raízdel problema. (Altube, 2021)

Los administradores de sistemas y de red lo utilizan para detectar dispositivos defectuosos que permanecen descartando paquetes, inconvenientes de latencia en pedidos causadas por máquinas defectuosas que en rutan el tráfico de red a cualquier lado de todo el mundo viable y ex filtraciones de datos o inclusive intento de ataque con malware o de piratería contra una organización. Se encuentre analizador de redes es un instrumento poderoso que necesita un entendimiento sólido de los conceptos de estas mismas. Aquello se traduce para las organizaciones de en la actualidad modernas en entender sobre protocolos HTTP y sus servicios, la pila de TCP / IP, examinar y entender los encabezados de los paquetes que se reciben con varios metadatos algunas veces complicados, así como el enrutamiento y como se entrelazan unos a otros, el reenvío de puertos y DHCP, ejemplificando. (Altube, 2021)

Características

Podríamos redactar solo un artículo nombrando las propiedades primordiales y todos sus poderes y que abanico de oportunidades nos traen, sin embargo, solo las comentaremos brevemente por arriba.

- Posibilita continuar el rastro a los paquetes TCP stream, tenemos la posibilidad de ver todo lo referente con dicho paquete, el previamente y el luego, logrando aplicarles filtros personalizados a dichos mismos sin perder el flujo.
- Se puede decodificar los paquetes y exportar en formatos específicos y guardar estos objetos.
- Posibilita ver estadísticas de los paquetes capturados incluyendo un resumen, jerarquía de protocolos, conversaciones, puntos de vista finales y gráfica de flujos entre otros.
- Estudio simple e informativo por medio de resolución de nombres por Mac, por red y reensamblaje de paquetes.
- Cuenta con un instrumento de líneas de comandos para llevar a cabo funciones llamada TShark, semejante al terminal de Linux. Entre los comandos más destacados, tenemos la posibilidad de nombrar rawshark, editcap, mergecap, text2pcap.

Ventajas y desventajas de uso

Whireshark siendo un programa tan enorme y robusto analizador de red y paquetes, es casi evidente que tiene más ventajas que desventajas, muchas más. Es lo cual provoca que sea un programa tan utilizado y conocido. Una vez que lo empiecen a utilizar se darán cuenta de todo lo que permite realizar.

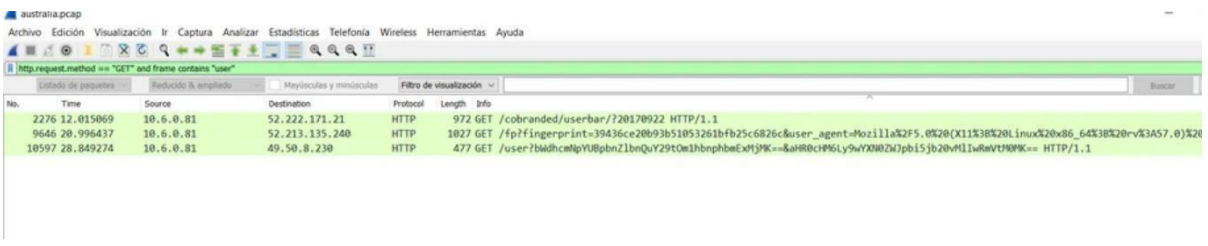
Entre sus ventajas más destacadas pudimos encontrar que tiene un soporte detrás de aquellas analíticas que saca brutal, con mucho personal al mando de novedosas funcionalidades, parches y solucionando errores que la sociedad detecta, aquello incluye su documentación vasta y no bastante laboriosa de leer y utilizar, aparte además cuenta con una sociedad monumental, que ayuda a la mínima de cambio una vez que alguien requiere buscar algo bastante específico en aquellos paquetes de red y disectores. Captura además toda clase de paquetes al examinar la red. Muestra errores y inconvenientes en niveles por abajo del protocolo HTTP. Guardar y restablecer los datos empaquetados capturados, en ficheros pcap. (Altube, 2021)

Entre sus desventajas, que además tiene, aunque sean lo de menos trascendencia, cabe resaltar que al examinar la red no se pueden cambiar datos de los paquetes, solo por medio de ficheros de red, sus pcap. Y la interfaz que usa no está mal, sin embargo, es poco intuitiva y se le podría ofrecer un pulido y ponerla más servible e intuitiva. (Altube, 2021)

Uso práctico y sencillo

Por medio de este ejemplo en la interfaz verán como hacer una averiguación por medio de GET para sacar solo los paquetes que nos interesan y no varios otros que no nos aportan nada. Tenemos la posibilidad de buscar de hecho protocolo, así sea GET, POST o cualquier otro y utilizando el operador “and” unirlo y concatenar dicha averiguación con más fronteras, como que aquellos paquetes contengan en la ruta cierta cadena, como la de “user”

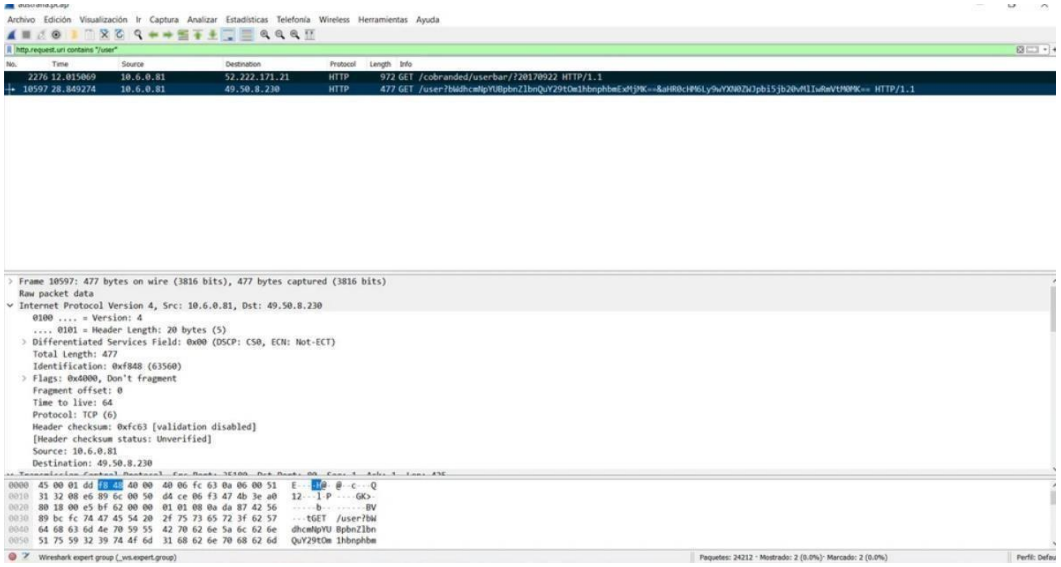
Imagen 5



Fuente: El Autor

O los tenemos la posibilidad de buscar para que en la url contenga “/user” que tal vez nos de algo más preciso en la url, como es esta situación, empero no supone que esto funcione continuamente.

Imagen 6



Fuente: El Autor

Finalmente se tratará en un fichero pcap, de hacer muchas búsquedas y rebuscar entre los paquetes, sus raw y demás información hasta obtener alguna incidencia. Finalmente va a ser un trabajo arduo, debido a que un estudio de red tiene muchísima información y no es simple identificar salvo que tengamos indicios claros, de dónde puede provenir cualquier actividad maliciosa o fuera de sitio en nuestra red. (Altube, 2021) Con cada acceso de datos, tendremos la posibilidad de desplegar y ver en detalle todo el paquete de datos, tanto a grado de aplicación, transporte, a grado de red, enlace y además a grado físico, o sea, Wireshark nos proporcionará la información por capas, para hallar más de forma fácil la información que nosotros mismos requerimos saber.

CONCLUSIONES

Al analizar la estructura de red existente en la empresa Danica Fruits S.A, se determinó las debilidades, vulnerabilidades y necesidades. Las mismas que han tenido presencia desde hace tiempo, y que gracias a este estudio se pudo descubrir y así tener un horizontedefinido en cuanto al direccionamiento de las posibles acciones que permitan optimizar las falencias.

Se pudo evidenciar los riesgos que representa la estructura de red implementada, ésta estructura hace referencia a la topología de bus pudiendo derivarse esto en futuras intervenciones de terceros, aprovechando las brechas que posee. Es por esto que se recomienda aplicar la topología de estrella, debido a su óptima funcionabilidad. Además, recomendar planes de contingencia que permitan salvaguardar información.

Es importante hacer cumplir una política de privacidad clara y revisarla con regularidad para evitar la pérdida o el desglose de la información. Esto debe ser responsabilidad de los empleados de la empresa o asignado a una agencia externa.

Ethernet ha sido durante mucho tiempo el estándar por defecto en las LAN. Su simplicidad y amplia aplicación la convierten en una tecnología muy popular en las redes TIC modernas. Por tal razón merece que las revisiones sean constantes, aplicandoprotocolos de seguridad que refuercen su funcionalidad.

BIBLIOGRAFIA

Altube, R. (7 de enero de 2021). *openwebinars*. Obtenido de Wireshark: Qué es y ejemplos de uso: https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/

ambit. (17 de 11 de 2020). *ambit-bst*. Obtenido de ¿Cómo hacer un análisis de la red de tu empresa?: https://www.ambit-bst.com/blog/c%C3%B3mo-hacer-un-an%C3%A1lisis-de-la-red-de-tu-empresa

Castillo Peñaherrera, C. (2013). *ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION EGSI.* SECRETARIO NACIONAL DE LA ADMINISTRACION PUBLICA.

cloudflare. (23 de noviembre de 2021). *cloudflare*. Obtenido de What is a network switch? | Switch vs. router: https://www.cloudflare.com/learning/network-layer/what-is-a-network-switch/

Darkcrizt. (3 de abril de 2020). *desdelinux.ne*. Obtenido de Después de parches de emergencia, llega la nueva versión de Wireshark 3.2.0 con estos cambios: https://blog.desdelinux.net/despues-de-parches-de-emergencia-llega-la-nueva-version-de-wireshark-3-2-0-con-estos-cambios/

Duque, Y. G., Eliecer, J., Ortiz, C., Iragorri, D., & Hoyos, E. (2017). *PLAN DE SEGURIDAD INFORMÁTICA.* Popayán: CORPORACIÓN AUTÓNOMA REGIONAL DEL CAUCA.

Empresas, B. d. (22 de Julio de 2018). *Plan de seguridad informática para una empresa.* Obtenido de uss: https://uss.com.ar/corporativo/plan-de-seguridad-informatica-para-una-empresa/

Especial, U. A. (2018). POLÍTICAS DE SEGURIDAD DE PROTECCIÓN Y RESPALDO

DE INFORMACIÓN. *Universidad Administrativa Especial de Rehabilitación y Mantenimiento Vial*, 9.

Información, C. d. (2016). ISO 27000 y el conjunto de estándares de Seguridad de la Información. *intedya*, S.P.

Morelo, D. (15 de diciembre de 2021). *netspotapp*. Obtenido de Por qué es posible que desee iniciar sesión en su router WiFi y cómo hacerlo: https://www.netspotapp.com/hardware/es/how-to-log-into-router/

Online, R. (25 de mayo de 2020). *rackonline.es*. Obtenido de Qué es un armario rack 19” y tipos de armarios rack 19": https://www.rackonline.es/content/que-es-un-armario-rack

A N E X O S

ANEXO I

Objetivo: Analizar el funcionamiento de la red informática de la empresa y proponer soluciones efectivas.

Encuesta dirigida a: Encargado del departamento de ofimática y demás empleados

ENCUESTA

1. **¿Qué tipo de dispositivo móvil utiliza en su empresa?**

Tabletas	
Celular	X
Similares	

2. **¿Para qué los utiliza?**

Navegación web, envío y recepción de correo electrónico.	X
Aplicaciones de gestión empresarial	

3. **¿Tiene ordenadores en su empresa?**

SI	X
NO	

4. **¿Cuántos ordenadores hay en su empresa?**

Uno	**X**
Dos	
Más de dos	

5. **¿Dispone su empresa de una red local (LAN)?**

SI	**X**
NO	

6. **¿Utiliza algún software en su empresa que le permita mantener su red segura?**

SI	
NO	**X**

7. **¿Dispone su empresa de un ERP? (**Programa que le permite compartir información entre todas las áreas funcionales como: contabilidad, gestión, almacén, personal, etc.**)**

SI	
NO	**X**

¿Posee la red de su empresa algún mecanismo para guardar la información que circula en ella?

SI	X
NO	

8. **¿Tiene externalizada toda o parte de la información de su empresa?**

SI	
NO	X

9. **¿Le gustaría contar con una herramienta que ayude a analizar su red y optimizarla?**

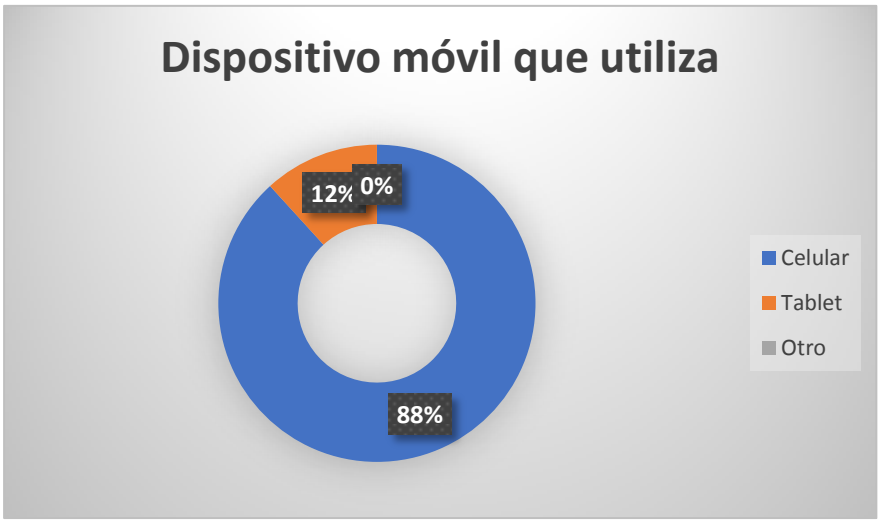
SI	X
NO	

ANEXO II

Tabulación de datos

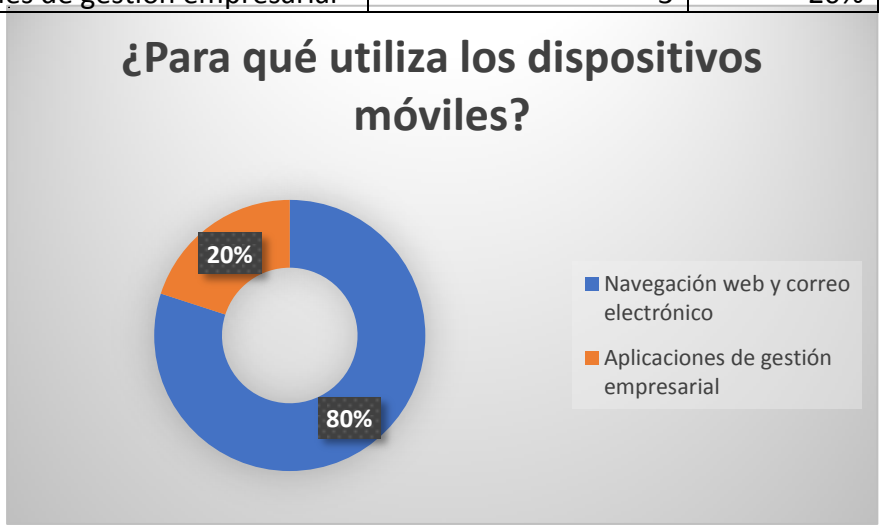
PREGUNTA 1.

¿Qué tipo de dispositivo móvil utiliza en su empresa?	Personas encuestadas	Porcentaje
Tabletas	2	12%
Celular	13	88%
Similares	0	0%



PREGUNTA 2.

¿Para qué utiliza el dispositivo móvil?	Personas encuestadas	Porcentaje
Navegación web y correo electrónico	12	80%
Aplicaciones de gestión empresarial	3	20%



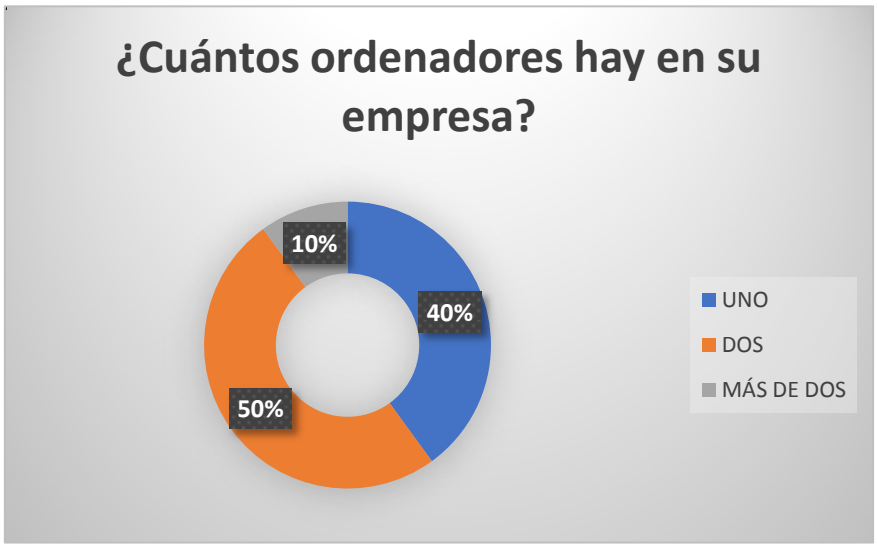
PREGUNTA 3.

¿Tiene ordenadores en su empresa?	Personas encuestadas	Porcentaje
SI	15	100%
NO	0	0%

PREGUNTA 4.

¿Cuántos ordenadores hay en su empresa?	Personas encuestadas	Porcentaje
UNO	6	40%
DOS	7	50%

MÁS DE DOS	2	10%



PREGUNTA 5.

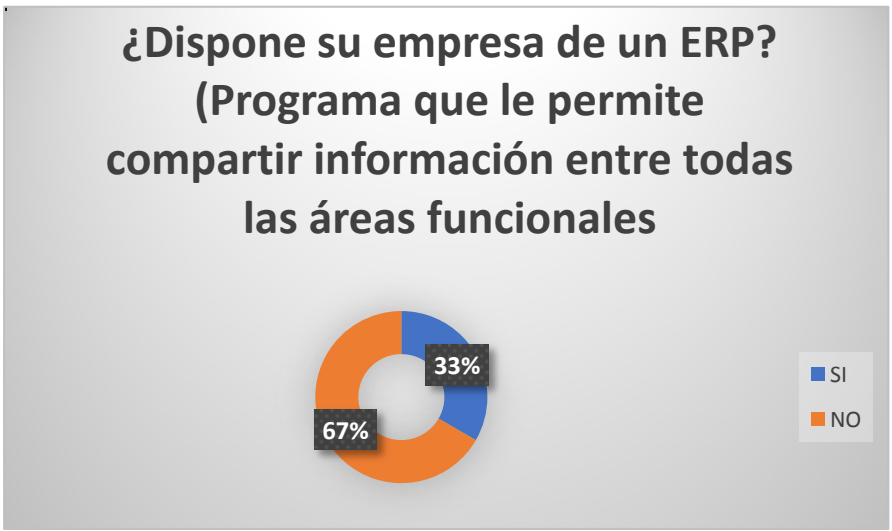
¿Dispone su empresa de una red LAN?	Personas encuestadas	Porcentaje
SI	15	100%
NO	0	0%

PREGUNTA 6.

¿Utiliza algún tipo de software que le permita mantener su red segura?	Personas encuestadas	Porcentaje
SI	5	33%
NO	10	67%

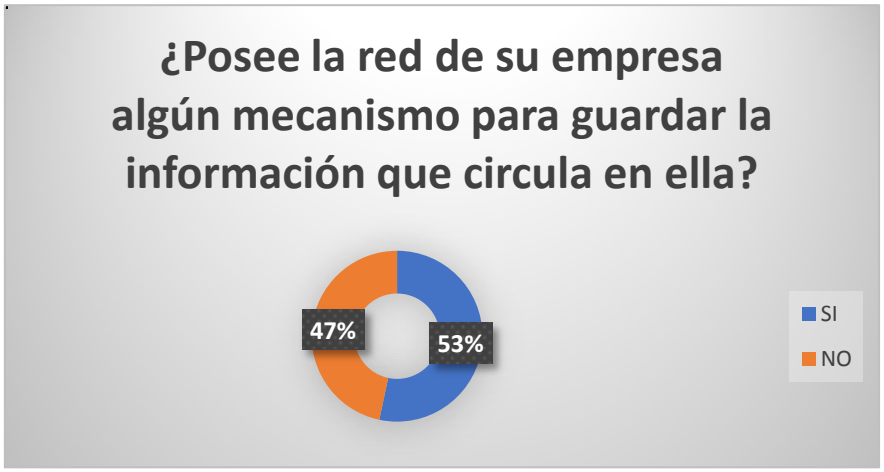
PREGUNTA 7.

¿Dispone su empresa de un ERP programa que le permite compartir información entre todas las áreas?	Personas encuestadas	Porcentaje
SI	5	33%
NO	10	67%



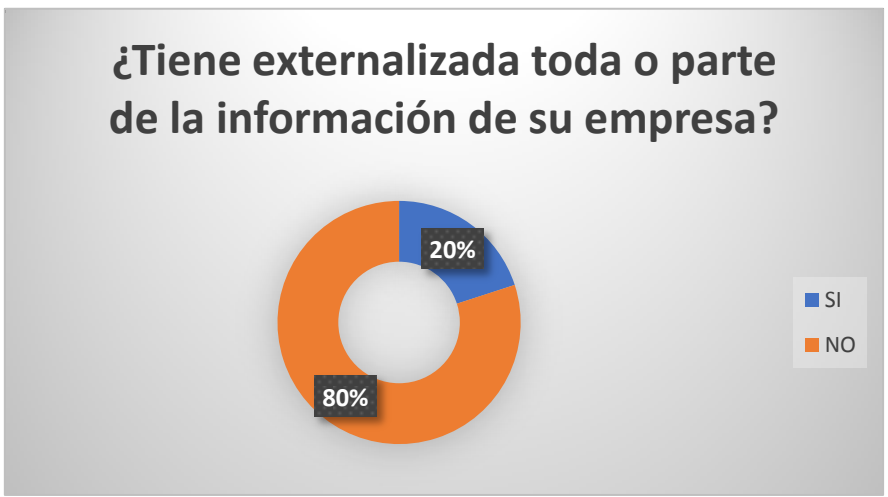
PREGUNTA 8.

¿Posee la red de su empresa algún mecanismo para guardar la información que circula en ella?	Personas encuestadas	Porcentaje
SI	8	53%
NO	7	47%



PREGUNTA 9.

¿Tiene externalizada toda o parte de la información de su empresa?	Personas encuestadas	Porcentaje
SI	3	20%
NO	12	80%



PREGUNTA 10.

¿Le gustaría contar con una herramienta que le ayude a analizar la red y optimizarla?	Personas encuestadas	Porcentaje
SI	14	93%
NO	1	7%