Journal **TechInnovation**
Volumen 3, Número 1, 2024
Universidad Estatal del Sur de Manabí
ISSN-e: 2953-6472

ARTÍCULO ORIGINAL

Seguridad en redes LAN: la protección de datos hasta la prevención de intrusiones

Security in LAN networks: data protection to intrusion prevention

https://doi.org/10.47230/Journal.TechInnovation.v3.n1.2024.4-14

Recibido: 11-01-2024 **Aceptado:** 10-03-2024 **Publicado:** 01-06-2024

José Luis Ponce Guerrero[1*]
http://orcid.org/0000-0003-4237-5225

1. Magíster en Tecnologías de la información y la Comunicación; Docente de la Carrera de Pedagogía de las Ciencias Experimentales: Informática, Facultad de Filosofía, Letras y Ciencias de la Educación Universidad de Guayaquil; Guayaquil, Ecuador.

Volumen: 3
Número: 1
Año: 2024
Paginación: 4-14
URL: https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/67
***Correspondencia autor:** jose.ponceg@ug.edu.ec

RESUMEN

La seguridad en redes LAN no se limita a la restricción de accesos, sino que abarca la protección de datos y la defensa contra intrusos lógicos como programas maliciosos y hackers. Esta investigación aborda la seguridad de la red desde múltiples perspectivas: la seguridad de los datos, la protección de accesos, la ubicación de los equipos, el cableado y los componentes hardware como los firewalls. El artículo verifica los medios físicos y lógicos necesarios para una defensa robusta de la red, proporcionando información práctica y medidas preventivas efectivas. La importancia del proyecto radica en ofrecer un análisis exhaustivo sobre la seguridad de las redes LAN, destacando la necesidad de proteger los datos almacenados en los servidores mediante métodos analíticos sistemáticos y exploratorios. Como resultado se conoció que es una herramienta útil para implementar una seguridad eficiente en redes LAN. Se concluye que los medios inalámbricos son los más vulnerables a ciberataques debido a su fácil acceso al router. Por lo cual se considera crucial para fortalecer la seguridad en este ámbito, además de implementar una estrategia integral que aborde tanto los aspectos físicos como lógicos de la red.

Palabras clave: Protección de datos, Redes, Seguridad.

ABSTRACT

Security in LAN networks is not limited to access restriction, but also covers data protection and defense against logical intruders such as malicious programs and hackers. This research addresses network security from multiple perspectives: data security, access protection, equipment location, cabling, and hardware components such as firewalls. The article verifies the physical and logical means necessary for robust network defense, providing practical information and effective preventive measures. The importance of the project lies in offering a comprehensive analysis of the security of LAN networks, highlighting the need to protect data stored on servers through analytical, systematic and exploratory methods. As a result, it was known that it is a useful tool to implement efficient security in LAN networks. It is concluded that wireless media are the most vulnerable to cyber-attacks due to their easy access to the router. Therefore, it is considered crucial to strengthen security in this area, in addition to implementing a comprehensive strategy that addresses both the physical and logical aspects of the network.

Keywords: Data protection, Networks, Security.

Introducción

La información es el ente más importante en la actualidad, quien posee la información pose el conocimiento y por ende controla todo, en el siguiente artículo se verifican los medios de seguridad en redes LAN, sabiendo que no solo la seguridad de los equipos son de medios lógicos sino también físicos, las TIC son el ente más importante en la seguridad de la información ya que son los pioneros en el conocimiento informático y por ende tienen que dar soluciones a las medidas de seguridad de las redes.

La seguridad física está distribuida desde la utilización de los hardware así como también de la ubicación de las mismas, es factible entender que el servidor es el ente más importante en una localidad de red, ya que es aquí donde la información proporcionada por los diferentes terminales reposa, así que la seguridad del mismo es el punto esencial desde la ubicación del mismo, el acondicionamiento y las medidas de seguridad en hardware como son los fireware (cortafuegos) y los Routers que juntos impiden o limitan el acceso del exterior, de igual manera los software son una parte crucial en la protección de las redes LAN ya que mediante los accesos y las restricciones también se puede controlar las medidas de seguridad como alternativa de defensa a los datos cruciales que pose los terminales como el servidor en sí.

Cada vez más empresas están desconectadas. Cargando algunas de sus necesidades de cómputo a proveedores de servicios en la nube, creando infraestructuras híbridas donde su propia red interna tiene que interoperar de forma fluida y segura con servidores alojados por terceros. A veces esta infraestructura en sí misma es una red autónoma, que puede ser física (varios servidores en la nube trabajando juntos) o virtual (varias instancias de VM ejecutándose juntas y "interconectando" entre sí en un solo servidor físico) (Díaz, 2018).

Una manera eficiente de seguridad de la red LAN es conectar un firewall de hardware o un Router, estos dispositivos protegen a la red restringiendo los accesos desde afuera de la red. Esto nos permite tener segura la red en todos los sentidos del hardware y así poder obstaculizar los ataques a los hackers que son los pioneros en la seguridad de red, permitiendo mantener la información de nuestro servidor libre y sin alteraciones.

Las redes son de vital importancia para el desarrollo continuo, y normal funcionamiento de las pequeñas y medianas organizaciones (Rodriguez Toala, Pincay Segovia, & Maldonado Zúñiga, 2022).

¿Qué es la seguridad de la red?

La seguridad de la red es la práctica de prevenir y proteger contra la intrusión no autorizada en redes corporativas. Como filosofía, complementa la seguridad del punto final, que se centra en dispositivos individuales; la seguridad de la red se centra en cómo interactúan esos dispositivos y en el tejido conectivo entre ellos (Orjuela Castillo, 2019).

El venerable SANS Institute lleva la definición de seguridad de red un poco más lejos: la seguridad de la red es el proceso de tomar medidas físicas y preventivas para proteger la red subyacente de uso indebido, mal uso, mal funcionamiento, modificación, destrucción o divulgación incorrecta. Funciones críticas dentro de un entorno seguro (Orjuela Castillo, 2019).

Pero el impulso general es el mismo: la seguridad de la red se implementa mediante las tareas y herramientas que utiliza para evitar que personas no autorizadas entren en sus redes. En esencia, su computadora no puede ser pirateada si los hackers no pueden acceder a ella a través de la red (Orjuela Castillo, 2019).

Historia de la red LAN

En épocas anteriores a los ordenadores personales, una empresa podía tener solamente un ordenador central, accediendo los usua-

rios a éste mediante terminales de ordenador con un cable simple de baja velocidad. Las redes como SNA de IBM (Arquitectura de Red de Sistemas) fueron diseñadas para unir terminales u ordenadores centrales a sitios remotos con líneas alquiladas. Las primeras LAN fueron creadas a finales de los años 1970 y se solían crear líneas de alta velocidad para conectar grandes ordenadores centrales a un solo lugar. Muchos de los sistemas fiables creados en esta época, como Ethernet y ARCNET, fueron los más populares (Carvajalino Ortíz, 2016).

El crecimiento CP/M y DOS basados en el ordenador personal significó que en un lugar físico existieran docenas o incluso cientos de ordenadores. La intención inicial de conectar estos ordenadores fue, generalmente, compartir espacio de disco e impresoras láser, pues eran muy caros en este tiempo. Había muchas expectativas en este tema desde 1983 y la industria informática declaró que el siguiente año sería "El año de las LAN" (Carvajalino Ortíz, 2016).

En realidad, esta idea fracasó debido a la proliferación de incompatibilidades de la capa física y la implantación del protocolo de red, y la confusión sobre la mejor forma de compartir los recursos. Lo normal es que cada vendedor tuviera tarjeta de red, cableado, protocolo y sistema de operación de red. Con la aparición de NetWare surgió una nueva solución, la cual ofrecía: soporte imparcial para los más de cuarenta tipos existentes de tarjetas, cables y sistemas operativos mucho más sofisticados que los que ofrecían la mayoría de los competidores. NetWare dominaba el campo de las LAN de los ordenadores personales desde antes de su introducción en 1983 hasta mediados de los años 1990, cuando Microsoft introdujo Windows NT Advance Server y Windows for Workgroups (Carvajalino Ortíz, 2016).

Conceptos básicos de seguridad de red

Las definiciones son buenas como declaraciones de intenciones de alto nivel. ¿Cómo planeas implementar esa visión? Stephen Northcutt escribió una introducción a los conceptos básicos de la seguridad de la red durante más de una década atrás CSOonline, nosotros nos fijamos en tres fases de la seguridad de la red que deberían ser el marco de referencia base para su estrategia (Flores Ortega, 2020).

Protección: debe configurar sus redes y redes lo más correctamente posible

Detección: debe ser capaz de identificar cuándo ha cambiado la configuración o si algún tráfico de red indica un problema

Reacción: después de identificar los problemas rápidamente, responderlos y regresar a un estado seguro.

Esto, en resumen, es una estrategia de defensa en profundidad. Si hay un tema común entre los expertos en seguridad, es cualquier herramienta defensiva individual puede ser derrotada por un adversario determinado. Su red no es una línea o un punto: es un territorio, e incluso si ha organizado su defensa correctamente (Flores Ortega, 2020).

Metodología

En el presente artículo se utilizaron métodos de la investigación científica como:

Método Análisis- síntesis

Se usó este método con el fin de analizar la seguridad de una red LAN, ya que es muy frecuente que esta se encuentre bajo amenaza constante, los ataques de los hackers cada vez son más efectivos es x eso que es necesario la utilización de la máxima seguridad posible y este articulo provee de herramientas necesarias para la seguridad del mismo creadas mediante un análisis.

Métodos de Investigación

Se utilizó el tipo de investigación: exploratoria

Investigación Exploratoria

Se usó este método en el desarrollo del artículo para saber de las herramientas tanto de hardware como de software que sean factibles

para la seguridad en la red, y así poder trabajar manteniendo resguardada la información que es el ente más importante de cualquier institución ya sea esta pública o privada.

Resultados

Métodos de seguridad de red

Para implementar este tipo de defensa en profundidad, hay una variedad de técnicas especializadas y tipos de seguridad de red.

Control de acceso: debe poder bloquear a usuarios y dispositivos no autorizados de su red. Los usuarios que tienen acceso autorizado a Internet solo han sido autorizados para utilizar el sitio web (Orjuela Castillo, 2019).

Antimalware: virus, gusanos y troyanos por definición de una red, y puede permanecer inactivo en las máquinas infectadas durante días o semanas. Su esfuerzo de seguridad debe hacerse para prevenir infecciones y también para el malware raíz que se dirige a su red. Seguridad de la Aplicación: su red suele acceder a las aplicaciones no seguras. Debe usar hardware, software y procesos de seguridad para bloquear esas aplicaciones (Orjuela Castillo, 2019).

Análisis de comportamiento: debe saber cómo es el comportamiento normal de la red para poder detectar anomalías o infracciones a medida que ocurren. Prevención de pérdida de datos: los seres humanos son inevitablemente el enlace de seguridad más débil. Debe implementar tecnologías y procesos para garantizar que los empleados no envíen deliberadamente o inadvertidamente datos confidenciales fuera de la red (Orjuela Castillo, 2019).

Seguridad del correo electrónico: el phishing es una de las formas más comunes de obtener acceso a una red. Las herramientas de seguridad de correo electrónico pueden bloquear tanto los mensajes entrantes como los salientes con datos confidenciales. Firewalls: quizás el abuelo del mundo de la seguridad de la red, siguen las reglas de su red o de Internet, estableciendo una barrera entre su zona de confianza y el salvaje oeste (Orjuela Castillo, 2019).

Información de seguridad y gestión de eventos (SIEM): estos productos pretenden reunir información de una variedad de herramientas de red para proporcionar los datos que necesita para identificar y responder a las amenazas (Orjuela Castillo, 2019).

VPN: Una herramienta (típicamente basado en IPsec o SSL) que autentica la comunicación entre un dispositivo y una red segura, creando un "túnel" seguro y encriptado a través de la Internet abierta (Orjuela Castillo, 2019).

Seguridad web: debe poder controlar el uso del personal interno para bloquear amenazas basadas en la web del uso de navegadores como vector para infectar su red (Orjuela Castillo, 2019).

Seguridad de la red y la nube

Cada vez más empresas están desconectadas. Cargando algunas de sus necesidades de cómputo a proveedores de servicios en la nube, creando infraestructuras híbridas donde su propia red interna tiene que interoperar de forma fluida y segura con servidores alojados por terceros. A veces esta infraestructura en sí misma es una red autónoma, que puede ser física (varios servidores en la nube trabajando juntos) o virtual (varias instancias de VM ejecutándose juntas y "interconectando" entre sí en un solo servidor físico) (Benito Páez, 2019).

Para manejar los aspectos de seguridad, muchos proveedores de servicios en la nube establecen políticas centralizadas de control de seguridad en su propia plataforma. Sin embargo, el truco aquí es que esos sistemas de seguridad no siempre coincidirán con sus políticas y procedimientos para sus redes internas, y esta falta de coincidencia puede aumentar la carga de trabajo para los profesionales de seguridad de redes. Hay una variedad de herramientas y

técnicas disponibles que pueden ayudar a aliviar parte de esta preocupación, pero la verdad es que esta área todavía está en flujo y la conveniencia de la nube puede significar problemas de seguridad para la red (Benito Páez, 2019).

Software de seguridad de red

Para cubrir todas esas bases, necesitará una variedad de herramientas de software y hardware en su kit de herramientas. Lo mejor son un elemento en su estrategia híbrida de defensa en profundidad. Algunas de estas herramientas son productos corporativos de grandes proveedores, mientras que otras vienen en la forma de utilidades gratuitas y de código abierto. Las categorías principales incluyen: analizadores de paquetes, que ofrecen una visión profunda del tráfico de datos, exploradores de vulnerabilidades como el software de detección y prevención de intrusos. En un entorno donde necesita obtener muchas herramientas para trabajar Juntos, es posible que también desee implementar el software SIEM, que mencionamos anteriormente (Benito Páez, 2019).

La seguridad en una red local debe contemplar diferentes problemas en relación a los recursos, los accesos, la información, los fallos y la alimentación del mismo.

Para tener una buena seguridad de la red, se deben aplicar varias medidas de seguridad y protección tanto en la seguridad física como en la lógica.

En la seguridad física se coma en consideración a los siguientes tipos de seguridad y protección:

- La seguridad física
- La seguridad de los datos
- La protección de acceso al ordenador
- La protección de acceso a los datos
- La protección en sí de los datos.
- En cuanto a la seguridad lógica se tiene a
- Secreto
- Validación de identificación
- No repudio
- Control de integridad

Cada uno de estos factores es indispensable para tener el equilibrio de seguridad en la red LAN o red de área local.

Protección contra los ruidos eléctricos

Los ruidos eléctricos son causados por las inconsistencias del suministro de la corriente eléctrica del ordenador. Para proteger al servidor contra los ruidos eléctricos, puede recurrirse a una línea dedicada de suministro eléctrico. No deben entonces conectarse otros dispositivos a este suministro de corriente dado que pueden generar ruidos que anulen las ventajas de la protección ofrecida por la fuente dedicada. La conexión a la fuente de energía ha de hacerse siempre con un cable estándar de tres hilos conectando a tierra el hilo correspondiente. La prevención contra altibajos de tensión y cortes de corriente suele realizarse mejorando la instalación con Sistemas de alimentación ininterrumpida (SAI) o en UPS (Uninterrumpible Power Suply) que permiten al servidor continuar activo durante un cierto tiempo ante un eventual corte de la corriente (Jupiter, 2016).

Clientes con aplicaciones críticas deberían, asimismo, disponer de SAI para evitar pérdidas de datos durante un corte de energía. Por último, cada dispositivo de red debería disponer de un filtro o estabilizador de corriente como protección a las sobretensiones. Si se dispone de un Sistema de Alimentación Ininterrumpida, éste puede configurarse, para su uso en Windows 2000, ejecutando el icono Opciones de Energía del Panel de control obteniéndose la pantalla adjunta al seleccionar la pestaña SAI (UPS) (Jupiter, 2016).

La seguridad de los datos

Para que la seguridad de los datos sea confiable en todo momento se debe tomar en consideración la seguridad del almace-

namiento del disco duro, así como también la configuración de seguridad y se deberá tener una copia de seguridad de los datos un backup.

En cuanto a la seguridad del almacenamiento se debe de considerar que la información siempre está segura para lo cual se debe de considerar trabajar con más discos duros inteligentes los cuales cumplen con el rol de detectar el daño que tenga y automáticamente transferir toda su información al siguiente disco duro que se encuentra conectado al servidor.

Para esto se tiene que denotar el tipo de disco para que se encuentren asignados según su función los cuales pueden ser SCSI, IDE y ESDI.

El disco SCSI es una controladora primaria los números van desde el 0 hasta el 6, cuando se encuentra llena se auxilia o recurre con la siguiente de la lista hasta completar las 4.

Los discos IDE y ESDI son controladoras primarias los cuales van desde 0 hasta 1, cuando esté llena o completa puede recurrir a la segunda controladora.

Tipos de protección de datos

La protección de los datos se puede realizar mediante dos tipos las cuales son las copias de seguridad y el copiado de archivos.

Habitualmente se realiza una copia de seguridad del sistema cuando existen errores humanos o mecánicos y así se protege el hardware para la recuperación del mismo.

En cuanto al copiado de archivos se guarda en cierto tiempo de la misma manera que se guarda las copias en el papel.

Los métodos para realizar la copia de seguridad son los siguientes:

- Copia de seguridad diaria, la cual se realiza diariamente
- La copia de seguridad diferencial, esta se realiza a los archivos creados o modificados y se puede respaldar cuando desee.
- La copia de seguridad incremental, se realiza a los archivos creados o modificados desde la última copia de seguridad.
- Copia de seguridad intermedia, se realiza a todos los archivos seleccionados.
- Copia de seguridad normal, se realizan a todos los archivos seleccionados hasta que se modifiquen.

Estos respaldos se los realiza con el fin de garantizar la seguridad de la información en la red LAN, esto se lo puede respaldar diariamente los archivos modificados, semanalmente el sistema entero y mensualmente los ficheros de datos (Jupiter, 2016).

Protección de acceso al ordenador

Hay varias posibilidades que permiten la protección al ordenador, entre ellas tenemos:

- Contraseñas CMOS
- Contraseña en el sector de arranque
- Contraseña en archivos de arranque

La protección por la contraseña CMOS, esta se ejecuta cuando el ordenador arrancha y realiza el chequeo, si la contraseña no es correcta no se procederá a arrancar el sistema operativo y se bloqueará el ordenador.

La protección por contraseña en el sector de arranque, se la ejecuta cuando el ordenador solicita la contraseña, esta se la puede incorporar desde el SETUP.

Seguridad de una red LAN

Al ser una red que se encuentra conectada al internet, se encuentra propensa a los cyber ataques los cuales pueden robar información de nuestro equipo o directamente ubicando malware al mismo.

Una manera eficiente seguridad de la red LAN es conectar un firewall de hardware o un Routers, estos dispositivos protegen a la red restringiendo los accesos desde afuera

de la red. Hay que tener pendiente que al instalar cualquier hardware se debe cambiar la configuración de acceso en este caso sería la contraseña ya que esta es universal y puede ser violentada por los atacantes.

Otra alternativa de seguridad es la verificación del log de acceso si se está trabajando con un Routers ya que con esto se puede verificar las IP que se han querido conectar a nuestra red y así prever ataques.

Para las redes inalámbricas

En la actualidad se usa con mucha frecuencia este tipo de conectividad ya que los atacantes buscan ingresar por donde se pueda y siendo este el más usado es el más propenso a ser usado como puente de ataque, es por esta razón que se conviene activar el cifrado WAP (WAP2 de preferencia) y activar el WEP, con esto se tendrá una seguridad adicional para los atacantes.

Es recomendable cambiar semanalmente el código SSID y autorizar el acceso a la red por direcciones MAC y apagar el Wifi cuando no se lo esté ocupando.

Seleccionar las contraseñas de seguridad WAP y WEP y cambiar el SSID son los pasos necesarios para mantener la red LAN protegida (Noguera, 2016).

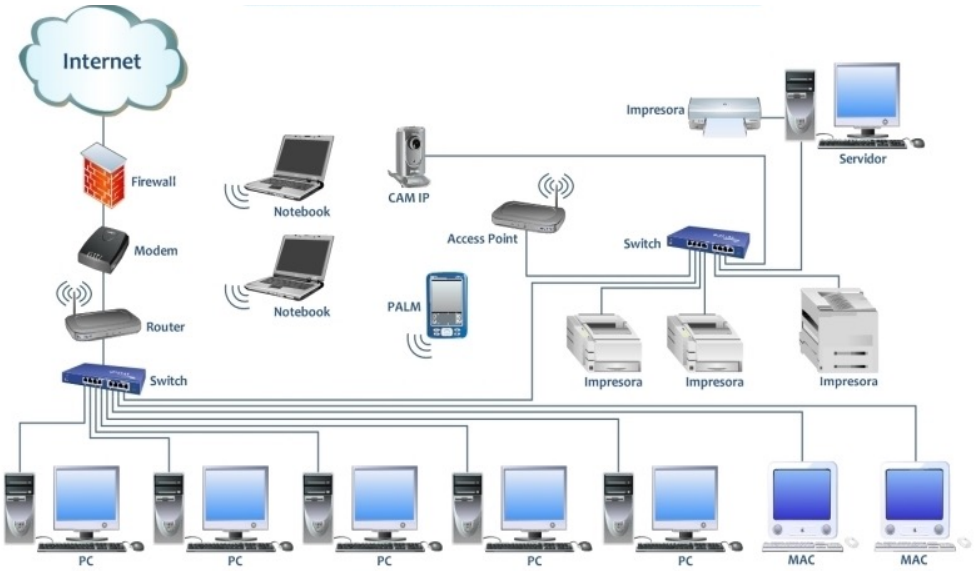

Figura 1. Esquema de una red de área local (LAN)

Fuente: (Django, 2021).

Estos son algunos de los puntos más importantes que tendríamos que revisar en nuestras redes para saber si cumplimos con los mínimos de seguridad que una red debe disponer:

- Tener un servidor de datos, en el cual guardamos todos los datos relevantes de la instalación y con su consiguiente proceso de copias bien definido.
- Tener montado en dicho servidor un DOMINIO, para la correcta administración de permisos de usuarios y facilidad de administración de la red local.
- Tener cortafuegos (físico o por software) para separar red local de la red de internet y tener control sobre los accesos a datos relevantes e internet por parte de los usuarios de la red local.

- Tener programa de antivirus “ACTUALIZADO” en todos los puestos de la red local, incluso en el servidor, para estar protegido casi al 100% sobre amenazadas de virus.
- Todos los puestos de la red deben tener sistema operativo profesional (xp, vista o win7), para la correcta validación de los usuarios en el “Active Directory” (dominio).
- Tener una política de contraseñas adecuada, cada usuario de la red local con su contraseña personal y además que esta caduque cada cierto tiempo (se puede definir).
- Tener una política de copias de seguridad definida y externalizada para posibles “desastres extremos” (robo, fuego)
- Llevar un correcto mantenimiento de los pc´s, actualizaciones de software y hotfix que van surgiendo (serviPack´s de Windows).
- Tener a alguien de la empresa o externalizada que controle los procesos de copia para detectar posibles problemas, actualización de antivirus, centralizar incidencias de la red local y así poder avisar a servicio técnico y llevar control sobre la resolución de las mismas.
- Tener localizadas todas las licencias de programas instalados en la red por posibles inspecciones por la autoridad competente (BSA) (Moreno, 2015).

Mecanismos de seguridad de una red LAN

Protección de hardware

El hardware es frecuentemente el elemento más caro de todo sistema informático. Por tanto, las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización, especialmente en las dedicadas a I+D. Universidades, Institutos tecnológicos, centros de investigación, suelen poseer entre sus equipos máquinas muy caras desde servidores con una gran potencia de cálculo hasta Routers de última tecnología, pasando por modernos sistemas de transmisión de datos como la fibra óptica. Ruidos Electromagnéticos Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios (Corredera de Colsa & García Fernández, 2019).

Cableado de Alto Nivel de Seguridad Son cableados de redes que se recomiendan para instalaciones con grado de seguridad militar. El objetivo es impedir la posibilidad de infiltraciones y monitoreo de la información que circula por el cable. Consta de un sistema de tubos (herméticamente cerrados) por cuyo interior circula aire a presión y el cable. A lo largo de la tubería hay sensores conectados a una computadora. Si se detecta algún tipo de variación de presión se dispara un sistema de alarma. Placas Extraíbles Los cables de alimentación, comunicaciones, interconexión de equipos, receptáculos asociados con computadoras y equipos de procesamiento de datos pueden ser, en caso necesario, alojados en el espacio que, para tal fin se dispone en los pisos de placas extraíbles, debajo del mismo. Sistema de Aire Acondicionado (Bolaines Portillo, Gómez Hernández, & Martínez Paíz, 2012).

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva (Guillén, 2013).

¿Qué es la seguridad lógica y en qué consiste?

La seguridad lógica se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información (Carrillo Jiu, 2014).

Consiste en generar la configuración adecuada del sistema para evitar el acceso a los recursos y configuración del mismo por

parte de personas no autorizadas, ya sea a nivel local o vía red.

La seguridad lógica de un sistema informático incluye:

- Restringir al acceso a programas y archivos mediante claves y/o encriptación.
- Asignar las limitaciones correspondientes a cada usuario del sistema informático.
- Asegurarse que los archivos y programas que se emplean son los correctos y se usan correctamente.
- Control de los flujos de entrada/salida de la información. Esto incluye que una determinada información llegue solamente al destino que se espera que llegue, y que la información llegue tal cual se envió (Unkanown, 2017).
- Sin dudas es una herramienta factible para aquellos que opten por una seguridad en su red LAN, la investigación brindada para saber cómo configurar la protección de una red, el uso de las herramientas que sean eficaces en la protección de los datos y la prevención de atacantes mediante dispositivos y así poder disminuir el índice de víctimas por parte de los ciberdelincuentes que son los pioneros en la destrucción de la seguridad.

Conclusiones

Se verificó los medios de seguridad tanto físicos como lógicos para mantener o salvaguardar la integridad del servidor y con él los datos que son la fuente principal de restricción.

Se conoció que el medio más propenso para los cyber atacantes en el medio inalámbrico, ya que es el que tiene mayor acceso al Routers y así a los dispositivos que se encuentran conectados al mismo, como son los terminales y el servidor.

La protección del servidor también incluye el control del ambiente físico, como la temperatura y la humedad. Se recomienda la instalación de sensores adicionales para detectar variaciones críticas y mecanismos automáticos de respuesta ante incendios o inundaciones.

El medio inalámbrico representa el vector de ataque más propenso para los ciberdelincuentes, debido a la accesibilidad a los routers y, por ende, a los dispositivos conectados. La falta de una adecuada configuración y la protección insuficiente del Wi-Fi aumentan significativamente el riesgo.

Mitigación de riesgos: Para mitigar estos riesgos, se sugiere implementar cifrado robusto (WPA3), segmentación de la red para aislar dispositivos críticos, y el uso de redes privadas virtuales (VPN) para asegurar las comunicaciones. Además, la realización de auditorías regulares de seguridad y pruebas de penetración pueden ayudar a identificar y corregir vulnerabilidades antes de que sean explotadas.

Bibliografía

Benito Páez, M. A. (2019). Montaje de un sistema de interconexión de computadores y recursos de. Universidad Distrital Francisco Jóse de Caldas.

Bolaines Portillo, R. E., Gómez Hernández, O., & Martínez Paíz, E. (2012). Propuesta de una guía de evaluación de seguridad informática a las empresas distribuidoras de telefonía móvil de la ciudad de San Miguel. Universidad de El Salvador. Obtenido de https://oldri.ues.edu.sv/id/eprint/5947/1/50107940.pdf

Carrillo Jiu, J. A. (2014). Fundamentos de seguridad lógica. Universidad Nacional de la Amazonia, Facultad de Ingenieria de Sistemas. Obtenido de https://repositorio.unapiquitos.edu.pe/bitstream/handle/20.500.12737/4487/Jose_Tesis_Titulo_2014.pdf?sequence=1&isAllowed=y

Carvajalino Ortíz, U. (2016). Implementación de la red de datos en la sala de informática del jardín Chiquilladas en Ocaña, Norte de Santander. Universidad Francisco De Paula Santander Ocaña, Facultad de Ingenierias. Obtenido de https://repositorioinstitucional.ufpso.edu.co/bitstream/handle/20.500.14167/1537/CUERPO%20DEL%20TRABAJO%20-%20IMPLEMETACION%20DE%20LA%20RED%20DE%20DATOS%20EN%20LA%20SALA%20DE%20INFORMATICA%20DEL%20JARDIN%20CHIQUILLADAS%20EN%20OCA%c3%91A%20NORTE_removed.pd

Corredera de Colsa, L. E., & García Fernández, F. (2019). Seguridad en gestión de redes y servicios. Ediciones Universidad de Salamanca .

Díaz, J. (1 de Marzo de 2018). pandorafms. Obtenido de https://pandorafms.com/blog/es/seguridad-de-redes/

Django, R. B. (2021). Quora. Obtenido de https://es.quora.com/Me-bloquearon-en-la-red-wifi-pero-aparece-conectado-pero-no-ingres%C3%B3-a-ninguna-p%C3%A1gina-y-me-dice-red-ni-disponible-C%C3%B3mo-le-hago

Flores Ortega, G. (2020). Reestructuración de la distribución y conectividad de los laboratorios de la Unidad Académica en la región de la montaña (UARM) Adscrita a la Universidad Tecnológica de la región norte de Guerrero (UTRNG). Tecnológico Nacional de México. Obtenido de http://51.143.95.221/bitstream/TecNM/5253/1/Tesis%20Gerardo%20Flores.pdf

Guillén, E. A. (2013). Estudio de la seguridad de red de datos de la Escuela Especializada en Ingeniería ITCA-FEPADE. Escuela Especializada En Ingeniería Itca, Dirección de Investigación y Proyección Social. Obtenido de http://redicces.org.sv/jspui/bitstream/10972/1667/1/07-%20Estudio%20de%20la%20seguridad%20de%20la%20red%20de%20datos%20de%20ITCA-FEPADE.pdf

Jupiter, F. (2016). jroliva. Obtenido de http://jroliva.com/fernando/Redes/Teoria/UD08d.pdf

Moreno, H. (2015). clave.i.es. Obtenido de https://www.clavei.es/blog/los-10-mandamientos-para-tener-una-red-local-segura/

Noguera, B. (2016). Obtenido de culturación.com: https://culturacion.com/como-proteger-una-red-lan/

Orjuela Castillo, D. J. (2019). Diseño de un Sistema de Videovigilancia por medio de Redes LAN para la Alcaldía del Municipio de Coper Boyacá. Universidad Cooperativa de Colombia, Facultad de Ingeniería. Obtenido de https://repository.ucc.edu.co/server/api/core/bitstreams/07fb8506-4469-44cb-9220-8630770eeb26/content

Rodríguez Toala, B. A., Pincay Segovia, E., & Maldonado Zúñiga, K. (2022). Las redes wan y su importancia para los ordenadores. UNESUM - Ciencias. Revista Científica Multidisciplinaria, 6(1), 1-14. doi:https://doi.org/10.47230/unesum-ciencias.v5.n4.2021.510

Unkanown. (12 de Marzo de 2017). Mecanismo de seguridad de una Red. Obtenido de unkanown: http://rene-redes.blogspot.com/2013/02/mecanismos-de-seguridad-de-una-red-lan.html

Cómo citar: Ponce Guerrero, J. L. . (2024). Seguridad en redes LAN: la protección de datos hasta la prevención de intrusiones. Journal TechInnovation, 3(1). https://doi.org/10.47230/Journal.TechInnovation.v3.n1.2024.4-14