UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA

CARRERA DE SISTEMAS DE INFORMACIÓN

PROCESO DE TITULACIÓN

DICIEMBRE 2022 – ABRIL 2023

EXAMEN COMPLEXIVO DE GRADO O FIN DE CARRERA PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE EQUIPOS DE COMUNICACIÓN Y LA PRIVACIDAD EN REDES INALÁMBRICAS APLICADO A LA EMPRESA ARTEFACTA DEL CANTÓN BABA

ESTUDIANTE:

CHIMBO ROCHINA HENRY MAURICIO

TUTOR:

ING. JOFFRE LEON ACURIO

AÑO

2023

ÍNDICE

RESUMEN Y PALABRAS CLAVE

Resumen

La seguridad inalámbrica es un elemento fundamental en la actualidad ya que existen personas con conocimientos y estrategias que pueden afectar a las empresas. Por esta razón, se ha planteado un estudio para que Artefacta del cantón Baba conozca los mejores equipos y configuraciones existentes en el mercado y puedan tener opciones referenciadas en el estudio para mejorar sus técnicas empresariales.

El Wireless Corporativo ofrece más funcionalidades que la inalámbrica planificada, lo que permite crear oportunidades de negocios y garantizar la continuidad de los procesos. Sin embargo es necesario tener en cuenta las limitaciones del Wireless Corporativo: como la falta de control de banda, visibilidad de tráfico y rastreo de usuarios. Por lo tanto, el estudio es importante para determinar un análisis y escenarios que permitan tener equipos de comunicaciones seguras para la empresa.

Este estudio se despliega en Artefacta del cantón Baba de la provincia de Los Ríos, donde existen varias incidencias de vulnerabilidades en cuanto al acceso a la información y la estabilidad empresarial, esto debido a las formas de trabajo del personal y a la falta de estrategias clave de seguridad. En este caso además se refleja que la mayoría de estas empresas dependen de conexiones inalámbricas deficientes y tienen problemas técnicos que no son abordados por falta de conocimiento especializado.

Estos problemas en la red pueden llevar a nuevas inversiones que no se integran adecuadamente con la demanda y la realidad de la empresa. Por lo tanto, es importante que las empresas busquen servicios especializados para implementar la red inalámbrica y adopten estrategias de seguridad para mejorar la estabilidad empresarial.

Abstract

Wireless security is a fundamental element today, since there are people with knowledge and strategies that can affect companies. For this reason, a study has been proposed so that Artifacta of the Baba canton knows the best equipment and configurations on the market and can have options referenced in the study to improve their business techniques.

The Corporate Wireless offers more functionalities than the planned wireless, which makes it possible to create business opportunities and guarantee the continuity of the processes. However, it is necessary to take into account the limitations of Corporate Wireless, such as the lack of band control, traffic visibility and user tracking. Therefore, the study is important to determine an analysis and scenarios that allow secure communications equipment for the company.

This study is deployed in Artefacta of the Baba canton of the province of Los Ríos, where there are several incidences of vulnerability in terms of access to information and business stability, this due to the ways of working of the personnel and the lack of key strategies of security. In this case, it is also reflected that most of these companies depend on poor wireless connections and have technical problems that are not addressed due to a lack of specialized knowledge.

These problems in the network can lead to new investments that are not adequately integrated with the demand and the reality of the company. Therefore, it is important for companies to seek specialized services to implement the wireless network and adopt security strategies to improve business stability.

Palabras claves

Equipos de comunicación, Firewall, Enlace de Radio, seguridades, conexiones inalámbricas, Wireless, VPN, Artefacta

PLANTEAMIENTO DEL PROBLEMA

En la empresa Artefacta del cantón Baba existen múltiples indicios de vulnerables en lo relacionado con el acceso a la información, esto tiene relación con las formas de trabajar del personal ademas es una forma común en las organizaciones donde trabajan y también existen agujeros que no garantizan su estabilidad empresarial para mantenerse de forma segura.

Es muy trillado el tema de que el activo más importante de una empresa es la información, pero en tal sentido es necesario que se sumen esfuerzos que permitan estrategias claves para mejorar estas seguridades que son de las que carecen las organizaciones en este territorio Baba de la provincia de Los Ríos, como lo es Artefacta.

La forma de conectividad de las muchas empresas que existen sobre todo del sector rural que pertenecen al sector agrícola y ganadero hacen que la forma de conectividad sea netamente inalámbrica muy pocas tienen acceso a fibra óptica y estas organizaciones presentan comúnmente inconvenientes de disponibilidad que es una de las problemáticas más constantes al depender netamente de las conexiones por antena.

Las conexiones inalámbricas hacen vulnerables a estas organizaciones que en su mayor parte se encuentran en el campo ya que por su condición y ubicación no les queda más alternativas de la utilización de tecnologías de conectividad inalámbrica y comúnmente estas son deficientes a nivel de equipos y a nivel de configuración

El Wireless es el tipo de conexión establecida en una red de ordenadores por señales de radiofrecuencia, basadas en el protocolo 802.11. A pesar de que esta tecnología tiene una definición que parece simple, el mercado corporativo debe estar atento con algunas cuestiones sobre cómo adquirirlas e integrarlas con la finalidad de obtener la mejor de la

solución y evitar problemas, actualmente los equipos de comunicación son esenciales para los negocios debido a la facilidad de uso que proporciona y de la movilidad.

Muchas empresas como Artefacta creen que esta es una solución tan simple que ni siquiera buscan servicios especializados para implementar la red inalámbrica, y todavía tratan de resolver problemas técnicos sin el conocimiento necesario.

Como resultado surgen los constantes problemas en la red porque se notan la falta de conexión. Situaciones como éstas llevan a las empresas a hacer nuevas inversiones que una vez más no se integran adecuadamente con la demanda y la realidad de la empresa.

OBJETIVOS

- **General**

Analizar las comunicaciones inalámbricas y su infraestructura relacionada con equipos existentes para fortalecer la privacidad y seguridad de la información en Artefacta del cantón Baba.

- **Específicos**

Fundamentar teorías inherentes a la privacidad en las redes inalámbricas.

Recopilar datos relacionados con la forma de conectividad y los equipos en Artefacta del cantón Baba.

Analizar la discusión de resultados para recomendar buenas prácticas orientadas a equipo y seguridad inalámbrica.

JUSTIFICACIÓN.

Este trabajo justifica de manera garantizada su realización ya que aporta con formas científicas y académicas a Artefacta del cantón baba que en su posterior podrán hacer uso de los datos y las recomendaciones que aquí se podrán encontrar.

La seguridad de la información es una industria que mueve cerca de 72 billones de dólares anuales en el mundo por lo tanto las aplicaciones y estudios derivados relacionados con esta aportan enormemente y en cualquier circunstancia.

La seguridad inalámbrica es uno de los elementos fundamentales hoy en día donde mucha gente tiene conocimiento y conoce estrategias que podrían afectar a las organizaciones y empresas por esa razón se ha planteado este caso de estudio que seguramente le permitirá a todas las empresas de este territorio conocer los mejores equipos y sus configuraciones existentes en el mercado y tener opciones referenciadas en este estudio para que sus técnicos las tengan como alternativas válidas para aportar de esta manera con sus técnicas empresariales.

Además, el wireless planificado ofrece ventajas por presentar robustez y muchas aplicaciones de seguridad y este al ser implementado con mayor cuidado técnico tiene al mismo tiempo limitaciones, pues no ofrece algunas funcionalidades como el control de banda (por red Wi-Fi, aplicación o usuario), la visibilidad de tráfico y el rastreo de usuarios, en tal sentido es necesario este estudio para determinar un análisis y escenarios que permitan tener equipos de comunicaciones seguras para las empresas.

Es aquí donde el Wireless Corporativo entra en escena, incrementando funcionalidades a la inalámbrica planificada ya que con estas soluciones pueden ofrecerse a las empresas recursos más audaces, dando soporte para que se creen oportunidades de negocios y garanticen continuidad de procesos.

LÍNEA DE INVESTIGACIÓN

Este documento hace referencia a la línea de investigación Sistemas de información y comunicación, emprendimiento e innovación, por ser de la carrera de sistemas de información y por involucrar empresas y sistemas de comunicaciones; así mismo relacionado con la sub línea Redes y tecnologías inteligentes de software y hardware qué pues los especialistas en esta profesión requieren de elementos fundamentales que les permitan comprender la lógica y la funcionalidad hace como la configuración de la infraestructura tecnológica relacionada con las telecomunicaciones para de esta manera adaptarse a las necesidades organizacionales.

MARCO CONCEPTUAL

Las telecomunicaciones marcando el avance tecnológico global

En la actualidad, el crecimiento tecnológico constante exige a los profesionales de la información potenciar sus habilidades con el apoyo de herramientas innovadoras para la generación, transmisión y acceso inmediato a la información (Turró, 2019).

De acuerdo con el informe "Telecomunicaciones 2020" de Deloitte, el campo de las telecomunicaciones es un sector en constante evolución gracias a la rápida transformación tecnológica y la regulación gubernamental en constante cambio. Esto implica que los profesionales de la información que trabajan en este campo deben estar preparados para enfrentar desafíos y cambios constantes en un mercado cada vez más competitivo e interconectado.

Según el informe "Tendencias Tecnológicas 2021" de Gartner, el crecimiento tecnológico ha aumentado la necesidad empresarial en el desarrollo de las telecomunicaciones, lo que ha generado una mayor demanda de profesionales capacitados en este campo.

En un artículo publicado en "El Telégrafo" en 2020, se señala que el alto nivel de inversión tanto del sector público como privado en el desarrollo de las telecomunicaciones en Ecuador ha permitido reducir la brecha en el analfabetismo digital, reducir las tarifas de telefonía móvil y aumentar la velocidad de internet gracias a proyectos de extensión de fibra óptica. Esto ha resultado en una alta tasa de empleabilidad para los profesionales graduados en esta carrera.

En su informe "La futura fuerza laboral de la industria digital", Accenture señala que la demanda de profesionales en el campo de las telecomunicaciones seguirá en aumento

debido a la "cuarta revolución industrial" o "revolución 4.0", en la que los robots de espacios ciberfísicos jugarán un papel clave en la transformación social.

En un artículo publicado en Forbes en 2021, se destaca que la revolución 4.0 también implicará un aumento en la demanda de profesionales capacitados en el "Internet de las cosas" en el campo de las telecomunicaciones, lo que generará nuevas demandas en velocidad, banda ancha y otros elementos necesarios para optimizar los nuevos estilos de vida.

BENEFICIO DE LAS TELECOMUNICACIONES EN LAS EMPRESAS

En la actualidad, las telecomunicaciones se han posicionado como un recurso altamente valioso para las empresas, ya que ofrecen una comunicación eficiente con los clientes y brindan una atención al cliente de alta calidad.

Asimismo, estas tecnologías son esenciales para el trabajo colaborativo, al facilitar la colaboración entre los empleados sin importar su ubicación geográfica. En este sentido, la posibilidad de trabajar de manera remota ha sido uno de los mayores beneficios que han traído las telecomunicaciones móviles, permitiendo a los empleados trabajar desde su hogar de manera eficiente.

La introducción de los teléfonos inteligentes ha sido especialmente relevante, ya que ha mejorado significativamente la productividad de los empleados y les ha brindado una mayor flexibilidad en cuanto a su movilidad.

En conclusión, las telecomunicaciones han demostrado ser un recurso fundamental en la actualidad porque brindan innumerables beneficios a las empresas y permitiendo una mayor eficiencia en el trabajo en equipo.

Servicio al Cliente

En la actualidad, el teléfono sigue siendo una herramienta clave en la estrategia de servicio al cliente de las empresas. A través de la implementación de técnicas de gestión de llamadas (Alkhatib, 2019), es posible administrar eficientemente las llamadas entrantes aun cuando las líneas se encuentren ocupadas, y redirigirlas a los empleados con las habilidades necesarias para atender cada caso.

Asimismo, (Alkhatib, 2019) indica, que es posible ofrecer a los clientes una serie de opciones a través de un sistema de menú, como "Presione '1' para cuentas" o "Presione '2' para ventas", lo que les permitirá obtener una atención personalizada. Además, el

teléfono también puede ser utilizado como un medio proactivo para comunicarse con los clientes, ya sea a través de un servicio de llamadas o después de una compra con el fin de fortalecer el vínculo con ellos y mejorar su experiencia general con la marca.

Colaboración

Según el autor de tecnología David Nield (2020), la colaboración entre diferentes departamentos en una empresa es fundamental para mejorar la eficiencia en proyectos como lo es el desarrollo de nuevos productos y la gestión de relaciones con clientes. La consultora McKinsey & Company, por su parte destaca que la resolución de problemas complejos mediante la colaboración es esencial para muchos empleados.

Las telecomunicaciones son una herramienta clave para mantener a los equipos de trabajo conectados y permitir la toma de decisiones importantes, incluso si no todos los miembros pueden asistir a reuniones físicas.

Remoto

Hernández, A. (2020), indica que la utilización de las telecomunicaciones móviles puede ser una herramienta importante para mantener la productividad y comunicación de empleados que pasan gran parte de su tiempo en contacto con clientes debido a que trabajan desde casa o en viajes como es el caso de los equipos de ventas, técnicos y servicio.

Según una encuesta realizada por Yankee Group Enterprise Mobility, el 40% de los encuestados considera que más de un tercio de sus empleados son trabajadores móviles o remotos.

Teléfonos Inteligentes

"La creciente sofisticación de los teléfonos inteligentes los convierte en una herramienta integral para la comunicación y conectividad, permitiendo a los empleados

acceder a datos para enviar y recibir correos electrónicos, trabajar en documentos y participar en conferencias multimedia, todo desde un solo dispositivo" (Johnson, 2021).

Según el estudio de Cisco Visual Networking Index, "las aplicaciones que requieren gran cantidad de datos son la principal causa del aumento del tráfico de comunicación en red" (Smith, 2020).

Telecomunicaciones y redes, cuatro problemas que afectan a tu empresa.

Sin embargo las telecomunicaciones y redes pueden presentar diversos problemas que afectan la actividad corporativa, ya sea en la comunicación interna o en el acceso a datos internos y externos. La complejidad de los sistemas de telecomunicaciones requiere sistemas de seguridad, velocidad y fiabilidad cada vez más sólidos y robustos que garanticen la continuidad del negocio.

Además en la pandemia de 2020 puso de relieve la brecha digital en América Latina, y aunque se centró en los sistemas de conexión domésticos se espera un aumento en la demanda de recursos de telecomunicaciones empresariales una vez que las empresas retornen a la normalidad, lo que puede generar fallos que afecten a la operación de las empresas. A continuación, se describen los cuatro errores más comunes que pueden afectar las redes de comunicación empresarial.

La Post Pandemia

Sin embargo, no todo sale como se esperaba. Las telecomunicaciones ecuatorianas tienen sus límites: cuando salgamos de la crisis actual, quedará claro que América Latina aún no ha procedido a cerrar la brecha digital.

Aunque la pandemia de 2020 ha llevado toda la atención a los sistemas de comunicación interna, una cosa está clara: cuando las empresas empiecen a volver a la normalidad, las necesidades de infraestructura empresarial aumentarán.

Debido a las crecientes necesidades comerciales de los dispositivos móviles, las posibles interrupciones pueden causar daños significativos a las empresas. A continuación, describimos cuatro errores comunes que pueden afectar su red comercial.

Problemas típicos de los sistemas de telecomunicaciones y redes empresariales.

Las redes de telecomunicaciones internas de las empresas deben seguir funcionando incluso si los empleados no están en las oficinas debido a los cortes eléctricos y las fallas en los operadores de telecomunicaciones y redes.

En la actualidad es crucial que las telecomunicaciones funcionen de manera confiable en cualquier momento y lugar, independientemente de la distancia. Por lo tanto, es esencial que la seguridad electrónica, los data center, los servidores, los racks y otros elementos estén en funcionamiento y tengan redundancia. (Telecom Reseller, 2021)

Si una empresa no instala los sistemas de telecomunicaciones y redes adecuados para el trabajo desde casa, es probable que tenga problemas que afecten su productividad y que se extiendan a toda la organización. Por lo tanto, la empresa debe proporcionar y garantizar los recursos necesarios para que los sistemas de telecomunicaciones funcionen de manera óptima en el hogar. (Revista Emprende TIC, 2020)

Si los sistemas de telecomunicaciones empresariales no están bien establecidos e implementados, los empleados pueden enfrentar problemas como trabajar con redes intermitentes debido a la necesidad de adquirir equipamiento más robusto y orientado a la disponibilidad del 100%.

También pueden enfrentar la falta de un especialista en tecnología de la información para solucionar en vivo las dificultades que surjan por lo que es necesario contar con un respaldo que soporte los procesos. (Revista Emprende TIC, 2020)

Según un informe de seguridad de Forrester, la gran mayoría (82%) de las organizaciones enfrentan dificultades para identificar y proteger los dispositivos conectados a su red, y no tienen claro quién es el responsable de administrarlos. Con la llegada del Internet de las Cosas, se han presentado una gran cantidad de necesidades de la red que eran impensables antes de la pandemia, lo que ha llevado a un aumento del consumo de datos y la tecnología sigue avanzando a una velocidad vertiginosa.

Según Gartner, en 2018 ya existían 8.400 millones de objetos conectados a la red (como vehículos, máquinas, sensores y cámaras) que generan y transmiten datos en tiempo real, lo que ha permitido a las empresas mejorar la eficiencia de sus productos y servicios. Sin embargo, esto también ha tenido un impacto en el tráfico de datos que se ha multiplicado debido al creciente número de dispositivos conectados a Internet. (Infobae, 2021)

Soluciones en telecomunicaciones empresariales.

Según se menciona en un artículo de la Revista Emprende TIC (2020), Aunque los líderes empresariales conocen la importancia de contar con sistemas de telecomunicaciones empresariales eficientes, a menudo la implementación de nuevas soluciones tecnológicas puede ser contraproducente. La complejidad de estas soluciones son la falta de capacitación, la inadecuación a las necesidades de los empleados y la producción de la empresa son algunas de las razones detrás de este problema.

Así mismo un artículo de la Revista Emprende TIC (2020), menciona que “es crucial que las empresas evalúen cuidadosamente sus necesidades y creen un plan claro para

mejorar sus sistemas de telecomunicaciones". Esto implica identificar las áreas en las que se necesita mejorar y las soluciones tecnológicas que mejor se ajustan a esas necesidades. De lo contrario, la tecnología podría convertirse en un problema más que en una solución y podrían acabar gastando una gran cantidad de su presupuesto anual en soluciones que no serán útiles a largo plazo.

La Seguridad en Redes Teleinformáticas y Telecomunicaciones.

Durante las últimas décadas, la seguridad de la información organizacional ha experimentado dos cambios significativos. Antes de la aparición generalizada de los dispositivos de información, la seguridad se consideraba importante solo para la organización en las oficinas administrativas, utilizando casilleros y otros mecanismos similares para proteger documentos importantes. (Tipton, H. F., & Krause, M., 2020).

La llegada de las computadoras hizo que se hiciera evidente la necesidad de herramientas automatizadas para proteger archivos y otra información almacenada, especialmente en sistemas compartidos, como los que se pueden acceder a través de redes telefónicas o de información. El término general utilizado para referirse a estas herramientas de protección de información, así como a la intrusión de hackers, es seguridad computacional. Bishop, M. (2019).

El segundo cambio que tuvo un impacto en la seguridad fue la implementación de sistemas distribuidos y el uso de redes e infraestructuras de comunicación para el intercambio de información entre servidores y computadoras, así como entre dos computadoras. Es crucial implementar medidas de seguridad en las redes para proteger la información mientras se transmite y para asegurarse de que sea auténtica. Tipton, H. F., & Krause, M. (2007).

La tecnología empleada en la protección de computadoras y redes automatizadas es la encriptación y se utilizan principalmente dos tipos: la encriptación convencional también conocida como simétrica, que se usa para garantizar la privacidad mediante la autenticación; y la encriptación de clave pública también conocida como asimétrica, que se utiliza para prevenir la falsificación de información y transacciones mediante algoritmos basados en operaciones matemáticas. A diferencia de la encriptación simétrica, la encriptación de clave pública utiliza dos claves para proteger áreas como la confidencialidad, el intercambio de claves y la autenticación. Bishop, M. (2019)

Según Tushman, M. L., & Anderson, P. (2019). Se ha observado un aumento significativo en el número de trabajos que involucran el uso de tecnología de la información en la actividad económica, lo que resulta en una relación creciente de terminales por empleado en todos los sectores industriales.

Así mismo Bishop, M. (2019) indica que esto se debe a la importancia de la información y su gestión en cualquier empresa. Al analizar la distribución de la información generada en un puesto de trabajo, se ha encontrado que aproximadamente el 90% de dicha información se dirige al propio departamento, mientras que el 75% se destina a un punto cercano dentro de un radio de 200 metros y hasta un 90% se mantiene dentro del edificio, dejando solo un 10% de la información dirigida a destinos remotos. Aunque estas cifras son estimaciones, muestran la tendencia general del uso de la información en los entornos laborales actuales.

SEGURIDAD EN CÓMPUTO

Según Infobae. (2021), Se puede afirmar que la Seguridad se refiere a un conjunto de herramientas tanto físicas como virtuales, que tienen como objetivo garantizar que los recursos de cómputo disponibles en un entorno determinado sean accesibles únicamente por aquellos usuarios que tienen la autorización necesaria. También se puede medir la

Seguridad de forma cualitativa, mediante una premisa que establece que un sistema es seguro si se comporta de acuerdo a las expectativas de los usuarios.

Propiedades de la Información que protegen la Seguridad Informática.

En cuanto a la seguridad informática, es fundamental que se protejan principalmente tres propiedades: la privacidad, la integridad y la disponibilidad de la información. La privacidad se refiere a que la información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad para hacerlo de lo contrario estaríamos frente a una divulgación de información confidencial, lo que constituiría un ataque a la privacidad.

La integridad, por su parte implica que la información debe ser consistente, fiable y no estar propensa a alteraciones no deseadas.

La modificación no autorizada de saldos en un sistema bancario o de calificaciones en un sistema escolar son ejemplos de ataques a la integridad.

La disponibilidad, se refiere a que la información debe estar disponible en el momento en que el usuario la requiera por lo que un ataque a la disponibilidad podría ser la negación de servicio o "tirar" el servidor.

En cuanto a las vulnerabilidades comunes en los dispositivos de infraestructura de red, estos elementos son esenciales para la comunicación y el transporte de datos dentro de las redes corporativas, por lo que se convierten en objetivos primordiales para los ciber-atacantes.

Los fallos en switches, puntos de acceso, servidores, firewalls y routers, entre otros dispositivos, pueden permitir intrusiones mal intencionadas y comprometer la

información que fluye por la red, lo que puede derivar en la penetración de amenazas a la infraestructura crítica y causar un alto potencial de daño.

Por tanto, es importante que se tomen medidas para resolver estas vulnerabilidades y proteger la infraestructura de red de posibles ataques.

A menudo, esta fragilidad es causada por omisiones o inadvertencias en ciertas configuraciones y ajustes definidos para estos dispositivos de red, dentro de los fallos más comunes se encuentran:

Contraseñas y credenciales de acceso de seguridad deficiente

El Reporte Anual de Investigaciones sobre Violación de Datos de Verizon indica que el 81% de los ataques de seguridad se deben a contraseñas débiles o robadas.

Protocolos y sistemas de regulación obsoletos

Además, los sistemas y protocolos de seguridad actuales pueden ser obsoletos y no cumplir con los estándares de ciberseguridad, lo que puede resultar en la pérdida de información, que es el 43% del costo total de un ciberataque según Accenture. Geier, E. (2019)

Tráfico de red y patrones de acceso no encriptados

En cuanto al cifrado de la información, menos del 30% de las empresas lo utilizan actualmente. Además, los códigos maliciosos se esconden a menudo detrás de archivos de Microsoft Office.

Configuraciones y ajustes predeterminados en dispositivos

La configuración predeterminada de los dispositivos también puede ser un problema, como se vio con el fallo del Small Business Switch de Cisco, que presentó una vulnerabilidad crítica debido a una cuenta de usuario con privilegios de administrador que no podía ser desactivada. Geier, E. (2019)

Para mejorar la seguridad de los dispositivos de infraestructura de red, se recomienda segmentar y microsegmentar las redes, limitar las comunicaciones innecesarias, endurecer los dispositivos, asegurar el acceso y validar la integridad del hardware y software.

Según Geier, E. (2019), Además es importante contar con una solución de seguridad digital, como el módulo de cumplimiento de dispositivos de red de openNAC Enterprise, para llevar la seguridad a un nuevo nivel. Este módulo permite determinar la brecha entre la configuración actual y la configuración segura de referencia emitida por el Centro Criptológico.

Análisis comprativo de Equipos

Según (Gomes, Ferreira, & de Souza, 2021), si cuenta con múltiples sistemas que son elementos esenciales de su pequeña empresa, contar con un firewall resulta una medida importante para mantener la seguridad. Un firewall dedicado y eficiente puede evitar ataques de ransomware, reducir las oportunidades para la ingeniería social y detener ataques virales. A continuación, presentamos nuestros firewalls favoritos para pequeñas empresas:

- El mejor firewall sencillo: Ubiquiti EdgeRouter
- El mejor firewall en general: Fortinet
- El mejor firewall de software libre: OPNSense
- El mejor firewall para empresas en el hogar: Firewalla
- El mejor firewall empresarial: Cisco NGFW
- El mejor firewall para empresas que dependen de datos: SonicWall
- Para pequeñas empresas, el mejor firewall es Fortinet Security Fabric.

Así mismo (Gomes, Ferreira, & de Souza, 2021) describe que, los firewalls de Fortinet controlados por hardware son altamente respetados en la industria por su seguridad. Además de una red troncal de software potente que proporciona una amplia gama de protecciones para pequeñas y medianas empresas, Fortinet es una de las pocas empresas que ha diseñado sus propios procesadores de circuitos integrados (ASIC) específicos para aplicaciones.

Estos chips de seguridad están diseñados para ofrecer una administración de red de alta velocidad que puede expandirse a medida que el negocio crece sin comprometer la seguridad.

Fortinet ofrece una variedad de excelentes enrutadores para pequeñas empresas, cada uno con soporte para su protección de firewall de próxima generación. Estos enrutadores ofrecen diferentes anchos de banda para diversas funciones, dependiendo de los requisitos únicos de la empresa, pero todos pueden aprovechar el sólido firewall de Fortinet y otras características de protección. La administración se realiza a través de una consola única que mantiene todas las conexiones agrupadas para una supervisión completa y sencilla. (Bhandari & Sharma, 2020)

Fortinet también ofrece el paquete Security Fabric, que es especialmente diseñado para pequeñas empresas y ofrece una solución integral que incluye protección de dispositivos de punto final, firewall y seguridad mejorada para dispositivos y aplicaciones individuales. La operación remota es totalmente posible ya que todo se gestiona en la nube. (Bhandari & Sharma, 2020)

Para empresas pequeñas, el Ubiquiti EdgeRouter es una excelente opción como firewall debido a su asequibilidad y firewall incorporado que bloquea el tráfico web entrante por defecto. Además, los enrutadores Ubiquiti permiten agregar reglas

personalizadas al firewall para una comunicación bidireccional con el mundo y una mayor protección. Esto significa que puede configurar su cortafuegos para bloquear todas las conexiones entrantes de Internet o permitir el tráfico para conexiones ya existentes, mientras bloquea todo lo demás. (Bhandari & Sharma, 2020)

> *Ubiquiti ofrece a sus clientes una guía detallada que les ayuda a iniciarse en el proceso de configuración de sus enrutadores Edge, y les permite personalizar algunas características de forma más modesta. Además, todos los componentes hardware de Edge que proporcionan acceso al firewall son asequibles, lo que los convierte en una opción ideal para pequeñas empresas que buscan centrarse en la gestión de su negocio en lugar de preocuparse por la expansión de su red.*

> *La configuración del firewall es fácil y no requiere un conocimiento profundo de las redes, por lo que incluso los usuarios sin experiencia en tecnología pueden realizarla. Sin embargo, es importante tener en cuenta que el firewall de Ubiquiti no incluye soluciones antimalware integradas ni una VPN. A pesar de esto, estos servicios pueden complementarse con otro software y, en última instancia, el firewall de Ubiquiti sigue siendo una excelente opción para aquellos que desean un firewall confiable que no requiera mucha administración.*

El mejor firewall empresarial: Cisco Meraki MX

> *Cisco ha sido una empresa líder en el mercado de redes durante muchas décadas debido a la calidad y eficiencia de sus productos. Aunque en general,*

sus productos son más comúnmente utilizados en organizaciones más grandes, la solución de firewall empresarial Meraki MX de Cisco es una excelente opción para empresas pequeñas que desean una solución premium y completa.

La línea Meraki MX de Cisco ofrece una amplia variedad de modelos para elegir, desde opciones de nivel de entrada hasta modelos más grandes que pueden manejar hasta 10,000 conexiones simultáneas y 1,500 conexiones en un túnel VPN. Esto significa que es muy probable que encuentre una opción que se adapte perfectamente a las necesidades de su empresa. (Bhandari & Sharma, 2020)

El modelo MX64 ofrece protección completa de firewall con estado, gestión basada en la nube, filtrado de contenido y protección avanzada contra malware. Además, tiene una configuración VPN automatizada para proteger todas las conexiones web salientes. Si necesita una solución aún más grande, los modelos de enrutadores más grandes también admiten conexiones de módem USB para conectividad 3G / 4G en caso de que la conexión a Internet principal falle.

Si se está buscando una solución de firewall empresarial que ofrezca funciones integrales y premium, la línea Meraki MX de Cisco es una excelente opción. Con una variedad de modelos para elegir y una amplia gama de características de seguridad adicionales, esta solución se adapta perfectamente a las necesidades de las pequeñas empresas que buscan una solución completa y de alta calidad.

El mejor firewall gratuito para pequeñas empresas: OPNSense

OPNSense es una solución de firewall de código abierto, fácil de usar y completamente gratuita ya que ofrece las mismas características que los firewalls de alta gama de los principales desarrolladores comerciales. Aunque puede ser necesario que proporcione su propio hardware, OPNSense ofrece actualizaciones de seguridad

semanales y lanzamientos semestrales de las principales actualizaciones de la plataforma. Además, cuenta con una gran comunidad y documentación extensa para aprender a manejarlo.

Bhandari & Sharma (2020), indica que “Aunque no es la mejor opción para principiantes, OPNSense sigue siendo fácil de administrar a través de su interfaz web y es un cortafuegos rápido y eficiente que es adecuado tanto para redes pequeñas como para organizaciones más grandes”. Para empezar con OPNSense, hay una guía para principiantes que lo guiará a través del tipo de hardware que necesitará para ejecutarlo, así como de las pautas básicas de configuración y de dónde ir desde allí.

El mejor firewall para pequeñas empresas dependientes de datos: SonicWall mejores firewalls para pequeñas empresas sonicwall.

Si usted tiene un negocio en crecimiento que necesita servicios en línea y gestión de datos, puede que aún no estés preparado para una solución de nivel empresarial como las que ofrece Cisco. Pero si buscas algo similar que sea ágil, versátil y adecuado para pequeñas empresas, entonces SonicWall puede ser lo que necesitas. (Khurana, & Khurana, 2020)

Las opciones de firewall de nivel de entrada de SonicWall son excelentes para pequeñas empresas que necesitan un alto rendimiento, seguridad mejorada con aprendizaje automático y opciones de configuración rápida con cero toques.

Además, su proceso de inspección de paquetes de una sola pasada es impresionante y puedes obtener Wi-Fi integrado si lo necesitas. En la categoría de nivel de entrada, tienes cinco dispositivos diferentes para elegir según tus necesidades. Si estás interesado en conocer más sobre la tecnología de SonicWall y sus precios, revisa sus opciones.

El mejor firewall para empresas en el hogar: Firewalla mejores cortafuegos para pequeñas empresas firewalla.

Para las nuevas empresas emergentes y empresas en el hogar que buscan una seguridad superior, puede resultar difícil encontrar una solución de firewall adecuada. Afortunadamente, Firewalla se enfoca directamente en este mercado. Ofrece una variedad de modelos, como el modelo Rojo para usuarios domésticos que no necesitan mucha velocidad y el modelo Azul para usuarios comerciales con mayores velocidades de transferencia de datos. Cualquiera de los modelos puede ser adecuado para situaciones específicas. Además, la marca también lanzará una versión más avanzada en 2020 para empresas más grandes, lo que significa que puede seguir confiando en Firewalla incluso después de que su negocio crezca. (Khurana, & Khurana, 2020)

Una de las características clave de Firewalla son sus alertas de amenazas robustas, que ayudan a detectar posibles ataques. También incluye opciones de VPN integradas, bloqueo de anuncios y muchas otras características de seguridad importantes. En resumen, si busca una solución de firewall para su pequeña empresa o negocio en el hogar, Firewalla es una excelente opción para considerar. (Khurana, & Khurana, 2020)

MARCO METODOLOGICO

Al seleccionar la metodología de investigación, se ha tomado en cuenta para esta área de estudio sobre seguridad en redes inalámbricas es importante que se seleccione una metodología de investigación adecuada que se adapte al problema de estudio y objetivos de investigación. Algunas de las metodologías de investigación comunes que se utilizan en la seguridad en redes inalámbricas incluyen:

El estudio detallado de uno o varios casos en profundidad para comprender mejor los problemas de seguridad en las redes inalámbricas en Artefacta y cómo abordarlos.

Entrevistas con expertos: estas metodologías se utilizan para recopilar datos de los usuarios de redes inalámbricas y obtener información sobre sus necesidades y problemas de seguridad.

Análisis de documentos: esta metodología implica el análisis de documentos relacionados con la seguridad en redes inalámbricas, como informes de seguridad, estándares y políticas de seguridad.

Utilizando además una metodología cualitativa, ya que responde a cuestionamientos que no son medibles y estos son enfocados a obtener datos e información de experiencias o percepciones de expertos relacionados con esta investigación.

Además, se llevará a cabo una comparación de los resultados obtenidos de la investigación a través de la realización de entrevistas. Estos resultados se analizarán y discutirán para validar y comprobar las contribuciones de los expertos que estén relacionados con la investigación propuesta.

RESULTADOS

Se han realizado preguntas a expertos conocedores del sector, todos ingenieros en informática que conocen del tema tecnológico y las redes y seguridades, en relación a las preguntas de: Que tipo de equipos de redes de telecomunicaciones inalámbricas conoce que puedan brindar una garantía de seguridad en las empresas; Responde el Ing. Saltos (Anexo1), lo siguiente:

Hay varios tipos de equipos de redes de telecomunicaciones inalámbricas que pueden brindar una garantía de seguridad en las empresas. Algunos de estos incluyen puntos de acceso inalámbricos seguros, cortafuegos inalámbricos, sistemas de detección y prevención de intrusiones (IDS/IPS), VPN inalámbricas y soluciones de gestión de movilidad empresarial (EMM). Estos dispositivos y soluciones utilizan tecnologías como Wi-Fi Protected Access (WPA) o WPA2, encriptación y control centralizado para proporcionar una conexión segura y una gestión más eficiente de la seguridad en las redes inalámbricas de las empresas.

Ing. Burbano Refiere:

Siempre es recomendable contar con equipos de vanguardia, con flexibilidad de tecnologías para la adopción de seguridades y métodos de autenticación además que sean capaces de bríndame niveles de comunicación e interconexión adoptando altos estándares e interoperabilidad con otros fabricantes de seguridad

Cuales considera que podrían ser los problemas más comunes entorno a la seguridad de las redes inalámbricas de Artefacta en el cantón Baba; Responde el Ing. Saltos (Anexo1), lo siguiente:

Los problemas comunes en la seguridad inalámbrica incluyen contraseñas débiles que permiten el acceso no autorizado, la interferencia de señal que afecta la confiabilidad de la conexión, la falta de actualizaciones de seguridad que hacen que los dispositivos sean vulnerables, el uso de redes públicas no seguras que pueden exponer a los usuarios a ataques y la presencia de malware que puede comprometer la seguridad de la red y propagarse a otros dispositivos.

Ing. Burbano Refiere:

Existen varios problemas en el ecosistema de seguridad sin embargo los problemas más comunes es la mala adopción seguridad, desconocimiento de tecnologías y mal despliegue no aterrizado a la realidad o basado a estudios

Que estrategias recomendaría para garantizar una mejora en las seguridades y la privacidad en redes inalámbricas de Artefacta en el cantón Baba;

Responde el Ing. Saltos (Anexo1), lo siguiente:

Para garantizar una mejora en la seguridad y privacidad de las redes inalámbricas, se deben implementar diversas medidas de seguridad. Entre ellas se encuentran: el uso de encriptación, aplicar actualizaciones de seguridad, utilizar una red privada virtual (VPN), utilizar un firewall, educar a los usuarios sobre prácticas de seguridad adecuadas, y aplicar control de acceso para limitar el acceso a usuarios autorizados solamente.

Ing. Burbano Refiere:

Las buenas prácticas de IT indican que los servicios ofrecidos deben ser sectorizados, segmentados, monitoreado.

Es recomendable que se efectúen consultorías de testing de seguridad y la solución debe ser escalable y cifrada, Es bueno que el proyecto sea desplegado como proyecto con políticas y procedimientos de servicios.

DISCUSION DE RESULTADOS

El mercado de las telecomunicaciones es altamente competitivo debido al rápido avance en el desarrollo de políticas y de las tecnologías. Este campo está en constante evolución y ha experimentado un gran progreso en los últimos años. Las telecomunicaciones son vitales en la mayoría de los sistemas tecnológicos, y su impacto ha modificado la forma en que nos relacionamos y comunicamos entre nosotros. Además, el sector de las telecomunicaciones es clave para la transformación del tejido productivo y del bienestar de la sociedad, y ha demostrado su potencia de fuego durante la pandemia. La digitalización se ha acelerado y esto presenta tanto desafíos como oportunidades para el futuro del sector.

Las empresas utilizan las telecomunicaciones como una herramienta importante para comunicarse de manera efectiva con los clientes y ofrecer un alto nivel de servicio al cliente. Además, las telecomunicaciones son un elemento clave en el trabajo en equipo y permiten a los empleados colaborar fácilmente desde cualquier lugar.

Las tecnologías de la información y comunicación también se han convertido en una excelente herramienta que permite a las empresas generar un valor agregado a las actividades operacionales, buscando ofrecer ventajas empresariales para lograr consolidarse en un mercado global.

Las telecomunicaciones son vitales para el éxito general de un negocio y afectan la forma en que las personas se conectan y hacen negocios a escala global

El uso creciente de la tecnología de la información en la actividad económica ha dado lugar a un incremento sustancial en el número de puestos de trabajo informatizados. Las tecnologías de la información y comunicación (TIC) se han convertido en una excelente herramienta que permite a las empresas generar un valor agregado a las actividades operacionales, buscando ofrecer ventajas empresariales para lograr consolidarse en un mercado global.

> *Es importante recalcar además la opinión de los entrevistados en estos casos, donde se menciona que: Los problemas comunes en la seguridad inalámbrica incluyen contraseñas débiles que permiten el acceso no autorizado, la interferencia de señal que afecta la confiabilidad de la conexión, la falta de actualizaciones de seguridad que hacen que los dispositivos sean vulnerables, el uso de redes públicas no seguras que pueden exponer a los usuarios a ataques y la presencia de malware que puede comprometer la seguridad de la red y propagarse a otros dispositivos.*

Las telecomunicaciones para Artefacta son una herramienta de importancia vital para los negocios hoy en día, permitiendo a las empresas comunicarse de manera efectiva con los clientes y ofrecer un alto nivel de servicio y atención al cliente. Además, las telecomunicaciones son un elemento clave en el trabajo en equipo y permiten a los empleados colaborar fácilmente desde cualquier lugar. En resumen, la tecnología de la información y las telecomunicaciones son fundamentales para el éxito de las empresas y para mejorar la productividad y optimizar los procesos.

Las telecomunicaciones son una herramienta importante para las empresas y representan un campo ocupacional en constante evolución. El crecimiento de las tecnologías ha aumentado la necesidad empresarial de mantenerse conectado e informado.

Las telecomunicaciones permiten a las empresas comunicarse de manera efectiva con los clientes y ofrecer un alto nivel de servicio al cliente, lo que refuerza la lealtad a la marca y aumenta la retención. Además, las telecomunicaciones son un elemento clave en el trabajo en equipo y permiten a los empleados colaborar fácilmente desde cualquier lugar. Las telecomunicaciones también pueden mejorar el rendimiento en los proyectos y la gestión de relaciones con los clientes. En resumen, las telecomunicaciones son fundamentales para el éxito de las empresas y pueden mejorar la productividad y optimizar los procesos

> *En tal sentido, es necesario brindar seguridad inalámbrica a las redes de datos de Artefacta del cantón Baba, existen equipos firewall que pueden realizar excelente trabajo, sin embargo, aquí el inconveniente detectado y gracias a la participación de los expertos no solamente es cuestión de equipos y la posible afectación por algún ataque de hackers, sino más bien de la continuidad de las operaciones o continuidad del negocio.*
>
> *Sin un enlace eficiente las comunicaciones se verán interrumpidas o por algún obstáculo en las líneas de vista las comunicaciones se van a ver afectadas, siendo el principal punto de vulnerabilidad, que por lo consiguiente es controlable, todo depende de la estrategia técnica de los enlaces y del presupuesto.*

CONCLUSIONES

En el sector de Baba, se identificaron empresas con la mayor participación en el área agrícola, es decir haciendas y estas mantienen sus formas de comunicación por radio enlace siendo esto una herramienta importante para las operaciones transaccionales de estas empresas que trabajan a campo abierto como lo es Artefacta.

Las comunicaciones inalámbricas de Artefacta en el cantón Baba efectivizan un alto nivel de servicio al cliente. Además, son un elemento clave en el trabajo en equipo, permitiendo a los empleados colaborar fácilmente desde cualquier lugar. Las telecomunicaciones móviles ofrecen a las empresas la oportunidad de presentar un trabajo más flexible al permitir a los empleados trabajar de manera eficiente desde casa.

En el cantón Baba, para implementar y mantener redes inalámbricas, es significativamente más alto el costo que en zonas urbanas debido a la falta de infraestructura existente y a los costos de implementación de nuevas torres de transmisión y equipos. Es uno de los principales inconvenientes, dado que Artefacta están desplegada en esta zona de baja cobertura.

La seguridad de la información de las empresas es vital en el campo de las telecomunicaciones. Los firewalls son una medida importante para mantener la seguridad de la información de la organización, sin embargo el principal problema es la disponibilidad de las comunicaciones, ya que mantener las operaciones en un menester importante para Artefacta.

Se han comparado varios equipos y se han identificado los mejores firewalls para pequeñas empresas, adecuada específicamente para su funcionamiento en Artefacta de Baba, estos controlados por hardware de Fortinet son algunos de los más seguros y

respetados en la industria, y están diseñados específicamente para ofrecer una administración de red de alta velocidad sin comprometer la seguridad.

La seguridad relacionada con la privacidad es un componente importante en este medio, ya que personas de otros lados, pueden infiltrarse o apropiarse de información útil y reservada afectando además las operaciones de Artefacta del cantón Baba.

RECOMENDACIONES

Se recomienda a los propietarios o gerentes de Artefacta del cantón Baba, disponer a quien corresponda la delegación técnica para que pueda aplicar lo siguiente:

Uso de cifrado WPA2, ya que la implementación de cifrado WPA2 (Wi-Fi Protected Access II) en la red inalámbrica ayudará a proteger la privacidad de los datos transmitidos a través de la red.

Es importante cambiar las contraseñas predeterminadas de las infraestructuras de comunicación y configurar contraseñas fuertes y únicas, así mismo, si su empresa tiene visitantes frecuentes, es recomendable que se configure una red separada para invitados para que los visitantes puedan acceder a Internet sin tener acceso a la red corporativa.

Mantener un control de acceso a la red inalámbrica y que se restrinja el acceso solo a los dispositivos autorizados. Esto puede hacerse a través de la configuración de filtros MAC, que permiten que solo los dispositivos cuyas direcciones MAC hayan sido aprobadas puedan conectarse a la red inalámbrica.

También es recomendable tener los firmwares de la infraestructura actualizados, los fabricantes a menudo liberan actualizaciones de seguridad para corregir vulnerabilidades.

Es necesario configurar un firewall para la red inalámbrica, que pueda ayudar a prevenir ataques desde Internet.

Sobre todo, es recomendable en este territorio mantener enlaces de backup que permitan la continuidad de las operaciones, ya que estas muchas veces son interrumpidos por diferentes factores.

Siguiendo estas recomendaciones, las Artefacta del cantón Baba puede mejorar significativamente la privacidad en sus redes inalámbricas y proteger la información confidencial transmitida a través de la red.

REFERENCIAS BIBLIOGRÁFICAS

Li, Y., Zhang, J., Li, J., Liu, L., & Li, C. (2021). Study on the Impact of 5G Technology on Telecom Industry Development. Journal of Telecommunications and Information Technology, (1), 54-61.

Singh, A., & Aggarwal, S. (2019). Evolution of 5G and its Impact on Telecom Industry. International Journal of Innovative Technology and Exploring Engineering, 8(9), 1205-1209.

Chan, H. K., Feng, Y., Leung, T. W., & Chan, F. T. (2020). A review of the applications of blockchain technology in the telecommunications industry. IEEE Access, 8, 16091-16110.

Chong, S. Y., Thurasamy, R., & Ooi, K. B. (2019). Understanding the determinants of customers' intention to use internet of things (IoT) services in the telecommunication industry. Telematics and Informatics, 38, 218-229.

Mahdavinejad, M. S., & Hosseini, S. M. (2018). The impact of e-commerce on telecom industry performance: Evidence from developing countries. Telematics and Informatics, 35(5), 1360-1368.

Zhou, L., Dai, Q., Yang, Y., & Xiang, Y. (2019). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal, 4(5), 1125-1142.

Zhang, Y., Chen, M., Hu, J., & Yin, B. (2020). Blockchain for the Internet of Things: A Comprehensive Survey. IEEE Access, 8, 91965-91988.

Pang, Z., Wu, H., Gao, F., & Yang, Z. (2019). An Artificial Intelligence Platform for Internet of Things Devices. IEEE Internet of Things Journal, 6(3), 4333-4343.

Ge, X., Yu, H., & Xue, Y. (2020). Industrial Internet of Things-Based Smart Manufacturing: A Review. IEEE Transactions on Industrial Informatics, 16(1), 530-539.

Carvalho, A. L., Luís, M. F., & Antunes, M. C. (2018). Internet of Things and Smart Cities: A Review of Literature and Case Studies. In Springer Proceedings in Complexity (pp. 13-24). Springer, Cham.

Fernández, P. G., & Mendoza, J. R. (2019). Identificación y solución de problemas en redes de telecomunicaciones empresariales. Revista Investigación Académica, 87, 1-11.

Sánchez, C. S., Pérez, A. F., & García, M. F. (2018). Problemas más comunes en la gestión de redes empresariales. Revista Tecnología en Marcha, 31(6), 89-98.

Fuentes, D. M. (2020). Gestión de problemas en redes de telecomunicaciones empresariales. Revista Gestión en el Tercer Milenio, 23(46), 41-50.

Pardo, A. R., & Paredes, J. M. (2018). Problemas y soluciones en la implementación de redes empresariales. Revista de Tecnología de la Información y Comunicación, 14(2), 15-24.

Navarro, J. G., & Castro, F. C. (2019). Gestión de problemas en redes de telecomunicaciones empresariales: estudio de caso. Revista de Investigación Científica, 7(1), 23-31.

ANEXO 1

Diseño de Entrevista

Universidad Técnica de Babahoyo

Entrevista relacionada con: ANÁLISIS DE EQUIPOS DE COMUNICACIÓN Y LA PRIVACIDAD EN REDES INALAMBRICAS APLICADO A LA EMPRESA ARTEFACTA DEL CANTÓN BABA

Nombre del Profesional:

Empresa: Cargo:

1 Que tipo de equipos de redes de telecomunicaciones inalámbricas conoce que puedan brindar una garantía de seguridad en las empresas.

2 Cuales considera que podrían ser los problemas más comunes entorno a la seguridad de las redes inalámbricas de Artefacta en el cantón Baba

3 Que estrategias recomendaría para garantizar una mejora en las seguridades y la privacidad en redes inalámbricas de Artefacta en el cantón Baba;

Respuestas de las Entrevistas:

Universidad Técnica de Babahoyo

Entrevista relacionada con: ANÁLISIS DE EQUIPOS DE COMUNICACIÓN Y LA PRIVACIDAD EN REDES INALAMBRICAS APLICADO A LA EMPRESA ARTEFACTA DEL CANTÓN BABA

Nombre del Profesional: ING. HARRY SALTOS VITERI

Empresa: UTB Cargo: DOCENTE

1 Que tipo de equipos de redes de telecomunicaciones inalámbricas conoce que puedan brindar una garantía de seguridad en las empresas.

Existen varios tipos de equipos de redes de telecomunicaciones inalámbricas que pueden brindar una garantía de seguridad en las empresas. Algunos de ellos son:

Puntos de acceso inalámbricos seguros: estos son dispositivos que permiten la conexión de dispositivos inalámbricos a la red de la empresa. Los puntos de acceso inalámbricos seguros utilizan tecnologías como Wi-Fi Protected Access (WPA) o WPA2 para proporcionar una conexión segura.

Cortafuegos inalámbricos: estos son dispositivos que se utilizan para filtrar el tráfico de la red inalámbrica y prevenir posibles amenazas de seguridad. Los cortafuegos inalámbricos también pueden incluir características como la detección de intrusos y la prevención de ataques de denegación de servicio.

Sistemas de detección y prevención de intrusiones (IDS/IPS): estos sistemas se utilizan para monitorear la red inalámbrica y detectar actividades sospechosas o intentos de intrusión. También pueden bloquear automáticamente los intentos de ataque mediante la prevención de intrusiones.

VPN inalámbricas: una red privada virtual (VPN) permite a los empleados acceder a la red de la empresa de forma segura desde fuera de la oficina. Las VPN inalámbricas utilizan tecnologías de encriptación para asegurar que la conexión sea segura.

Soluciones de gestión de movilidad empresarial (EMM): estas soluciones proporcionan un control centralizado sobre los dispositivos móviles de la empresa, lo que permite una gestión más eficiente de la seguridad. Los EMM pueden incluir características como la gestión de dispositivos, la gestión de aplicaciones y la gestión de políticas de seguridad.

2 Cuales considera que podrían ser los problemas más comunes entorno a la seguridad de las redes inalámbricas de Artefacta en el cantón Baba

Contraseñas débiles: las contraseñas débiles son un problema común en la seguridad inalámbrica. Si se utilizan contraseñas fáciles de adivinar o que no cumplen con los requisitos de seguridad, los atacantes pueden utilizar herramientas de fuerza bruta para descifrar la contraseña y obtener acceso a la red.

Interferencia de señal: la interferencia de señal puede afectar la seguridad de las redes inalámbricas al hacer que la conexión sea menos confiable. La interferencia de señal

también puede ser causada por dispositivos que no están autorizados en la red, lo que aumenta el riesgo de acceso no autorizado.

Falta de actualizaciones de seguridad: la falta de actualizaciones de seguridad en los dispositivos de red inalámbrica es un problema común. Si los dispositivos no se actualizan regularmente, pueden ser vulnerables a nuevas amenazas y ataques.

Redes públicas no seguras: las redes públicas, como las de los aeropuertos, bibliotecas y cafeterías, son a menudo inseguras. Los usuarios que se conectan a estas redes pueden ser vulnerables a ataques de sniffing y otros ataques de red.

Malware: el malware es un problema común en la seguridad inalámbrica. Si un dispositivo se infecta con malware, puede comprometer la seguridad de la red inalámbrica al enviar información confidencial a un atacante o propagar el malware a otros dispositivos en la red.

3 Que estrategias recomendaría para garantizar una mejora en las seguridades y la privacidad en redes inalámbricas de Artefacta en el cantón Baba

Encriptación: se debe utilizar encriptación en la red inalámbrica para proteger la información que se transmite a través de la red. Es recomendable usar protocolos de encriptación como WPA2 para garantizar la seguridad de la red.

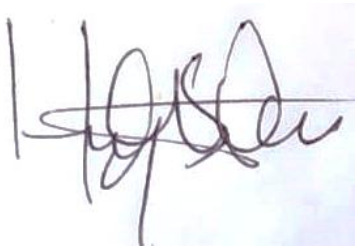
Actualizaciones de seguridad: se deben aplicar regularmente actualizaciones de seguridad para dispositivos y software de red inalámbrica para corregir vulnerabilidades conocidas y prevenir ataques.

Uso de VPN: se puede utilizar una red privada virtual (VPN) para proteger la privacidad de la información que se transmite a través de la red inalámbrica. Esto ayuda a mantener la información segura y privada, especialmente cuando se accede a la red desde lugares públicos como aeropuertos, bibliotecas y cafeterías.

Firewall: se debe utilizar un firewall para proteger la red inalámbrica de ataques externos. El firewall ayuda a bloquear el tráfico malicioso y a mantener la red segura.

Educación del usuario: es importante educar a los usuarios de la red inalámbrica sobre las prácticas de seguridad adecuadas. Se debe enseñar a los usuarios sobre el uso de contraseñas seguras, la importancia de las actualizaciones de seguridad y cómo evitar el phishing y otros ataques.

Control de acceso: se debe implementar un control de acceso para limitar el acceso a la red inalámbrica a usuarios autorizados solamente. Se puede usar la autenticación de usuario, el filtrado de dirección MAC y otras técnicas para asegurarse de que sólo los usuarios autorizados puedan acceder a la red.



Entrevista relacionada con: **ANÁLISIS DE EQUIPOS DE COMUNICACIÓN Y LA PRIVACIDAD EN REDES INALAMBRICAS APLICADO A LA EMPRESA ARTEFACTA DEL CANTÓN BABA**

Nombre del Profesional: ING. Ricardo Burbano Ferrin

Empresa: EPA Cargo Cargo: oficial de seguridad de la Información

1 Que tipo de equipos de redes de telecomunicaciones inalámbricas conoce que puedan brindar una garantía de seguridad en las empresas.

Siempre es recomendable contar con equipos de vanguardia, con flexibilidad de tecnologías para la adopción de seguridades y métodos de autenticación además que sean capaces de bríndame niveles de comunicación e interconexión adoptando altos estándares e interoperabilidad con otros fabricantes de seguridad

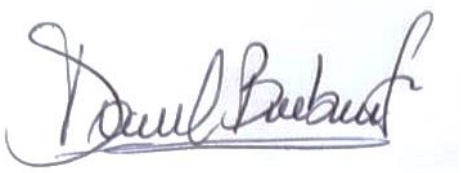
2 Cuales considera que podrían ser los problemas más comunes entorno a la seguridad de las redes inalámbricas de Artefacta en el cantón Baba

Existen varios problemas en el ecosistema de seguridad sin embargo los problemas más comunes es la mala adopción seguridad, desconocimiento de tecnologías y mal despliegue no aterrizado a la realidad o basado a estudios

3 Que estrategias recomendaría para garantizar una mejora en las seguridades y la privacidad en redes inalámbricas de Artefacta en el cantón Baba

Las buenas prácticas de IT indican que los servicios ofrecidos deben ser sectorizados, segmentados, monitoreado.

Es recomendable que se efectúen consultorías de testing de seguridad y la solución debe ser escalable y cifrada, Es bueno que el proyecto sea desplegado como proyecto con políticas y procedimientos de servicios.



Entrevista relacionada con: **ANÁLISIS DE EQUIPOS DE COMUNICACIÓN Y LA PRIVACIDAD EN REDES INALAMBRICAS APLICADO A LA EMPRESA ARTEFACTA DEL CANTÓN BABA**

Nombre del Profesional: ING. JACINTO AGUIRRE

Empresa: GOBIERNO PROVINCIAL DE LOS RIOS Cargo: ANALISTAS DE REDES

1 Que tipo de equipos de redes de telecomunicaciones inalámbricas conoce que puedan brindar una garantía de seguridad en las empresas.

creo que para las empresas puedan tener una mejor comunicación tanto en la velocidad y seguridad pueden aplicar equipos uniFi 6 pro de Ubiquiti estos equipos son gama media profesional para redes inalámbricas dónde pueden aplicar reglas de filtrado y gestionar varias redes en un mismo equipo según las necesidades de la empresa, aplicando vlan.

2 Cuales considera que podrían ser los problemas más comunes entorno a la seguridad de las redes inalámbricas de Artefacta en el cantón Baba

Los principales problemas son: la seguridad de la información y la disponibilidad de ancho de banda, en la actualidad el internet brinda una variedad de plataformas que consumen mucho ancho de banda como YouTube, TvIp, videos de redes sociales, etc... Esto se soluciona con una buena gestión del ancho demanda mediante Qos.

3 Que estrategias recomendaría para garantizar una mejora en las seguridades y la privacidad en redes inalámbricas de Artefacta en el cantón Baba

Reglas de filtrado, Qos, ocultar las redes más importantes de la empresa y brindar una red invitado dónde se destine un mínimo de ancho de banda para celulares y equipos que se conectan momentáneamente y que no pertenecen a la empresa. Así see podria mejorar

la disponibilidad de un buen ancho de banda, brindando mediante vlan las opciones de varias redes de acuerdo a la necesidades de la empresa.