REDES INALAMBRICAS

Las redes inalámbricas (WLAN: Wireless LAN) utilizan medios de transmisión inalámbricos (No guiados), haciendo uso de ondas electromagnéticas RF (Radio Frecuencia).

COMPARACIÓN RESPECTO A REDES INALÁMBRICAS

Ventajas

- Movilidad
- Mayor rapidez y flexibilidad en la instalación
- Menor costo
- Mayor escalabilidad

Desventajas

- Menor seguridad
- Menor velocidad
- Menor alcance

NORMA PARA REDES INALAMBRICAS

- Norma IEEE 802.11 (Estándar WiFi)

Parámetros especificados:

- Frecuencia (GHz) ➔ Capa Física
  - Dos valores: 2.4 GHz y 5 GHz
  - Alcance(distancia) es inversamente proporcional a la frecuencia. Es decir:

    mayor frecuencia ➔ menor alcance

    menor frecuencia ➔ mayor alcance
- Velocidad (Mbps) ➔ Capa Enlace de datos

Norma	Velocidad máxima (Mbps)	Frecuencia (GHz)
802.11 b	11	2.4
802.11 a	54	5
802.11 g	54	2.4
802.11 n	600	2.4/5
802.11 ac	1300	5

DISPOSITIVOS DE ACCESO INALÁMBRICO

- Router inalámbrico ➔ WiFi + Ethernet

A pesar del nombre "router" estos dispositivos en la mayoría de los casos son dispositivos de capas física y enlace de datos (acceso de red). Muy pocos tienen funciones completas de capa de red.

- Punto de acceso (Access Point) ➔ WiFi
- Extensores/Repetidores

Equipos que se utilizan para extender la cobertura de una red inalámbrica.

MODOS DE CONFIGURACION WIFI

- Modo WiFi de Infraestructura

En este modo "todos" los dispositivos de una red se conectan a través de un equipo de acceso: Access Point ó router inalámbrico.

- Modo WiFi Ad-Hoc

Este modo también conocido como modo "peer to peer", no requiere un punto de acceso centralizado. En su lugar, los dispositivos de la red inalámbrica se conectan directamente entre si, dentro de un rango definido. Por ejemplo: dos computadoras, una computadora con un celular.

INTRODUCCION AL DISEÑO DE REDES INALÁMBRICAS

Principales criterios/parámetros a considerar

- Cobertura
- *Frecuencia*
- *Antenas*
  - Omnidireccionales: cobertura 360°, corto alcance (30-100 m)
  - Direccionales: dirección única y muy exacta, largo alcance
  - Sectoriales: mezcla de las direccionales y omnidireccionales, cobertura 80° a 180°
  - *Potencia*
- Tráfico

Es necesario considerar el crecimiento exponencial de tráfico de red, sobre todo con aplicaciones que incluyen video de alta definición.

INTRANET

Es una red privada dentro de una empresa u organización que utiliza tecnología muy similar a la de Internet la cual permite a sus usuarios buscar, utilizar y compartir información y recursos.

En palabras técnicas, una Intranet, es generalmente una red de Área Local (LAN). Tiene la característica, de ser de uso exclusivo, de la empresa u organización que la ha instalado. Debido a ello, es que utiliza protocolos HTML, TCP/IP, HTTP, HTTPS, FTP, entre otros.

Beneficios

- Capacidad de compartir recursos (impresoras, escáner, cámaras IP, etc) y posibilidad de conexión a Internet.
- Alojamiento de páginas web, que pueden consultarse con los navegadores desde todos los ordenadores de la Intranet o desde cualquier ordenador externo que esté conectado a Internet.
- Servicios de almacenamiento de información. Espacios de almacenamiento virtual a los que se puede acceder para guardar y recuperar información desde los ordenadores del centro y también desde cualquier equipo externo conectado a Internet.

Beneficios

- Servicio de e-mail, que puede incluir diversas funcionalidades (buzón de correo electrónico, servicio de webmail, servicio de mensajería instantánea...)
- Foros, canales bidireccionales de comunicación entre los miembros. Algunos de estos foros pueden estar permanentemente en funcionamiento, y otros pueden abrirse temporalmente a petición. Por ejemplo, tablones de anuncios y servicios de chat y videoconferencia.
- Instrumentos diversos que permiten, a las personas autorizadas a ello, la realización de diversos trabajos.

Ventajas

- Sistema universal
- Costo asequible
- Adaptación a las necesidades específicas
- Fácil acceso a la información permitida
- Mejora la comunicación interna
- Facilita la formación del personal
- Seguridad
- Acceso a Internet (si se desea)

EXTRANET

Una Extranet es parte de la Intranet de una empresa u organización que se extiende a usuarios fuera de ella, usualmente utilizando Internet y sus protocolos.

- El acceso es más limitado que en la Intranet, proporcionando varios niveles de accesibilidad a los foráneos.
- Las Extranet ayudan a extender el alcance de las aplicaciones y los servicios basados en Intranet, asegurando el acceso a empresas y usuarios externos.

Beneficios

- Permite hacer transacciones seguras entre los sistemas internos de la empresa u organización.
- Mediante aplicaciones de la extranet los trabajadores de una empresa pueden obtener fácil y rápidamente la información sobre los clientes, proveedores y socios.
- Reducción de costos y ahorro económico para la empresa u organización.
- Totalmente basada en Internet.

Beneficios

- Desarrollado en cualquier herramienta de programación.
- Independiente del motor de Base de datos.
- Dirección en Internet bajo su propio dominio.
- Conexión a las bases de datos.
- Diseñada armónicamente con el mismo estilo del sitio web de la empresa u organización.

Principales Usos/Aplicaciones

- Banca online
- Groupware: diversas empresas u organizaciones participan en el desarrollo de nuevas aplicaciones con un objetivo común.
- E-learning corporativo: empresas u organizaciones participan y desarrollan programas educativos o de formación.
- Para empresas u organizaciones que son parte de un objetivo común de trabajo, mediante la extranet, pueden dirigir y controlar los proyectos comunes.

Principales Usos/Aplicaciones

- Una empresa u organización puede participar en redes de conocimiento junto con universidades, asociaciones y demás centros en programas de formación, en actividades de investigación y desarrollo, en bolsas de trabajo, etc.
- Manejo de sistemas comerciales: presupuestos, pedidos, catálogos, ofertas, etc.
- Asistencia técnica.
- Descarga de software.

REDES VITUALES PRIVADAS
(VPN: Virtual Private Network)

- Como su nombre lo indica, es una red privada de datos que hace uso de una infraestructura pública de telecomunicaciones, principalmente Internet, manteniendo la privacidad a través del uso de un protocolo de entubamiento y de procedimientos de seguridad.
- La tecnología de tubos ó túneles ("Tunneling") es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original.
- Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados.

VENTAJAS DE LAS VPN

- **Seguridad**

  Provee encriptación y encapsulación de datos de manera que hace que estos viajen codificados y a través de un túnel.

- **Costos**

  Ahorran grandes sumas de dinero en líneas dedicadas o enlaces físicos.

- **Mejor administración**

  Cada usuario que se conecta puede tener un número de IP fijo asignado por el administrador, lo que facilita algunas tareas como por ejemplo mandar impresiones remotamente, aunque también es posible asignar las direcciones IP dinámicamente si así se requiere.

- **Facilidad de uso**

  Para los usuarios con poca experiencia para conectarse a grandes redes corporativas transfiriendo sus datos de forma segura.

- **Calidad de servicio (QoS)**

  Mejora el rendimiento de las redes sobre todo en servicios en tiempo real.

FUNCIONAMIENTO DE VPN

- Haciendo uso de firewalls en ambos sitios, permite una conexión segura a través de Internet.
- Involucra cifrar o encriptar los datos antes de enviarlos a través de la red pública y descifrarlos instantes antes de entregarlos a su destino final.

REDES VIRTUALES PRIVADAS VPN

TIPOS DE CONEXIÓN VPN

- **DE RED INTERNA A RED INTERNA (LAN to LAN)**

Permite conectar virtualmente dos redes locales separadas geográficamente a través de dos enrutadores o firewalls. Hace uso del servidor VPN en una de las intranets y el cliente VPN en la otra (acceso remoto dedicado o temporal).

- **DE CLIENTE A RED INTERNA (Client to LAN)**

Conecta usuarios remotos (dispositivos finales: computadoras, impresoras, sensores…) que utilizarán servicios o aplicaciones que se encuentran en uno o más equipos dentro de la red interna.

- **DE CLIENTE A SERVIDOR (Client to Server):**

También conocidas como conexiones Web VPN, son las más modernas y usadas actualmente para brindar servicios de empresas u organizaciones. No es necesaria la instalación, ni configuración de ningún programa o software para realizar conexiones VPN. Simplemente accediendo a una Web (acceso remoto) y con un usuario y contraseña, tendremos la conexión Web VPN para acceder a recursos internos de la empresa u organización de manera fácil y segura.

- **VPN over LAN**

Este tipo de conexión es el menos difundido pero uno de los mas poderosos para utilizar dentro de una empresa u organización. Es una variante del tipo Client to LAN, pero en vez de utilizar Internet como medio de conexión (acceso remoto), emplea la misma LAN de la empresa u organización (acceso local). Se utiliza para aislar zonas y/o servicios de la red interna. Esta capacidad la hace muy conveniente para mejorar las prestaciones de seguridad principalmente en las redes inalámbricas WiFi.

REQUERIMIENTOS PARA UNA VPN

- **Servidor VPN**

Básicamente es una computadora conectada a Internet esperando por conexiones de usuarios VPN y si estos cumplen con el proceso de autenticación, el servidor aceptara la conexión y dará acceso a los recursos de la red interna.

- **Cliente VPN**

Este puede ser un usuario local o remoto o un enrutador o firewall de otra LAN.

- **Conexión a Internet**

Dedicada o temporal.

- **Asegurarse que la VPN sea capaz de:**
  - Encapsular los datos.
  - Encriptar los datos.
  - Autentificar usuarios.
  - Asignar direcciones IP de manera estática y/o dinámica.

REDES DE AREA LOCAL VITURALES (VLAN: VIRTUAL LAN)

VIRTUAL LAN

- Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.
- Cada VLAN creada representa una red (subred) diferente y separada. Por ejemplo, la red de un campus universitario puede separar los usuarios en tres grupos: alumnos, profesores y administración.
- Requieren switches que las soporten.
- Las VLAN se configuran mediante software en lugar de hardware, lo que las hace extremadamente fuertes.

LAN COMUNES

- Los switches básicos (capa 2) son utilizados para crear las redes comunes en las que tenemos un solo dominio de difusión.

LAN COMUNES

- A medida que la red crece, se genera un problema con la circulación de paquetes de broadcast debido a que tenemos un solo dominio de difusión.
- Otro problema se relaciona con la seguridad, ya que cada computadora puede ver todos los demás equipos conectados a la red, lo cual incrementa la posibilidad de ataques.

Ventajas

- Mejoran el rendimiento de la red, reduciendo el tamaño del dominio de difusión.
- Al reducir el tráfico de difusión, se reduce el consumo de CPU por procesado de tráfico broadcast no deseado.
- Mejoran la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local.
- Mejoran la seguridad, reduciendo la posibilidad de ataques.
- Ayudan a reducir el costo de inversión en equipo.

CLASIFICACION DE LAS VLAN

Las redes de área local virtuales se pueden clasificar en cinco tipos según el nivel/capa de la jerarquía OSI en el que operen:

- **VLAN de nivel 1 (por puerto)**

  También conocida como "port switching" son las más habituales . Se especifica qué puertos del switch pertenecen a la VLAN, los miembros de dicha VLAN son los que se conecten a esos puertos. No permite la movilidad de los usuarios, habría que reconfigurar las VLAN si el usuario se mueve físicamente.

- **VLAN de nivel 2 por direcciones MAC**

  Se asignan hosts a una VLAN en función de su dirección MAC. Tiene la ventaja de que no hay que reconfigurar el dispositivo de conmutación si el usuario cambia su localización, es decir, se conecta a otro puerto de ese u otro dispositivo. El principal inconveniente es que si hay cientos de usuarios habría que asignar los miembros uno a uno.

- **VLAN de nivel 2 por tipo de protocolo**

  La VLAN queda determinada por el contenido del campo tipo de protocolo de la trama MAC. Por ejemplo, se asociaría VLAN 1 al protocolo IPv4, VLAN 2 al protocolo IPv6, VLAN 3 a AppleTalk, VLAN 4 a IPX...

- **VLAN de nivel 3 por direcciones de subred (subred virtual)**

  La cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece. En este tipo de VLAN son los paquetes, y no las estaciones, quienes pertenecen a la VLAN. Estaciones con múltiples protocolos de red (nivel 3) estarán en múltiples VLAN.

- **VLAN de niveles superiores**

  Se crea una VLAN para cada aplicación: FTP, flujos multimedia, correo electrónico... La pertenencia a una VLAN puede basarse en una combinación de factores como puertos, direcciones MAC, subred, hora del día, forma de acceso, condiciones de seguridad del equipo...

Seguridad en Redes

Las redes informáticas sean convertidas en una parte integral de nuestra vida cotidiana. Todos los tipos de empresas y organizaciones utilizan las redes para funcionar de manera eficiente.

Las redes se utilizan para copilar, procesar, compartir y almacenar grandes cantidades de información digital, la protección de esta información se vuelve incluso más importante para nuestra seguridad nacional y estabilidad económica.

La ciberseguridad es el esfuerzo constante por proteger estos sistemas de red y todos los datos contra el uso no autorizado o los daños.

A nivel nacional, debe protegerse su identidad, sus datos y sus dispositivos informáticos. A nivel comparativo, es responsabilidad de todos proteger la reputación, los datos y los clientes de la empresa u organización. A nivel del estado, la seguridad nacional, y la seguridad y bienestar de los ciudadanos están en juego.

Exigencia de seguridad (TRIADA)

Confidencialidad (Privacidad)

Los políticos informáticos de una empresa u organización deben restringir el acceso a la información los entes autorizados y garantiza que solo las personas autorizadas tendrán acceso a estos datos

Integridad (Autenticidad)

La integridad es precisión, consistencia y confiabilidad de los datos dentro de su ciclo de vida. Los datos deben permanecer inalterados durante la transferencia y no deben ser modificados por entidades no autorizadas. La modificación incluye escribir, cambiar, cambiar de estado, suprimir y crear.

Disponibilidad

Requiere que los recursos informáticos estén siempre disponibles a los entes autorizados. Mantener los equipos, realizar reparaciones de hardware, mantener actualizados los sistemas operativos y el software, así como crear respaldos, garantiza la disponibilidad de la red y los datos a dichos entes autorizados.

Amenazas de seguridad

Interrupción:

Un recurso del sistema se distribuye o no llega a estar disponible o se inutiliza. Esta en una agresión de disponibilidad.

Intercepción:

Un ente no autorizado consigue acceder a un recurso. El ente no autorizado puede ser una persona, un programa o un computador. Esto es una agresión a la confidencialidad.

Modificación:

Un ente no autorizado no solamente gana acceso, sino que deteriora el recurso. Esto es una agresión a la integridad.

Fabricación

Una parte no autorizada inserta objetos falsos en el sistema. Esto es una agresión a la integridad.

Tipos de ataques

Pasivos:

La meta del atacante es tener acceso a la información que está siendo transmitida. Son el tipo de escuchas o monitorizaciones ocultas de la trasmisión. Son difíciles de detectar ya que no implican la alteración de los datos.

Activos:

Estas agresiones suponen la modificación del flujo de datos o la creación de flujos falsos con la intención de rehacer acciones fraudulentas, obtener ventajas o causar daños a una empresa u organización.

Ataques Pasivos:

Tipos:

Divulgación del contenido: Consiste en el acceso sin autorización a un mensaje, una conversación telefónica, mensaje de correo eléctrico.

Análisis del tráfico: consiste en el monitoreo de las transmisiones entre dos sistemas para obtener la información. Aunque los mensajes estén enmascarando, con el tiempo se puede llegar a conocer la naturaleza de comunicación.

Ataques activos:

Tipos:

Enmascaramiento: tiene lugar cuando una entidad pretende ser otra entidad diferente. Una agresión de enmascaramiento normalmente incluye una de las otras formas de agresión activa.

Repetición: Supone la captura pasiva de unidades de datos y su retransmisión subsecuente para producir un efecto no autorizado.

Modificación de mensajes: significa que alguna porción de mensaje legítimo se altera, o que el mensaje se retrasa o se reordena para producir un efecto no autorizado y poder tener ventaja.

Denegación de un servicio: impide o inhibe el uso de gestión normal de las facilidades de comunicación o de cualquier de los recursos disponibles en la red.

Protección de la información

La protección y privacidad en los datos que se transmitan a través de las redes públicas es a través del encriptamiento, ósea, ocultando el verdadero contenido del mensaje de tal forma que si es interceptado lo puede hacer descifrado.

Principales tipos de encriptamiento

-Encriptamiento convencional -Encriptamiento de clave pública o asimétrica

Encriptamiento Convencional

Este proceso consta de dos elementos principales:

- Un algoritmo.
- Una clave: es un valor independiente del texto nativo que controla al algoritmo.

El algoritmo producirá una salida diferente dependiendo de la clave específica que se utilice en ese momento.

Cambiando la clave cambia la salida del algoritmo.

Se recomiendan claves de 8 caracteres, letras, números, caracteres especiales.

Entre más compleja, mucho más difícil será la decodificación del mensaje en caso de ser interceptado.

Encriptamiento de clave pública o asimétrica

Se basa en una clave para el encriptamiento y en una clave diferente, pero relacionada, para el desencriptado.

Las claves de encriptamiento son intercambiados antes de iniciar la transferencia de información.

La clave de desencriptado permanecen en cada extremo (nunca se hacen públicas). El algoritmo producirá una salida diferente dependiendo de la clave específica que se utilice en ese momento.

No es factible determinar la clave de desencriptado solamente dando el algoritmo de criptografía y la clave de encriptado.

Cualquier clave, de las 2 que se utilicen se puede utilizar para el encriptado y el desencriptado.

Seguridad en redes inalámbricas

La seguridad es el mayor problema que presentan las redes inalámbricas. Cualquier dispositivo dentro del alcance de nuestro punto de acceso puede capturar el tráfico enviado desde los clientes:

Información delicada (contraseñas)

Privacidad (conversaciones, chat, telefonía, IP)

Archivos privados

Manipulación de la información

Delitos informáticos desde tu IP

Principales medidas de seguridad:

Ocultación del SSID (Service Set Identifier), nombre único de hasta 32 caracteres para identificar a la red wireless. Todos los componentes de la misma red WLAN deben de usar el mismo.

Filtrado MAC, número de identificación único de cada dispositivo de red.

Clave WEP: es el código de seguridad que permite a un grupo de computadoras, impresoras u otros dispositivos en la red intercambiar información en la red oculta de dispositivos fuera de la red.

Tamaños: 64, 128, 256 bits.

Uso de función de encriptado WPA(WiFi Protecten Access), WPA 2 PSK (Pre-Shared Key), WPA 3 con clave robusta evitando SSID común. Mejora la autentificación y cifrado, así como la integridad de la información cifrada.

Equipos de Seguridad en Redes

Cuando hablamos de seguridad en conexión a través de Internet 2 tecnologías usadas:

- Proxy Server
- Firewall

PROXY SERVER

Es y servidor que actúa como intermediario entre un usuario de una red interna y la Internet (Gateway) a fin de facilitar la conexión entre 2 puntos. Le permite a la empresa u organización tener una sola conexión segura a la Internet, y no una por cada equipo que se quiere.

Funcionalidades:

1. Registro del tráfico
2. Restricción a determinados tipos de tráfico
3. Control de acceso
4. Mejora de rendimiento
5. Anonimato de la comunicación

Ventajas:

1. Controla el acceso al internet
2. Precio bajo
3. Limita el acceso desde el exterior

Ejemplos web: HTTP/HTTPS, FTTP/FTTPS

FIREWALL

Desmotivo de seguridad puesto entre una red privada y el internet publica para mantener a los intrusos fuera del alcance de los trabajos que son propiedad de la empresa u organización. Su propósito principal es evitar que personas no autorizadas puedan establecer una conexión y el acceso a la red. Pueden ser implementados en el hardware y software, o una combinación de ambos.

Tipos de Firewall de Red:

- De filtrado de paquetes
  Proveen acceso a nivel de IP (Capa de Red).
  Se examinan los paquetes de acuerdo a las reglas de filtrado.
  Son muy utilizados para enlaces a internet.
  No son difíciles de configurar.
- Nivel Aplicativo
  Provee control de acceso a nivel de capa de aplicación
  Se instala software específico para cada aplicación.
  Son muy seguros.
  Cuentan con herramientas de auditoria.
  No son transparentes para los usuarios.
  Existe variedad de software de firewall de este nivel.

- Híbridos
  Combinación de las características del filtrado de paquetes y nivel aplicativo.
  Corrigen muchas de las debilidades de los firewalls de filtrado de paquetes.
  Mantienen algunos de los problemas de seguridad del filtrado de paquetes.

Políticas de configuración:

- Restrictiva: se denigra todo el tráfico excepto el que esta explícitamente permitido
  Nota (Cerrar todo y habilitar una que otra pago).

- Permisiva: se permite todo el tráfico excepto el que esta explícitamente denegado. Nota (Se deja todo y se va cerrando poco a poco).

Administración de Redes

Problemática:

Con el tiempo:

1. las redes se expanden geográficamente.
2. aumenta el número de usuarios
3. aumenta el número de nodos.

Al carecer las redes aparecen más exigencias:

1. Mayor disponibilidad (funcionamiento continuo)
2. Funcionalidad (todos los elementos operando bien)
3. Diversas aplicaciones (diferente tipo de trafico)
4. Calidad de servicio (trato especial cierto tráfico)
5. Adaptación de nuevas tecnologías
6. Mayor seguridad

Telecomuniction manegment network (TMN)

Es un modelo defiendo la serie M.3000 de la ITU – TI

Divide la administración de las redes en 5 áreas funcionales:

Administración de configuración:

Objetivos:

1. Satisfacer los requerimientos actuales y futuros de la red.
2. Mantener un manejo adecuado de los recursos de hardware y software.

-Tareas Asociadas:

3. Planeación y diseño de la red.
4. Selección de los recursos necesarios para mantener los sistemas y dispositivos.
5. Administración del hardware.
6. Administración del software

Manejo de configuraciones en equipos.

7. Políticas y procedimientos asociados:
8. Procedimiento de instalación de aplicaciones más utilizadas.
9. Políticas de respaldo de configuraciones
10. Procedimiento para la instalación de una nueva versión de sistema operativo en enrutadores.

Administración del Requerimiento:

Objetivos:

1. Mantener en el nivel planeado el desempeño de la red.
2. Monitorear y analizar el tráfico que circula por la red.

3. Prevención de problemas futuros.
4. Administración proactiva.

Tareas Asociadas:

1. Análisis de la informacion para la toma de decisiones:
    - Utilización elevada o proyecciones
    - Trafico inusual
    - Control de tráfico (ruteo)
    - Calidad de servicios

Administración de Fallas:

Objetivos:

1. Detectar y solucionar situaciones anormales en la red.

Etapas:

1. Monitoreo de alarmas (sistema de alarmas)
2. Localización de fallas
3. Pruebas de diagnostico
4. Corrección de fallas
5. Administración de reportes.

Políticas y procedimientos asociados:

1. Procedimiento de pruebas de diagnostico
2. Procedimiento general de corrección de fallas.
3. Políticas de seguimiento a reportes

Administración de contabilidad:

Objetivos:

1. Realizar los cobros correspondientes a la utilización de los recursos de la red.

Tareas:

1. Obtener informacion de la utilización de los recursos de la red.
2. Calcular las cuotas de acuerdo a los recursos utilizados.

Administración de la seguridad:

Objetivos:

1. Proporcionar servicios de seguridad a los elementos de la red.
2. Crear estrategias para prevención y detención de ataques
3. Crear estrategias para la respuesta a incidentes

Proceso:

1. Análisis de riesgos para definir requerimientos.
2. Politices de seguridad que sean consecuentes con la misión de seguridad.

Políticas y procedimientos asociados:

1. Políticas de contraseña.
2. Políticas de acceso remoto a ruteadores.
3. Políticas de lista de acceso.
4. Políticas de respaldo.

Conclusiones:

Un sistema de administración debe de revisarse constantemente.

Todas las áreas deben contar con sus propias políticas y procedimientos

PREGUNTAS DE EXAMEN

Una tarea de administración de la contabilidad en el modelo TMN es obtener información de la utilización de recursos de la red

VERDADERO

Para el acceso de los clientes a servicios de e-bankin se recomiendan las VPN del tipo “Client to Server”

VERDADERO

En el Encriptamiento convencional se recomiendan clases de un máximo de 8 caracteres

Falso

Una ventaja de las redes inalámbricas es que ofrecen menor seguridad

FALSO

En el modo WIFI “peer to peer” los dispositivos de la red inalámbrica se conectan directamente entre si, dentro de un rango definido.

VERDADERO

El Enmascaramiento es un tipo de ataque pasivo

Falso

La Divulgación del contenido de un mensaje es un ejemplo de ataque activo

Falso

Una Extranet brinda seguridad en el acceso a una Intranet a usuarios internos

Falso

Las antenas direccionales utilizadas en redes inalámbricas son de largo alcance

V

Un Cliente VPN puede ser un router de otra LAN

V

El uso de VLAN mejora la seguridad en redes WAN

F

En una conexión VPN LAN to LAN el cliente VPN debe tener un acceso remoto dedicado

F

Un objetivo de la administración de fallas en el modelo TMN es mantener un manejo adecuado de los recursos de hardware y software

F

En el Encriptamiento asimétrico es factible determinar la clave de desencriptado dando el algoritmo de criptografía y la clave de encriptado.

F

Una página web alojada en una intranet puede consultarse únicamente desde los ordenadores de la red interna

F

Las conexiones Web VPN sin las más modernas y usadas actualmente para brindar servicios de empresas u organizaciones

V

Uno de los valores de Frecuencia definidos en el Estándar WiFi es 2.4 MHz

F

En una VPN todas las direcciones IP deben ser estáticas

F

Una VPN es una conexión física de datos que hace uso de una infraestructura pública de telecomunicaciones

F

En el modo WiFi de Infraestructura los dispositivos de la red inalámbrica se conectan directamente entre sí, dentro de un rango definido

F

En seguridad en Redes, la Modificación es una agresión la disponibilidad

F

La confidencialidad requiere que los recursos informáticos estén siempre disponibles en los entes autorizados

F

Los Firewalls Híbridos corrigen muchas de las debilidades de los firewalls de nivel aplicativo

F

Una ventaja de las redes inalámbricas es que tienen mayor escalabilidad

V

Todos los Router inalámbricos tienen funciones completas de capa de red

F

En seguridad en Redes, la intercepción es cuando un ente no autorizado consigue acceder a un recurso y lo deteriora

F

El uso de VLN reduce el tamaño del dominio de difusión

V

Las conexiones VPN over LAN utilizan Internet como medio de conexión

F

Las políticas de respaldo de configuraciones están asociadas a la administración de la seguridad del modelo TMN

F

1. El uso de VLAN reduce el tamaño del dominio de difusión VERDADERO

2. Una dirección MAC (Media Access Control) es un número de identificación único de cada dispositivo de red VERDADERO

3. La confidencialidad requiere que los recursos informáticos estén siempre disponibles a los entes autorizados. FALSO

4. Un cliente VPN puede ser un router de otra LAN. VERDADERO

5. En seguridad en redes, la modificación es una agresión a la integridad. VERDADERO

6. En el encriptamiento convencional se recomiendan claves de un máximo de 8 caracteres FALSO

7. En el encriptamiento asimétrico, el algoritmo producirá una salida diferente dependiendo de la clave específica que se utilice en ese momento. VERDADERO

8. Las conexiones VPN over LAN utilizan internet como medio de conexión. FALSO

9. Las conexiones VPN LAN to LAN son las más modernas y usadas actualmente para brindar servicios de empresas u organizaciones. FALSO

10-Una extranet brinda seguridad en el acceso a un internet a usuarios externos. VERDADERO
11-El costo de un proxy server generalmente es mayor que el costo de un firewall. FALSO

12-Una VPN es una conexión física de datos que hace uso de una infraestructura pública de telecomunicaciones. FALSO

13-Un firewall facilita la conexión entre dos puntos FALSO

14-La intercepción es un tipo de ataque activo. FALSO

15-El enmascaramiento es un tipo de ataque activo. VERDADERO

16- En seguridad en redes, la intercepción es una agresión de disponibilidad. FALSO

17-Una página web alojada en un internet podría consultarse desde cualquier ordenador externo que esté conectado a internet. VERDADERO

18-El encriptamiento convencional se basa en un clave para el encriptado y en una clave diferente para el desencriptado. FALSO

19-El uso de VLAN mejora la seguridad en redes WAN. FALSO

20-En la Política Restrictiva de configuración de un Firewall se deniega todo el tráfico excepto el que esta explícitamente permitido. VERDADERO

21-En una conexión VPN LAN to LAN el cliente VPN debe tener un acceso remoto dedicado. FALSO

22-En las VLAN de nivel 3 son las aplicaciones quienes pertenecen a la VLAN. FALSO

23-Los firewalls híbridos corrigen muchas de las debilidades de los firewalls de nivel aplicativo. FALSO

24-Un firewall le permite a la empresa u organización tener una sola conexión segura al internet. FALSO

25- En las VLAN de nivel 1 es necesario reconfigurar las VLAN si el usuario se mueve físicamente. VERDADERO 2

6-El uso de VLAN facilita la segmentación física de una LAN. FALSO 27-Denegacion de un servicio es un tipo de ataque pasivo. FALSO

28-Un ataque activo puede crear flujos de datos falsos con la intención de realizar acciones fraudulentas. VERDADERO

29-Las redes informáticas ayudan, a las empresas y organizaciones que las utilizan, funcionar de manera eficiente y eficaz. VERDADERO

Uno de los valores de Frecuencia definidos en el Estándar WiFi es 5 MHz FALSO