|  |  |
| --- | --- |
| proyecto de red  Equipo: Emily Renata Miranda Franco, Sofía Valeria Meza García, Alan Fajardo Loeza, Adrián Oswaldo Torres Díaz. | CENTRO COMERCIAL  En esta propuesta de red nos enfocaremos en un centro comercial, que contará con distintos dispositivos y una organización. |

**SEGURIDAD DE RED INALAMBRICA**

**¿Qué es la seguridad informática?**

La seguridad informática se trata de mantener su internet inalámbrico, como el Wi-Fi, seguro de hackers o usuarios no autorizados. Utiliza contraseñas y métodos de cifrado especiales para asegurar que solo las personas permitidas puedan acceder a él y que los datos enviados a través de él estén protegidos. Esto ayuda a prevenir que personas externas roben o vean su información, como sus mensajes o qué sitios web visita.

**SSID**

El **SSID** es un identificador utilizado en redes Wi-Fi para distinguir diferentes redes dentro de una misma área geográfica. Es el nombre visible que aparece cuando buscas redes Wi-Fi disponibles en tu dispositivo.

Características del SSID:

* **Visibilidad**: El SSID puede ser visible o no visible. Si está configurado como "visible", se muestra en la lista de redes disponibles para que los usuarios puedan seleccionarlo. Si está "oculto", no aparecerá en la lista, pero los usuarios pueden conectarse si conocen el nombre exacto.
* **Longitud**: Un SSID puede tener hasta 32 caracteres alfanuméricos.
* **Personalización**: El SSID puede ser personalizado por el administrador del router o punto de acceso para reflejar la identidad de la red, como "CasaDeJuan" o "RedOficina".
* **Redes Wi-Fi públicas**: Muchos puntos de acceso, como los de cafés o aeropuertos, ofrecen SSID públicos que permiten a los usuarios conectarse fácilmente a la red.

¿Para qué sirve?

* El SSID se utiliza para identificar y distinguir una red Wi-Fi específica entre las muchas que pueden estar disponibles en una zona.
* Al conectarte a una red Wi-Fi, tu dispositivo busca los SSID disponibles y selecciona el que corresponde a la red que deseas utilizar.

**BSSID**

2. BSSID (Basic Service Set Identifier)

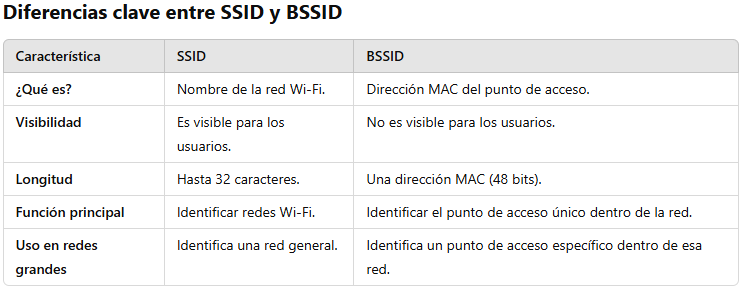
El **BSSID** es un identificador único para el punto de acceso (AP) que proporciona una red Wi-Fi. Este identificador corresponde a la dirección MAC (Media Access Control) de la interfaz de red del punto de acceso (por ejemplo, el router o el punto de acceso Wi-Fi). Cada punto de acceso tiene su propio BSSID único.

Características del BSSID:

* **Dirección MAC**: El BSSID es, en la práctica, la dirección MAC de la interfaz inalámbrica del punto de acceso. Esta dirección es única en todo el mundo.
* **Redes con múltiples puntos de acceso**: En una red con múltiples puntos de acceso (por ejemplo, una red de oficina o campus), cada punto de acceso tendrá su propio BSSID, pero todos compartirán el mismo SSID. Esto permite que los dispositivos se conecten a la red sin importar cuál de los puntos de acceso específicos estén dentro de su alcance, ya que todos proporcionan la misma red (SSID) pero con diferentes BSSIDs.

¿Para qué sirve?

* El **BSSID** es útil para las redes de múltiples puntos de acceso, donde varios routers o puntos de acceso están proporcionando cobertura para la misma red SSID. Aunque todos compartan el mismo nombre de red (SSID), cada punto de acceso tendrá su propio **BSSID**, lo que permite a los dispositivos saber a qué punto de acceso están conectados.
* Los BSSIDs también ayudan a los dispositivos a tomar decisiones sobre cómo conectarse a la red. Por ejemplo, un dispositivo puede cambiar de un punto de acceso con un BSSID débil a otro con una señal más fuerte si la red está configurada para manejar esas transiciones automáticamente.



**CIFRADO**

**Cifrado** es el proceso de convertir datos legibles (texto plano) en una forma ilegible (texto cifrado) para proteger la información de accesos no autorizados. Es una técnica utilizada en seguridad informática para asegurar la confidencialidad de los datos durante su transmisión o almacenamiento.

¿Cómo funciona el cifrado?

El cifrado usa algoritmos matemáticos y claves para transformar la información original en una secuencia de caracteres aparentemente aleatoria. Solo las personas o sistemas que posean la clave de descifrado adecuada pueden revertir este proceso y obtener la información original.

Tipos de Cifrado

Cifrado Simétrico:

* + En este tipo de cifrado, se utiliza la misma clave tanto para cifrar como para descifrar la información.
  + Ejemplo: AES (Advanced Encryption Standard), DES (Data Encryption Standard).
  + Ventaja: Rápido y eficiente, adecuado para cifrar grandes volúmenes de datos.
  + Desventaja: Si la clave se pierde o es interceptada, el sistema se vuelve vulnerable.

Cifrado Asimétrico:

* + Utiliza dos claves diferentes: una clave pública para cifrar y una clave privada para descifrar.
  + Ejemplo: RSA, ECC (Elliptic Curve Cryptography).
  + Ventaja: La clave privada nunca se comparte, lo que hace más seguro el proceso.
  + Desventaja: Es más lento que el cifrado simétrico.

Cifrado de Hash (Funciones de hash):

* + No es un cifrado tradicional, sino un proceso en el cual se convierte la entrada (mensaje) en una cadena de longitud fija (el hash), que no se puede revertir al mensaje original.
  + Ejemplo: SHA-256, MD5.
  + Uso: Validación de integridad de datos, almacenamiento seguro de contraseñas.

**Importancia del Cifrado**

* **Confidencialidad**: Solo los usuarios o sistemas autorizados pueden acceder a la información sensible.
* **Integridad**: Asegura que los datos no hayan sido alterados o manipulados durante la transmisión.
* **Autenticidad**: Garantiza que los datos provienen de una fuente confiable

**Autenticación**

La autenticación es el proceso de verificar la identidad de una persona, dispositivo o sistema para asegurarse de que sean quienes dicen ser. Es como cuando te piden tu identificación en un aeropuerto o en un banco para comprobar que eres tú mismo.

En el mundo digital, la autenticación se utiliza para proteger la seguridad de los sistemas y redes. Por ejemplo, cuando te conectas a una cuenta de correo electrónico o a una red social, debes introducir tu nombre de usuario y contraseña para autenticarte.

**Existen diferentes métodos de autenticación, como:**

1. **Autenticación de contraseña**: utiliza una contraseña para verificar la identidad.

2. **Autenticación biométrica**: utiliza características físicas, como huellas dactilares o reconocimiento facial.

3. **Autenticación de dos factores:** requiere una combinación de dos métodos de autenticación, como una contraseña y un código de verificación enviado al teléfono móvil.

La autenticación es fundamental para proteger la seguridad y la privacidad en el mundo digital.

**Protocolos de seguridad inalámbricos**

Los protocolos de seguridad inalámbricos son estándares y tecnologías diseñadas para proteger la comunicación y los datos transmitidos a través de redes inalámbricas, como Wi-Fi, Bluetooth, etc.

Estos protocolos buscan prevenir ataques y vulnerabilidades comunes en las redes inalámbricas, como:

**1. Intercepción de datos**

**2. Acceso no autorizado**

**3. Malware y virus**

**4. Ataques de hombre en el medio (Man-in-the-Middle, MitM)**

Algunos de los protocolos de seguridad inalámbricos más comunes son:

**1. WPA (Wi-Fi Protected Access):** un estándar de seguridad para redes Wi-Fi que utiliza cifrado y autenticación.

**2. WPA2 (Wi-Fi Protected Access 2):** una versión actualizada de WPA que ofrece mayor seguridad y cifrado más fuerte.

**3. WPA3 (Wi-Fi Protected Access 3):** la versión más reciente de WPA, que ofrece aún mayor seguridad y protección contra ataques.

**4. TLS (Transport Layer Security):** un protocolo de seguridad que cifra la comunicación entre dispositivos y servidores.

**5. HTTPS (Hypertext Transfer Protocol Secure):** un protocolo de seguridad que utiliza TLS para cifrar la comunicación entre navegadores web y servidores.

**6. EAP (Extensible Authentication Protocol):** un protocolo de autenticación que permite a los dispositivos autenticarse en redes inalámbricas.

Estos protocolos de seguridad inalámbricos son fundamentales para proteger la privacidad y la seguridad de los datos transmitidos a través de redes inalámbricas.

**Wep**

WEP (Wired Equivalent Privacy) es un protocolo de seguridad inalámbrica que se usaba para *cifrar datos y proteger redes Wi-Fi. Actualmente se considera obsoleto y inseguro.*

***Características***

* Se incluyó en el estándar IEEE 802.11 en 1999
* Utiliza el algoritmo RC4 para cifrar los paquetes de datos
* Utiliza claves de 64 o 128 bits
* Ofrece dos formas de autenticación: Open System Authentication y Shared Key Authentication

***Vulnerabilidades***

* A partir de 2001 se fueron identificando vulnerabilidades en el protocolo WEP
* Los criminales pudieron explotar estos defectos con mayor facilidad a medida que aumentaba la potencia informática
* En 2004, la Wi-Fi Alliance retiró oficialmente WEP

Alternativas WPA (Wi-Fi Protected Access), WPA2, WPA3.

***Recomendaciones***

* WPA2 es la mejor opción, aunque consume más potencia de procesamiento para proteger la red
* WPA3 es el más avanzado y resistente a las amenazas actuales
* Herramientas de cifrado como VPN pueden proteger aún más

## WPA

**WPA** (Wi-Fi Protected Access) es un conjunto de protocolos de seguridad para redes Wi-Fi que fueron diseñados para mejorar la seguridad de las redes inalámbricas, reemplazando a la vulnerabilidad del protocolo anterior **WEP** (Wired Equivalent Privacy). WPA fue introducido en 2003 por la **Wi-Fi Alliance** como una solución intermedia antes de la llegada de **WPA2**.

### **Evolución de WPA**

1. **WPA (Wi-Fi Protected Access) – 2003:**
   * **Objetivo**: Proporcionar una seguridad mejorada que mitigara las principales vulnerabilidades de WEP, como la debilidad en la clave de cifrado.
   * **Cifrado**: WPA utiliza el algoritmo de cifrado **TKIP** (Temporal Key Integrity Protocol) para garantizar la seguridad de las comunicaciones, en lugar del ya obsoleto RC4 de WEP.
   * **Autenticación**: WPA introduce la autenticación **802.1X** para controlar el acceso a la red, lo que lo hace más seguro que WEP.

Aunque WPA fue un avance significativo sobre WEP, aún presentaba algunas limitaciones, como la debilidad de TKIP y la falta de un cifrado más robusto.

1. **WPA2 (Wi-Fi Protected Access 2) – 2004:**
   * **Objetivo**: Reemplazar WPA con un protocolo más seguro y robusto.
   * **Cifrado**: WPA2 reemplaza TKIP por el algoritmo **AES** (Advanced Encryption Standard), que es mucho más fuerte y resistente a ataques de fuerza bruta.
   * **Autenticación**: Al igual que WPA, WPA2 también usa el estándar **802.1X** para autenticar a los usuarios, pero el protocolo de cifrado AES lo hace más seguro.
2. **WPA3 – 2018**: Como se mencionó previamente, WPA3 es la versión más reciente y ofrece aún más mejoras en seguridad, como protección contra ataques de diccionario, cifrado de 192 bits en redes empresariales, y mayor protección en redes abiertas.

### **Características principales de WPA:**

1. **Cifrado TKIP (Temporal Key Integrity Protocol)**:
   * TKIP mejora la seguridad de WEP al agregar un proceso de cambio dinámico de claves para cada paquete transmitido.
   * Aunque mejor que WEP, TKIP no es tan seguro como el cifrado AES utilizado en WPA2 y WPA3. Por eso, en redes más modernas, WPA2 con AES es la opción preferida.
2. **Autenticación 802.1X**:
   * WPA utiliza el protocolo **802.1X** para autenticar a los usuarios antes de que se les permita acceder a la red, asegurando que solo los usuarios autorizados puedan conectarse a la red inalámbrica.
3. **Integridad de Datos**:
   * WPA mejora la integridad de los datos al protegerlos de modificaciones no autorizadas durante la transmisión, asegurando que los paquetes de datos no sean alterados por un atacante.

### **Comparación de WPA con WEP y WPA2:**

| **Característica** | **WEP** | **WPA (TKIP)** | **WPA2 (AES)** |
| --- | --- | --- | --- |
| **Cifrado** | RC4 | TKIP | AES |
| **Autenticación** | Ninguna o WEP Key | 802.1X, Pre-Shared Key (PSK) | 802.1X, Pre-Shared Key (PSK) |
| **Seguridad** | Baja (fácil de hackear) | Mejor que WEP, pero aún vulnerable | Alta seguridad (muy difícil de hackear) |
| **Ideal para** | Redes simples y de baja seguridad | Redes de usuario común, mejores que WEP | Redes corporativas, redes domésticas modernas con alta seguridad |

### **¿Por qué usar WPA?**

* **Mejora la seguridad**: Al usar protocolos de cifrado más avanzados como TKIP (en WPA) y AES (en WPA2), WPA proporciona una mayor seguridad que WEP, que es muy vulnerable.
* **Protección contra ataques**: Utilizando técnicas como la rotación de claves y la autenticación 802.1X, WPA mejora la protección frente a ataques de interceptación y alteración de datos.
* **Compatibilidad**: WPA fue diseñado para ser compatible con dispositivos más antiguos que no soportan WPA2, aunque es recomendable actualizar a WPA2 o WPA3 cuando sea posible.

## WPA2 (PERSONAL Y EMPRESARIAL)

## ¿Qué es WPA2?

WPA2 se introdujo en el 2004 y era una versión mejorada de WPA. WPA2 se basa en el mecanismo de red de seguridad robusta (RSN, por sus siglas en inglés) y funciona en dos modos:

* **Modo personal o clave precompartida (WPA2-PSK)**: se basa en un código de acceso compartido y generalmente se usa en entornos domésticos.
* **Modo empresarial (WPA2-EAP)**: como sugiere el nombre, este modo es más adecuado para uso en empresas u organizaciones.

Ambos modos utilizan CCMP, que significa Protocolo de código de autenticación de mensajes de encadenamiento de bloques de cifrado en modo contador. El protocolo CCMP se basa en el algoritmo estándar de cifrado avanzado (AES), el cual proporciona una verificación de la autenticidad e integridad de los mensajes.

CCMP es más resistente y confiable que el protocolo de integridad de clave temporal (TKIP) original de WPA, lo cual dificulta que los atacantes detecten patrones.

Sin embargo, WPA2 también tiene sus inconvenientes. Por ejemplo, es vulnerable a ataques de reinstalación de claves (KRACK, por sus siglas en inglés). Un ataque KRACK explota una debilidad en WPA2, lo que permite a los atacantes hacerse pasar por una red clonada y obligar a la víctima a conectarse a una red maliciosa.

Esto permite al hacker descifrar una pequeña parte de los datos, la cual se puede agregar a otras para descifrar la clave de cifrado. Sin embargo, los dispositivos se pueden reparar y WPA2 todavía se considera más seguro que WEP o WPA.

WPA2-Personal es un protocolo de seguridad inalámbrica que se utiliza para proteger redes domésticas y pequeñas empresas. Utiliza una clave precompartida (PSK) para autenticar a los usuarios.

**Características de WPA2-Personal**

* Se basa en el mecanismo de red de seguridad robusta (RSN)
* Utiliza el estándar de cifrado avanzado (AES) para codificar los datos transmitidos
* Requiere que los dispositivos tengan la contraseña correcta para conectarse a la red

**Cómo configurar WPA2-Personal en un enrutador**

1. Abrir un navegador web en un dispositivo conectado al enrutador
2. Iniciar sesión en la consola de administración del enrutador
3. Ir al menú Inalámbrico o Configuración inalámbrica
4. Hacer clic en Seguridad
5. Seleccionar WPA2-PSK en las opciones de cifrado
6. Crear una contraseña segura
7. Guardar la configuración
8. Reiniciar el enrutador
9. Volver a conectar los dispositivos utilizando el nuevo SSID de WiFi y la contraseña creada

**EMPRESARIAL**

WPA2 también tiene una versión empresarial, WPA2-Enterprise, que se utiliza en empresas u organizaciones.

WPA2-Enterprise es un protocolo de seguridad de red inalámbrica que se usa en empresas y organizaciones. Se basa en el protocolo 802.1X y en el mecanismo de red de seguridad robusta (RSN).

**Características**

* Ofrece cifrado por aire y un alto nivel de seguridad
* Utiliza distintos protocolos de autenticación, cada uno con distintos niveles de cifrado
* Requiere un servidor RADIUS para verificar las credenciales de acceso
* Permite que los dispositivos cumplan con los requisitos más recientes de seguridad de la información

**Autenticación**

* Cada usuario debe autenticarse de forma individual utilizando sus propias credenciales
* El servidor RADIUS contiene la base de datos de credenciales permitidas
* El servidor verifica las credenciales del usuario, como nombre de usuario y contraseña, o certificados digitales

**Uso**

* WPA2-Enterprise es el estándar de oro para la seguridad de redes inalámbricas
* Es más adecuado para uso en empresas u organizaciones
* No es una buena solución si lo que deseas es instalar una red doméstica sin mantenimiento y ninguna molestia

## WPA3

**WPA3** (Wi-Fi Protected Access 3) es la última versión del protocolo de seguridad Wi-Fi, diseñado para mejorar la seguridad de las redes inalámbricas. Introducido por la Wi-Fi Alliance en 2018, WPA3 es el sucesor de **WPA2** y tiene como objetivo resolver las vulnerabilidades existentes, ofreciendo características más robustas para la protección de las redes Wi-Fi.

### **Características clave de WPA3:**

1. **Mayor seguridad en redes abiertas (sin contraseña):**
   * **Oportunidad de autenticación individualizada (SAE, Simultaneous Authentication of Equals):** En redes abiertas, WPA3 utiliza el protocolo SAE, un mecanismo de autenticación basado en una contraseña, para evitar ataques de tipo "man-in-the-middle" y mejorar la protección contra ataques de diccionario. Esto significa que incluso en redes abiertas (sin una contraseña), el tráfico entre los dispositivos es más seguro que en WPA2.
2. **Protección contra ataques de diccionario:**
   * WPA3 protege las contraseñas contra ataques de fuerza bruta y diccionario. En WPA2, los atacantes podían interceptar el tráfico y, a través de un ataque de diccionario, intentar adivinar las contraseñas. WPA3 hace más difícil realizar estos ataques debido a sus mejoras en el proceso de intercambio de claves.
3. **Cifrado de 192 bits (para WPA3 Enterprise):**
   * Para redes corporativas, WPA3 introduce un nivel de seguridad superior con el **cifrado de 192 bits** en WPA3 Enterprise. Esto proporciona un mayor nivel de protección para entornos que manejan datos sensibles.
4. **Mejora en la protección de la privacidad de la red:**
   * WPA3 hace que la conexión sea más segura incluso cuando se conecta a redes Wi-Fi públicas o compartidas. Utiliza un cifrado de extremo a extremo (conocido como **Protected Management Frames** o PMF) para proteger la información sensible y evitar que un atacante pueda escuchar las comunicaciones.
5. **Autenticación más fácil y segura en dispositivos IoT (Internet de las cosas):**
   * WPA3 facilita la conexión y autenticación de dispositivos IoT mediante el uso de **Easy Connect**. Esto mejora la facilidad de instalación y hace que la red sea más segura al evitar la transmisión de credenciales en texto plano.
6. **Cifrado de tráfico más fuerte:**
   * WPA3 utiliza un proceso de negociación de claves más robusto para el intercambio de información entre dispositivos, lo que evita que los atacantes puedan descifrar el tráfico intercambiado en la red.

### **Comparación de WPA3 con WPA2:**

| **Característica** | **WPA2** | **WPA3** |
| --- | --- | --- |
| **Cifrado** | AES (Advanced Encryption Standard) | AES, cifrado de 192 bits (para Enterprise) |
| **Protección contra ataques de diccionario** | Vulnerable a ataques de fuerza bruta | Resistente a ataques de diccionario (SAE) |
| **Redes abiertas (sin contraseña)** | Ninguna protección adicional | SAE proporciona mayor seguridad |
| **Cifrado de gestión de frames** | No | Sí (PMF - Protected Management Frames) |
| **Facilidad de conexión para dispositivos IoT** | Limitada | Mejora con WPA3 Easy Connect |

### **Ventajas de WPA3:**

* **Mayor seguridad** en redes tanto privadas como públicas.
* **Protección mejorada** contra ataques de interceptación y diccionario.
* **Cifrado más fuerte** para redes empresariales y dispositivos IoT.
* **Mejora de la privacidad** y la seguridad en redes abiertas.

### **Consideraciones:**

* **Compatibilidad**: Los dispositivos más antiguos que solo soportan WPA2 no podrán aprovechar las mejoras de WPA3, por lo que es importante asegurarse de que tanto los puntos de acceso como los dispositivos cliente sean compatibles con WPA3.
* **Adopción gradual**: Aunque WPA3 ofrece una mayor seguridad, aún no todos los dispositivos soportan este estándar, por lo que muchas redes aún operan con WPA2.

## METODO DE AUTENTICACION RADIUS

El **método de autenticación RADIUS** (Remote Authentication Dial-In User Service) es un protocolo de red utilizado para gestionar el acceso a servicios de red. RADIUS permite a las organizaciones autenticar a los usuarios y controlar sus accesos a través de un servidor centralizado, proporcionando un proceso seguro y eficiente para la autenticación, autorización y contabilidad (AAA, por sus siglas en inglés: Authentication, Authorization, and Accounting).

### **Funcionamiento básico:**

1. **Autenticación**: El servidor RADIUS verifica las credenciales del usuario (como nombre de usuario y contraseña) que se envían desde un dispositivo cliente (como un router, switch o punto de acceso inalámbrico). Si las credenciales son correctas, se permite el acceso; de lo contrario, se deniega.
2. **Autorización**: Una vez que el usuario ha sido autenticado, el servidor RADIUS puede asignar políticas específicas que determinen qué recursos o servicios puede acceder el usuario (como el acceso a una red de datos, a una VPN, etc.).
3. **Contabilidad**: El servidor RADIUS también lleva un registro de las actividades del usuario, como el tiempo de conexión, la cantidad de datos transferidos, etc., lo que ayuda en la auditoría y facturación, si corresponde.

### **Proceso típico de autenticación RADIUS:**

1. **Solicitud de acceso**: El cliente (por ejemplo, un router o un punto de acceso inalámbrico) recibe la solicitud de un usuario que intenta acceder a la red, y transmite esta solicitud junto con las credenciales al servidor RADIUS.
2. **Verificación de credenciales**: El servidor RADIUS recibe la solicitud y verifica las credenciales del usuario contra una base de datos (como un servidor LDAP, Active Directory, o una base de datos local de RADIUS).
3. **Respuesta del servidor RADIUS**:
   * Si las credenciales son correctas, el servidor RADIUS responde con un "Access-Accept", lo que permite que el usuario acceda a los recursos.
   * Si las credenciales son incorrectas, el servidor responde con un "Access-Reject" y el acceso es denegado.
4. **Contabilidad**: El servidor RADIUS también puede generar registros sobre la duración de la sesión, el uso de recursos y otros aspectos de la conexión.

### **Beneficios de RADIUS:**

* **Centralización**: Permite centralizar la autenticación y autorización de usuarios, lo que facilita la gestión de acceso en redes grandes.
* **Seguridad**: Utiliza métodos de encriptación para proteger las credenciales y los datos transmitidos entre el cliente y el servidor.
* **Escalabilidad**: Es adecuado para redes de diferentes tamaños, desde pequeñas redes hasta grandes infraestructuras corporativas.

### **Protocolos relacionados:**

* **TACACS+ (Terminal Access Controller Access-Control System Plus)**: Otro protocolo de autenticación similar a RADIUS, pero con diferencias en su manejo de la autenticación, autorización y contabilidad.

## ****método de filtrado MAC****

El **método de filtrado MAC** (Media Access Control) es una técnica de seguridad utilizada en redes inalámbricas y cableadas para controlar el acceso a la red mediante la **dirección MAC** de los dispositivos. Cada dispositivo de red, como un ordenador, un teléfono móvil, una impresora o un router, tiene una dirección MAC única asignada de fábrica, que se utiliza para identificar de manera unívoca al dispositivo en una red.

### ¿**Cómo funciona el filtrado MAC?**

El filtrado MAC funciona comparando la dirección MAC de un dispositivo que intenta conectarse a una red con una lista de direcciones MAC permitidas (lista blanca) o denegadas (lista negra) en el punto de acceso o el router. Dependiendo de si la dirección MAC del dispositivo está en la lista permitida o no, el acceso a la red será concedido o denegado.

### **Tipos de filtrado MAC:**

1. **Filtrado MAC en lista blanca (Allow List)**:
   * Solo los dispositivos que tienen sus direcciones MAC incluidas en la lista blanca pueden conectarse a la red. Los dispositivos con direcciones MAC no registradas en la lista serán rechazados.
2. **Filtrado MAC en lista negra (Deny List)**:
   * En este caso, el filtrado MAC bloquea el acceso a los dispositivos que tienen sus direcciones MAC registradas en la lista negra, mientras que todos los demás dispositivos que no estén en la lista podrán conectarse a la red.

### **Proceso de filtrado MAC:**

1. Un dispositivo intenta conectarse a la red Wi-Fi (o red cableada).
2. El punto de acceso o el router verifica la dirección MAC del dispositivo.
3. Si la dirección MAC del dispositivo está en la lista blanca (permitida) o no está en la lista negra (denegada), el dispositivo recibe acceso a la red.
4. Si la dirección MAC no está permitida, el dispositivo no podrá conectarse.

### **Ventajas del filtrado MAC:**

* **Control de acceso adicional**: Ayuda a controlar quién puede acceder a la red, añadiendo una capa de seguridad extra.
* **Fácil de implementar**: Muchos routers y puntos de acceso permiten configurar el filtrado MAC de manera sencilla a través de su interfaz de administración.

### **Desventajas del filtrado MAC:**

* **Fácil de eludir**: El filtrado MAC no es una solución completamente segura. Un atacante puede falsificar (o "spoof") la dirección MAC de su dispositivo para coincidir con una dirección permitida en la red. Esto hace que el filtrado MAC sea vulnerable a este tipo de ataques.
* **Mantenimiento**: Si tienes una red grande con muchos dispositivos, gestionar las direcciones MAC y asegurarte de que todas las direcciones de los dispositivos autorizados estén actualizadas puede ser una tarea tediosa.

### **¿Cuándo usar el filtrado MAC?**

Aunque el filtrado MAC no debe ser la única medida de seguridad en una red, puede ser útil en escenarios donde:

* Se quiera agregar una capa adicional de seguridad, como en redes pequeñas o redes domésticas.
* Se desea controlar de manera más estricta qué dispositivos pueden acceder a la red, especialmente si no se está utilizando una solución más avanzada como **WPA2** o **WPA3**.

### **¿Alternativa mejor al filtrado MAC?**

Para una seguridad más robusta, es recomendable usar **WPA2** o **WPA3**, que proporcionan cifrado fuerte y una autenticación adecuada. El filtrado MAC puede complementar estas medidas de seguridad, pero no debe ser el único mecanismo de protección.

## Políticas de seguridad de una red inalámbrica

Las **políticas de seguridad de una red inalámbrica** son un conjunto de reglas, prácticas y directrices que se implementan para proteger los datos, dispositivos y accesos dentro de una red Wi-Fi. Estas políticas tienen como objetivo prevenir accesos no autorizados, proteger la confidencialidad de los datos transmitidos y garantizar la integridad de la red frente a amenazas como intrusos, ataques de denegación de servicio (DoS), malware, y otros riesgos.

Aquí te describo algunas de las políticas de seguridad clave que se deben implementar en una red inalámbrica:

### 1. **Uso de Cifrado Fuerte (WPA2/WPA3)**

* **Política**: Utilizar siempre un cifrado fuerte como **WPA2** o **WPA3** en lugar de WEP o WPA, que son vulnerables.
* **Explicación**: WPA2 y WPA3 proporcionan cifrado AES (Advanced Encryption Standard), mucho más seguro que los métodos anteriores. WPA3 es el estándar más reciente y ofrece mejoras en la protección de redes abiertas y mayor resistencia a ataques de diccionario.

### 2. **Autenticación Segura (Contraseña Fuerte)**

* **Política**: Establecer contraseñas complejas y difíciles de adivinar para acceder a la red Wi-Fi.
* **Explicación**: Las contraseñas deben ser largas (al menos 12 caracteres), contener una combinación de letras mayúsculas, minúsculas, números y caracteres especiales. También se debe cambiar la contraseña regularmente y no usar contraseñas predeterminadas proporcionadas por el fabricante del router.

### 3. **Filtrado de Direcciones MAC**

* **Política**: Implementar el filtrado de direcciones MAC en el router o punto de acceso.
* **Explicación**: Esta política solo permite que dispositivos con direcciones MAC específicas se conecten a la red. Aunque no es una solución de seguridad infalible, puede agregar una capa adicional de control sobre qué dispositivos pueden acceder a la red.

### 4. **Desactivar la Difusión del SSID (Identificador de la Red)**

* **Política**: Configurar el router o el punto de acceso para que no emita el SSID (nombre de la red) de forma pública.
* **Explicación**: Al ocultar el SSID, se reduce la visibilidad de la red para los dispositivos que no conocen el nombre. Sin embargo, este método no es completamente seguro, ya que los atacantes avanzados pueden detectar redes ocultas.

### 5. **Autenticación de Usuarios (802.1X)**

* **Política**: Utilizar autenticación basada en **802.1X** para redes corporativas o de alta seguridad.
* **Explicación**: 802.1X es un protocolo de autenticación que requiere que los dispositivos que intentan conectarse a la red se autentiquen con un servidor central (RADIUS). Esto asegura que solo los usuarios autorizados puedan acceder a la red.

### 6. **Red Separada para Invitados**

* **Política**: Crear una **red de invitados separada** para usuarios que no forman parte de la red principal.
* **Explicación**: Una red separada para invitados garantiza que los visitantes no tengan acceso a la red interna y a los recursos compartidos. Esto es especialmente importante en entornos empresariales, ya que protege los sistemas críticos.

### 7. **Monitoreo y Detección de Intrusos**

* **Política**: Implementar sistemas de monitoreo para detectar y prevenir accesos no autorizados.
* **Explicación**: El monitoreo continuo de la red permite identificar actividades inusuales que puedan indicar intentos de intrusión. Los sistemas de detección de intrusos (IDS) pueden generar alertas si se detectan comportamientos sospechosos, como ataques de denegación de servicio (DoS) o intentos de acceso no autorizado.

### 8. **Desactivación de Funcionalidades Innecesarias**

* **Política**: Desactivar funciones que no se usan, como **WPS (Wi-Fi Protected Setup)**.
* **Explicación**: WPS es una función que permite a los usuarios conectar dispositivos fácilmente, pero también puede ser vulnerable a ataques. Desactivar esta funcionalidad ayuda a reducir el riesgo de exposición a ataques.

### 9. **Actualización de Firmware**

* **Política**: Asegurarse de que el **firmware del router o punto de acceso** esté siempre actualizado.
* **Explicación**: Los fabricantes de routers y puntos de acceso lanzan actualizaciones de firmware para corregir vulnerabilidades de seguridad. Es crucial mantener el firmware actualizado para proteger la red contra ataques conocidos.

### 10. **Limitación del Acceso a la Red (Control de Ancho de Banda)**

* **Política**: Implementar **políticas de control de acceso** y **limitación de ancho de banda**.
* **Explicación**: Limitar el acceso a la red mediante el control de la cantidad de dispositivos conectados y el ancho de banda que pueden usar ayuda a evitar el abuso de recursos y facilita la gestión de la red. Además, puede proteger contra ciertos ataques, como los ataques de denegación de servicio.

### 11. **Prevención de Ataques de Denegación de Servicio (DoS)**

* **Política**: Implementar medidas para prevenir ataques de denegación de servicio, como **filtros de IP** y **restricciones de acceso**.
* **Explicación**: Los ataques DoS o DDoS pueden sobrecargar un punto de acceso y hacerlo inaccesible. Usar cortafuegos, sistemas de prevención de intrusos (IPS) y limitar las conexiones simultáneas puede ayudar a mitigar estos riesgos.

### 12. **Seguridad Física del Punto de Acceso**

* **Política**: Asegurar que el **router o punto de acceso** esté ubicado en un lugar seguro.
* **Explicación**: Los puntos de acceso deben estar físicamente protegidos para evitar que sean manipulados o resetados por personas no autorizadas. Además, es importante que el área de cobertura de la red esté limitada, para reducir el riesgo de que alguien acceda desde fuera del alcance físico de la red.

### 13. **Educación y Capacitación de los Usuarios**

* **Política**: Proporcionar formación sobre buenas prácticas de seguridad a los usuarios de la red.
* **Explicación**: La seguridad de la red no solo depende de la infraestructura, sino también del comportamiento de los usuarios. Educar a los usuarios sobre la importancia de no compartir contraseñas, reconocer correos electrónicos de phishing, y asegurarse de usar dispositivos seguros puede mejorar significativamente la seguridad de la red.

## ****pilares de la seguridad****

Los **pilares de la seguridad** en el contexto de redes y sistemas informáticos son los principios fundamentales que guían la protección de la información, recursos y sistemas de una organización o usuario. Estos pilares son esenciales para establecer y mantener un entorno seguro. Los tres pilares clásicos de la seguridad de la información se conocen como **CIA**, que representan **Confidencialidad**, **Integridad** y **Disponibilidad**. Sin embargo, algunos modelos incluyen más aspectos como **Autenticación** y **No Repudio**. A continuación, te explico cada uno de estos pilares:

### 1. **Confidencialidad** (Confidentiality)

* **Definición**: La confidencialidad se refiere a la protección de la información de accesos no autorizados. Solo las personas o entidades autorizadas deben poder acceder a la información sensible.
* **Objetivo**: Evitar que los datos sean vistos o leídos por personas no autorizadas, lo que implica proteger la privacidad de la información.
* **Ejemplos de técnicas para asegurar la confidencialidad**:
  + Cifrado (AES, RSA, etc.) para proteger los datos durante la transmisión o almacenamiento.
  + Control de acceso basado en roles (RBAC) y autenticación de múltiples factores (MFA) para limitar el acceso a información sensible.

### 2. **Integridad** (Integrity)

* **Definición**: La integridad asegura que la información y los datos no sean alterados, manipulados o dañados de forma no autorizada, ya sea en reposo o durante la transmisión.
* **Objetivo**: Garantizar que los datos sean precisos, completos y confiables, y que no hayan sido modificados de manera inapropiada.
* **Ejemplos de técnicas para garantizar la integridad**:
  + Uso de **sumas de verificación** (hashing) y **firmas digitales** para verificar que los datos no han sido modificados.
  + Protocolos de **control de versiones** para evitar la alteración no autorizada de los archivos.
  + **Checksum** o algoritmos de hash (MD5, SHA-256) para verificar la integridad de los archivos descargados.

### 3. **Disponibilidad** (Availability)

* **Definición**: La disponibilidad asegura que los sistemas, servicios y datos estén accesibles y operativos cuando sean necesarios por los usuarios autorizados.
* **Objetivo**: Garantizar que los recursos de la red y la información estén disponibles para su uso en el momento que se necesiten, minimizando el tiempo de inactividad o interrupciones.
* **Ejemplos de técnicas para asegurar la disponibilidad**:
  + **Redundancia** (copias de seguridad, servidores de respaldo, etc.) para garantizar que si un sistema falla, haya otro disponible.
  + **Sistemas de recuperación ante desastres** (disaster recovery) que aseguran la continuidad de los servicios.
  + **Monitoreo y alertas** para identificar posibles fallos en los sistemas y prevenir pérdidas de disponibilidad.

### 4. **Autenticación** (Authentication)

* **Definición**: La autenticación es el proceso mediante el cual se verifica que una persona o entidad es quien dice ser, generalmente mediante el uso de credenciales como contraseñas, biometría o tokens de seguridad.
* **Objetivo**: Asegurar que solo los usuarios y dispositivos legítimos tengan acceso a los recursos y servicios.
* **Ejemplos de técnicas de autenticación**:
  + Contraseñas fuertes y complejas.
  + **Autenticación multifactor (MFA)**, que requiere múltiples métodos de verificación (contraseña + código enviado a un teléfono móvil).
  + **Autenticación biométrica**, como el uso de huellas dactilares o reconocimiento facial.

### 5. **No Repudio** (Non-repudiation)

* **Definición**: El no repudio se refiere a garantizar que una persona no pueda negar haber realizado una acción o transacción en un sistema, como enviar un correo electrónico o realizar una transferencia de dinero.
* **Objetivo**: Asegurar que las acciones realizadas por los usuarios sean verificables y no puedan ser rechazadas posteriormente.
* **Ejemplos de técnicas para asegurar el no repudio**:
  + **Registros de auditoría** que guardan un historial detallado de las acciones realizadas por los usuarios.
  + **Firmas digitales** que proporcionan evidencia de que un usuario específico realizó una acción o transacción.

### Resumen de los 5 pilares de la seguridad:

| **Pilar** | **Descripción** | **Objetivo principal** | **Ejemplos de técnicas** |
| --- | --- | --- | --- |
| **Confidencialidad** | Protección de la información frente a accesos no autorizados. | Garantizar que solo usuarios autorizados tengan acceso a la información. | Cifrado, control de acceso, autenticación multifactor. |
| **Integridad** | Garantizar que los datos no sean alterados sin autorización. | Asegurar que los datos sean precisos y completos. | Hashing, firmas digitales, control de versiones. |
| **Disponibilidad** | Garantizar que los datos y servicios estén disponibles cuando sean necesarios. | Asegurar que los recursos estén accesibles en todo momento. | Redundancia, backup, recuperación ante desastres. |
| **Autenticación** | Verificación de la identidad de usuarios y dispositivos. | Asegurar que solo los usuarios legítimos accedan a la red. | Contraseñas, MFA, biometría. |
| **No Repudio** | Asegurar que las acciones de los usuarios sean verificables. | Evitar que los usuarios nieguen sus acciones o transacciones. | Registros de auditoría, firmas digitales. |

## Confidencialidad

**Confidencialidad** es uno de los pilares fundamentales de la seguridad de la información, y se refiere a la protección de la información contra accesos no autorizados. El objetivo principal de la confidencialidad es asegurarse de que solo las personas o entidades autorizadas puedan acceder a ciertos datos, manteniéndolos fuera del alcance de individuos o sistemas no autorizados.

En resumen, **la confidencialidad asegura que la información sensible no se revele a personas o entidades no autorizadas**.

### **Principales Objetivos de la Confidencialidad:**

* **Proteger los datos sensibles**: Asegurar que la información personal, financiera, médica, corporativa, entre otras, esté protegida de la visualización, robo o exposición no deseada.
* **Mantener la privacidad de los usuarios**: Proteger la información personal de los usuarios, como contraseñas, datos bancarios, historial de navegación, etc.
* **Cumplir con regulaciones**: Garantizar que las organizaciones cumplan con normativas de privacidad y protección de datos, como el **RGPD** (Reglamento General de Protección de Datos) en Europa, que exige que los datos de los usuarios sean manejados con estricta confidencialidad.

### **Ejemplos de Información Confidencial:**

* **Datos personales**: Nombre, dirección, número de teléfono, fecha de nacimiento.
* **Datos financieros**: Información bancaria, tarjetas de crédito, estados financieros.
* **Datos médicos**: Historial médico, diagnósticos, tratamientos.
* **Propiedad intelectual**: Información sobre patentes, diseños, proyectos en desarrollo.
* **Contraseñas y credenciales de acceso**: Todo lo relacionado con la autenticación y **autorización.**

### **Métodos para Proteger la Confidencialidad:**

1. **Cifrado (Encryption)**:
   * El cifrado es una de las herramientas más efectivas para garantizar la confidencialidad. Mediante algoritmos de cifrado, los datos se convierten en un formato ilegible para cualquier persona que no posea la clave adecuada para descifrarlos.
   * Ejemplo: **AES (Advanced Encryption Standard)** es un algoritmo comúnmente utilizado para cifrar información.
2. **Control de acceso**:
   * Implementar **autenticación** y **autorización** asegura que solo los usuarios con permisos específicos puedan acceder a ciertos datos. Por ejemplo, el uso de **autenticación multifactor** (MFA) fortalece la confidencialidad, requiriendo que los usuarios proporcionen múltiples formas de verificación.
   * Ejemplo: **RBAC (Role-Based Access Control)**, donde se asignan permisos a usuarios según sus roles en la organización.
3. **Redes privadas y VPN (Virtual Private Network)**:
   * Usar redes privadas y VPNs cifra la conexión entre los dispositivos y las redes, asegurando que los datos no sean interceptados durante la transmisión.
   * Ejemplo: Cuando un empleado trabaja desde casa, la empresa puede proporcionar una VPN para asegurar que la comunicación con la red interna esté cifrada y sea segura.
4. **Protección en el almacenamiento**:
   * Además del cifrado de los datos en tránsito, también es importante cifrar los datos almacenados en discos duros, servidores o bases de datos.
   * Ejemplo: **BitLocker** es una herramienta de cifrado de discos en sistemas Windows que protege la confidencialidad de los datos en el almacenamiento.
5. **Políticas de contraseñas fuertes**:
   * Las contraseñas deben ser largas, complejas y difíciles de adivinar, lo que dificulta el acceso no autorizado a los sistemas.
   * Ejemplo: Utilizar contraseñas de al menos 12 caracteres que incluyan letras mayúsculas, minúsculas, números y símbolos.
6. **Destrucción segura de datos**:
   * Asegurarse de que los datos confidenciales se destruyan de manera segura cuando ya no sean necesarios, para evitar que caigan en manos equivocadas.
   * Ejemplo: Utilizar software que destruya permanentemente archivos eliminados y dispositivos de almacenamiento como discos duros, utilizando técnicas como la sobrescritura de datos.
7. **Uso de sistemas de gestión de claves (KMS)**:
   * Para la protección de la confidencialidad en sistemas cifrados, es necesario contar con un sistema de gestión de claves que proteja las claves utilizadas para cifrar y descifrar los datos.
   * Ejemplo: **AWS Key Management Service (KMS)** es un servicio de Amazon que permite gestionar y almacenar claves de cifrado de manera segura.

### **Amenazas a la Confidencialidad:**

1. **Intercepción de datos (Eavesdropping)**:
   * Los atacantes pueden interceptar las comunicaciones para robar datos sensibles. Este tipo de ataque puede ocurrir en redes públicas no cifradas, como Wi-Fi abierto.
2. **Phishing**:
   * Los atacantes engañan a los usuarios para que revelen información confidencial, como contraseñas o datos bancarios, a través de correos electrónicos o sitios web falsos.
3. **Malware**:
   * Software malicioso, como **keyloggers** (registradores de teclas) o **troyanos**, puede ser utilizado para robar contraseñas y otros datos confidenciales.
4. **Accesos no autorizados**:
   * Los atacantes pueden obtener acceso a sistemas protegidos mediante el uso de **exploits**, **fuerza bruta** o **suplantación de identidad**, obteniendo así información confidencial.
5. **Filtración de datos**:
   * A veces, las personas dentro de una organización pueden filtrar información confidencial, ya sea de forma accidental o intencional.

### **Buenas Prácticas para Mantener la Confidencialidad:**

* **Educación y Conciencia**: Asegúrate de que todos los usuarios comprendan la importancia de la confidencialidad y las mejores prácticas para proteger los datos, como evitar compartir contraseñas y no hacer clic en enlaces sospechosos.
* **Auditorías y Monitoreo**: Implementar auditorías regulares y sistemas de monitoreo para detectar y responder rápidamente a accesos no autorizados o actividades sospechosas.
* **Uso de cifrado en todas las comunicaciones**: Asegurarse de que todas las comunicaciones (como correos electrónicos, comunicaciones VoIP y navegadores web) estén cifradas utilizando protocolos seguros como **TLS** (Transport Layer Security).

## Disponibilidad

**Disponibilidad** es uno de los pilares fundamentales de la **seguridad de la información** y se refiere a la capacidad de los sistemas, aplicaciones, datos y recursos para estar **accesibles y operativos** cuando los usuarios legítimos los necesiten. En términos simples, la disponibilidad asegura que los servicios, plataformas y sistemas de información estén siempre disponibles y funcionen correctamente sin interrupciones innecesarias.

### **Objetivo de la Disponibilidad**

El objetivo principal de la disponibilidad es garantizar que los recursos y servicios estén accesibles en el momento que sean necesarios, lo cual es esencial para la continuidad de las operaciones de una organización o el acceso de un usuario a servicios cruciales. Esto significa que los sistemas deben ser capaces de resistir fallos, ataques y otros problemas que puedan interrumpir su funcionamiento.

### 

Varios factores pueden afectar la disponibilidad de los servicios o sistemas, entre los que se incluyen:

* **Fallas de hardware**: Dispositivos como servidores, routers o discos duros pueden fallar, lo que interrumpe el acceso a los sistemas.
* **Ataques cibernéticos**: Los ataques de **Denegación de Servicio Distribuida (DDoS)** o intrusiones pueden afectar la disponibilidad al sobrecargar los sistemas o comprometer su integridad.
* **Errores humanos**: La configuración incorrecta, la eliminación accidental de datos o fallos en las operaciones pueden llevar a la inactividad de los sistemas.
* **Desastres naturales**: Factores como incendios, inundaciones, terremotos u otros desastres pueden destruir o dañar los centros de datos y los sistemas.
* **Actualizaciones o mantenimiento**: Las actualizaciones de software o el mantenimiento de la infraestructura pueden causar tiempos de inactividad planificados.

### **Ejemplos de Situaciones Relacionadas con la Disponibilidad**

* **Acceso a un servidor web**: Si un servidor web está caído o no funciona correctamente, los usuarios no pueden acceder al sitio web. Esto afecta la disponibilidad de la red.
* **Servicios bancarios en línea**: Si una aplicación de banca en línea está inactiva debido a un fallo en el servidor, los clientes no pueden realizar transacciones, lo que afecta la disponibilidad del servicio.
* **Sistemas de comunicación**: Si los sistemas de correo electrónico o mensajería en una empresa dejan de funcionar, la disponibilidad de la comunicación se ve comprometida.

### Métodos y Técnicas para Asegurar la Disponibilidad

Para garantizar que los sistemas y servicios estén siempre disponibles, se implementan varias estrategias y técnicas, tales como:

#### 1. **Redundancia** (**Redundancy)**

La redundancia implica la duplicación de componentes o sistemas críticos para que, si uno falla, haya otro disponible para asumir la carga. Esto es una de las mejores prácticas para garantizar la disponibilidad.

* **Ejemplos**:
  + **Redundancia de servidores**: Si un servidor principal falla, un servidor de respaldo puede tomar su lugar de manera automática (balanceo de carga).
  + **Redundancia de energía**: Uso de generadores o UPS (Sistemas de Alimentación Ininterrumpida) para mantener los sistemas operativos durante cortes de energía.

#### 2. **Copias de Seguridad (Backup)**

Realizar **copias de seguridad regulares** de los datos es crucial para poder restaurarlos en caso de pérdida o daño. Las copias de seguridad deben almacenarse de manera segura y ser accesibles rápidamente para restaurar la información.

* **Ejemplos**:
  + **Backups incrementales**: Realizar copias de seguridad solo de los datos que han cambiado desde la última copia de seguridad.
  + **Backup en la nube**: Almacenar copias de seguridad en servicios de nube para asegurar que los datos estén disponibles incluso si los sistemas locales fallan.

#### 3. **Planificación de Recuperación ante Desastres (DRP)**

Un **Plan de Recuperación ante Desastres (Disaster Recovery Plan)** define los pasos que deben seguirse para restaurar los sistemas y servicios a su estado normal después de un desastre o incidente grave.

* **Ejemplos**:
  + **Planes de contingencia** para restaurar servidores críticos en diferentes ubicaciones geográficas.
  + **Sistemas de conmutación por error** (failover) para cambiar rápidamente a un sistema de respaldo en caso de fallo del sistema principal.

#### 4. **Escalabilidad** (Scalability)

La **escalabilidad** asegura que un sistema pueda manejar un aumento en la carga de trabajo o en el número de usuarios sin perder rendimiento ni disponibilidad.

* **Ejemplos**:
  + **Escalabilidad vertical**: Aumentar la capacidad de un solo servidor añadiendo más recursos, como CPU, RAM o almacenamiento.
  + **Escalabilidad horizontal**: Añadir más servidores o recursos distribuidos en la red para manejar un mayor volumen de tráfico.

#### 5. **Monitoreo y Alertas Proactivas**

El monitoreo constante de los sistemas y servicios permite identificar posibles problemas antes de que se conviertan en fallos graves. Las alertas pueden ser configuradas para notificar al equipo de TI sobre cualquier anomalía.

* **Ejemplos**:
  + **Sistemas de monitoreo de servidores** como **Nagios** o **Zabbix** para supervisar el estado de los servidores y generar alertas de problemas.
  + **Monitoreo de red** para verificar la disponibilidad de los servicios y detectar caídas o sobrecargas en la red.

#### 6**. Mantenimiento Regular**

Realizar mantenimiento preventivo, como actualizaciones de software, hardware y parches de seguridad, es crucial para asegurar que los sistemas sigan siendo confiables y disponibles.

* **Ejemplos**:
  + **Actualizaciones periódicas de software** para corregir vulnerabilidades de seguridad y mejorar la estabilidad.
  + **Reemplazo de hardware obsoleto** para evitar fallos en los equipos críticos.

### **Desafíos en la Garantía de la Disponibilidad**

* **Costos**: Implementar redundancia, copias de seguridad y otras medidas puede ser costoso, especialmente en grandes infraestructuras.
* **Equilibrio entre disponibilidad y rendimiento**: Mientras más redundante sea un sistema, más recursos puede consumir, lo que podría afectar el rendimiento si no se gestiona adecuadamente.
* **Amenazas externas**: Los ataques DDoS y otras amenazas externas pueden poner en riesgo la disponibilidad de los servicios, incluso si los sistemas están bien configurados internamente.

## Analisis de requerimientos de la red inalambrica

El **análisis de requerimientos de una red inalámbrica** es un paso crucial para diseñar e implementar una infraestructura de red que sea adecuada para las necesidades de la organización o el entorno donde se va a desplegar. Este análisis tiene como objetivo identificar y definir las necesidades y expectativas de los usuarios y aplicaciones, de modo que la red inalámbrica sea eficiente, segura y escalable.

A continuación, se detallan los principales aspectos que deben ser considerados en el **análisis de requerimientos de una red inalámbrica**:

### 1. **Requerimientos de cobertura**

* **Ubicación geográfica**: Determinar el área geográfica que la red debe cubrir. Esto incluye la distribución de oficinas, edificios, zonas de acceso público, plantas de producción, etc. Es importante realizar un estudio de cobertura para identificar las áreas donde se necesitarán puntos de acceso (AP) adicionales.
* **Propagación de la señal**: Las características del entorno (paredes, materiales de construcción, interferencias, etc.) afectan la propagación de la señal inalámbrica. Es necesario realizar un **análisis de sitio** para determinar el número de puntos de acceso, sus ubicaciones y la potencia de señal necesaria para cubrir todo el espacio sin crear zonas muertas.
* **Densidad de usuarios**: Dependiendo de la cantidad de usuarios que se conectarán simultáneamente, se deben diseñar las capacidades de la red para evitar cuellos de botella. Por ejemplo, un área con mucha gente, como una sala de conferencias, puede requerir más capacidad de acceso.

### 2. **Requerimientos de rendimiento**

* **Ancho de banda**: La red inalámbrica debe ser capaz de soportar el ancho de banda requerido por las aplicaciones y usuarios. Esto incluye aspectos como la transmisión de datos, video en vivo, conferencias, descargas de archivos, etc. El análisis debe definir la velocidad mínima de conexión que se espera para los usuarios y aplicaciones.
  + **WPA3** y otros protocolos de cifrado avanzados también deben ser considerados, ya que pueden afectar ligeramente el rendimiento de la red.
* **Latencia**: La latencia debe ser baja para aplicaciones sensibles al tiempo, como VoIP o videoconferencias. Un análisis detallado del rendimiento ayudará a determinar las ubicaciones óptimas de los puntos de acceso para minimizar la latencia.
* **Calidad del Servicio (QoS)**: Es importante priorizar el tráfico de red según las necesidades de las aplicaciones. Por ejemplo, las videoconferencias deben tener prioridad sobre el tráfico de correo electrónico o navegación web para garantizar una experiencia fluida.

### 3. **Requerimientos de seguridad**

* **Autenticación**: Determinar el tipo de autenticación que se utilizará para garantizar que solo los usuarios autorizados puedan conectarse a la red. Esto puede incluir autenticación basada en contraseñas, autenticación de múltiples factores (MFA), o el uso de sistemas de autenticación como **802.1X**.
* **Cifrado**: Elegir el estándar de cifrado adecuado (WPA2, WPA3, etc.) para garantizar que los datos transmitidos a través de la red inalámbrica estén protegidos contra accesos no autorizados.
* **Redes separadas**: Si se requiere segmentar la red para diferentes grupos de usuarios (empleados, visitantes, dispositivos IoT, etc.), se deben implementar redes separadas y políticas de aislamiento, utilizando **VLANs** o tecnologías de **SSID** múltiples.
* **Firewall y control de acceso**: Implementar un firewall adecuado para proteger la red y controlar el tráfico entrante y saliente. Además, debe existir un control de acceso para evitar que dispositivos no autorizados se conecten a la red.
* **Detección de intrusiones**: Utilizar sistemas de **IDS/IPS** para detectar y prevenir posibles ataques a la red inalámbrica.

### 4. **Requerimientos de escalabilidad**

* **Crecimiento futuro**: La red inalámbrica debe ser diseñada para crecer con la organización. Esto incluye la posibilidad de agregar más puntos de acceso o aumentar el ancho de banda sin problemas. Los puntos de acceso deben ser escalables y deben considerarse las tecnologías emergentes (como Wi-Fi 6) que pueden ofrecer mayor capacidad y rendimiento.
* **Expansión geográfica**: Si la red inalámbrica puede expandirse a otras ubicaciones o edificios, es necesario considerar cómo integrar estas nuevas ubicaciones a la infraestructura existente sin comprometer la calidad del servicio.

### 5. **Requerimientos de movilidad**

* **Roaming**: Si los usuarios van a moverse dentro de la red (por ejemplo, dentro de una oficina o entre edificios), es esencial que la red admita **roaming** sin interrupciones, permitiendo que los usuarios cambien entre puntos de acceso sin perder la conexión.
* **Gestión de sesiones de usuario**: La red debe ser capaz de gestionar las sesiones de usuario de forma eficiente, permitiendo que los usuarios se mantengan conectados mientras se desplazan dentro de la cobertura de la red.

### 6. **Requerimientos de compatibilidad**

* **Dispositivos y estándares**: Verificar la compatibilidad con los dispositivos que se conectarán a la red. Esto incluye asegurarse de que los puntos de acceso y el resto de la infraestructura sean compatibles con los dispositivos existentes en la red (teléfonos inteligentes, laptops, tabletas, impresoras, etc.). También es importante que la infraestructura soporte los estándares modernos como **Wi-Fi 6 (802.11ax)**.
* **Interoperabilidad**: Asegurar que los diferentes dispositivos y tecnologías sean capaces de trabajar juntos sin problemas, desde puntos de acceso hasta dispositivos de gestión.

### 7. **Requerimientos de gestión y monitoreo**

* **Visibilidad de la red**: Implementar herramientas de **gestión de red** que proporcionen visibilidad en tiempo real del estado de la red inalámbrica, el rendimiento y los posibles problemas. Las plataformas de gestión permiten configurar, monitorizar y solucionar problemas de manera centralizada.
* **Alertas y notificaciones**: Establecer alertas para situaciones críticas, como caídas de puntos de acceso, congestión de tráfico o problemas de rendimiento, para permitir una respuesta rápida.
* **Informes de uso**: Generar informes detallados sobre el tráfico, el uso de la red y los problemas potenciales, para evaluar la eficiencia de la red y planificar futuras mejoras.

### 8**. Requerimientos de costo y presupuesto**

* **Presupuesto disponible: El costo de implementación** y mantenimiento de la red inalámbrica debe ser considerado dentro del presupuesto disponible para la infraestructura. Esto incluye el costo de los puntos de acceso, el hardware adicional necesario, la contratación de servicios de gestión o consultoría, etc.
* **Costos de operación**: Se deben considerar también los costos operativos continuos, como la actualización de software, el mantenimiento de hardware y la capacitación de personal.

### 9. **Requerimientos medioambientales**

* **Condiciones físicas**: Las condiciones físicas del entorno pueden influir en el rendimiento de la red inalámbrica. Por ejemplo, en entornos industriales, las interferencias electromagnéticas, el calor extremo o la humedad pueden afectar la calidad de la señal.
* **Sostenibilidad**: Considerar el impacto ambiental de los equipos que se van a utilizar y la eficiencia energética de los puntos de acceso y otros dispositivos de red.

## Comunicación land

La **comunicación LAN** (Local Area Network, o Red de Área Local) se refiere a la transmisión de datos entre dispositivos dentro de una red localizada, que generalmente cubre un área geográfica pequeña, como una oficina, un edificio o un campus. A través de esta red, los dispositivos (computadoras, impresoras, servidores, etc.) pueden compartir recursos, acceder a internet o a servicios centralizados, y comunicarse entre sí.

### **Componentes principales de la comunicación LAN:**

1. **Dispositivos de la red (End Devices)**:
   * **Computadoras**: Son los dispositivos más comunes en una LAN, donde los usuarios pueden trabajar, almacenar información y ejecutar aplicaciones.
   * **Impresoras, cámaras y otros periféricos**: Dispositivos compartidos dentro de la red.
   * **Dispositivos móviles**: Teléfonos inteligentes, tabletas y laptops que pueden estar conectados a través de conexiones cableadas o inalámbricas.
2. **Equipos de red (Networking Devices)**:
   * **Switches**: Son dispositivos que conectan los dispositivos dentro de una LAN de manera eficiente, asegurando que los datos se envíen solo a los dispositivos correspondientes. Operan en la capa 2 del modelo OSI (nivel de enlace de datos).
   * **Routers**: Conectan diferentes redes, como una LAN a una red más grande, como Internet. Además, permiten dirigir el tráfico entre diferentes segmentos de la red.
   * **Puntos de acceso (Access Points, AP)**: En redes inalámbricas LAN, los puntos de acceso proporcionan conectividad Wi-Fi a dispositivos móviles o computadoras sin cables.
   * **Cables**: Los cables Ethernet (cat 5e, cat 6, etc.) son comúnmente utilizados en conexiones cableadas, proporcionando comunicación entre los dispositivos de la red.
3. **Protocolo de Comunicación**:
   * El **Ethernet** es el protocolo estándar más utilizado para la transmisión de datos en redes LAN cableadas. Opera en la capa 2 del modelo OSI.
   * En las redes inalámbricas LAN, el **Wi-Fi** (basado en los estándares IEEE 802.11) es el protocolo principal para la comunicación inalámbrica.
4. **Servicios en una LAN**:
   * **Compartición de archivos**: Los dispositivos en una LAN pueden compartir archivos y recursos (como impresoras) a través de protocolos como SMB (Server Message Block).
   * **Acceso a Internet**: Una LAN puede estar conectada a Internet a través de un router, permitiendo que todos los dispositivos de la LAN accedan a recursos en línea.
   * **Impresión compartida**: Las impresoras conectadas a la LAN pueden ser accedidas y utilizadas por todos los dispositivos en la red.

### **Tipos de comunicación en una LAN:**

1. **Comunicación unicast**:
   * En este tipo de comunicación, los datos son enviados de un único dispositivo a otro único dispositivo en la red. Es la forma más común de transmisión en redes LAN.
   * Ejemplo: Cuando un usuario envía un archivo de su computadora a otra.
2. **Comunicación broadcast**:
   * En la comunicación **broadcast**, los datos son enviados a todos los dispositivos dentro de la red local. En una LAN, el **broadcast** se utiliza para enviar mensajes que todos los dispositivos deben recibir.
   * Ejemplo: El **ARP (Address Resolution Protocol)** es un protocolo de **broadcast** que se usa para mapear direcciones IP a direcciones MAC dentro de una LAN.
3. **Comunicación multicast**:
   * En la comunicación **multicast**, los datos se envían desde un dispositivo a un grupo de dispositivos dentro de la red. Es útil cuando se necesita enviar información a varios dispositivos sin que llegue a todos los dispositivos de la red (como en el caso de una transmisión en vivo o videoconferencias).
   * Ejemplo: Cuando un servidor de streaming envía datos de video a varios usuarios dentro de una LAN.

### **Tipos de Redes LAN**

1. **LAN Cableada**:
   * En una LAN cableada, todos los dispositivos están conectados físicamente mediante cables Ethernet. La comunicación en esta red es más estable y rápida en comparación con una red inalámbrica.
2. **LAN Inalámbrica (Wi-Fi)**:
   * Una LAN inalámbrica utiliza **puntos de acceso Wi-Fi** para permitir la comunicación entre dispositivos sin cables. Esta red es flexible y permite mayor movilidad, pero puede ser más vulnerable a interferencias y problemas de cobertura en comparación con una LAN cableada.
3. **LAN Híbrida**:
   * Es una combinación de LAN cableada e inalámbrica, donde algunos dispositivos se conectan a través de cables Ethernet y otros a través de Wi-Fi.

### **Protocolos utilizados en LANs**

1. **Ethernet (IEEE 802.3)**:
   * Es el estándar más común para redes LAN cableadas. Ethernet utiliza **frames** para transmitir datos y opera principalmente en la capa de enlace de datos (capa 2) del modelo OSI.
   * La velocidad de transmisión varía desde 10 Mbps hasta 100 Gbps (en versiones avanzadas como **Ethernet de 100 Gb**).
2. **Wi-Fi (IEEE 802.11)**:
   * Para LAN inalámbricas, Wi-Fi es el protocolo principal que proporciona conectividad de red sin cables. Existen diversas versiones de Wi-Fi, como **802.11a/b/g/n/ac/ax** (Wi-Fi 6), que ofrecen diferentes velocidades y rangos de cobertura.
3. **IP (Internet Protocol)**:
   * Aunque Ethernet o Wi-Fi son los protocolos de enlace, los dispositivos de la LAN suelen usar **TCP/IP** para la transmisión de datos entre los dispositivos a través de la red.
4. **ARP (Address Resolution Protocol)**:
   * Es utilizado para mapear direcciones IP a direcciones MAC, permitiendo que los dispositivos dentro de una LAN se encuentren entre sí.

### **Ventajas de una LAN**

1. **Alta velocidad**: Las LANs permiten una transmisión rápida de datos, lo que es ideal para actividades que requieren altas tasas de transferencia, como el uso compartido de archivos grandes y la transmisión de video.
2. **Eficiencia en la compartición de recursos**: Los recursos, como impresoras, servidores de archivos, aplicaciones, y dispositivos de red, pueden ser compartidos entre varios usuarios dentro de la LAN.
3. **Bajo costo**: Comparada con las redes de área amplia (WAN), las LAN son más económicas, tanto en términos de hardware como de mantenimiento.
4. **Control centralizado**: Las LANs permiten una fácil gestión y control de acceso a los recursos compartidos, permitiendo que los administradores controlen qué dispositivos pueden conectarse y qué servicios pueden usar.

### **Desventajas de una LAN**

1. **Alcance limitado**: Las LANs están diseñadas para cubrir un área pequeña, lo que significa que no son adecuadas para cubrir grandes distancias, como entre ciudades o países (para eso se usan WANs).
2. **Interferencia en redes inalámbricas**: Las redes Wi-Fi pueden verse afectadas por interferencias de otras redes inalámbricas, dispositivos electrónicos o estructuras físicas que bloqueen la señal.
3. **Vulnerabilidad a ataques locales**: Una LAN localmente gestionada puede ser más susceptible a ataques internos, como el acceso no autorizado a datos o la manipulación de dispositivos dentro de la misma red.