**Los estándares WiFi han ido evolucionando a lo largo de los años. Se han introducido mejoras relativas al alcance, al rendimiento y al funcionamiento cuando se trabaja con varios dispositivos. Un problema que se plantea es si los distintos routers recogen las mejoras más actuales.**

**Realizar un trabajo que recoja la investigación sobre los estándares actuales WPA, WPA2 y WP3, que explique las características de cada uno de ellos:**

* **Fecha de uso generalizado.**
* **Métodos de codificación, explicando cada uno de ellos.**
* **Longitud y formato de la contraseña.**
* **Ámbito de uso.**
* **Fecha del primer fallo de seguridad.**
* **Tipos de ataques que pueden sufrir, explicando en qué consiste cada uno de esos ataques.**
* **Routers reales indicando qué estándares admiten**.

**Estándar WPA**

WPA, Wi-Fi Protected Access o, en español, acceso Wi-Fi protegido, es un sistema de seguridad diseñado para redes inalámbricas que ha sido creado por WiFi Alliance, la entidad reguladora de esta tecnología.

WPA surgió como una solución inmediata y temporal sobre WEB ya que se volvió vulnerable a diversos ataques. Una de las mejoras clave de WPA sobre WEP es la forma en que maneja las claves de seguridad. Mientras que WEP utiliza una clave estática, WPA emplea el Protocolo de Integridad de Clave Temporal (TKIP), que cambia las claves de manera dinámica. WPA dificulta que un intruso descifre la clave mediante autenticación robusta y mejora la integridad de los datos cifrados con un código de integridad de mensajes.

WPA ofrece dos modos de autenticación. El primero utiliza un servidor para almacenar credenciales y contraseñas de los usuarios y el segundo emplea una clave precompartida que se debe introducir en todos los equipos de la red. Además usa comprobaciones de integridad de los mensajes para verificar si un atacante ha capturado o alterado paquetes de datos

A pesar de estas mejoras, se encontraron vulnerabilidades en WPA, lo que llevó al desarrollo de una segunda versión (WPA2)

* **Fecha de uso generalizado**

WPA se publicó en 2003 como norma provisional para responder a la necesidad de un protocolo más seguro que WEP, y se ha consolidado como el protocolo de referencia en conexiones inalámbricas.

* **Métodos de codificación, explicando cada uno de ellos**

**TKIP  *(Temporal Key Integrity Protocol)*:**

Es un método de codificación. El TKIP proporciona una clave por paquete que mezcla la integridad de un mensaje con un mecanismo de reescritura.

* Genera una clave única para cada paquete de datos, conocida como clave por paquete, dificultando los ataques que explotan claves estáticas
* Combina la integridad de los mensajes con un mecanismo de reescritura, verificando que los datos no se hayan alterado durante la transmisión

**AES *(Advanced Encryption Standard):***

Estándar de cifrado fuerte adoptado por WiFi Alliance para garantizar comunicaciones seguras en redes inalámbricas.

* Utiliza un cifrado basado en bloques con claves de 128, 192 o 256 bits, aunque WPA y WPA2 generalmente emplean claves de 128 bits
* Implementa CCMP que proporciona cifrado y autenticación simultáneos para cada paquete.
* **Longitud y formato de la contraseña.**

Según los estándares de seguridad de WPA, la longitud de la contraseña debe tener un mínimo de 8 caracteres y un máximo de 63 caracteres

* **Longitud mínima:** 8 caracteres.
* **Longitud máxima:** 63 caracteres
* **Caracteres permitidos:** Los caracteres ASCII imprimibles con valor binario entre 32 y 126, que incluyen el espacio, símbolos, números y letras mayúsculas y minúsculas.
* **Recomendación:** Se recomienda utilizar contraseñas de al menos 12 caracteres para aumentar la seguridad.
* **Mezcla de caracteres**: Las contraseñas más seguras incluyen una mezcla de letras mayúsculas y minúsculas, números y símbolos.
* **Cambio regular:** Es recomendable cambiar la contraseña periódicamente para mantener la seguridad.
* **Contraseñas por defecto:** No es recomendable utilizar las contraseñas predeterminadas de los routers, ya que pueden ser menos seguras

Es probable que hayas escuchado el término "clave WPA" en relación con el protocolo WPA. Una clave WPA es una contraseña que se utiliza para conectarse a una red inalámbrica. La persona encargada de la red es la que proporciona la contraseña WPA. En algunos casos, puede haber una contraseña o frase de contraseña WPA predeterminada impresa en un router inalámbrico. Si no puedes determinar la contraseña en tu router, quizás puedas restablecerla

* **Ámbito de uso.**

WPA fue diseñado como una mejora significativa respecto a WEP, brindando mayor seguridad en redes inalámbricas y adaptándose a diversos entornos según las necesidades de seguridad. Su flexibilidad lo hizo popular tanto en redes domésticas como en pequeñas empresas, aunque con limitaciones frente a estándares posteriores.

* **Modo personal o clave precompartida (WPA-PSK):** Utiliza una clave precompartida (PSK) que debe ser conocida por todos los dispositivos que se conecten a la red. Es ideal para redes domésticas y pequeñas oficinas donde no se requiere autenticación individual para cada usuario
* **Modo empresarial (WPA-EAP):** Se basa en el uso de un servidor de autenticación, como un servidor RADIUS, para validar las credenciales de cada usuario. Es adecuado para redes empresariales, instituciones educativas y otras organizaciones que requieren mayor control y seguridad en el acceso a la red.

Aunque WPA sigue presente en algunos dispositivos antiguos, su seguridad está desactualizada y es más vulnerable frente a ataques modernos. Por ello, su uso está limitado principalmente a situaciones donde no se puede actualizar el hardware o el software.

* **Fecha del primer fallo de seguridad.**

El primer fallo significativo de seguridad en WPA se identificó en el 2006 con la aparición del ataque TKIP. Este fallo explotó debilidades en el mecanismo de reescritura de claves de TKIP, permitiendo ataques de reinyección de claves, lo que ponía en riesgo la integridad de los datos cifrados.

En este ataque los atacantes podían enviar datos malformados o alterar paquetes enviados para inducir a los clientes a usar las mismas claves reutilizadas. Esto resultaba en la posibilidad de descifrar datos o interceptar las comunicaciones sin necesidad de romper la clave completa

Este fallo puso en peligro la integridad de los datos transmitidos en las redes WPA, abriendo la puerta a ataques como:

* Reinfección de paquetes cifrados.
* Intercepción y manipulación de datos durante la transmisión.
* Vulnerabilidades en la autenticación al no garantizar la protección frente a ataques de replay.

Este problema llevó a la evolución del estándar WPA hacia WPA2 en 2004, que incorporó el uso de AES junto con CCMP.

* **Tipos de ataques que pueden sufrir, explicando en qué consiste cada uno de esos ataques.**

**Ataque por fuerza bruta:**

Consiste en probar todas las posibles combinaciones de contraseñas hasta encontrar la correcta. Aunque WPA implementa medidas como la protección con claves temporales (TKIP y AES), los ataques de fuerza bruta siguen siendo una amenaza potencial.

Para ponerle solución se recomienda utilizar contraseñas fuertes y habilitar la verificación en dos pasos cuando esté disponible

#### 

#### **Ataque de denegación de servicio (DoS):**

Un ataque DoS busca sobrecargar los recursos del sistema para impedir que los usuarios legítimos accedan a la red. Si un cliente no soporta las autenticaciones específicas del punto de acceso, como aquellas que utilizan WPA, puede ser desconectado, dejando la red vulnerable.

Para ponerle solución se recomienda una configuración adecuada del punto de acceso y monitoreo constante para detectar anomalías.

**Ataque de diccionario:**

Los ataques de diccionario utilizan listas predefinidas de contraseñas para tratar de adivinar la clave PSK. Si se utiliza una clave débil, los atacantes pueden aprovechar esta vulnerabilidad para obtener acceso a la red.

Para ponerle solución se recomienda utilizar servidores RADIUS que generan claves únicas y complejas, algo que es más común en entornos empresariales

**Ataque KRACK:**

KRACK es un ataque que afecta a redes WPA2 y permite a los atacantes interceptar y manipular datos enviados a través de Wi-Fi. Utiliza un fallo en el protocolo de cifrado WPA2 para reusar claves ya negociadas.

Para protegerse de KRACK, es necesario actualizar los routers y dispositivos con las últimas versiones de firmware que apliquen los parches de seguridad

* **Routers reales indicando qué estándares admiten**.

[**TP-Link ArcherAX6000**](https://www.amazon.es/TP-Link-Archer-AX6000-Quad-Core-co-procesadores/dp/B07PXTG7R9)

[**Netgear R7000**](https://www.amazon.es/Netgear-Nighthawk-R7000-100PES-tecnolog%C3%ADa-compatible/dp/B00HBYGCOG)

[**Linksys EA7500**](https://www.amazon.es/Linksys-EA7500-EU-MAX-Stream-Monitorizaci%C3%B3n-Administraci%C3%B3n/dp/B01AJOMDSI)

[**ASUS RT-AC67U**](https://www.amazon.es/ASUS-RT-AC66U_B1-inal%C3%A1mbrico-Dual-band-Gigabit/dp/B07D8WNM6C)

**Estándar WPA2**

WPA2 (Wi-Fi Protected Access 2) es el estándar avanzado de seguridad diseñado para proteger las redes inalámbricas, desarrollado por la Wi-Fi Alliance como una evolución del protocolo WPA. Su objetivo principal es garantizar una comunicación segura al cifrar y autenticar las conexiones Wi-Fi, protegiendo los datos transmitidos frente a posibles intrusiones.

WPA2 surgió como respuesta a las vulnerabilidades identificadas en su predecesor, WPA, implementando técnicas más robustas y confiables. Este protocolo utiliza cifrados fuertes como el AES y el TKIP para asegurar la integridad y privacidad de los datos transmitidos. Además, WPA2 cuenta con un sistema de autenticación que puede utilizar tanto una clave precompartida como un servidor de autenticación (RADIUS), ofreciendo mayor flexibilidad para su aplicación en diversos entornos

El protocolo también emplea CCMP, que asegura tanto el cifrado como la autenticación simultánea para cada paquete, garantizando que los datos no sean alterados durante la transmisión.

Todos los protocolos de seguridad funcionan mediante el uso de claves criptográficas para cifrar los datos y hacerlos indescifrables. Se usa la misma clave para descifrar los datos.

Pero no todos los protocolos de seguridad utilizan la misma tecnología. En la actualidad, WPA2 es el estándar de seguridad de redes gracias a sus avanzados métodos de cifrado de datos. En función de sus necesidades, puede elegir también configuraciones específicas dentro de WPA2 para optimizar la seguridad.

* **Fecha de uso generalizado**

WPA2 se lanzó oficialmente en 2004 como una actualización significativa de WPA. Desde su implementación, ha sido ampliamente adoptado como el estándar de seguridad en redes inalámbricas, proporcionando cifrado más fuerte y una protección superior frente a ataques.

* **Métodos de codificación, explicando cada uno de ellos**

En una red inalámbrica doméstica puede utilizar una gran variedad de sencillos procedimientos de seguridad para proteger la conexión inalámbrica. Éstos incluyen:

* Activar el acceso protegido Wi-Fi\* (WPA).
* Cambiar su contraseña.
* Cambiar el nombre de la red (SSID).

La codificación de acceso protegido Wi-Fi (WPA) ofrece protección de sus datos en la red. WPA utiliza una clave de codificación llamada clave precompartida (PSK) para codificar los datos antes de la transmisión. Introduzca la misma contraseña en todos los equipos y punto de acceso de su red doméstica o de pequeña empresa. Sólo los dispositivos que utilicen la misma clave de codificación pueden tener acceso a la red o descodificar los datos codificados transmitidos por otros equipos. La contraseña inicia automáticamente el Protocolo de integridad de claves temporales (TKIP) o el protocolo AES-CCMP para el proceso de codificación de datos**.**

El uso de AES en WPA2 ofrece un método de codificación más seguro y sofisticado, lo que lo hace el estándar de seguridad de redes inalámbricas actualmente recomendado

* **Longitud y formato de la contraseña.**

Según los estándares de seguridad de WPA2, la longitud de la contraseña debe tener un mínimo de 8 caracteres y un máximo de 63 caracteres

* **Longitud mínima**: 8 caracteres.
* **Longitud máxima**: 63 caracteres.
* **Caracteres permitidos**: Los caracteres ASCII imprimibles entre 32 y 126, que incluyen letras mayúsculas, minúsculas, números y símbolos.
* **Recomendación**: Se recomienda utilizar contraseñas de al menos 12 caracteres para una mayor seguridad.
* **Mezcla de caracteres**: Las contraseñas más seguras incluyen una combinación de letras mayúsculas y minúsculas, números y símbolos.
* **Cambio regular**: Es importante cambiar las contraseñas periódicamente para mantener la seguridad.
* **Contraseñas por defecto**: Evitar utilizar contraseñas predeterminadas de los routers, ya que estas son menos seguras.
* **Ámbito de uso.**

WPA2 fue diseñado para ofrecer una mayor seguridad en redes inalámbricas, adaptándose a diversos entornos según las necesidades de seguridad. Su flexibilidad lo ha hecho popular tanto en redes domésticas como en pequeñas empresas.

* **Modo personal o clave precompartida (WPA2-PSK):** En este modo, se utiliza una clave precompartida (PSK) que todos los dispositivos deben conocer para conectarse a la red. Es ideal para redes domésticas y pequeñas oficinas, donde no se requiere una autenticación individual para cada usuario
* **Modo empresarial (WPA2-EAP):** Este modo se basa en el uso de un servidor de autenticación, como un servidor RADIUS, para validar las credenciales de cada usuario. Es adecuado para redes empresariales, instituciones educativas y otras organizaciones que necesitan un mayor control y seguridad en el acceso a la red.

Sin embargo, es importante mencionar que, aunque WPA2 ofrece una seguridad significativamente mejorada, también ha sido vulnerado en el pasado, lo que ha llevado al desarrollo de WPA3, el estándar más reciente que ofrece mejoras adicionales en seguridad

* **Fecha del primer fallo de seguridad.**

El primer fallo significativo de seguridad en WPA2 se identificó en 2017, cuando se reveló el **ataque KRACK (Key Reinstallation Attack)**. Este ataque explotó un fallo en el protocolo de cifrado WPA2, permitiendo a los atacantes interceptar y manipular datos enviados a través de Wi-Fi sin necesidad de romper la clave completa. En este ataque, los atacantes podían reusar claves de cifrado ya negociadas, lo que ponía en riesgo la integridad y confidencialidad de las comunicaciones.

* **Tipos de ataques que pueden sufrir, explicando en qué consiste cada uno de esos ataques.**

**Ataque por fuerza bruta:**

Consiste en probar todas las posibles combinaciones de contraseñas hasta encontrar la correcta. Aunque WPA implementa medidas como la protección con claves temporales (TKIP y AES), los ataques de fuerza bruta siguen siendo una amenaza potencial.

Para ponerle solución se recomienda utilizar contraseñas fuertes y habilitar la verificación en dos pasos cuando esté disponible

#### 

#### **Ataque de denegación de servicio (DoS):**

Un ataque DoS busca sobrecargar los recursos del sistema para impedir que los usuarios legítimos accedan a la red. Si un cliente no soporta las autenticaciones específicas del punto de acceso, como aquellas que utilizan WPA, puede ser desconectado, dejando la red vulnerable.

Para ponerle solución se recomienda una configuración adecuada del punto de acceso y monitoreo constante para detectar anomalías.

**Ataque de diccionario:**

Los ataques de diccionario utilizan listas predefinidas de contraseñas para tratar de adivinar la clave PSK. Si se utiliza una clave débil, los atacantes pueden aprovechar esta vulnerabilidad para obtener acceso a la red.

Para ponerle solución se recomienda utilizar servidores RADIUS que generan claves únicas y complejas, algo que es más común en entornos empresariales

**Ataque KRACK:**

KRACK es un ataque que afecta a redes WPA2 y permite a los atacantes interceptar y manipular datos enviados a través de Wi-Fi. Utiliza un fallo en el protocolo de cifrado WPA2 para reusar claves ya negociadas.

Para protegerse de KRACK, es necesario actualizar los routers y dispositivos con las últimas versiones de firmware que apliquen los parches de seguridad

* **Routers reales indicando qué estándares admiten**.

[**TP-Link ArcherAX6000**](https://www.amazon.es/TP-Link-Archer-AX6000-Quad-Core-co-procesadores/dp/B07PXTG7R9)

[**Netgear R7000**](https://www.amazon.es/Netgear-Nighthawk-R7000-100PES-tecnolog%C3%ADa-compatible/dp/B00HBYGCOG)

[**Linksys EA7500**](https://www.amazon.es/Linksys-EA7500-EU-MAX-Stream-Monitorizaci%C3%B3n-Administraci%C3%B3n/dp/B01AJOMDSI)

[**ASUS RT-AC67U**](https://www.amazon.es/ASUS-RT-AC66U_B1-inal%C3%A1mbrico-Dual-band-Gigabit/dp/B07D8WNM6C)

**Estándar WPA3**

WPA3 es el último estándar de seguridad diseñado por la Wi-Fi Alliance para redes inalámbricas, desarrollado como una mejora significativa frente a sus predecesores WPA y WPA2. Este protocolo fue creado para mitigar las vulnerabilidades detectadas en versiones anteriores, ofreciendo una mayor seguridad en las comunicaciones inalámbricas, especialmente frente a ataques modernos como el descifrado por fuerza bruta y las vulnerabilidades en la configuración de redes abiertas.

Existen tres formas principales de WPA3: WPA3 personal, WPA3 para empresas y wifi abierto mejorado. Como su nombre indica, WPA3 personal es esencial para el uso personal o doméstico y es fácil de implantar y utilizar, mientras que WPA3 para empresas suele ser utilizado por organizaciones y suele ser más seguro que WPA3 personal.

Las tecnologías de seguridad para la conectividad wifi de próxima generación deben poder prestar una mayor protección de los datos en entornos sensibles a la seguridad, como instituciones financieras, organizaciones sanitarias y departamentos gubernamentales. Desde entornos empresariales altamente controlados hasta redes residenciales más flexibles, wifi CERTIFICADO WPA3 presta la funcionalidad necesaria para satisfacer las necesidades de los distintos despliegues de red.

* **Fecha de uso generalizado**

WPA3 fue publicado en junio de 2018 como el estándar oficial para reemplazar WPA2. Su adopción ha sido gradual, con una mayor prevalencia en dispositivos nuevos lanzados después de su publicación.

* **Métodos de codificación, explicando cada uno de ellos**

**AES-128 y AES-256**:

AES es un cifrado basado en bloques que proporciona alta seguridad para la protección de datos. WPA3 emplea estas versiones para cifrar la información de manera robusta, mejorando la confidencialidad y la integridad de los datos transmitidos.

**SAE (Simultaneous Authentication of Equals)**:

SAE es un nuevo protocolo de autenticación que reemplaza al TKIP y al PSK. Este método permite una negociación segura y robusta de claves de seguridad entre el cliente y el punto de acceso, reduciendo el riesgo de ataques por fuerza bruta.

* **Longitud y formato de la contraseña.**

Las contraseñas en redes WPA3 deben seguir estas pautas para garantizar una alta seguridad:

* **Longitud mínima**: 8 caracteres.
* **Longitud máxima**: 63 caracteres.
* **Caracteres permitidos**: ASCII imprimibles entre 32 y 126, que incluyen letras mayúsculas, minúsculas, números y símbolos.
* **Recomendación**: Se recomienda utilizar contraseñas de al menos 12 caracteres para una seguridad más robusta.
* **Mezcla de caracteres**: Combinación de letras mayúsculas y minúsculas, números y símbolos para contraseñas seguras.
* **Cambio regular**: Se recomienda cambiar las contraseñas periódicamente para mantener la seguridad.
* **Contraseñas por defecto**: No utilizar las contraseñas predeterminadas de los routers, ya que son fácilmente explotables
* **Ámbito de uso.**

WPA3 ha sido diseñado para brindar una seguridad mejorada en redes inalámbricas, tanto para entornos domésticos como para empresas e instituciones gubernamentales. Este estándar es compatible con los dispositivos más recientes y se adapta a diversas necesidades de seguridad, desde pequeñas oficinas hasta grandes corporaciones.

* **Modo personal o clave precompartida (WPA3-PSK)**: Utiliza una clave precompartida (PSK) para que los dispositivos se conecten a la red. Es ideal para redes domésticas y pequeñas oficinas, donde no se requiere autenticación individual para cada usuario.
* **Modo empresarial (WPA3-EAP):** Este modo se basa en el uso de un servidor de autenticación, como un servidor RADIUS, para validar las credenciales de cada usuario. Es adecuado para redes empresariales, instituciones educativas y otras organizaciones que necesitan un mayor control sobre el acceso a la red.
* **Fecha del primer fallo de seguridad.**

El primer fallo significativo de seguridad en WPA3 se identificó en 2019, cuando se descubrió un ataque llamado Dragonblood. Este ataque explotó vulnerabilidades en el protocolo de autenticación SAE, permitiendo que los atacantes interceptaran paquetes y obtuvieran información del proceso de autenticación.

* **Tipos de ataques que pueden sufrir, explicando en qué consiste cada uno de esos ataques.**

**Ataque por fuerza bruta:**

Consiste en probar todas las posibles combinaciones de contraseñas hasta encontrar la correcta. WPA3 ha introducido el protocolo SAE que dificulta estos ataques mediante una negociación segura de claves. Sin embargo, es esencial usar contraseñas fuertes y habilitar la verificación en dos pasos para minimizar el riesgo

#### 

#### **Ataque del tipo "men-in-the-middle":**

En este ataque, los intrusos se interceptan y manipulan la comunicación entre dos dispositivos. WPA3 introduce un cifrado mejorado que impide estos ataques al cifrar cada paquete de manera individual.

**Ataque de diccionario:**

Los ataques de diccionario buscan adivinar la clave PSK utilizando listas predefinidas. WPA3 emplea una autenticación robusta con SAE, lo que hace que estos ataques sean más difíciles de realizar. Para protegerse, se recomienda usar servidores RADIUS que generen claves únicas.

**Ataque KRACK:**

KRACK sigue siendo una amenaza para WPA3, aunque se han implementado medidas para proteger a los dispositivos contra ataques de reutilización de claves. Aún así, es vital mantener los sistemas actualizados con las últimas versiones de firmware para mitigar este riesgo.

* **Routers reales indicando qué estándares admiten**.

[**TP-Link ArcherAX6000**](https://www.amazon.es/TP-Link-Archer-AX6000-Quad-Core-co-procesadores/dp/B07PXTG7R9)

[**NETGEAR Nighthawk AX4**](https://www.amazon.com/NETGEAR-Nighthawk-12-Stream-Router-RAX120/dp/B07P3FGKYD)

[**Linksys MR9600**](https://www.amazon.es/Linksys-Compatible-Controles-parentales-aplicaci%C3%B3n/dp/B08C31D2C3)

[**ASUS GT-AX11000**](https://www.amazon.es/ASUS-ROG-Rapture-GT-AX11000-AiProtection/dp/B07HR8ZFG8)