

RESTRINGIDA



WIFI Gotortzea

Contenido

Abstract	3
Antecedentes	4
Problemas Existentes	5
Objetivos	7
Solución propuesta	9
Características Adicionales	15
Mejores Prácticas	16
Requerimientos Legales	20
Conclusiones	20
Vulnerabilidades.....	20

Abstract

En la era digital en la que nos encontramos, el acceso a internet en instituciones educativas como en el resto de empresas es esencial para el aprendizaje, pero también conlleva riesgos relacionados con la seguridad y la privacidad. Este proyecto propone un modelo de WiFi segura para colegios, garantizando conectividad eficiente sin comprometer la protección de estudiantes y docentes. Se analizan vulnerabilidades comunes en redes escolares y se presentan estrategias de mitigación basadas en cifrado robusto, segmentación de red, autenticación avanzada y filtrado de contenidos. Además, se integran normativas y mejores prácticas para cumplir con estándares de ciberseguridad y protección de la información en entornos digitales. La implementación de este modelo contribuirá a crear un ambiente de aprendizaje seguro y tecnológicamente accesible.

Antecedentes

El acceso a internet en instituciones educativas se ha convertido en una herramienta fundamental para la enseñanza y el aprendizaje. Sin embargo, su implementación sin medidas adecuadas de seguridad puede exponer a estudiantes y docentes a múltiples riesgos, como ataques cibernéticos, robo de información, acceso a contenido inapropiado y vulnerabilidades en la infraestructura de red.

El uso de este tipo de redes ha aumentado exponencialmente en los últimos años debido, entre otras razones, a una cada vez mayor oferta de servicios por parte del centro de recursos formativos, didácticos, ocio etc., así como a la creciente y exclusiva utilización por parte de los usuarios de dispositivos móviles para su uso cotidiano de ocio y formativo. La conjunción de estas dos realidades hace que las redes inalámbricas sean objeto de deseo por parte de los usuarios con el objetivo de realizar sus tareas formativas diarias posibilitando su uso personal.

Ante esta situación, es imprescindible definir estrategias que permitan establecer un modelo de wifi segura para colegios, asegurando una conexión estable y protegida. La implementación de protocolos de autenticación robustos, segmentación de red, cifrado avanzado y sistemas de monitoreo se vuelve crucial para mitigar riesgos y garantizar un ambiente digital seguro para el desarrollo educativo.

Este proyecto se basa en estudios previos y normativas vigentes para diseñar una solución integral que garantice *confidencialidad, disponibilidad e integridad* en las redes wifi escolares, promoviendo un entorno seguro para el uso de la tecnología en la educación.

Problemas Existentes

A pesar de la creciente adopción de tecnología en la educación, muchas instituciones educativas enfrentan dificultades para garantizar la seguridad de sus redes WiFi. Entre los principales problemas detectados en los centros analizados se encuentran los siguientes:

1. Falta de Políticas de Seguridad y Control de Acceso

- No se evidencia la existencia de normativas claras sobre el uso de la red WiFi.
- Falta de segmentación de la red, permitiendo que estudiantes, docentes y personal administrativo comparten la misma infraestructura sin restricciones.

2. Cifrado y Autenticación Inadecuados

- Uso de protocolos de seguridad obsoletos en lugar de estándares más robustos como WPA3.
- Contraseñas débiles y falta de autenticación multifactor para prevenir accesos no autorizados.

3. Falta de Filtrado y Control de Contenidos

- Insuficiente control sobre los sitios web y aplicaciones accesibles desde la red escolar, lo que puede exponer a los estudiantes a contenidos inadecuados o peligrosos.
- Ausencia de soluciones de firewall y listas de control de acceso (ACLs) que limiten la navegación a sitios educativos y seguros.

4. Vulnerabilidades ante Ataques Ciberneticos

- Redes WiFi expuestas a ataques debido a la falta de protección avanzada.
- Dispositivos conectados sin actualizaciones de seguridad, lo que los hace susceptibles a infecciones de malware y explotación de vulnerabilidades.

5. Capacidad y Estabilidad de la Red

- Redes que podrían en breve estar saturadas debido a la creciente demanda de conexión y aumento de servicios ofertados, lo que afecta el rendimiento y la experiencia del usuario.
- Falta de puntos de acceso estratégicamente distribuidos para garantizar cobertura y calidad de conexión en todas las áreas del colegio.

6. Falta de personal especializado

- Personal administrativo y docente con conocimientos limitados en ciberseguridad, lo que dificulta la correcta gestión de la red.
- Falta de concienciación en estudiantes sobre el uso responsable y seguro del internet.

7. Aumento de necesidades

- Demanda muy elevada de este tipo de redes debido al uso prácticamente exclusivo de dispositivos móviles (Tablet, Tfno. móvil, portátil) entre los usuarios, tanto para tareas docentes como personales.
- Mayor necesidad de dotar de conectividad a servicios (recursos didácticos, formativos, etc) en la totalidad de las instalaciones de ellos centros.

Estos problemas resaltan la necesidad de una estrategia integral que contemple soluciones técnicas y normativas para establecer una red WiFi segura y eficiente en entornos escolares.

Objetivos

Diseñar e implementar un modelo de WiFi segura para colegios que garantice una conectividad eficiente, protegida contra amenazas cibernéticas y alineada con normativas de seguridad, asegurando un entorno digital seguro para estudiantes, docentes y personal administrativo.

1. Establecer una infraestructura de red segura y eficiente

- Diseñar una arquitectura de red segmentada para separar los accesos de estudiantes, docentes y personal administrativo.
- Implementar estándares de cifrado avanzados, como WPA3, para proteger las comunicaciones inalámbricas.

2. Optimizar el control de acceso y la autenticación de usuarios

- Implementar un sistema de autenticación robusto, como autenticación multifactor (MFA) o acceso mediante credenciales individuales.
- Configurar una gestión de permisos adecuada para garantizar que cada usuario acceda solo a los recursos que le corresponden.

3. Garantizar la protección contra amenazas cibernéticas

- Implementar firewalls, sistemas de prevención de intrusiones (IPS) y listas de control de acceso (ACLs) para mitigar riesgos de ataques.
- Utilizar herramientas de monitoreo en tiempo real para detectar accesos no autorizados o comportamientos sospechosos.

4. Controlar y filtrar el acceso a contenidos no apropiados

- Establecer sistemas de filtrado de contenidos que bloquen sitios web peligrosos o inapropiados para el entorno educativo.
- Aplicar políticas de uso responsable de internet para prevenir abusos y garantizar la seguridad de los estudiantes.

5. Garantizar la estabilidad y rendimiento de la red

- Optimizar el ancho de banda y la distribución de la red para evitar saturaciones y garantizar una conexión estable.
- Implementar puntos de acceso estratégicos para ofrecer una cobertura uniforme en todas las áreas del colegio.

6. Fomentar la capacitación y concienciación en ciberseguridad

- Diseñar programas de formación en buenas prácticas de seguridad digital para docentes, estudiantes y personal administrativo.
- Promover una cultura de ciberseguridad mediante campañas de concienciación sobre el uso seguro de la red y los dispositivos conectados.

7. Cumplir con normativas y regulaciones de seguridad

- Asegurar que la red WiFi cumpla con estándares de protección de datos y normativas legales vigentes, como la GDPR (Europa), COPPA (EE.UU.) o regulaciones locales.
- Desarrollar políticas internas que regulen el uso de la red y establezcan medidas disciplinarias en caso de incumplimiento.

El cumplimiento de estos objetivos permitirá la creación de un entorno digital seguro, confiable y eficiente para el desarrollo educativo en los colegios.

Solución propuesta

La solución propuesta en este proyecto, la vamos a dividir en dos partes, como respuesta a las dificultades técnicas y económicas que puede tener la solución identificada como optima al momento de la redacción de este texto.

La primera de las propuestas, denominada propuesta de mínimos identifica las medidas de seguridad y activos de información mínimos necesarios para que la red inalámbrica de cualquier centro pueda contar con unos mínimos elementos de seguridad, pero con deficiencias y vulnerabilidades que podrían llegar a ser explotadas. Algunos de los elementos de los que carecería o prescindiría este tipo de red podrían ser:

- Elementos obsoletos o vulnerables
- Falta de autenticación MAC
- Políticas NPS
- Monitorización

En la segunda de las propuestas, la propuesta deseable, se identifican las medidas de seguridad y activos de información óptimos desde el punto de vista de la seguridad, para que la red inalámbrica de centro la podamos considerar como red inalámbrica segura.

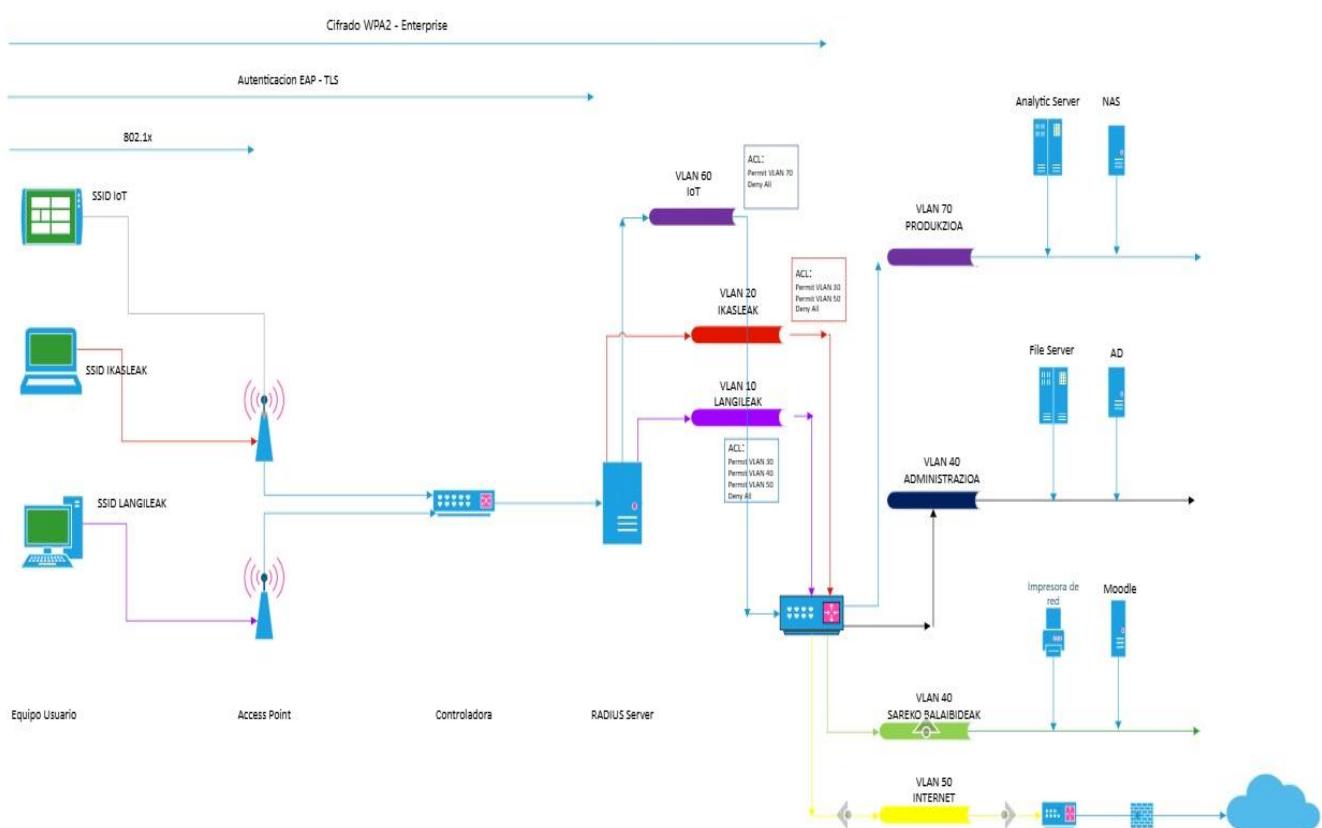
Solución Mínimos

El diseño de esta solución se ha ideado teniendo en cuenta los mínimos de seguridad necesarios existentes al momento para considerar una red o conexión inalámbrica como segura.

Características

- Protocolo de cifrado: WPA2 - Enterprise (AES 128bits)
- Autenticación: PEAP-MSCHAPv2
- Asignación de rol (VLAN, caudal, políticas...) mediante ACL
- Monitorización

Arquitectura Mínimos



Ejemplo de Comunicación Conexión Segura en solución de minimos

1. Conexión: Equipo cliente intenta conectarse a la WLAN que se encuentre activa en que el Identificador del conjunto de servicios (SSID) haya identificado.

2. Autenticación: El punto de acceso configura un canal restringido que permite al cliente comunicarse únicamente con el servidor RADIUS. El cliente intenta autenticarse en el servidor RADIUS a través del canal restringido por medio de 802.1X. La negociación de la sesión genera una clave que el cliente y el servidor RADIUS utilizan, el cliente se autentica en el servidor RADIUS utilizando el protocolo PEAP MS-CHAP v2.

3. Autorización: El servidor RADIUS comprueba las credenciales del cliente en relación con el directorio. Si el cliente se autentica correctamente, el servidor RADIUS recabará información con la que decidirá si autoriza al cliente a usar la WLAN y las ACL que le corresponden. Así, si el cliente obtiene acceso, el servidor RADIUS transmitirá la clave maestra al punto de wifi. El cliente y el punto wifi comparten claves comunes que utilizan para cifrar el tráfico que fluye entre ellos.

4. Cifrado WLAN: El punto de acceso une la conexión de la WLAN del cliente a la LAN interna. Ahora el tráfico que fluye entre el cliente y el punto de acceso está cifrado.

Este esquema aun siendo el más fácil de implementar y el que menos dedicación y recursos necesitará tanto para la puesta en marcha como para el mantenimiento de la misma, también es verdad que tiene una serie de debilidades y/o vulnerabilidades como las siguientes:

- **Rogue Access Points (Puntos de Acceso Falsos):** Configuración de puntos de acceso no autorizados. Para prevenir los RAP, es esencial utilizar una combinación de medidas técnicas y administrativas. Entre las medidas técnicas podriamos enumerar los sistemas NAC, implementar protocolo WPA3, actualizar los dispositivos y el firmware con regularidad y tambien el deshabilitar puertos en desuso. Entre los administrativos identificamos el establecer políticas claras sobre las redes inalámbricas, capacitar a los usuarios y al personal y evitar el acceso físico a los dispositivos WIFI y puntos de red.
- **FragAttacks:** No son una única vulnerabilidad, sino un conjunto de fallos que pueden ser explotados para comprometer la seguridad de las redes inalámbricas. Como medidas de protección se recomienda utilizar WPA3, desactivar funciones innecesarias, usar herramientas de seguridad (FW, WIDS)

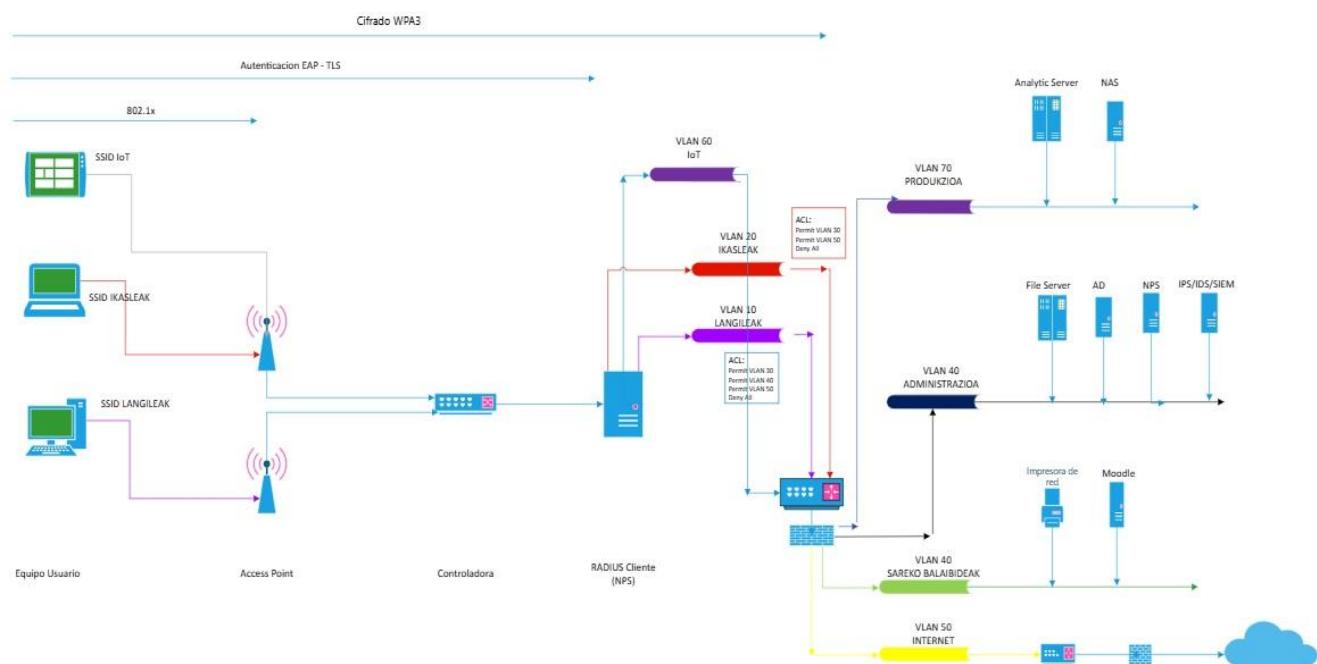
Solución Deseable

El diseño de esta solución se ha ideado teniendo en cuenta las buenas prácticas en redes inalámbricas seguras, así como en las últimas novedades y avances tecnológicos en el ámbito de la ciberseguridad existentes al momento de la redacción del proyecto, con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de los activos de información de los centros de formación.

Características

- Protocolo de cifrado: WPA3 - Enterprise (AES 192 bits) WPA2 - Enterprise (AES 128bits) → Se recomienda el primero por existir vulnerabilidades en WPA2
- Autenticación: EAP-TLS: El principal reto es establecer la Infraestructura de Clave Pública (PKI) necesaria para gestionar el ciclo de vida de los certificados.
- Filtrado MAC
- Asignación de rol (VLAN, caudal, políticas...) mediante ACL seguros
- Servidor NPS protegido por FW
- Monitorización y alerta temprana

Arquitectura Deseable



Ejemplo de Comunicación Conexión Segura en entorno deseable

- 1.- Equipo Usuario solicita acceso a red WIFI
- 2.- Punto de acceso y Equipo usuario negocian el método de autenticación
- 3.- Punto de acceso solicita info (MAC y otros atributos) a Equipo Usuario
- 4.- Punto de acceso valida MAC contra cliente RADIUS
- 5.- Punto de acceso establece comunicación segura (cert. Digital) entre Equipo usuario y cliente RADIUS
- 6.- Cliente RADIUS solicita credenciales a Equipo Usuario
- 7.- Equipo Usuario responde con credenciales a Cliente RADIUS
- 8.- Cliente RADIUS autentica credenciales con servidor NPS (Radius) y asignan ACL

Puesta en marcha de la solución deseada

La puesta en marcha de la solución deseada implicara dedicación mas alta por parte de los recursos asignados, tanto en instalación de la solución como en el mantenimiento del mismo.

Por una parte, durante la fase de instalacion, existe la necesidad de poner en marcha y configurar diferentes servicios de seguridad y validacion que en la solucion de minimos no existe:

- Listado de MACs a filtrar
- Instalacion y configuracion de IPS/SIEM
- Cliente-Server NPS (Radius)
- Configuración y puesta en marcha de FW
- Configuración y puesta en marcha de infraestructura de PKI

En cuanto al mantenimiento de la instalacion, el recurso asignado necesitara tiempo extra para las siguientes tareas, que no tendra que realizar o dedicar en la solucion de minimos:

- Revisión de herramientas de monitorización como IDS y SIEM:
recomendable dedicar una hora mínimamente a la semana
- Listas Blancas/Negras: Mínimamente será necesario dedicar una hora para revisar y añadir o eliminar las MAC de usuarios dados de altas, bajas o modificaciones

-
- Mantenimiento de infraestructura claves: Una hora el mes de dedicación
 - El resto de infraestructura también necesitará de dedicación para mantenimiento y actualización de los dispositivos, lo que puede llevar alrededor de una hora a la semana. Esta dedicación, puede que en menor medida, será necesaria también en el caso del entorno de mínimos.

Características Adicionales

Las características adicionales que la red wifi identificada como deseable debe tener sobre la red de mínimos las enumeramos en los siguientes puntos:

- **Cifrado:** El nuevo protocolo de autenticación y el aumento del nivel de cifrado refuerzan la protección de WPA3 Wi-Fi contra las principales amenazas de las redes wifi.
- **Monitorización constante:** es importante monitorizar regularmente las distintas SSID que gestionamos para detectar cualquier actividad inusual o no autorizada. La monitorización y los sistemas de alerta temprana ayudan a detectar actividades sospechosas y/o maliciosas de forma temprana, especialmente cuando se trata de redes con uso tan extensivo y diverso.
- **Actualizaciones Hw/Sw:** Actualizar el firmware y software de los sistemas, así como renovar la electrónica de red cuando queda fuera de soporte, evitan vulnerabilidades en nuestros sistemas aumentando de forma considerable el nivel de seguridad de las redes wifi.
- **Servidor NPS:** La asignación de roles y permisos a los usuarios finales, así como el resto de los sistemas y servicios de nuestra red quedan securizados y gestionados mediante un firewall aumentando considerablemente el nivel de seguridad de nuestra red.

Mejores Prácticas

Para garantizar la seguridad, estabilidad y eficiencia de la red WiFi en entornos educativos, se recomienda aplicar las siguientes prácticas:

1. Seguridad en la Infraestructura de Red

- Segmentación de Red: Separar el tráfico de estudiantes, docentes, administrativos e invitados mediante VLANs para evitar accesos no autorizados.
- Administración: Separar el tráfico de gestión de electrónica de red WIFI para personal dedicado específicamente con ese fin
- Uso de WPA3-Enterprise: Implementar el estándar de cifrado más reciente para proteger las conexiones inalámbricas.
- Red Invitados: Implementar un portal cautivo sobre esta red para controlar y gestionar el tráfico de esta. Sin ser un requerimiento legal si es una recomendación de seguridad y optimización de la red.
- Control de dispositivos: Restringir la conexión a dispositivos autorizados mediante listas blancas de direcciones MAC.

2. Autenticación y Control de Acceso

- Implementación de Autenticación Multifactor (MFA): Requerir un segundo factor de autenticación para usuarios administrativos o docentes.
- Uso de Portales Cautivos: Requerir credenciales antes de conceder acceso a la red, especialmente para usuarios invitados.
- Roles y Permisos: Asignar niveles de acceso según el rol del usuario dentro de la institución.

3. Protección contra Amenazas Cibernéticas

- Firewalls y Sistemas de Prevención de Intrusiones (IPS): Filtrar el tráfico malicioso y detectar ataques en tiempo real.
- Monitoreo Continuo: Implementar herramientas de análisis de tráfico y alertas ante actividades sospechosas.
- Actualización de Firmware y Parches de Seguridad: Mantener siempre actualizados los routers, puntos de acceso y sistemas de control de red.

4. Filtrado y Control de Contenidos

- Filtrado de Web y DNS Seguro:** Usar herramientas para bloquear sitios web peligrosos, contenido inapropiado y phishing.
- Control de Aplicaciones:** Restringir aplicaciones no educativas que puedan consumir ancho de banda innecesario.
- Horarios de Acceso:** Configurar restricciones horarias para limitar el uso de la red en momentos no académicos.

5. Optimización del Rendimiento y Cobertura

- Distribución Estratégica de Puntos de Acceso:** Garantizar una cobertura óptima sin zonas muertas ni interferencias.
- Balanceo de Carga y Ancho de Banda:** Configurar prioridades para tráfico educativo y limitar el uso de descargas pesadas.
- Uso de QoS (Quality of Service):** Priorizar videoconferencias y aplicaciones educativas sobre el tráfico recreativo.

6. Capacitación y Concienciación en Ciberseguridad

- Formación a Docentes y Administrativos:** Crear cursos sobre buenas prácticas de seguridad digital.
- Concienciación en Estudiantes:** Incluir talleres sobre el uso responsable de la tecnología y riesgos en internet.
- Simulacros de Seguridad:** Realizar ejercicios periódicos para evaluar la respuesta ante incidentes cibernéticos.

7. Cumplimiento Normativo y Políticas de Uso

- Adecuación a Normativas:** Cumplir con regulaciones como GDPR (Europa), COPPA (EE.UU.) o normativas locales de protección de datos.
- Política de Uso Aceptable:** Establecer reglas claras sobre el acceso y uso de la red WiFi.
- Registro y Auditoría:** Mantener logs de actividad para detectar incidentes y mejorar la seguridad continuamente.

Requerimientos legales

Es recomendable crear y mantener un registro de actividad de la red por parte de los usuarios que se conectan a la misma como salvaguarda, en el caso de que se realicen actividades ilícitas a través de ella. En los términos y condiciones debe incluirse, de forma clara, la motivación por la que se almacena esta información y recabar el consentimiento explícito y pleno del usuario.

En el caso de que el usuario no haya dado su consentimiento o no se le haya informado debidamente de dicho registro, no se podrá guardar dicha información. Por otra parte, el artículo 25.1 de la Ley de Seguridad Ciudadana obliga a los centros que cuenten entre sus servicios con una red wifi abierta para sus clientes a conservar el registro de conexiones a esa red. Esta información deberá estar a disposición de las Fuerzas y Cuerpos de Seguridad del Estado durante los plazos que establezcan las disposiciones aplicables en cada caso.

Por último, si los administradores o los propietarios de la conexión detectaran la comisión de un delito por parte de los usuarios de la red que atente contra la libertad de las personas (coacciones o amenazas), deberán notificar a las Fuerzas y Cuerpos de Seguridad del Estado, ya que en caso de que no se hiciera, se incurría en un delito de omisión del deber de impedir delitos o de promover su persecución.

- **Excepciones**

En el caso de organizaciones sin ánimo de lucro, que no pudieran realizar los procesos anteriormente descritos debido a los costes asociados o a la imposibilidad técnica de implantarlos, podrán recoger en un documento colocado a la vista de todo el mundo las reglas de uso de la red wifi, así como indicar la no responsabilidad por el mal uso de la red por parte de los usuarios.

- **Logs**

Aunque no es obligatorio, si es útil y además recomendable tener un sistema de logs: información básica sobre quién se conectó, cuándo y durante cuánto tiempo. Eso sí, si los guardas, tienes que informar al usuario, guardar solo lo necesario, no conservar los datos más tiempo del necesario y protegerlos adecuadamente.

Si almacenas los datos sin decírselo al usuario o sin su consentimiento puede ser motivo de sanción.

Conclusión

La configuración de los centros analizados, así como la información recogida en los mismos, muestra que la realidad de la mayor parte de los centros formativos se acerca mucho o es muy similar a la red descrita en este texto como red wifi *mínima*. Eso significa que, aunque todavía se debe mejorar en varios aspectos para conseguir que la red, sus usuarios y datos sean totalmente seguros, también es cierto que los requerimientos mínimos de seguridad de los usuarios, así como de sus datos se están viendo mínimamente cubiertos hoy en día.

Existen en este esquema de mínimos una serie de elementos vulnerables por obsolescencia o actualización, cifrados vulnerables, autenticación limitada, así como una monitorización y gestión de red e incidentes limitadas que deberían ser subsanados para aumentar de forma considerable el nivel de seguridad de la red.

La aplicación de buenas prácticas (cumplimiento, concienciación, optimización y gestión) así como de la arquitectura descrita e identificada como red wifi *deseable*, garantizará una red wifi mucho más segura, estable y eficiente, minimizando riesgos y promoviendo un ambiente digital adecuado para el entorno educativo.

Como conclusión, enumeramos los siguientes puntos críticos que harán mejorar la seguridad de nuestra red:

1. **Mejora de la seguridad:** Implementar medidas de seguridad avanzadas, como la encriptación WPA3, reduce significativamente el riesgo de accesos no autorizados y ciber ataques.
2. **Optimización del rendimiento:** La configuración adecuada de los canales y la gestión de la banda ancha harán que mejore la velocidad, la estabilidad de la conexión y el control y gestión de la conexión.
3. **Actualización:** Mantener nuestros elementos de red actualizados y en soporte de fabricante es vital para mejorar los niveles de seguridad
4. **Cumplimiento normativo:** Una red que cumpla con las normativas y estándares de seguridad, garantizando la protección de datos sensibles es crucial para mejorar la seguridad de la red.
5. **Concienciación y formación:** La capacitación de los usuarios sobre buenas prácticas de seguridad aumentara la conciencia y la prevención de riesgos.

Vulnerabilidades

A continuación, se detallan las vulnerabilidades de los Access Points y Controlador de Ubiquiti que se han identificado hasta el momento:

CVE	Exploit Disponible	Fuente
CVE-2013-3572	Sí (inyección XSS)	Blog de Moritz Frenzel – ejemplo de hostname malicioso
CVE-2020-27888	No	Sin exploit público conocido. Mencionado en foros de Ubiquiti
CVE-2019-5456	No	NVD – solo MITM vía proxy SMTP, sin PoC publicado
CVE-2014-2226	No	Advisory oficial – vulnerabilidad pasiva (hash expuesto en syslog)
CVE-2014-2225	Sí (CSRF)	Exploit-DB #32994 – creación de admin vía CSRF
CVE-2016-7792	Sí	Packet Storm Security – acceso directo a MongoDB
CVE-2023-38034	No	Ubiquiti Bulletin 035
CVE-2018-5264	Sí	Red4Sec Advisory – manipulación de tiempo libre vía cookie
CVE-2024-22054	No	Ubiquiti Bulletin 037
CVE-2023-35085	No	Ubiquiti Bulletin 035
CVE-2024-42028	No	Ubiquiti Bulletin 043
CVE-2023-41721	No	Ubiquiti Bulletin 036
CVE-2024-37380	No	Ubiquiti Bulletin 041
CVE-2024-54750	Sí	Notion Leak Report – contraseña root hardcoded (Fireitup)
CVE-2024-27981	No	NVD, Ubiquiti Bulletin 038

Las versiones mínimas aconsejadas para la infraestructura UBIQUITY es la siguiente:

Controlador UNIFI NETWORK SERVER

Versión actual del controlador	Versión mínima recomendada
v9.1.120	v8.5.6

UNIFI AP U6

Versión actual del firmware	Versión mínima recomendada
v6.6.78	v6.6.55