Alejandro Molina De Haro

06/02/2026

Tabla de contenido

Caso de uso

Eres el responsable de IT de un instituto. En una semana han pasado estas tres cosas:

1. **Alumnado y visitantes se conectan a una Wi-Fi llamada IES_GUEST. De repente aparece otra red muy parecida llamada IES_GUEST_FREE y varias personas dicen que les han robado la contraseña de Instagram después de conectarse.**
2. **Un profesor recibe un PDF "firmado" con una solicitud importante. Al abrirlo, el visor muestra que la firma no es válida. El profesor dice que alguien lo ha modificado.**
3. **El técnico nuevo activó WPS en el router "para ir más rápido" y dejó la misma contraseña en todas las redes.**

Parte 1

Dos posibles causas del problema de la Wi-Fi

- Evil Twin: alguien ha creado una red falsa con un nombre casi igual para que la gente se conecte sin darse cuenta.
- Mala configuración del router: usar la misma contraseña y WPS facilita que cualquiera copie la red original.

Qué significa que una firma digital sea inválida

- Que el documento ha sido modificado después de firmarse o que la firma no es de quien dice ser.

Por qué activar WPS es una mala idea

- Porque se puede atacar por fuerza bruta y entrar a la Wi-Fi sin saber la contraseña real.

Parte 2

A. Wi-Fi y robo de cuentas

Amenaza principal elegida: Evil Twin

- Porque apareció una red casi igual y después de conectarse robaron contraseñas.

Tres señales de un Evil Twin

- Hay dos redes con nombres casi iguales.
- La red falsa no pide contraseña o es diferente.
- Al conectarte, las páginas web no usan HTTPS o piden iniciar sesión rara.

Cuatro medidas técnicas para proteger la Wi-Fi

- Usar WPA3 o WPA2-Enterprise.
- Desactivar WPS en todos los routers.
- Separar redes con VLANs.
- Usar certificados para autenticar la red del profesorado.

B. Firma digital y certificado

Diferencia entre certificado digital y firma digital

- El **certificado digital** identifica a una persona o entidad.
- La **firma digital** sirve para asegurar que un documento no se ha modificado y quién lo firmó.

Tres garantías de una firma digital correcta

- **Autenticidad**: sabes quién firma.
- **Integridad**: el documento no ha cambiado.
- **No repudio**: el firmante no puede negarlo.

C. Identificación y MFA

Tres tipos de factores de autenticación

- **Algo que sabes**: contraseña o PIN.
- **Algo que tienes**: móvil o token.
- **Algo que eres**: huella o cara.

Por qué MFA reduce el riesgo

- Porque aunque roben la contraseña, falta el segundo factor para entrar.

Parte 3 – Plan de acción para el instituto

Configuración final de Wi-Fi

- Usar **WPA3** o **WPA2-Enterprise**.
- **Desactivar WPS** siempre.
- Crear tres redes separadas con VLANs: profes, alumnado e invitados.
- Contraseñas largas, únicas y aleatorias (mínimo 16 caracteres).
- Revisar cada semana logs, dispositivos conectados y redes sospechosas.

Gestión de firmas y certificados

- Firmar PDFs con un **certificado digital válido** y reconocido.
- Comprobar siempre la firma con un visor oficial.
- Guardar la clave privada cifrada y con contraseña.
- Revocar el certificado si se sospecha robo.
- Formar al profesorado en uso de firmas digitales.

Política de autenticación

- Contraseñas largas, sin reutilizar y con complejidad.
- MFA obligatorio en correos, intranet y gestión académica.
- Prohibir cuentas compartidas.
- Bloquear cuentas tras varios intentos fallidos.
- Avisar, cambiar contraseñas y analizar si hay phishing.

Parte 4 – Frases finales

- La amenaza más probable fue un **Evil Twin**.
- La medida más importante es usar **Wi-Fi segura sin WPS y con redes separadas**.
- Lo que más cuesta es entender la **firma digital**, porque mezcla criptografía y certificados.