1. **Protocolos y estándares seguros en eHealth**

* FHIR: estándar para el intercambio de información sanitaria HTTP sobre TLS.
* IHE ATNA: perfil para la autenticación entre nodos y usuarios TLS, asocia acción con la idetnida unica.
* IHE XUA: se complementa con ATNA. perfil para transmitir la identida de un usuario ya uatenticado usa tokens SAML.
* DICOM: estándar internacional para imágenes médicas.
* IEEE 11073: interoperabilidad de dispositivos de salud.

1. **Soluciones** **comerciales**

Imprivata OneSign

* SSO para rapidez, MFA, TAp-and-go el cambio de sesion es mas rapido en estaciones compartidas y cumple com GDPR y HIPAA.

Claroty xDome

plataforma de cibersguridad.

* monitorizacion en tiempo real, segmentacion de red dinamica, huella digital por dispositivo, inventario inteligente (descubrimiento y clasificación precisa de dispostiivos médicos y tecnológicos).

Cisco Medical NAC

* segmentacion de rede, autenticacion y control d accesom udebtificacion por huella digital, monitorizacion continua.

PKI e identidades de salud

* certificados digitales, cifrado y firmas electronicas, MFA, integracion con HSMs certificados.

Soluciones moviles especializadas

* acceso seguro a EHR, autenticacion fuertea y cifrado de extremo a extremo, monitorizacion remota y gestion de idpositivos compartidos.

1. **Problemas**

Es difícil integrar unos centros médicos con otros.

* hl7: no impone medidas de seguridad por defecto, exposición a riesgos web.
* IHE ATNA: alta complejidad técnica, riesgos por tokens SAML mal gestionados.
* DICOM: bajo uso sobre TLS, falta de monitoreo del puerto seguro, metadatos sensibles no anonimizados, controles de acceso y auditoría débilmente integrados.
* IEEE 11073: baja compatibilidad.

1. **Conclusión**

Se tiene que mejorar la interoperabilidad para que sea viable.

* Usará sistemas inteligentes y zero trust
* Security-by-design
* Identidades digitales soberanas