Antonio Abad Correa

José Maria Solís

Pedro Lacarcel

Índice

## 

## Portada

## Índice

## Resumen ejecutivo

## Core

## Pruebas

## Conclusión

## Bibliografía

## Resumen ejecutivo

## El presente proyecto desarrolla una infraestructura segura de acceso remoto basada en tecnología VPN SSL (Secure Sockets Layer), enmarcada dentro de la política BYOD (Bring Your Own Device) adoptada por una universidad pública. El propósito fundamental consiste en permitir que el personal autorizado acceda a los recursos institucionales —tales como bases de datos, servicios de correo electrónico y sistemas corporativos— mediante sus dispositivos personales, garantizando los principios de confidencialidad, integridad, autenticidad y disponibilidad definidos por el Esquema Nacional de Seguridad (ENS).

## La solución técnica implementada se sustenta en una arquitectura cliente-servidor utilizando sockets seguros SSL/TLS, que posibilitan el establecimiento de canales de comunicación cifrados bajo TLS 1.3 y el uso de Cipher Suites criptográficamente robustas. El sistema incorpora mecanismos de gestión y verificación segura de credenciales, control de sesiones y registro persistente de mensajes, implementando medidas de protección frente a ataques de fuerza bruta, interceptación y manipulación de datos.

## El modelo propuesto ha sido diseñado conforme a los requisitos funcionales, de información y de seguridad establecidos, asegurando la protección de los datos personales conforme al Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD). Para la validación de la solución se ejecutaron pruebas de rendimiento y de seguridad empleando herramientas de análisis de tráfico de red (Wireshark, RawCap, tcpdump), verificando la correcta implementación de los canales cifrados y la imposibilidad de lectura del tráfico interceptado.

## Los resultados obtenidos demuestran la eficacia y robustez del canal VPN SSL para proteger las comunicaciones entre usuarios remotos y servidores institucionales, así como la viabilidad operativa del entorno BYOD en el ámbito de la Administración Pública, sin degradación significativa del rendimiento del sistema ni vulneración de la normativa aplicable en materia de seguridad y protección de la información.

## Core

## Pruebas

## Conclusión

El desarrollo e implementación de la VPN SSL Road Warrior ha permitido verificar la viabilidad técnica de un sistema de comunicaciones seguras basado en TLS 1.3, que cumple de manera efectiva los principios de seguridad de la información definidos en el Esquema Nacional de Seguridad (ENS) y las directrices europeas de protección de datos.

Las pruebas experimentales realizadas con sniffers de red y herramientas de monitorización de tráfico evidenciaron la correcta encapsulación y cifrado de los paquetes transmitidos a través de los sockets SSL, garantizando la confidencialidad del flujo de información, la autenticidad del emisor y receptor y la integridad de los datos frente a ataques de interceptación o alteración. Asimismo, los resultados de rendimiento muestran una pérdida marginal de eficiencia, confirmando que el cifrado no supone un impacto operativo significativo sobre la capacidad concurrente estimada de 300 usuarios.

El sistema propuesto satisface de manera completa los requisitos funcionales, de información y de seguridad establecidos en el análisis inicial, integrando medidas de protección de credenciales, gestión segura de sesiones, registro persistente de mensajes y validación criptográfica del canal de comunicación. Desde una perspectiva arquitectónica, la solución es escalable, interoperable y adaptable a otros entornos institucionales que requieran la implementación de políticas BYOD seguras.

En conclusión, el proyecto BYODSEC – Road Warrior VPN SSL constituye una propuesta tecnológica sólida y conforme con las normas de seguridad vigentes, demostrando la capacidad de las infraestructuras VPN SSL para proporcionar conectividad remota segura en entornos de Administración Pública. Su correcta integración contribuye a la madurez de las políticas de seguridad de la información institucionales y representa una referencia práctica en el ámbito del aseguramiento de la información y las comunicaciones seguras basadas en TLS.

## Bibliografía