

# Sistema de comunicaciones seguras con segmentación virtual de dominios

Avance de proyecto

Alberto Daniel Lange

Ingeniería en Telecomunicaciones  
Instituto Balseiro

19 de febrero de 2025



## ① Introducción

## ② Revisión bibliográfica

## ③ Desarrollo

## ④ Conclusiones

# 1 Introducción

## 2 Revisión bibliográfica

## 3 Desarrollo

## 4 Conclusiones

# Introducción

- Desarrollo de un encriptador para asegurar las comunicaciones entre sitios.

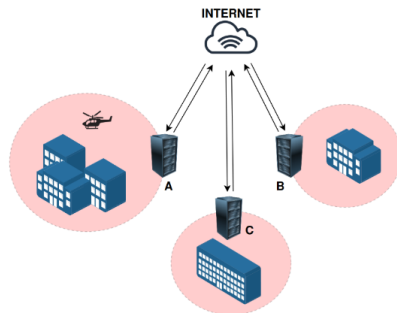


Figura 1: Esquema simplificado de operación del sistema.

# Motivación

- Abordaje novedoso a las soluciones de encriptación de redes.
- Necesidad de una solución propia y auditable.

# Objetivos

- Validar la viabilidad de realizar segmentación de dominios basada en hipervisores.
- Realizar una prueba de concepto del enfoque propuesto.
- Implementar una propuesta de solución auditable y documentada.

- 1 Introducción
- 2 Revisión bibliográfica**
- 3 Desarrollo
- 4 Conclusiones

## Triada CID



Figura 2: Modelo CID.



# Encriptación simétrica

- Clave única.
- Requiere un canal seguro para el intercambio de la clave.
- La confidencialidad y autenticación dependen tanto de A como de B.
- Método eficiente.

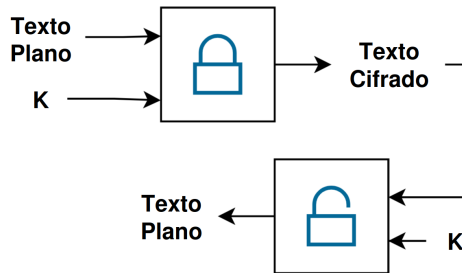


Figura 3: Esquema simplificado de la encriptación simétrica.

# Encriptación asimétrica

- Par de claves relacionadas.
- Mantener la autenticidad y confidencialidad de lo que recibe A depende solo de A.
- Mayor costo computacional.

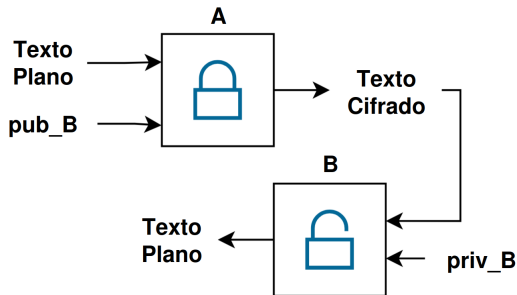


Figura 4: Esquema simplificado de la encriptación asimétrica.

## Acuerdo de claves Diffie-Hellmann

- Método para generar una clave compartida sin intercambio directo.
- Mitiga un problema de la encriptación simétrica.

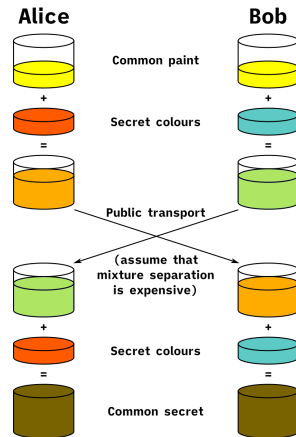


Figura 5: Proceso Diffie-Hellmann simplificado.

## Arquitectura red/black

- Lineamientos para identificar y separar correctamente dominios de información.

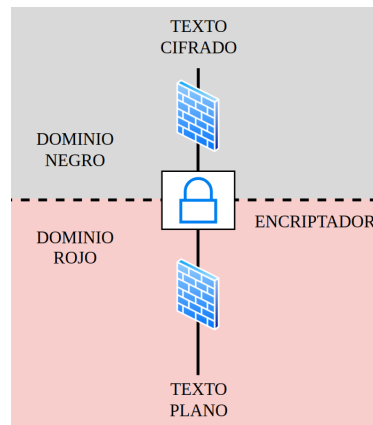


Figura 6: Esquema simplificado dominios red/black.

# Hipervisores

Software que permite la ejecución de entidades virtuales independientes sobre hardware compartido.

- Tipo 1: ejecución sobre hardware.
- Tipo 2: ejecución sobre un sistema operativo.



Figura 7: Ejemplo de hipervisores.

## 1 Introducción

## 2 Revisión bibliográfica

## 3 Desarrollo

Propuesta de solución

Laboratorios virtuales

## 4 Conclusiones

## Plan de trabajo

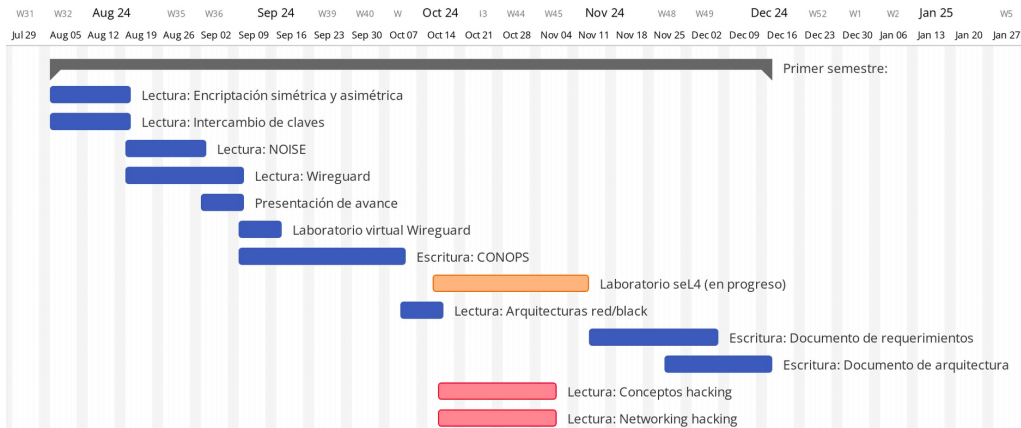


Figura 8: Plan de trabajo del primer semestre de proyecto.

## 1 Introducción

## 2 Revisión bibliográfica

## 3 Desarrollo

Propuesta de solución

Laboratorios virtuales

## 4 Conclusiones



# Método ARCADIA

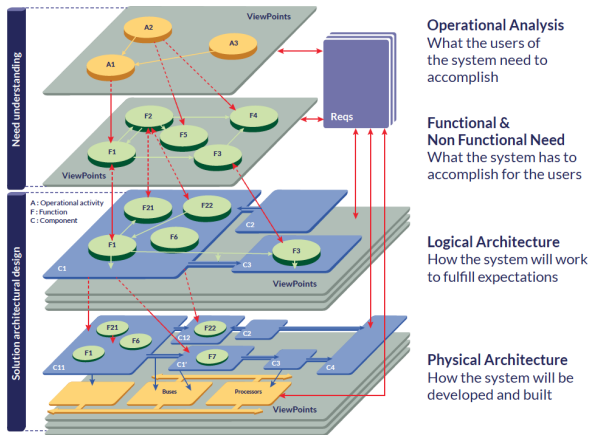


Figura 9: Desglose del método adoptado.

# Análisis operacional

- Definición del problema.
- Planteo de las necesidades del usuario.
- Alcance de la solución.



Figura 10: Concepto de operaciones.

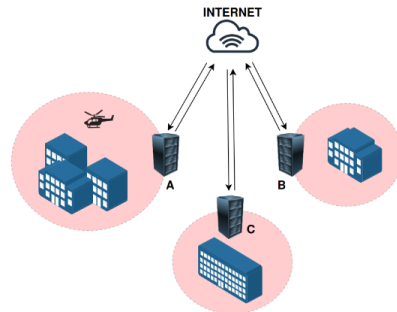


Figura 11: Esquema simplificado del sistema propuesto.

# Modos de operación

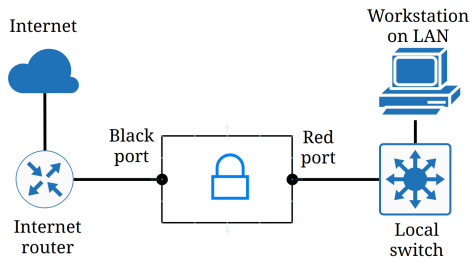


Figura 12: Despliegue en sitio sin infraestructura de red.

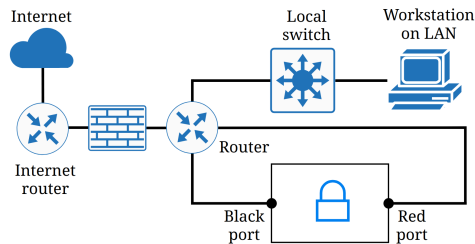


Figura 13: Despliegue en sitio con infraestructura de red.

# Requerimientos

- **Funcionales:** renovación de claves, manejo de ataques DoS.
- **Rendimiento:** tasa de transferencia, número de nodos.
- **Interfaz:** administración, interfaces físicas.



Figura 14: Documento de requerimientos.

# Arquitectura lógica

- Uso de un hipervisor con tres máquinas virtuales independientes.



Figura 15: Documento de arquitectura.

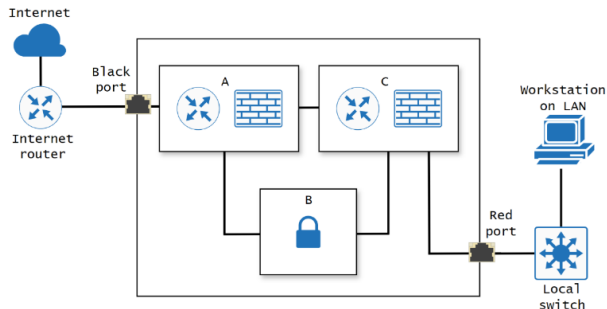


Figura 16: Arquitectura lógica de la solución propuesta.

# Tecnologías a usar

## NOISE

- Framework para el desarrollo de protocolos seguros.

## Wireguard

- Software VPN.
- Opera a nivel de capa 3.
- Base de código reducida.

## seL4

- Microkernel.
- Hipervisor tipo 1.
- Formalmente probado.

## 1 Introducción

## 2 Revisión bibliográfica

## 3 Desarrollo

Propuesta de solución  
Laboratorios virtuales

## 4 Conclusiones

# Laboratorio virtual - Wireguard

- Fundamentos de redes.
- Utilización de Wireguard.

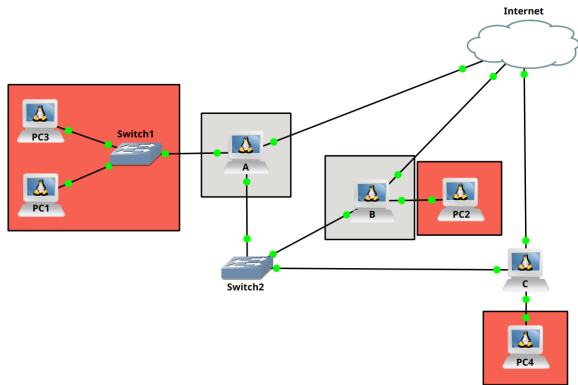


Figura 17: Primeras pruebas con Wireguard en GNS3.



# Laboratorio virtual - Wireguard

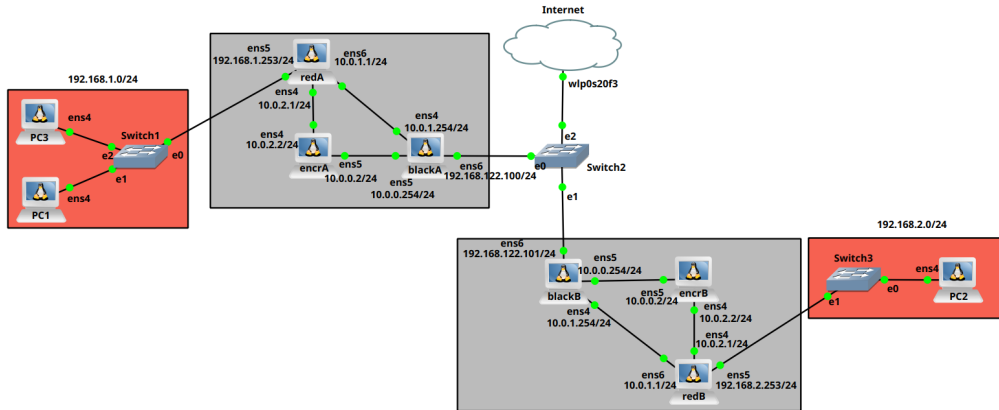


Figura 18: Implementación de la propuesta de solución en GNS3.

- 1 Introducción
- 2 Revisión bibliográfica
- 3 Desarrollo
- 4 Conclusiones**

# Resumen

- Introducción a los conceptos de sistemas de comunicaciones seguras.
- Elaboración e implementación simulada de una propuesta de solución.
- Familiarización con el software a utilizar.

## Trabajo a futuro

- Reformular la implementación simulada del encriptador en seL4 y posteriormente implementarlo en hardware.
- Adquirir conceptos de hacking para realimentar el diseño de la solución.
- Continuar con la documentación del proyecto.

¡Muchas gracias!  
¿Preguntas?