

25 de febrero de 2025

2025-02-11

25 de febrero de 2025

1

Introducción

2

Revisión bibliográfica

3

Desarrollo

4

Conclusiones

1

Introducción

2

Revisión bibliográfica

3

Desarrollo

4

Conclusiones

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

Este proyecto surge como una posibilidad de abordar una solución de encriptación de redes de datos con un enfoque novedoso como es la segmentación virtual de dominios. Motivados por casos como el de Crypto AG, una empresa proveedora de equipos de cifrado cuya neutralidad es discutible puesto que entre 1970 y 2018 fue, en secreto, propiedad de entidades gubernamentales, es que se plantea la necesidad de contar con una solución propia, cuyo desarrollo y mantenimiento no dependa de terceros y que pueda ser auditada.

Plan de trabajo

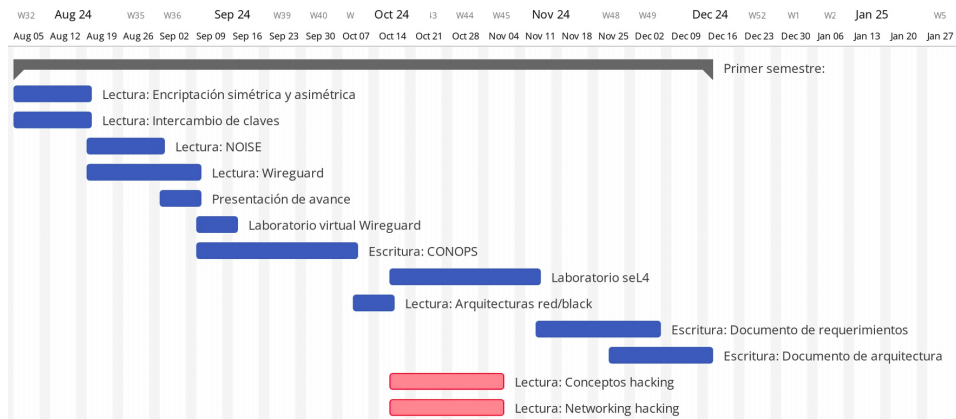


Figura 1: Plan de trabajo del primer semestre de proyecto.

2025-02-11

Sistema de comunicaciones seguras con segmentación virtual de dominios

Introducción

Plan de trabajo



Quiero presentar antes que nada lo que fue el primer paso en este proyecto, que fue realizar el plan de trabajo del semestre. Esto me permitió mantener una metodología de trabajo ordenada en lo que es el proyecto.

Algunas tareas involucraron la lectura como introducción a los conceptos necesarios para comprender el fin del proyecto y otras que permitieron aprender de forma práctica sobre las tecnologías a utilizar. También hay cierta documentación pensada como entregables que consideramos importante para enmarcar la propuesta de solución.

En azul están marcadas las tareas que ya fueron completadas, en rojo las que quedaron pendientes para el segundo semestre.

4 Conclusiones

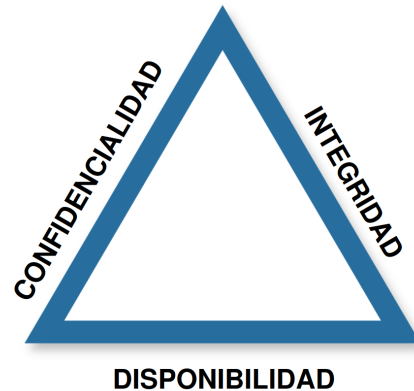


Figura 2: Modelo CID.

2025-02-11

Sistema de comunicaciones seguras con segmentación virtual de dominios

- Revisión bibliográfica
 - Sistemas de seguridad y conceptos de encriptación
 - Triada CID



La triada CID es un modelo que constituye la base para el diseño de sistemas de seguridad. Se compone de estos tres conceptos fundamentales.

La confidencialidad implica garantizar que los datos no sean accesibles por usuarios no autorizados. Los esfuerzos en esta área se centran en los métodos de encriptación.

La integridad asegura la autenticidad de los datos, es decir, que estos estén libres de alteraciones. Aquí se pueden mencionar el uso de hashes o firmas digitales.

La disponibilidad garantiza que los datos estén disponibles cuando se los necesita. Un sistema débil en este aspecto puede ser víctima de ataques de denegación de servicio, por ejemplo. Para esto se refuerza el sistema incluyendo redundancia y algoritmos de detección de ataques.

Encriptación simétrica

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

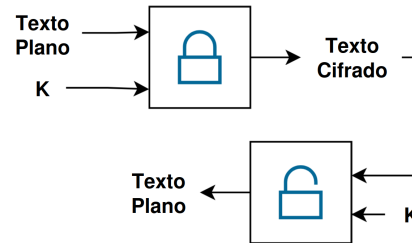


Figura 3: Esquema simplificado de la encriptación simétrica.

2025-02-11

Sistema de comunicaciones seguras con segmentación virtual de dominios

- Revisión bibliográfica
- Sistemas de seguridad y conceptos de encriptación
 - Encriptación simétrica

note text

Encriptación simétrica

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

Figura 3: Esquema simplificado de la encriptación simétrica.

Encriptación asimétrica

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

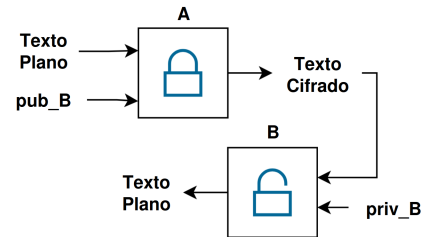


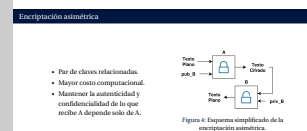
Figura 4: Esquema simplificado de la encriptación asimétrica.

2025-02-11

Sistema de comunicaciones seguras con segmentación virtual de dominios

- Revisión bibliográfica
- Sistemas de seguridad y conceptos de encriptación
 - Encriptación asimétrica

note text



Acuerdo de claves Diffie-Hellmann

- Método para generar una clave compartida sin intercambio directo.
- Mitiga un problema de la encriptación simétrica.
- No resuelve el problema de autenticación.

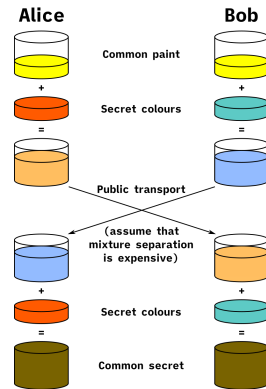


Figura 5: Esquema simplificado del proceso de acuerdo de claves Diffie-Hellmann.

2025-02-11

Sistema de comunicaciones seguras con segmentación virtual de dominios

- Revisión bibliográfica
- Sistemas de seguridad y conceptos de encriptación
- Acuerdo de claves Diffie-Hellmann

Acuerdo de claves Diffie-Hellmann

- Método para generar una clave compartida sin intercambio directo.
- Mitiga un problema de la encriptación simétrica.
- No resuelve el problema de autenticación.

Figura 5: Esquema simplificado del proceso de acuerdo de claves Diffie-Hellmann.

El acuerdo de claves Diffie-Hellmann es un método para generar una clave compartida sobre un canal inseguro sin necesidad de intercambiarla directamente. De esta forma se evita el problema de la encriptación simétrica, que es la necesidad de un canal seguro para el intercambio de claves. Esto permite utilizar el método para generar una clave simétrica, que es un método eficiente para encriptar grandes volúmenes de información.

Este método se basa en la dificultad matemática del problema del logaritmo discreto en números grandes. Por lo general, los protocolos utilizados utilizan claves de 32 a 56 bytes.

Este esquema simplificado con pinturas representa el proceso de acuerdo de claves Diffie-Hellmann. A y B generan claves privadas y públicas, y luego intercambian las claves públicas. A partir de las claves públicas de A y B y sus claves privadas propias, cada uno puede obtener la misma clave como resultado.

Arquitectura red/black

- Lineamientos para identificar y separar correctamente dominios de información.

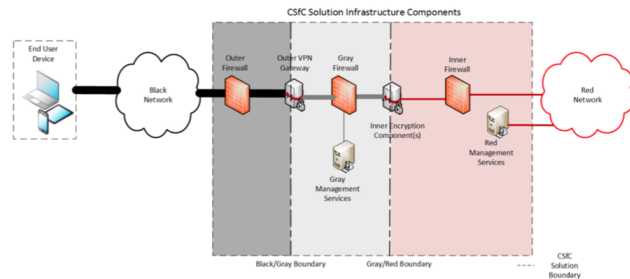


Figura 6: Aquí va otra imagen propia.

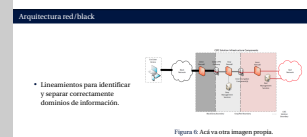
Sistema de comunicaciones seguras con segmentación virtual de dominios

2025-02-11

- Revisión bibliográfica
- Segmentación de dominios
- Arquitectura red/black

El concepto de arquitectura red/black representa la separación de los dominios que contienen información clasificada, o texto plano de aquellos que contienen información encriptada, o texto cifrado. Adoptar esta metodología permite identificar las interfaces entre dominios y diseñar medidas de seguridad adecuadas para aislarlas correctamente.

Esta idea de segregación de interfaces surge de las especificaciones militares TEMPEST, que provee lineamientos en el diseño físico de los equipos para evitar fugas de información a través de emisiones electromagnéticas. Aquí se encuentra el mayor desafío de este proyecto, que es lograr una implementación segura de esta arquitectura en un entorno virtualizado.



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 hipervisor tipo 1.

2025-02-11

Sistema de comunicaciones seguras con segmentación virtual de dominios

- Revisión bibliográfica
 - Segmentación de dominios
 - Hipervisores

Un hipervisor es un software que permite la ejecución y administración de máquinas virtuales sobre un hardware compartido. Gestiona los recursos de hardware y asegura el aislamiento entre las máquinas virtuales fuera de sus interfaces de comunicación.

Un hipervisor tipo 1 se ejecuta directamente sobre el hardware, sin necesidad de un sistema operativo intermediario. Ofrece mayor rendimiento y seguridad a costa de mayor complejidad de implementación. Un ejemplo de este tipo de hipervisor es seL4, el cual describiré más adelante.

Un hipervisor tipo 2 se ejecuta sobre un sistema operativo, es más versátil respecto a su implementación. Un ejemplo de este tipo de hipervisor es VirtualBox.

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 hipervisor tipo 1.

1

Introducción

2

Revisión bibliográfica

3

Desarrollo

Propuesta de solución

Laboratorios virtuales

4

Conclusiones

2025-02-11

1

Introducción

2

Revisión bibliográfica

3

Desarrollo

Propuesta de solución

Laboratorios virtuales

4

Conclusiones

Método ARCADIA

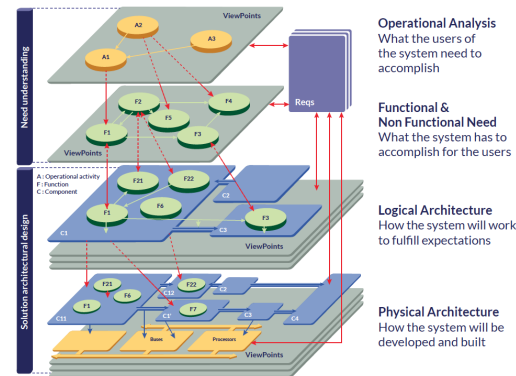
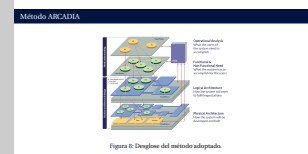


Figura 8: Desglose del método adoptado.

2025-02-11

Sistema de comunicaciones seguras con segmentación virtual de dominios

- Desarrollo
 - Propuesta de solución
 - Método ARCADIA



Quiero presentar brevemente la forma de trabajo que adoptamos para la elaboración de la propuesta de solución. El método ARCADIA es un método de trabajo que se basa en la identificación de los requerimientos del usuario y la definición de los objetivos del sistema.

Se trabajó primero en entender las necesidades del usuario, esto es la capa superior de la figura, y comprende el análisis operacional. Luego definimos los requerimientos del sistema como las funciones que debe realizar el sistema para cumplir estas necesidades. Ya con esto documentado se puede abordar el diseño de la solución.

Si bien ya recorrimos todas etapas a lo largo del semestre, el diseño de la solución no está completo, y es probable que se identifiquen más necesidades, requerimientos a medida que se avance en el proyecto. Esto es más bien un proceso iterativo entre estas etapas, por lo que consideramos importante documentar cada necesidad, requerimiento y decisión de diseño.

Análisis operacional

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



Figura 9: Concepto de operaciones.

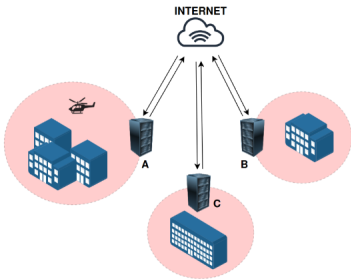


Figura 10: Esquema simplificado del sistema propuesto.

2025-02-11

Sistema de comunicaciones seguras con segmentación virtual de dominios

Desarrollo

Propuesta de solución

Análisis operacional

Análisis operacional

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




Figura 9: Concepto de operaciones.

Figura 10: Esquema simplificado del sistema propuesto.

Partiendo de la primer capa del modelo, planteamos el concepto de operaciones del sistema, que se encuentra documentado y puede accederse a una copia desde este QR.

Esta etapa involucró definir el problema y el contexto en el que se desarrolla la solución. Se manifiestan las suposiciones y limitaciones del sistema propuesto, como puede ser el análisis de encriptación en capa física respecto a hacerlo en capa de red, por ejemplo.

Se documentó también el alcance de la solución, que es la definición de los límites del sistema y las funciones que debe cumplir, sin profundizar en cómo se va a lograr esto.

Este es un esquema simplificado del sistema propuesto. Cada nodo de la red segura se comunica con los demás a través de una conexión a Internet.

Modos de operación

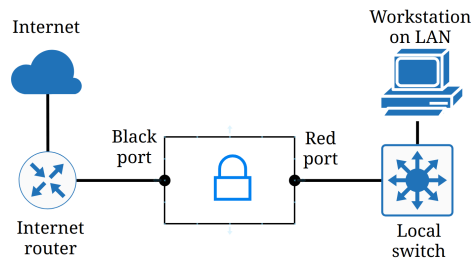


Figura 11: Nodo pequeño.

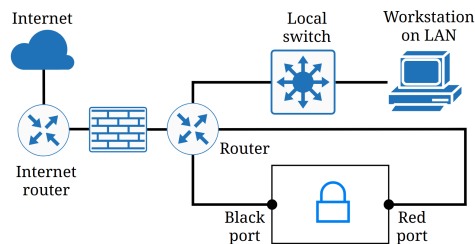
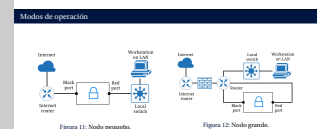


Figura 12: Nodo grande.

2025-02-11

Sistema de comunicaciones seguras con segmentación virtual de dominios

- Desarrollo
- Propuesta de solución
- Modos de operación



Teniendo en cuenta una configuración de hardware genérica donde se implementará la solución se plantea la posibilidad de dos modos de operación. Se considera nodo pequeño a un sitio con poco tráfico, en el que el hardware del encriptador es capaz de direccionar todo el tráfico de la red según su destino sea Internet u otro nodo de la red segura. Si se trata de un nodo grande, puede que el hardware del encriptador no sea capaz de direccionar todo el tráfico. En este caso es necesario un router que cumpla esta función, de manera que solo el tráfico destinado a otro nodo red segura pasa por el encriptador.

Requerimientos

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



Figura 13: Documento de requerimientos.

2025-02-11

Sistema de comunicaciones seguras con segmentación virtual de dominios

- Desarrollo
 - Propuesta de solución
 - Requerimientos

En un nivel menor de abstracción se definieron los requerimientos del sistema, estos son las cosas que el sistema debe hacer para cumplir con las necesidades planteadas en el concepto de operaciones. Como ejemplos están el tiempo asociado a la renovación de claves, la tasa máxima de transferencia entre nodos y las interfaces de administración del encriptador. Estos requerimientos se documentaron y pueden accederse a una copia desde este QR.

Requerimientos

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



Figura 13: Documento de requerimientos.

- Uso de un hipervisor con tres máquinas virtuales independientes.



Figura 14: Arquitectura.

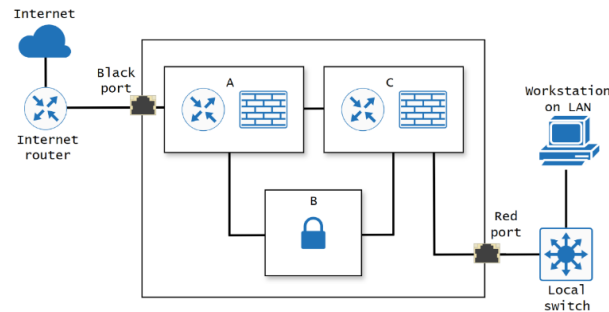


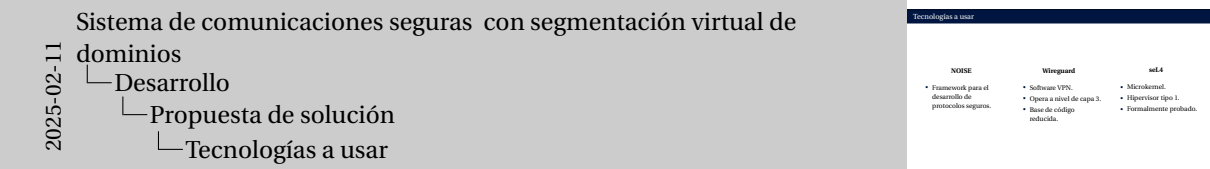
Figura 15: Descripción de la imagen

- Sistema de comunicaciones seguras con segmentación virtual de dominios
 - Desarrollo
 - Propuesta de solución
 - Arquitectura lógica

Como última etapa del método ARCADIA queda proponer una arquitectura lógica para hacer cumplir los requerimientos del sistema.

Se planteó el uso de un hipervisor con tres máquinas virtuales independientes y aislados salvo por ciertas interfaces de comunicación definidas.

NOISE	Wireguard	seL4
<ul style="list-style-type: none">Framework para el desarrollo de protocolos seguros.	<ul style="list-style-type: none">Software VPN.Opera a nivel de capa 3.Base de código reducida.	<ul style="list-style-type: none">Microkernel.Hipervisor tipo 1.Formalmente probado.



Para implementar la propuesta de solución se plantea el uso de tres tecnologías open-source.

- En primer lugar está NOISE, un framework para el desarrollo de protocolos seguros basado en el método Diffie-Hellmann que cuenta con una serie de protocolos formalmente probados, aplicaciones como WhatsApp son un ejemplo de uso de este framework en el cifrado de mensajería.
- Wireguard es un software que permite la creación de VPNs de forma sencilla y segura. Utiliza protocolos derivados del framework NOISE para el establecimiento de conexiones. Opera a nivel de capa 3 del modelo OSI, por lo que un encriptador recibe paquetes IP, los encripta y vuelve a transmitir paquetes IP, cuyo payload son los paquetes originales que luego son descifrados en otro nodo.
- seL4 es un microkernel que se ejecuta directamente sobre hardware con capacidad de funcionar como hipervisor. En este modo, la aislación de máquinas virtuales está formalmente probado, lo cuál es crítico en nuestro sistema. Está diseñado para ser seguro en sistemas críticos sin comprometer el rendimiento.

1	Introducción
2	Revisión bibliográfica
3	Desarrollo Propuesta de solución Laboratorios virtuales
4	Conclusiones

2025-02-11

Sistema de comunicaciones seguras con segmentación virtual de dominios

- Desarrollo
 - Laboratorios virtuales

- Introducción
- Revisión bibliográfica
- Desarrollo
 - Propuesta de solución
 - Laboratorios virtuales
- Conclusiones

Sobre Wireguard y seL4 se implementaron pruebas en un laboratorio virtual para interiorizar conceptos de forma práctica.

Laboratorio virtual - Wireguard

- Fundamentos de redes.
- Utilización de Wireguard.

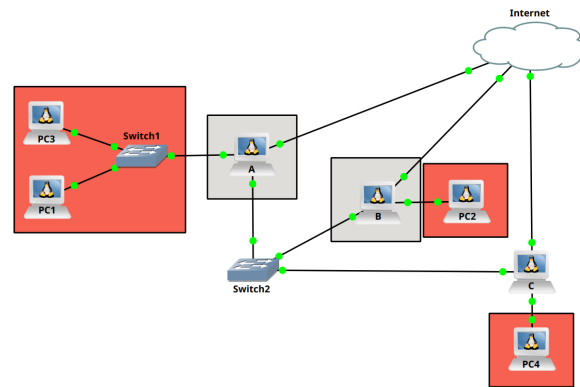


Figura 16: Primeras pruebas con Wireguard en GNS3.

2025-02-11

Sistema de comunicaciones seguras con segmentación virtual de dominios

- Desarrollo
 - Laboratorios virtuales
 - Laboratorio virtual - Wireguard

- Fundamentos de redes.
- Utilización de Wireguard.



Figura 16: Primeras pruebas con Wireguard en GNS3.

Sobre GNS3, un hipervisor de tipo 1 se implementó una red como la de la imagen utilizando máquinas virtuales Linux. Se configuraron dos nodos, A y B, a modo de encriptadores usando Wireguard. Analizando el tráfico de la red se verificó que la comunicación entre los nodos esté encriptada y que el tráfico con destino a Internet se direcciona por fuera del túnel VPN.

Laboratorio virtual - Wireguard

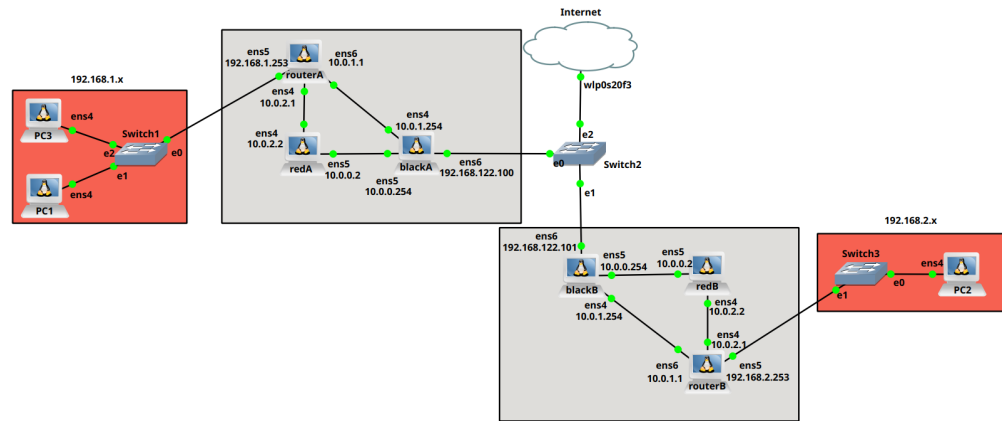


Figura 17: Implementación de la propuesta de solución en GNS3.

2025-02-11

Sistema de comunicaciones seguras con segmentación virtual de dominios

Desarrollo
Laboratorios virtuales
Laboratorio virtual - Wireguard

Laboratorio virtual - Wireguard

Figura 17: Implementación de la propuesta de solución en GNS3.

También se verificó esto sobre una red donde implementamos la arquitectura propuesta para los encriptadores utilizando tres máquinas virtuales independientes. Dos actuando como routers y una como encriptador. En este caso los paquetes con destino otro nodo de la red segura llegan a router", se encriptan en redz salen a Internet a través de la interfaz física de "black". El tráfico que no debe ser encriptado se dirige desde router"directamente a "black".

- Introducción a seL4.
- Introducción al desarrollo de software utilizando contenedores.

Respecto a seL4 se realizaron unos pocos tutoriales introductorios propios de la documentación oficial, que si bien fueron no mucho más que instalar el entorno en mi PC y correr un Hello World, fueron útiles para familiarizarse con el entorno de desarrollo.

Todo esto se implementó usando contenedores Docker, algo muy útil para mantener un entorno de desarrollo limpio y reproducible en otros equipos.

- Introducción a sel4.
- Introducción al desarrollo de software utilizando contenedores

1

Introducción

2

Revisión bibliográfica

3

Desarrollo

4

Conclusiones

- Si

<div>Introducción</div> <div>○○○○</div>	<div>Revisión bibliográfica</div> <div>○○○○○○○○○</div>	<div>Desarrollo</div> <div>○○○○○○○○○○○○○</div>	<div>Conclusiones</div> <div>○○●</div>
<div>Trabajo a futuro</div>			
<div><ul style="list-style-type: none">Mucho.</div>			
<div>Alberto Daniel Lange</div>			

<div>Sistema de comunicaciones seguras con segmentación virtual de dominios</div> <div>2025-02-11</div> <div><div>Conclusiones</div><div>Trabajo a futuro</div></div>	<div>Trabajo a futuro</div> <div><ul style="list-style-type: none">Mucho.</div>
<div>30 / 30</div>	