Universidad Siglo 21

Trabajo Final de Grado. Prototipado Tecnológico

Carrera: Licenciatura en Informática

ArgusNet Suite colaborativa para gestión, monitoreo y auditoría de sistemas firewall en entornos corporativos.

Autor: Pablo M. Coronel

Legajo: VINF12094

Cordoba, junio de 2025

Índice

Resumen

El presente trabajo describe el diseño y desarrollo de ArgusNet, una plataforma web destinada a la gestión colaborativa de reglas de firewall en entornos corporativos. La propuesta surge ante la necesidad concreta de organizar, auditar y optimizar los procesos de configuración de seguridad perimetral, reduciendo errores humanos y favoreciendo la trazabilidad y gobernanza sobre los activos críticos de red. A lo largo del proyecto se llevó a cabo un relevamiento técnico y funcional, seguido del diseño de casos de uso, prototipos visuales, arquitectura técnica, análisis de seguridad, costos y riesgos. ArgusNet integra tecnologías open source, sistemas de autenticación corporativos y mecanismos automatizados de respaldo. Como resultado, se obtuvo una solución versátil, escalable y centrada en las buenas prácticas de administración de infraestructura. Desde una mirada profesional, el desarrollo de ArgusNet permitió aplicar conocimientos avanzados en seguridad informática, administración de proyectos y desarrollo de software. En el plano personal, la experiencia representó un crecimiento significativo, consolidando la capacidad de resolver problemas reales mediante soluciones tecnológicas innovadoras.

Palabras clave: gestión de firewalls, seguridad informática, colaboración, trazabilidad, automatización**.**

Abstract

This project presents the design and development of ArgusNet, a web platform aimed at collaborative firewall rule management in corporate environments. The solution addresses the need to organize, audit, and optimize the configuration of perimeter security, reducing human error and enhancing traceability and governance over critical network assets. The project involved a thorough technical and functional survey, followed by the design of use cases, visual prototypes, system architecture, and an analysis of security, costs, and risks. ArgusNet integrates open-source technologies, corporate authentication systems, and automated backup mechanisms. As a result, the platform provides a scalable, flexible, and governance-oriented solution aligned with best practices in infrastructure administration. Professionally, developing ArgusNet enabled the application of advanced knowledge in cybersecurity, project management, and software development. On a personal level, it was a valuable experience that strengthened the ability to solve real-world problems with innovative technological solutions.

Keywords: firewall management, cybersecurity, collaboration, traceability, automation.

Título

ArgusNet Suite colaborativa para gestión, monitoreo y auditoría de sistemas firewall en entornos corporativos.

Introducción

La seguridad informática es un aspecto crucial para las organizaciones modernas, especialmente ante el constante crecimiento de las amenazas cibernéticas (Stallings, W., 2017). Dentro de este ámbito, los sistemas firewall representan una de las primeras líneas de defensa en las redes empresariales. Sin embargo, la complejidad de su gestión, sumada a la necesidad de colaboración entre distintos equipos técnicos, plantea nuevos desafíos.

Este proyecto tiene como objetivo principal desarrollar ArgusNet, una suite de software colaborativa orientada a la gestión, monitoreo y auditoría de sistemas firewall en entornos corporativos. El nombre Argus hace referencia al gigante de la mitología griega que poseía cien ojos y todo lo veía, simbolizando la capacidad de supervisión constante que se busca replicar en la plataforma. La terminación Net se relaciona directamente con su ámbito de acción: las redes informáticas.

ArgusNet estará pensada para adaptarse tanto a infraestructuras medianas como grandes, integrando herramientas intuitivas y procesos colaborativos que permitan a las organizaciones mantener altos estándares de seguridad informática de manera eficiente y organizada.

Antecedentes

La gestión de redes informáticas y la seguridad cibernética son áreas de crucial importancia en la era digital actual. A medida que las amenazas en línea se diversifican y se intensifican, la necesidad de contar con sistemas de protección robustos y eficientes ha aumentado considerablemente. Los firewalls se posicionan como una de las primeras líneas de defensa, pero su correcta gestión y monitoreo siguen siendo un desafío, especialmente en organizaciones de gran tamaño.

Con más de 20 años de experiencia en el área de IT, he tenido la oportunidad de administrar equipos de firewalls en diversas organizaciones, lo que me ha permitido conocer de cerca las limitaciones y necesidades de las herramientas existentes. Mis certificaciones como CCNA, CCNP, Linux CLA y MKTCNA han sido fundamentales para profundizar en la comprensión de los sistemas de seguridad y redes, y he sido testigo de los desafíos recurrentes que enfrentan los equipos de seguridad en su trabajo diario.

Diversos estudios (Pfleeger, C., 2018; Anderson, R., 2020) destacan que, a pesar de la adopción generalizada de firewalls, muchos equipos de seguridad no cuentan con las herramientas adecuadas para realizar un análisis profundo y colaborativo de sus eventos y configuraciones. Esta carencia de herramientas colaborativas dificulta la resolución de incidentes y la implementación de mejoras continuas en los sistemas de seguridad.

Además, el concepto de trabajo colaborativo en redes ha ganado relevancia, ya que múltiples equipos de seguridad deben interactuar para resolver amenazas de manera eficiente y ágil. La integración de diferentes plataformas de seguridad, la automatización de tareas y la mejora de la comunicación entre equipos técnicos son esenciales para mantener una infraestructura segura.

En este contexto, ArgusNet surge como una respuesta a esta necesidad, ofreciendo una plataforma colaborativa diseñada para optimizar la gestión, monitoreo y auditoría de los sistemas firewall, garantizando un enfoque integral y eficiente para los equipos de seguridad.

Descripción del Área Problemática

En la actualidad, la gestión de firewalls y sistemas de seguridad en redes presenta desafíos significativos, especialmente cuando se requiere una solución colaborativa eficiente entre diversos equipos de trabajo. En organizaciones de tamaño medio y grande, la administración de los firewalls no solo implica la configuración y monitoreo de estos dispositivos, sino también la gestión de alertas, auditorías de seguridad y la resolución de incidentes en tiempo real. Sin embargo, muchas de las herramientas actuales no permiten un análisis profundo ni una interacción fluida entre los equipos técnicos, lo que retrasa la toma de decisiones y complica la mejora continua de los sistemas de protección.

La falta de una plataforma que facilite la colaboración efectiva entre equipos de seguridad, y que centralice la gestión de eventos y configuraciones de firewall, contribuye a

una mayor exposición a riesgos. Esta situación se ve reflejada en diversas empresas y organizaciones que enfrentan problemas similares, desde la detección tardía de amenazas hasta la incapacidad de realizar auditorías de seguridad de manera eficiente.

ArgusNet propone abordar esta problemática mediante el desarrollo de una plataforma colaborativa que permita a los equipos de seguridad gestionar, monitorear y auditar los firewalls de manera conjunta, centralizada y eficiente. Esta solución facilitará la detección temprana de amenazas, mejorará la comunicación entre los equipos y optimizará el tiempo de respuesta ante incidentes, promoviendo una mayor seguridad en las infraestructuras de red.

Justificación

El constante aumento de ciberamenazas y la creciente complejidad de las infraestructuras tecnológicas en las organizaciones hacen que la gestión de firewalls sea una de las áreas más críticas en la seguridad informática. Sin embargo, muchas empresas siguen enfrentando desafíos significativos en la administración eficiente de estos sistemas debido a la falta de herramientas colaborativas que permitan una gestión centralizada, en tiempo real, y que sean aplicables a diferentes marcas de firewalls.

Durante mis más de 20 años de experiencia en el ámbito de IT, especialmente en la administración de firewalls y con certificaciones como CCNA, CCNP, Linux CLA y MKTCNA, he observado cómo la falta de una plataforma integrada y adaptada a diversas marcas de firewall genera demoras en la resolución de incidentes y dificulta la coordinación entre los diferentes equipos de seguridad. En el mercado actual, las soluciones existentes están diseñadas generalmente para marcas específicas de firewalls, lo que limita su aplicabilidad a entornos más heterogéneos y crea una barrera para la integración de sistemas múltiples. Esta falta de una herramienta flexible y generalista ha sido una de las motivaciones principales para el desarrollo de ArgusNet, que busca llenar este vacío al ofrecer una solución que permita la administración eficiente y colaborativa de firewalls, independientemente de la marca.

El proyecto tiene como objetivo no solo optimizar la gestión y el monitoreo de firewalls, sino también mejorar la respuesta ante incidentes, reduciendo significativamente

los tiempos de resolución y promoviendo una mayor colaboración entre los equipos técnicos. Esta capacidad de trabajo en equipo y la centralización de información son esenciales para fortalecer la seguridad de las redes, permitiendo una detección temprana de amenazas y mitigando riesgos que podrían tener un impacto grave en la infraestructura tecnológica de la organización.

Además, la relevancia de este proyecto se extiende especialmente a las empresas que gestionan infraestructuras críticas o datos sensibles. Una gestión eficiente y colaborativa de los firewalls es esencial para proteger estos entornos contra las amenazas cibernéticas, que evolucionan constantemente y exigen respuestas rápidas y precisas.

Basicamente ArgusNet no solo responde a una necesidad técnica en la gestión de firewalls, sino que también ofrece una innovación en los procesos de trabajo colaborativo en seguridad informática. Al brindar una plataforma adaptada a múltiples marcas y modelos de firewall, este proyecto contribuye a una mejor protección, mejora la eficiencia operativa y facilita una gestión proactiva de las amenazas cibernéticas en las infraestructuras tecnológicas de las organizaciones.

Objetivo General del Proyecto

Desarrollar ArgusNet, una plataforma colaborativa e integrada para la gestión de firewalls, que permita a las organizaciones administrar sus sistemas de seguridad de manera centralizada y en tiempo real, adaptándose a diferentes marcas de firewall. Esta herramienta busca optimizar los tiempos de respuesta ante incidentes, mejorar la coordinación entre los equipos de seguridad y fortalecer la protección de las redes empresariales, contribuyendo a una mayor eficiencia operativa y seguridad en la infraestructura tecnológica.

Objetivos Específicos del Proyecto

- Desarrollar una plataforma colaborativa para la gestión centralizada de firewalls de distintas marcas y modelos, permitiendo la administración unificada de reglas y configuraciones.

- Implementar un generador de dashboards gráficos que permita visualizar en tiempo real información crítica como: cantidad de usuarios VPN conectados, intentos de login externos, ancho de banda utilizado en enlaces WAN y LAN, y métricas de tráfico general.

- Incorporar funcionalidades de geolocalización para el análisis de tráfico entrante y para la creación de reglas de bloqueo específicas por regiones geográficas.

- Diseñar un módulo de gestión y almacenamiento de logs y eventos en servidores de bases de datos, posibilitando la generación de estadísticas avanzadas y la automatización de acciones preventivas.

- Integrar herramientas de escaneo de vulnerabilidades internas, con alertas tempranas y recomendaciones automáticas de remediación.

- Desarrollar un sistema de detección y bloqueo automático de direcciones IP asociadas a actividades maliciosas, como distribución de ransomware o malware.

- Implementar funcionalidades de monitoreo y bloqueo de correos electrónicos provenientes de dominios incluidos en listas negras (RBLs) o catalogados como emisores de spam, fortaleciendo la protección de las comunicaciones corporativas.

Marco Teórico Referencial

La gestión de la seguridad perimetral mediante firewalls es un componente fundamental en la protección de los activos de información de las organizaciones. Según Stallings (2019), los firewalls representan la primera línea de defensa al controlar el tráfico que entra y sale de una red, basándose en políticas de seguridad establecidas. Sin embargo, el crecimiento en complejidad de las infraestructuras de red y la evolución de las amenazas cibernéticas han evidenciado la necesidad de soluciones que permitan una administración centralizada, ágil y colaborativa de estos dispositivos.

Diversos estudios destacan que una respuesta rápida ante incidentes de seguridad puede reducir significativamente el impacto de los ataques (SANS Institute, 2020). Para lograrlo, las organizaciones deben contar con herramientas que faciliten la detección temprana de anomalías y la coordinación efectiva entre los equipos técnicos. En este sentido, las Tecnologías de la Información y la Comunicación (TIC) juegan un rol clave, ofreciendo plataformas colaborativas que integran monitoreo, alertas, gestión de logs, visualización de métricas y mecanismos de respuesta automatizada.

La tendencia actual en ciberseguridad apunta hacia la centralización de la información y la automatización de acciones correctivas, empleando paneles de control (dashboards) y análisis de datos (datamining) para mejorar la toma de decisiones (ENISA, 2022). También se considera fundamental el uso de bases de datos para el almacenamiento histórico de eventos de seguridad, lo que permite realizar auditorías, identificar patrones de ataque y cumplir con normativas de cumplimiento como ISO/IEC 27001.

La propuesta de ArgusNet se sustenta en estas premisas, integrando buenas prácticas de gestión de seguridad de redes, automatización de acciones de mitigación y trabajo colaborativo, buscando fortalecer la capacidad de respuesta ante incidentes en entornos de múltiples marcas de firewalls, donde tradicionalmente no existen herramientas unificadas.

Para el desarrollo de este proyecto se adoptará la metodología ágil Scrum, debido a su flexibilidad, enfoque incremental e iterativo, y su orientación a la obtención de entregables funcionales en cortos períodos de tiempo (sprints). Esta metodología permitirá realizar entregas parciales del sistema para recibir retroalimentación temprana y ajustar el desarrollo a las necesidades reales detectadas en cada etapa.

Desde el punto de vista técnico, el proyecto combinará diversas tecnologías:

- Lenguajes de programación: HTML5 y PHP para el desarrollo de la interfaz web.
- Base de datos: MySQL para almacenamiento de registros, configuraciones, métricas y logs.

- **Herramientas de integración:**
  - Logstash, Elasticsearch y Kibana (pila ELK) para la recolección, procesamiento, búsqueda y visualización gráfica de datos de tráfico, eventos e incidentes.
  - Snort como sistema de detección de intrusiones (IDS) para monitoreo activo de amenazas.
- **Frameworks y librerías de front-end:**
  - Bootstrap para el diseño responsivo de las interfaces y componentes visuales prediseñados.
  - Chart.js para la creación de gráficos dinámicos e interactivos dentro de los tableros.
  - DataTables para el manejo de tablas dinámicas y búsqueda avanzada de eventos y registros.
  - Leaflet.js para integrar mapas de geolocalización de tráfico y eventos de seguridad.
- **Frameworks y librerías back-end:**
  - Se evaluará la utilización de librerías de PHP como PHPMailer para gestión de alertas por correo electrónico en caso de incidentes.

Para el relevamiento de requerimientos y validación de necesidades, se tomará como entorno de estudio el puesto actual de Coordinador de IT en la empresa Geex, donde se gestionan firewalls Cisco ASA (modelos 5520, 5515-X y 5516-X) y servidores Linux con configuraciones de firewall basadas en iptables. La experiencia diaria en este entorno permitirá relevar datos reales sobre las dificultades de administración, monitoreo y respuesta a incidentes de seguridad en infraestructuras mixtas.

La recolección de datos se realizará mediante:

- Observación directa de las operaciones de gestión de firewalls en producción.
- Entrevistas informales y encuestas a técnicos de soporte y administradores de red.
- Análisis de incidentes y reportes de seguridad históricos.

También, se realizará un breve estado del arte considerando las herramientas existentes en el mercado, concluyendo que si bien hay soluciones para la administración de firewalls, estas suelen ser específicas para una marca o familia de productos, sin existir una herramienta versátil y abierta que integre gestión, monitoreo, detección de incidentes y generación de acciones para múltiples plataformas.

Finalmente, se elaborará un diagrama de Gantt detallando las actividades a realizar a lo largo del TFG, desde la recolección de datos, diseño, implementación, pruebas, hasta la entrega final del proyecto.

Cronograma de Tareas

Nº	Actividad	Fecha de Inicio	Fecha de Fin	Duración	Responsable
1	Relevamiento del entorno actual (Geex, firewalls y servidores Linux)	1/5/2025	7/5/2025	1 semana	Pablo
2	Definición de requisitos funcionales y técnicos del proyecto	8/5/2025	10/5/2025	3 días	Pablo
3	Análisis de herramientas y librerías a integrar (Bootstrap, ELK, Snort, Chart.js)	8/5/2025	12/5/2025	5 días	Pablo
4	Diseño preliminar de arquitectura de solución	13/5/2025	17/5/2025	5 días	Pablo
5	Configuración de ambiente de desarrollo (servidores, base de datos, etc.)	18/5/2025	21/5/2025	4 días	Pablo
6	Desarrollo de prototipo de dashboard (HTML5, PHP, Bootstrap)	22/5/2025	4/6/2025	2 semanas	Pablo
7	Integración de Logstash y Elasticsearch para captura de logs	5/6/2025	11/6/2025	1 semana	Pablo
8	Desarrollo de funciones de geolocalización y bloqueo por IP/Dominio	12/6/2025	18/6/2025	1 semana	Pablo
9	Implementación de sistema de alertas y acciones automáticas	19/6/2025	25/6/2025	1 semana	Pablo
10	Testeo de funcionalidades	26/6/2025	2/7/2025	1 semana	Pablo
11	Ajustes finales y optimización	3/7/2025	7/7/2025	3 días	Pablo
12	Documentación del sistema	8/7/2025	12/7/2025	5 días	Pablo
13	Presentación final y entrega	13/7/2025	15/7/2025	3 días	Pablo

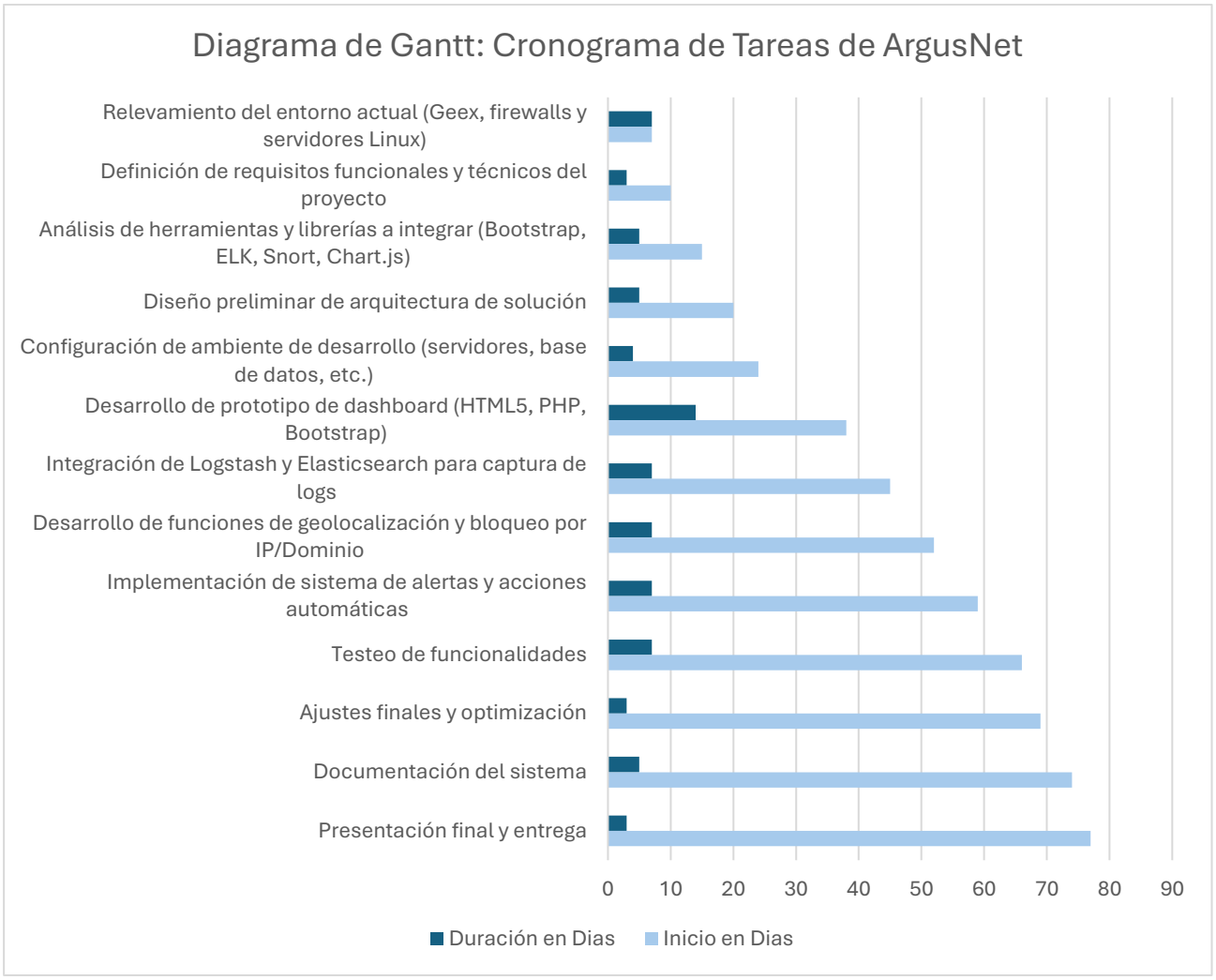


Diagrama de Gantt: Cronograma de Tareas de ArgusNet
Relevamiento del entorno actual (Geex, firewalls y servidores Linux)
Definición de requisitos funcionales y técnicos del proyecto
Análisis de herramientas y librerías a integrar (Bootstrap, ELK, Snort, Chart.js)
Diseño preliminar de arquitectura de solución
Configuración de ambiente de desarrollo (servidores, base de datos, etc.)
Desarrollo de prototipo de dashboard (HTML5, PHP, Bootstrap)
Integración de Logstash y Elasticsearch para captura de logs
Desarrollo de funciones de geolocalización y bloqueo por IP/Dominio
Implementación de sistema de alertas y acciones automáticas
Testeo de funcionalidades
Ajustes finales y optimización
Documentación del sistema
Presentación final y entrega
0
10
20
30
40
50
60
70
80
90
Duración en Dias
Inicio en Dias

Relevamiento

Relevamiento Estructural

El proyecto se desarrolla sobre una organización real: Geex, ubicada en Córdoba, Argentina, en Avenida Colón 4450.
Geex es una empresa surgida de Continuum Global, especializada en ofrecer soluciones de Customer Service.

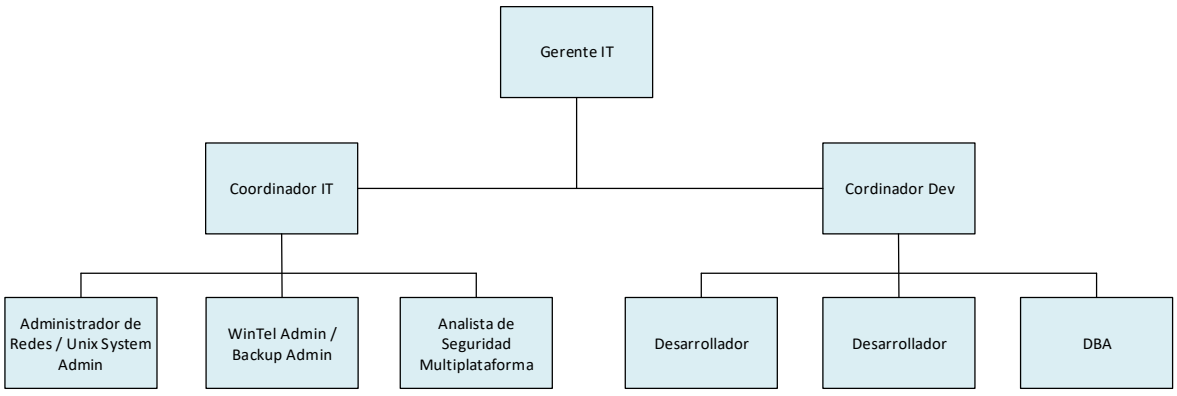
Respecto a la infraestructura tecnológica, la organización cuenta con una topología de red en estrella, conectada mediante gateways Cisco ASA (modelos 5520, 5515X y 5516X).
Los servidores principales utilizan sistemas operativos Linux, protegidos con firewalls activos mediante Iptables.

Actualmente, Geex no posee sucursales adicionales; toda su infraestructura está centralizada en su sede principal.

Relevamiento Funcional

Roles y Áreas Involucradas

Organigrama del Area de Tecnología y Sistemas



Los principales roles involucrados en el proyecto son:

- Coordinador IT: supervisa la infraestructura tecnológica y la seguridad de la red y sistemas.
- Administrador de Redes: gestiona la configuración, mantenimiento y seguridad de dispositivos de red.
- Analista de Seguridad Informática: realiza auditorías de seguridad, gestiona vulnerabilidades y coordina la respuesta ante incidentes.
- Mesa de Monitoreo: realiza el monitoreo en tiempo real de alertas de seguridad.

Procesos Intervinientes

Proceso: Gestión de la Seguridad de la Red

Roles:

- Coordinador IT
- Administrador de Redes
- Analista de Seguridad Informática

Pasos:

1. El Administrador de Redes implementa las configuraciones de seguridad.
2. El Analista de Seguridad realiza escaneos de vulnerabilidades periódicos.
3. El Coordinador IT supervisa los informes y define medidas correctivas.
4. En caso de incidentes, se activa el protocolo de respuesta (aislamiento de dispositivos y notificación).

Proceso: Respuesta ante Incidentes de Seguridad

Roles:

- Analista de Seguridad Informática
- Coordinador IT
- Administrador de Redes
- Mesa de Monitoreo

Pasos:

1. La Mesa de Monitoreo genera alertas de seguridad.
2. El Analista de Seguridad analiza la alerta y verifica brechas.
3. Se activa el plan de respuesta ante incidentes.
4. El Administrador de Redes aísla los sistemas comprometidos.
5. El Coordinador IT supervisa y asegura la correcta recuperación de los sistemas.

Proceso: Gestión de Configuración y Best Practices

Roles:

- Administrador de Redes
- Analista de Seguridad Informática

Pasos:

1. El Administrador configura dispositivos siguiendo las mejores prácticas.
2. El Analista audita y verifica las configuraciones de seguridad.
3. Se ajustan o modifican las configuraciones si es necesario para mantener la seguridad.

Relevamiento de Documentación

Los documentos principales relevados son:

1. Informes de escaneos de vulnerabilidades: detección de riesgos en la infraestructura.
2. Protocolos de respuesta a incidentes: procedimientos ante incidentes de seguridad.
3. Documentación de configuraciones de dispositivos de red: prácticas recomendadas y configuraciones validadas.

Metodología utilizada para la obtención de la documentación:

- Observación directa de la gestión de firewalls en producción.
- Entrevistas informales y encuestas a técnicos de soporte y administradores de red.
- Análisis de incidentes y reportes históricos de seguridad.

Estos documentos serán incluidos como anexos para mayor detalle.

Anexos

Anexo I: Informe de Escaneo de Vulnerabilidades

Fecha: 15 de abril de 2025
Herramienta utilizada: OpenVAS
Alcance: Dispositivos Cisco ASA 5520, 5515X, 5516X y servidores Linux internos.

Resumen de Resultados:

- Vulnerabilidad crítica detectada en firmware de ASA 5515X (recomendación: actualización inmediata).
- Servicios SSH detectados en servidores sin autenticación por clave pública (recomendación: endurecimiento de configuración).
- Puertos abiertos innecesarios en red interna (recomendación: cierre de puertos no utilizados).

Anexo II: Protocolo de Respuesta ante Incidentes

Nombre del Documento: Protocolo de Respuesta a Incidentes de Seguridad – Geex S.A.

Versión: 1.2

Responsable: Analista de Seguridad Informática.

Pasos principales:

1. Recepción de alerta de incidente.
2. Verificación inicial y clasificación del incidente.
3. Aislamiento del dispositivo afectado.
4. Análisis forense preliminar.
5. Comunicación a Coordinador IT y equipo de redes.
6. Implementación de medidas de contención y recuperación.
7. Generación de informe de incidente.

Anexo III: Documentación de Configuración de Dispositivos de Red

Dispositivo: Cisco ASA 5516X

Configuraciones destacadas:

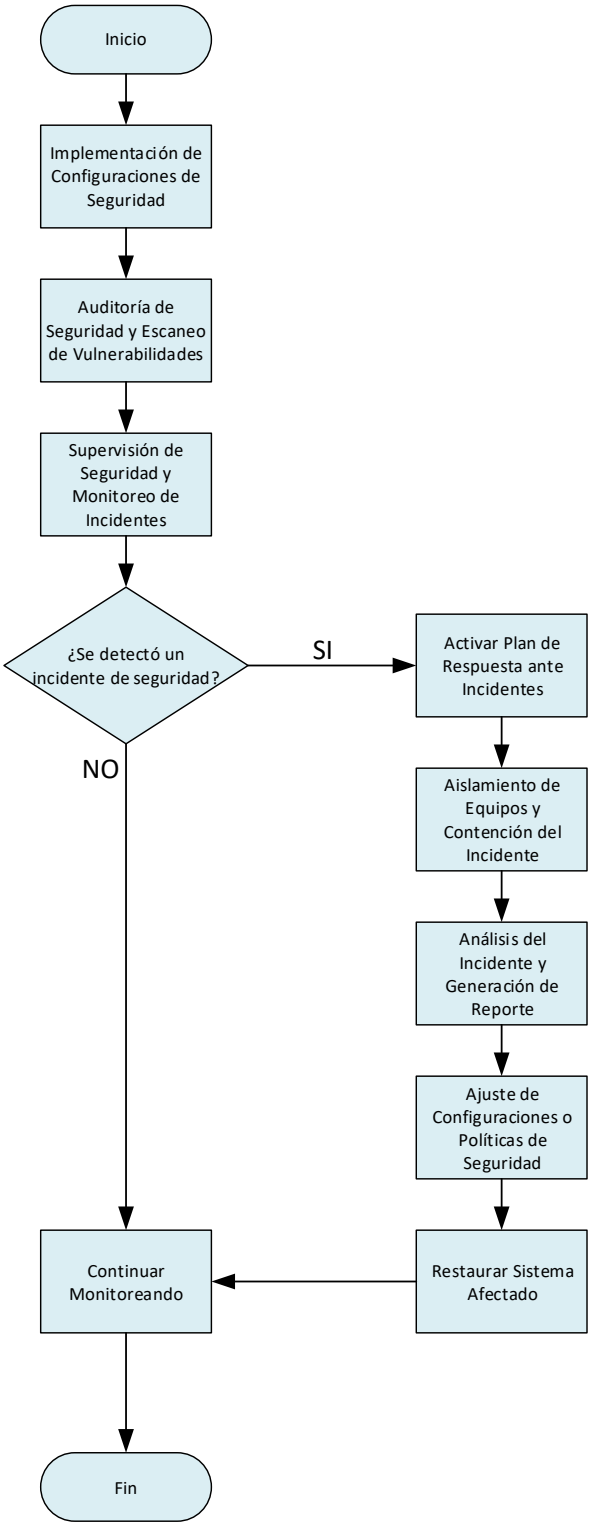
- VPN configurada con autenticación multifactor.
- Políticas de firewall aplicando principio de menor privilegio.
- SNMP deshabilitado para reducir superficie de ataque.
- Actualización de firmware a la versión recomendada por Cisco (versión 9.16).

Observaciones del Analista de Seguridad:

- Configuración cumple con las Best Practices recomendadas por Cisco.
- Se sugiere agregar logging de eventos críticos a SIEM centralizado.

Proceso de Negocio

Proceso Genérico: Gestión Integral de la Seguridad de la Infraestructura



Diagnóstico y propuesta

(Procesos relevados: Gestión de la Seguridad de la Red,

Respuesta ante Incidentes de Seguridad, y Gestión de Configuración y Best Practices)

Problemas detectados	Causas identificadas
Gestión de la Seguridad de la Red – Los reportes de vulnerabilidades llegan con demoras de hasta 48 h, lo que retrasa la aplicación de medidas correctivas.	• Los escaneos de vulnerabilidades se programan manualmente y dependen de la disponibilidad del analista. • No existe un calendario formal aprobado por el Coordinador IT que priorice activos críticos.
Gestión de la Seguridad de la Red – Algunas reglas del firewall se encuentran duplicadas o en conflicto, generando riesgos y sobrecarga de mantenimiento.	• No hay control de versiones centralizado ni revisión cruzada entre Administrador de Redes y Analista de Seguridad. • Cambios urgentes se documentan a posteriori o quedan sin registrar.
Respuesta ante Incidentes de Seguridad – El tiempo promedio de contención (TTC) supera 30 min en horas no laborales.	• La mesa de monitoreo notifica por correo, pero el Analista de Seguridad carece de alertas automáticas por canal crítico (SMS/app). • Los procedimientos de guardia no asignan responsable de primer nivel fuera del horario comercial.
Respuesta ante Incidentes de Seguridad – Después de un incidente, los informes forenses tardan semanas en completarse, dificultando la retroalimentación.	• No existe plantilla estandarizada para el informe post-incidente. • La evidencia se recopila en múltiples formatos y requiere normalización manual.
Gestión de Configuración y Best Practices – Las auditorías detectan discrepancias entre la configuración respaldada y la que corre en producción.	• Los backups de configuración se hacen ad-hoc; no hay tarea automatizada diaria. • Cambios de emergencia se aplican directamente en producción sin repositorio intermedio.
Gestión de Configuración y Best Practices – La documentación de hardening de Linux no refleja el estado real de los servidores.	• Las guías de hardening se actualizan en documentos aislados (Word/pdf) y no en un repositorio central. • Falta un flujo de aprobación que exija actualizar la documentación cada vez que se aplica un cambio.

Propuesta de alto nivel (avance)

1. Automatizar escaneos y alertas
    - Programar tareas recurrentes en la herramienta de vulnerabilidades y enviar notificaciones críticas por canal instantáneo (SMS/app).
2. Control de versiones y repositorio único
    - Adoptar un sistema Git interno para políticas de firewall y scripts de configuración; requerir “merge request” revisado por Analista de Seguridad.
3. Plan de guardias y escalamiento
    - Definir rotación 24×7 con responsable primario + backup y tablero de incidentes con SLA medible (TTC ≤ 10 min).
4. Plantilla estandarizada de informe forense
    - Crear formato único con campos obligatorios; automatizar volcados de logs en ELK para agilizar análisis.
5. Backups automáticos y validación
    - Script diario que exporte configuraciones de ASA y servidores, compare hash con versión previa y alerte diferencias inesperadas.
6. Repositorio central de hardening
    - Migrar documentación a wiki corporativa; cada cambio aprobado en producción debe acompañarse de actualización inmediata del wiki.

Objetivo

Diseñar y desarrollar un prototipo que centralice, automatice y audite en tiempo real la gestión de configuraciones, monitoreo de alertas y respuesta ante incidentes de los firewalls corporativos de Geex.

Límite

Desde la generación de un evento o alerta en cualquiera de los firewalls corporativos de Geex hasta la aplicación y verificación de la acción correctiva aprobada (bloqueo, ajuste de regla o actualización de configuración) y el cierre documentado del incidente en el repositorio central de seguridad.

Alcance del prototipo (procesos comprendidos dentro del límite)

- Detección y registro automático de eventos/alertas de firewall.
- Clasificación y priorización inicial del incidente de seguridad.
- Escalamiento y notificación al equipo responsable.
- Análisis técnico y selección de acción correctiva.
- Aplicación de la acción correctiva en el firewall afectado.
- Verificación de la efectividad de la corrección.
- Documentación y cierre del incidente en el repositorio central.
- Actualización del tablero de métricas y reportes de seguridad asociados.

Requerimientos funcionales de ArgusNet

(acotados al límite "desde la detección del evento hasta la aplicación de la acción correctiva y su registro")

Código	Descripción del requerimiento
RF-01	**Recibir logs y alertas:** el sistema deberá recibir, en tiempo real, eventos provenientes de firewalls Cisco ASA (5520/5515X/5516X), Fortinet FortiGate y Palo Alto Networks, así como de servidores Linux (iptables), mediante syslog seguro, API REST o mecanismos equivalentes.
RF-02	**Correlacionar eventos**: deberá agrupar eventos relacionados para identificar incidentes únicos y asignarles un ID de incidente.
RF-03	**Clasificar severidad**: deberá evaluar cada incidente y asignar un nivel (Crítico, Alto, Medio, Bajo) según reglas configurables por el Analista de Seguridad.
RF-04	**Notificar incidentes críticos**: deberá enviar alertas automáticas (e-mail y panel web) a la Mesa de Monitoreo cuando la severidad sea Crítica o Alta.
RF-05	**Registrar acciones**: deberá permitir que el Administrador de Redes cargue o seleccione la acción correctiva aplicada (aislamiento, bloqueo IP, rollback de configuración, etc.).
RF-06	**Aplicar bloqueos automáticos**: cuando la regla de respuesta esté habilitada, deberá generar y enviar comandos de bloqueo IP/puerto al dispositivo afectado.
RF-07	**Actualizar estado del incidente**: deberá cambiar automáticamente el estado (Abierto → En progreso → Resuelto → Cerrado) y registrar marcas temporales.
RF-08	**Dashboard en tiempo real**: deberá mostrar métricas clave (incidentes abiertos, intentos de login externos, sesiones VPN activas, uso de ancho de banda, geolocalización de IPs bloqueadas).
RF-09	**Búsqueda y filtrado**: deberá permitir al Analista consultar incidentes por rango de fechas, dispositivo, severidad y acción aplicada.
RF-10	**Exportar reportes**: deberá generar informes PDF/CSV con estadísticas semanales y el histórico de incidentes para auditorías.
RF-11	**Gestión de usuarios y roles**: deberá admitir alta, baja y modificación de usuarios con roles predefinidos (Coordinador IT, Administrador Redes, Analista Seguridad, Observador).
RF-12	**Auditoría de cambios**: deberá registrar en un log inmutable cada configuración o acción ejecutada dentro del sistema (usuario, fecha, acción).
RF-13	**Parámetros configurables**: deberá permitir que el Coordinador IT ajuste umbrales de severidad, políticas de bloqueo automático y periodos de retención de logs.

Requerimientos no funcionales (RNF)

Código	Categoría	Requisito de calidad
RNF-01	**Usabilidad**	La interfaz web debe ser **intuitiva** y coherente; los menús y controles deben seguir las guías de diseño de Bootstrap.
RNF-02	**Usabilidad**	El sistema debe incluir **ayuda contextual** y manual en línea accesible desde cualquier pantalla.
RNF-03	**Usabilidad**	Todos los avisos, alertas y errores deben mostrarse en lenguaje claro, indicando acción recomendada.
RNF-04	**Rendimiento**	Para consultas de dashboard o búsqueda de eventos, el **tiempo de respuesta** no debe superar **2 s** para 95 % de las peticiones bajo carga normal (≤ 200 usuarios concurrentes).
RNF-05	**Confiabilidad**	La plataforma debe estar disponible **24 × 7** con un SLA mínimo del **99,5 %** mensual.
RNF-06	**Confiabilidad**	Debe garantizarse la **integridad** de los logs mediante hash SHA-256 y registros inmutables en Elasticsearch.
RNF-07	**Seguridad**	Todo acceso se realizará sobre **HTTPS/TLS 1.3**; las credenciales se almacenarán con hashing bcrypt (≥ 12 rounds).
RNF-08	**Seguridad**	Implementar **autenticación multifactor (MFA)** para usuarios con rol Administrador y Analista de Seguridad.
RNF-09	**Seguridad**	El sistema debe registrar auditoría completa (quién, qué, cuándo, desde dónde) de cada cambio de política.
RNF-10	**Portabilidad**	El backend deberá poder desplegarse en **Linux** (Ubuntu 22.04+) y **Windows Server 2019+** mediante contenedores Docker.
RNF-11	**Compatibilidad**	UI funcional en navegadores soportados: Chrome 110+, Firefox 100+, Edge 110+, Safari 15+.
RNF-12	**Escalabilidad**	Debe permitir la adición horizontal de nodos de ingestión Logstash sin tiempo de inactividad.
RNF-13	**Mantenibilidad**	El código seguirá la guía **PSR-12** (PHP) y estará documentado con PHPDoc; se exigirá cobertura de pruebas ≥ 80 %.
RNF-14	**Portabilidad**	Soporte para ingestión de eventos de **Cisco ASA, Fortinet FortiGate y Palo Alto Networks** vía syslog estándar o API REST, sin requerir agentes propietarios.

Diagrama de Caso de uso General

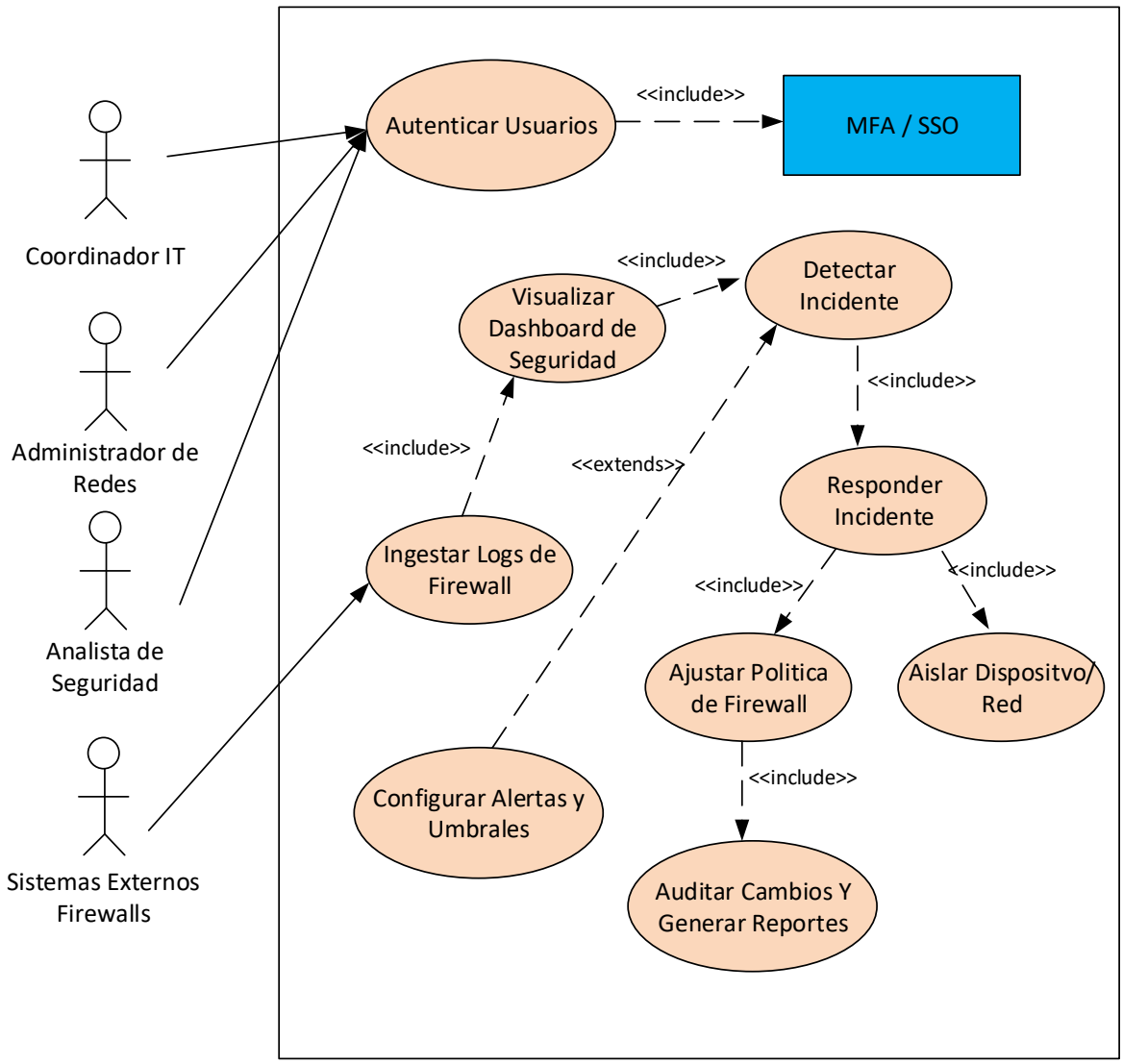
Actores

Actor	Descripción
Coordinador IT	Responsable de la estrategia de ciberseguridad y aprobación de cambios.
Administrador de Redes	Configura dispositivos y políticas; opera el día a día.
Analista de Seguridad	Monitorea eventos, analiza incidentes y ejecuta acciones de respuesta.
Mesa de Monitoreo	Consola 24×7 que recibe alertas y deriva al Analista.
Sistema Externos Firewall	Dispositivos Cisco ASA, Fortinet y Palo Alto que envían logs y aceptan cambios mediante API/syslog.

Casos de Uso

Código	Caso de uso	Actores primarios
CU-01	*Ingestar Logs de Firewall*	Sistema Externos Firewall
CU-02	*Visualizar Dashboard de Seguridad*	Coordinador IT, Administrador de Redes, Analista de Seguridad
CU-03	*Detectar Incidente*	Mesa de Monitoreo, Analista de Seguridad
CU-04	*Responder Incidente*	Analista de Seguridad, Administrador de Redes
CU-05	*Aislar Dispositivo/Red*	Administrador de Redes
CU-06	*Ajustar Política de Firewall*	Administrador de Redes (aprobación: Coordinador IT)
CU-07	*Auditar Cambios y Generar Reportes*	Coordinador IT, Analista de Seguridad
CU-08	*Configurar Alertas y Umbrales*	Analista de Seguridad
CU-09	*Autenticar Usuario*	Todos los actores humanos

Diagrama de Caso de uso General



Casos de Uso

Ficha Caso de un CU-01

Campo	Contenido
ID del requisito	CU-01
Nombre del requisito funcional	Monitorear Incidentes
Versión	1.0 – 22 / 05 / 2025
Objetivos asociados	Detectar y registrar en tiempo real los eventos de seguridad provenientes de múltiples firewalls para iniciar, si corresponde, el proceso de Respuesta ante Incidentes.
Descripción	El sistema ArgusNet recibe continuamente eventos de seguridad (syslog, API, traps) de dispositivos Cisco ASA, Fortinet y Palo Alto. Clasifica la criticidad, genera alertas visuales/sonoras y abre un ticket preliminar con la información esencial. El Analista de Seguridad revisa el tablero en tiempo real, confirma o descarta la alerta y, si procede, deriva al caso CU-02 – Aislar Equipo.
Precondición	1. Los dispositivos de seguridad están configurados para enviar logs/eventos a ArgusNet.
	2. El servicio de ingesta y parsing está operativo.
Secuencia normal	**Paso**
Postcondición	• Alerta registrada y visible en el dashboard.
	• Ticket creado con el estado adecuado (Confirmada / Falsa Alarma).
Curso alternativo	**Paso 3a** – Falla de Parsing: Si el mensaje llega con formato desconocido, se enruta a la cola “No Clasificado” para revisión manual.
	Paso 5a – Analista no disponible: Si pasados 5 min no hay acción, se notifica al Coordinador IT por e-mail / SMS.
Frecuencia esperada	~800 eventos/hora – de los cuales ~5 % generan alerta (≈ 40 ejecuciones del caso CU-01 por hora).
Importancia	Muy importante – es el disparador principal para la respuesta ante incidentes.
Comentarios	• La usabilidad del dashboard se rige por los RNF-01 (Usabilidad) y RNF-02 (Rendimiento).
	• Futuras versiones incluirán analítica predictiva para reducir falsos positivos.

Ficha Caso de un CU-02

Campo	Contenido
ID del requisito	CU-02
Nombre del requisito funcional	Aislar Equipo Comprometido
Versión	1.0 – 22 / 05 / 2025
Objetivos asociados	Contener rápidamente un incidente bloqueando el tráfico del host afectado hasta completar el análisis forense.
Descripción	Ante una alerta confirmada (CU-01), el Analista de Seguridad ordena a ArgusNet que coloque el IP/FQDN involucrado en modo "Cuarentena". El sistema aplica reglas de bloqueo en el firewall correspondiente (Cisco ASA, Fortinet o Palo Alto) y documenta la acción en el ticket del incidente.
Precondición	1. El caso CU-01 está finalizado con estado **Confirmada**.
	2. El Analista tiene privilegios para ejecutar acciones remotas en los firewalls.
Secuencia normal	**Paso**
Postcondición	• Tráfico entrante/saliente del host comprometido bloqueado.
	• Bitácora y ticket actualizados con evidencia de la acción.
Curso alternativo	**Paso 3a** – Error de Conexión: Si el dispositivo no responde, se reintenta 3 veces; de persistir la falla, el sistema crea una tarea para el Administrador de Redes y eleva la prioridad del incidente.
	Paso 4a – Regla ya existente: Si la IP ya estaba en cuarentena, se registra el hecho y se omite la duplicación.
Frecuencia esperada	1–3 veces por día (depende de la cantidad de incidentes confirmados).
Importancia	Muy importante – reduce superficie de ataque y evita propagación interna.
Comentarios	• Se valida contra los RNF-02 (Rendimiento) para aplicar bloqueos en <3 s.
	• La reversión de cuarentena se gestiona en CU-03 – Restaurar Conectividad.

Ficha Caso de un CU-03

Campo	Contenido
ID del requisito	CU-03
Nombre del requisito funcional	Restaurar Conectividad
Versión	1.0 – 22 / 05 / 2025
Objetivos asociados	Rehabilitar un host previamente puesto en cuarentena cuando el análisis forense confirma que está limpio o ha sido re-imaginado.
Descripción	El Analista de Seguridad solicita a ArgusNet quitar las reglas de bloqueo que afectan al host. El sistema revierte la política en el firewall (Cisco ASA, Fortinet o Palo Alto), actualiza el ticket y notifica a los interesados.
Precondición	1. El host se encuentra en estado **Cuarentena aplicada**.
	2. El Coordinador IT o el Analista dispone de un informe de remediación OK.
Secuencia normal	**Paso**
Postcondición	• El tráfico del host vuelve a la política normal.
	• Ticket con evidencia de remediación y cierre documentado.
Curso alternativo	**Paso 3a** – Falla de eliminación: Si la regla no existe o el dispositivo no responde, ArgusNet alerta al Administrador de Redes y mantiene el estado **Cuarentena** hasta resolver.
Frecuencia esperada	Similar a CU-02: 1–3 veces por día.
Importancia	Alta – minimiza downtime y restablece operaciones normales.
Comentarios	• Verifica RNF-02 (Rendimiento) para completarse en <3 s.
	• Solo usuarios con rol “Analista Senior” o superior pueden ejecutar este CU.

Ficha Caso de un CU-04

Campo	Contenido
ID del requisito	CU-04
Nombre del requisito funcional	Generar Dashboard de Seguridad
Versión	1.0 – 22 / 05 / 2025
Objetivos asociados	Proveer visualizaciones en tiempo real de métricas críticas para la toma de decisiones (usuarios VPN, intentos de log-in, BW, geolocalización de amenazas).
Descripción	El Coordinador IT solicita la actualización o creación de un dashboard. ArgusNet recupera datos de Elasticsearch, aplica paneles Kibana prediseñados o genera uno nuevo y lo publica en la consola.
Precondición	1. El usuario posee rol “Coordinador IT” o superior.
	2. Existe conexión activa con la base de datos de logs.
Secuencia normal	**Paso**
Postcondición	Dashboard guardado; URL compartible internamente.
Curso alternativo	**Paso 3a** – Datos incompletos ➜ ArgusNet muestra mensaje de error y sugiere verificaciones de ingesta.
Frecuencia esperada	10–15 ejecuciones por día.
Importancia	Muy alta – insumo principal de decisiones operativas.
Comentarios	Cumple RNF-01 (Usabilidad) y RNF-02 (Respuesta < 2 s con 7 días de datos).

Ficha Caso de un CU-05

Campo	Contenido
ID del requisito	**CU-05**
Nombre del requisito funcional	Registrar Configuración de Dispositivo
Versión	1.0 – 22 / 05 / 2025
Objetivos asociados	Mantener un historial versionado de las configuraciones de firewalls y switches para auditoría y rollback.
Descripción	El Administrador de Redes solicita a ArgusNet capturar la *running-config* del dispositivo seleccionado. La configuración se almacena con un hash de integridad y metadatos (versión, fecha, autor).
Precondición	1. Dispositivo accesible por **SSH** o **API**.
	2. El usuario posee credenciales de backup.
Secuencia normal	**Paso**
Postcondición	Nueva versión de configuración disponible para auditoría y comparación.
Curso alternativo	**Paso 3a – Timeout/Autenticación fallida** → ArgusNet muestra error y sugiere reintento.
Frecuencia esperada	1 – 2 veces por dispositivo al día (tarea programada + manual).
Importancia	Alta – clave para cumplimiento normativo y recuperación rápida.
Comentarios	Relacionado con **RNF-04 (Seguridad)**: almacenamiento cifrado y control de acceso estricto.

Diagrama de Secuencia

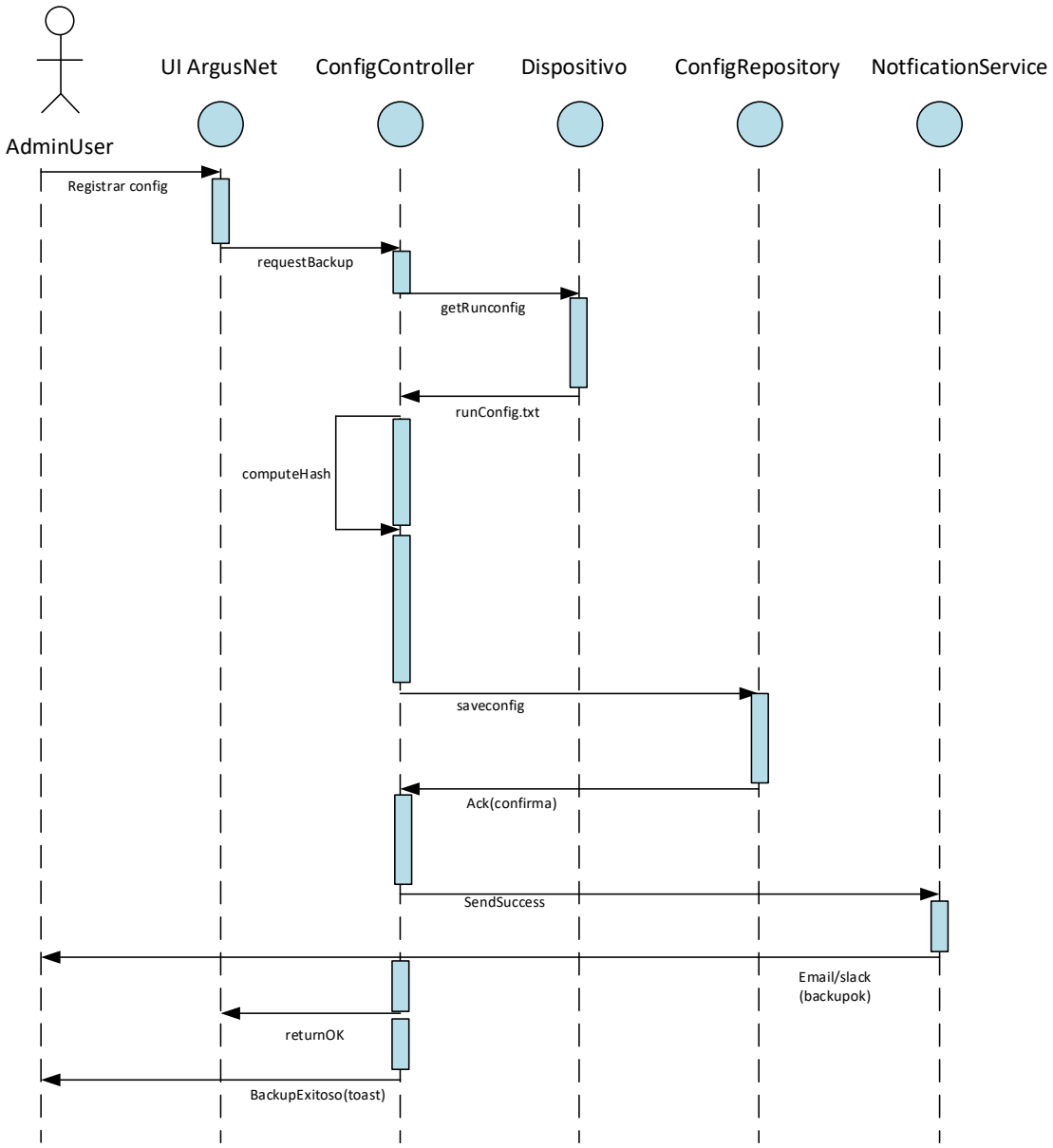


Diagrama de Clase

El Diagrama de Clases de ArgusNet representa la estructura lógica del sistema desde el enfoque orientado a objetos. Define las clases principales, sus atributos, métodos y las relaciones entre ellas, reflejando cómo se modelan los dispositivos, configuraciones, eventos de seguridad, usuarios, notificaciones, reportes y políticas dentro del prototipo. Este diagrama proporciona una visión clara de la arquitectura del sistema y su comportamiento esperado.

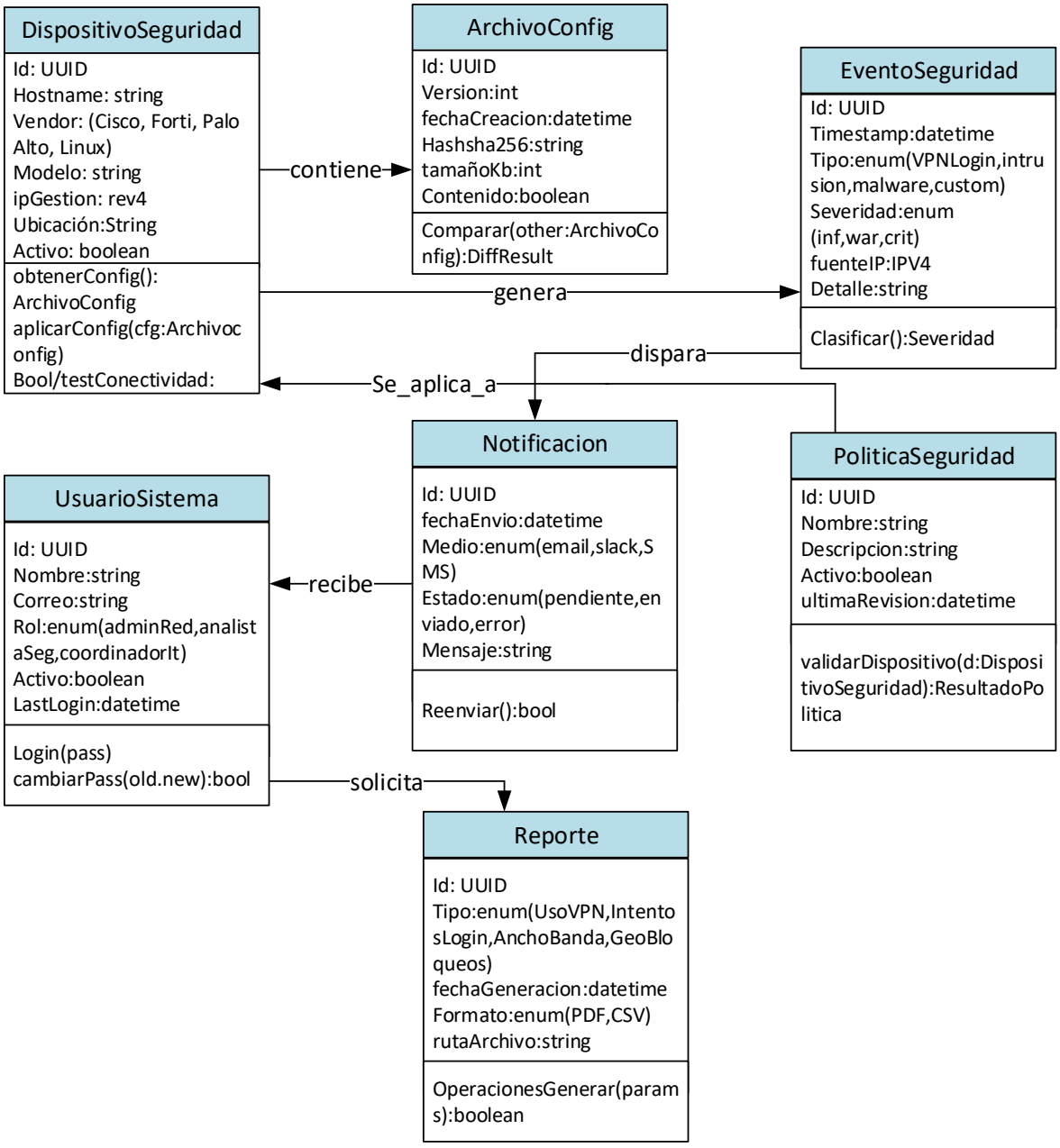


Diagrama Entidad Relacion

El Diagrama Entidad-Relación (DER) de ArgusNet describe las entidades principales del sistema, sus atributos clave y las relaciones entre ellas. Este modelo permite visualizar cómo se organizan y vinculan los datos relacionados con dispositivos de red, configuraciones, eventos de seguridad, usuarios, notificaciones, reportes y políticas, garantizando una estructura eficiente, normalizada y coherente para la base de datos del sistema.

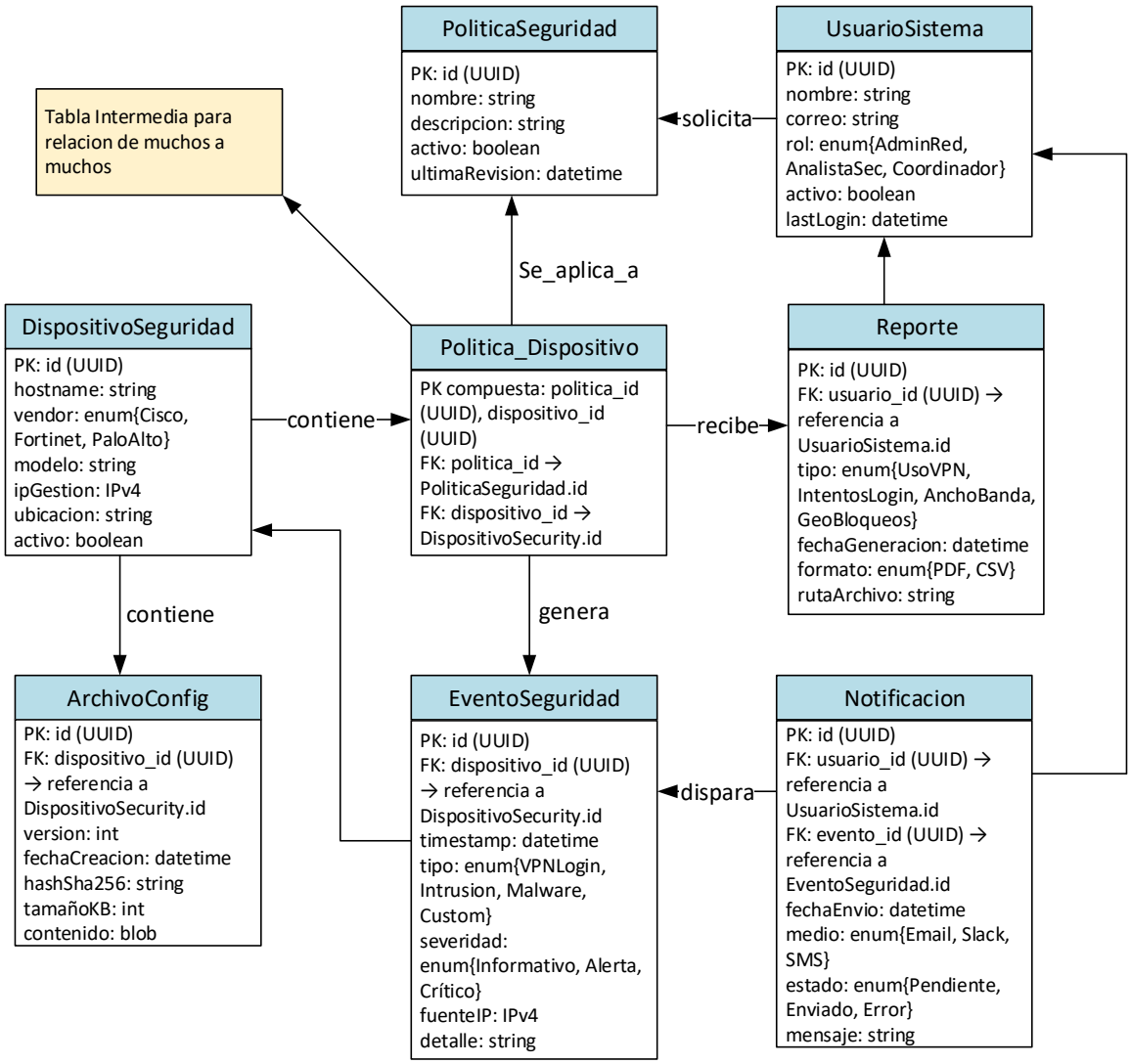
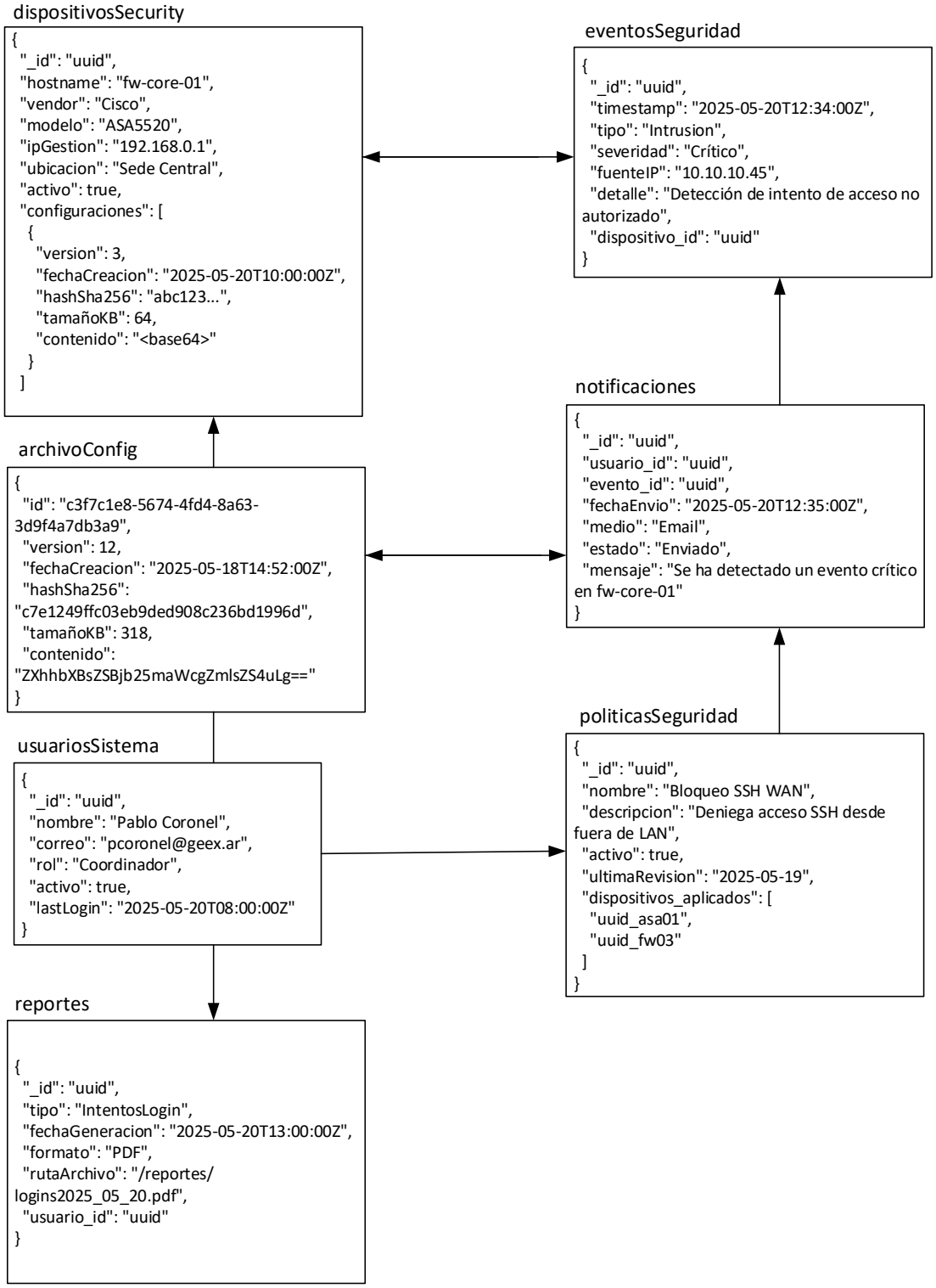


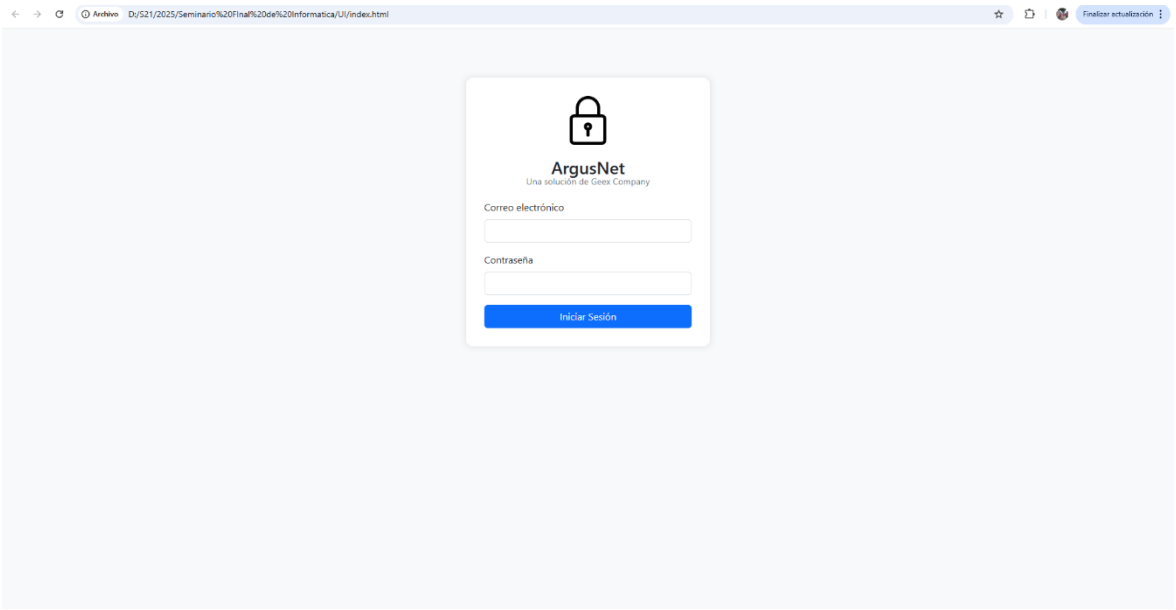
Diagrama NoSql



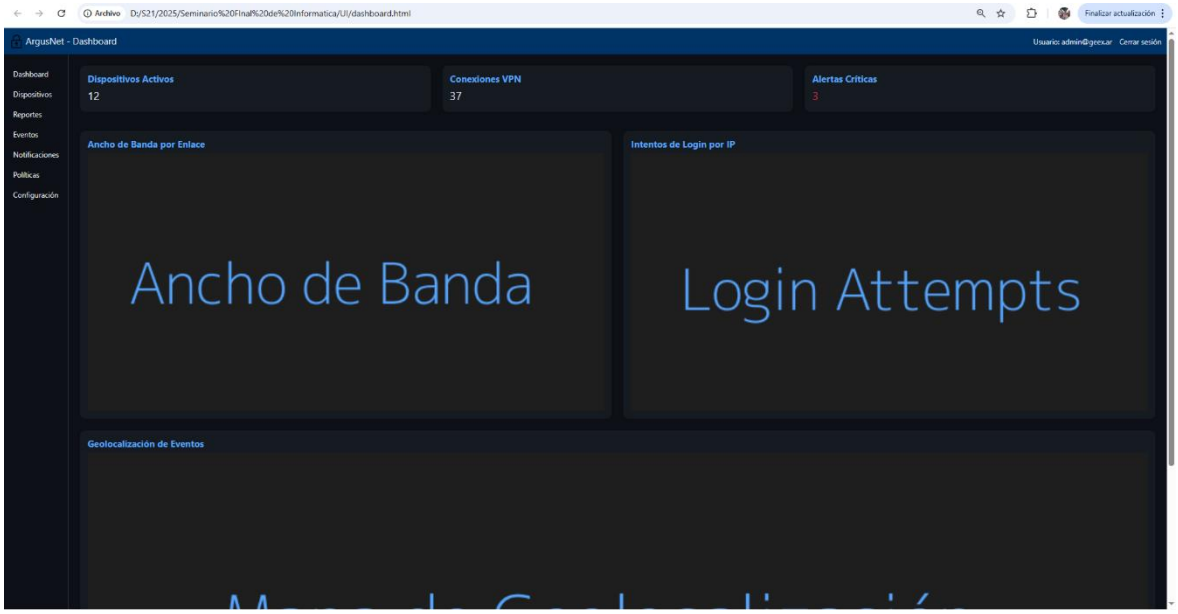
Prototipado de Interfaz Grafica de Aplicación

A fin de representar de manera visual la funcionalidad del sistema ArgusNet, se desarrolló un conjunto de interfaces gráficas prototípicas que simulan el entorno operativo de la plataforma. Estas pantallas permiten recorrer funcionalidades clave como el inicio de sesión, panel principal (dashboard), visualización de reportes, gestión de eventos de seguridad y notificaciones. El diseño adopta una estética profesional con una paleta de colores oscuros, celestes y blancos, priorizando la usabilidad, la legibilidad y la coherencia visual. Las interfaces están desarrolladas con tecnologías web como HTML5, Bootstrap y PHP, y permiten tomar una visión clara de la estructura que tendrá el sistema desde el punto de vista del usuario.

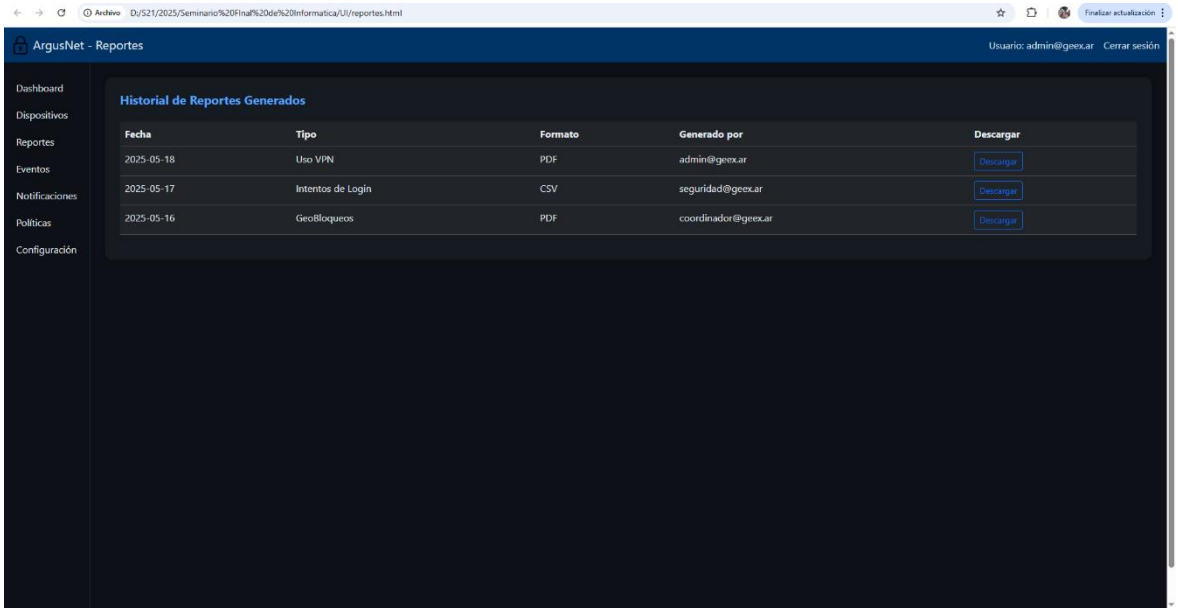
Pantalla de Logueo



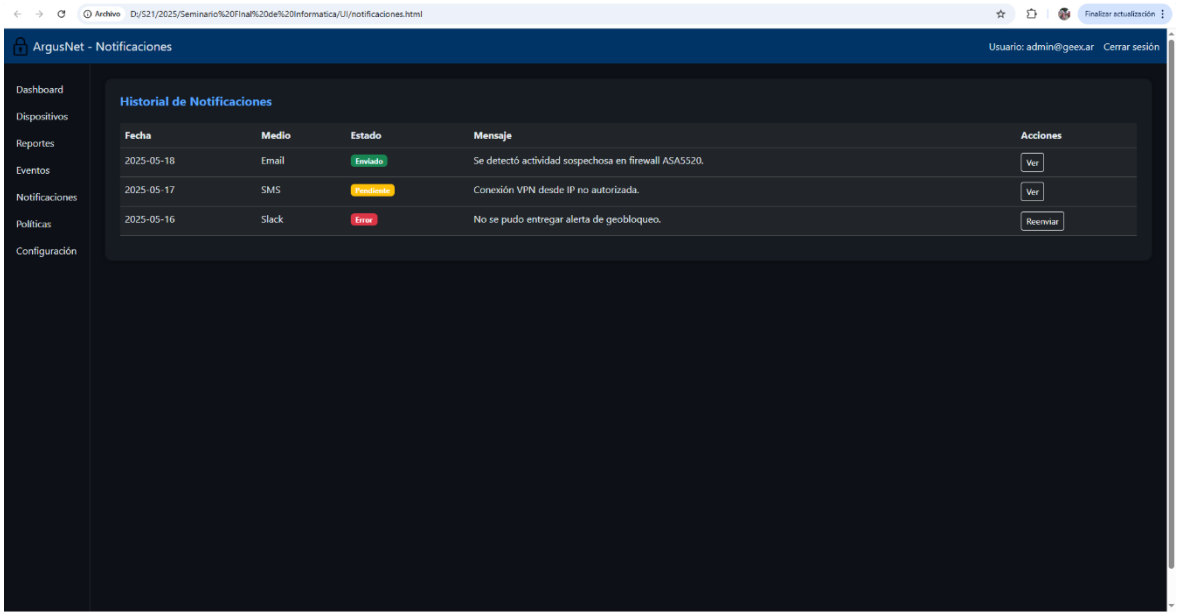
Dashboard



Reportes



Notificaciones



Incidente de Seguridad

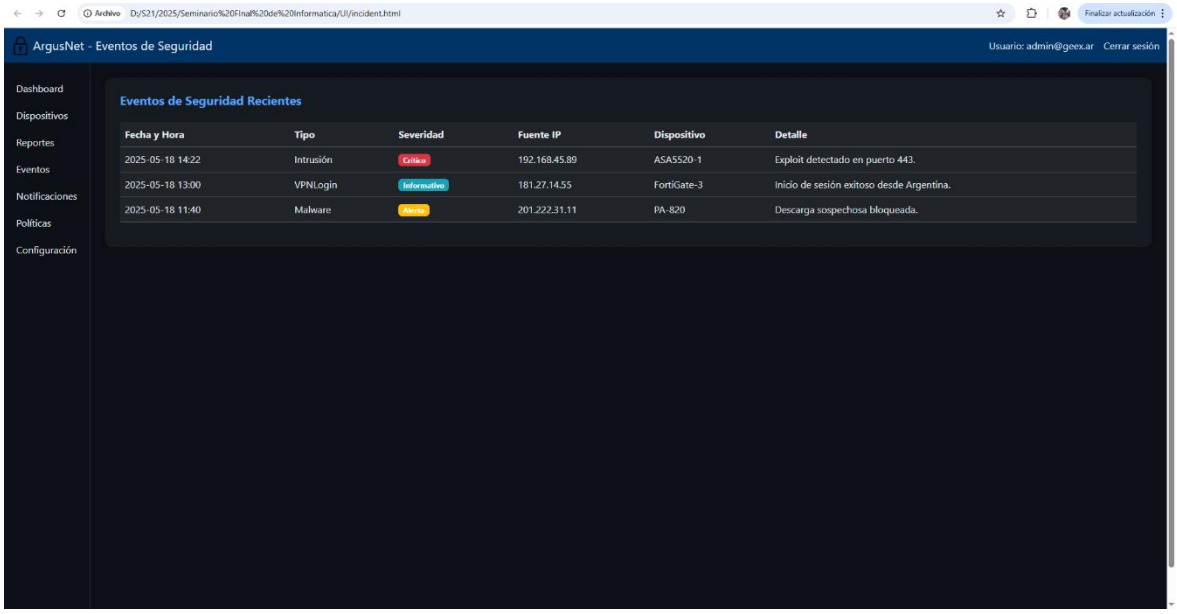


Diagrama de Despliegue

El diagrama de despliegue de ArgusNet ilustra la arquitectura física del sistema, representando los nodos involucrados en su funcionamiento, los componentes lógicos que se ejecutan en ellos y la forma en que interactúan. Se contempla un entorno web donde los usuarios acceden al sistema a través de navegadores, y la aplicación se aloja en servidores distribuidos que procesan la lógica del sistema, gestionan bases de datos relacionales y no relacionales, y reciben eventos de seguridad provenientes de firewalls corporativos. Esta representación permite comprender cómo se distribuyen las cargas, qué tecnologías intervienen y cómo fluye la información dentro del ecosistema de ArgusNet.

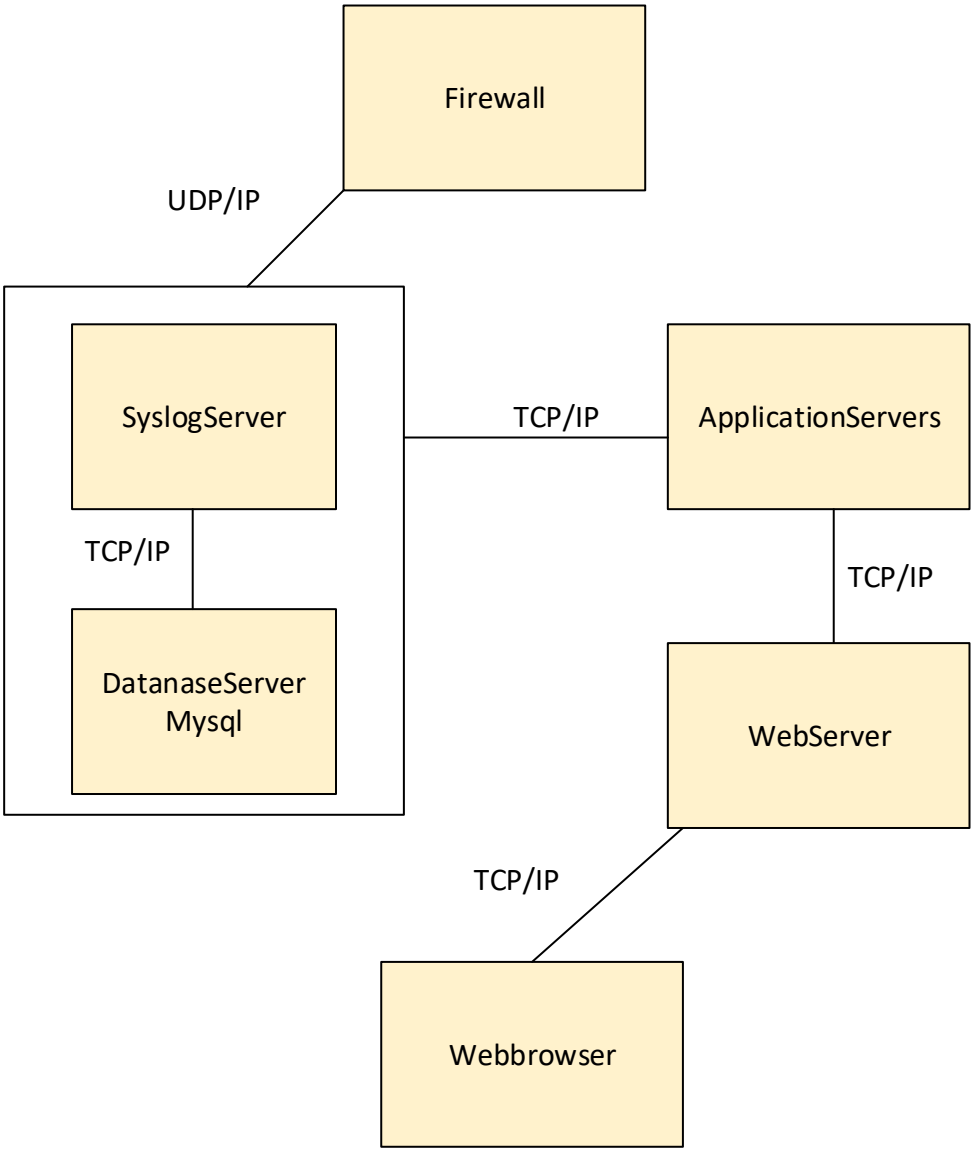
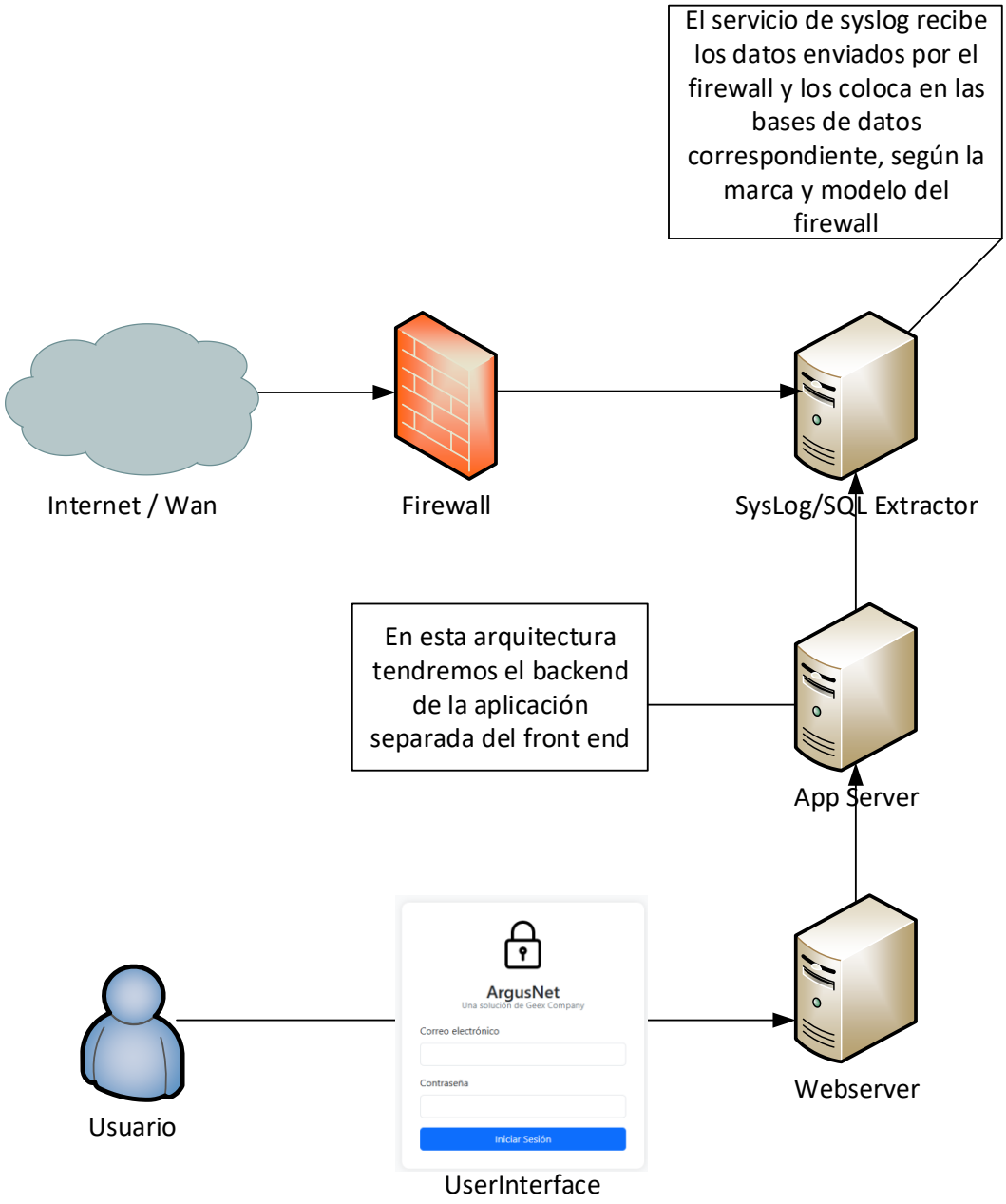


Diagrama de Arquitectura



Seguridad

La seguridad es uno de los pilares fundamentales en el desarrollo de ArgusNet, dado que se trata de una suite destinada a gestionar, monitorear y auditar infraestructuras críticas de firewall en entornos corporativos. Se han definido políticas técnicas y operativas alineadas con buenas prácticas de ciberseguridad y normativas legales aplicables, como la Ley N.º 25.326 de Protección de los Datos Personales y su decreto reglamentario 1558/2001 en la República Argentina. ArgusNet incorpora mecanismos que garantizan la confidencialidad, integridad y disponibilidad de la información gestionada, tanto en tránsito como en reposo.

Acceso a la Aplicación

Para garantizar que solo personal autorizado acceda a la plataforma, ArgusNet implementa un sistema robusto de autenticación y gestión de identidades basado en los siguientes lineamientos:

Integración con Directorio Corporativo

ArgusNet se integra con servicios de directorio como Microsoft Active Directory (AD), permitiendo el uso de credenciales corporativas y facilitando la administración centralizada de usuarios. Esta integración se realiza mediante LDAP seguro (LDAPS) o, en entornos modernos, mediante SSO basado en SAML 2.0 o OpenID Connect.

También se contempla compatibilidad con otros sistemas de autenticación como FreeIPA, Azure AD y autenticadores externos que permitan federación de identidades.

Autenticación Multifactor (MFA)

El sistema obliga a la utilización de un segundo factor de autenticación para todos los usuarios con roles críticos, como "Administrador de Redes" o "Analista de Seguridad". Se permite configurar autenticación vía:

- Microsoft Authenticator
- Google Authenticator
- U2F (como YubiKey)

- Códigos SMS o email, como fallback

Políticas de Contraseña

Para los accesos locales o sin federación, se aplican políticas estrictas:

- Longitud mínima: 10 caracteres
- Al menos una mayúscula, una minúscula, un número y un símbolo
- Caducidad cada 90 días
- Historial de las últimas 5 contraseñas
- Bloqueo tras 5 intentos fallidos durante 15 minutos
- Captcha tras múltiples intentos de autenticación

Gestión de Perfiles y Roles

ArgusNet implementa un modelo de roles basado en privilegios mínimos. Los roles predefinidos incluyen:

- Coordinador IT
- Administrador de Redes
- Analista de Seguridad
- Mesa de Monitoreo
- Observador

Cada rol tiene acceso acotado a funciones específicas, y los privilegios se auditan en cada sesión iniciada.

Trazabilidad

Todos los accesos son registrados y auditados en un log inmutable, almacenado en Elasticsearch con hash SHA256 y firma digital. Esta información está disponible para procesos de auditoría o respuesta ante incidentes.

Política de Respaldo de Información

La integridad y disponibilidad de los datos gestionados por ArgusNet se aseguran mediante una política de respaldo automatizada, flexible y segmentada por tipo de dato, basada en las buenas prácticas del estándar 3-2-1 de respaldos. La estrategia se inspira en herramientas robustas como la utilizada por VMware vCenter Server 7, permitiendo granularidad, portabilidad y múltiples puntos de recuperación.

Tipos de Datos Resguardados

ArgusNet distingue tres niveles de respaldo para mejorar la recuperación ante fallos parciales o totales:

- Configuración del sistema: Incluye archivos de entorno, scripts, y parámetros operativos.
- Base de datos: Copia íntegra de las tablas MySQL que almacenan eventos, configuraciones, reglas y usuarios.
- Datos estadísticos e históricos: Contenidos en Elasticsearch, incluyendo métricas, dashboards y reportes generados.

Cada categoría puede seleccionarse de forma independiente en el sistema de backup.

Métodos y Programación

El sistema de respaldo ofrece opciones programables con periodicidad diaria, semanal o bajo demanda. Los métodos admitidos incluyen:

- Protocolo SCP (Secure Copy) hacia destinos seguros en red.
- Protocolo FTP/SFTP, para respaldos en entornos mixtos o dispositivos NAS.
- HTTP/HTTPS POST, para integración con API REST de servicios en la nube.

La programación se realiza desde una consola web del sistema, permitiendo configurar ventanas horarias (por ejemplo, entre las 02:00 y 04:00 horas AM) y establecer políticas de retención diferenciadas por tipo de dato.

Redundancia y Almacenamiento

Se implementa el modelo 3-2-1, asegurando tres copias de los datos:

- Copia local en disco redundante del servidor (RAID 1 o RAID 5).
- Copia externa vía SCP o FTP hacia un repositorio NAS o servidor fuera del perímetro.
- Copia en la nube, utilizando AWS S3, Azure Blob Storage o Google Cloud Storage.

Además, se permite configurar 2 o más puntos de restauración (restore points), con retención de hasta 60 días, lo cual permite recuperación granular ante cambios accidentales, ataques o corrupción de datos.

Seguridad y Control de Integridad

- Todos los backups son cifrados con GPG y firmados digitalmente.
- Se generan hashes SHA256 para control de integridad tras la copia.
- Un sistema de alertas notifica al Administrador de Redes si el proceso falla.

Intervención Humana

- El Administrador de Redes supervisa el proceso y recibe informes diarios.
- El Coordinador IT valida semanalmente pruebas de restauración aleatoria para garantizar la recuperación efectiva ante un evento.

Análisis de Costos

El desarrollo del sistema ArgusNet, orientado a la gestión colaborativa de firewalls en entornos corporativos, requiere una inversión en recursos humanos, infraestructura tecnológica, servicios y hardware especializado. Este análisis contempla valores de mercado actualizados a junio de 2025, utilizando referencias como el CPCIBA, proveedores oficiales de servicios cloud, y sitios de tecnología en Argentina.

Costos de Recursos Humanos para el Desarrollo

Los siguientes valores son estimaciones basadas en la guía de honorarios profesionales publicada por el Consejo Profesional de Ciencias Informáticas de la Provincia de Buenos Aires (CPCIBA), con actualización a 2025. Se estima un esfuerzo de 3 meses para el desarrollo inicial del MVP de ArgusNet.

Rol	Costo hora (ARS)	Horas estimadas	Subtotal
Líder de Proyecto	$ 28.000	160	$ 4.480.000
Backend Developer (PHP/SQL)	$ 24.500	200	$ 4.900.000
Frontend Developer (HTML/CSS/JS)	$ 23.000	160	$ 3.680.000
Administrador de Base de Datos	$ 22.000	120	$ 2.640.000
Especialista en Seguridad IT	$ 21.000	100	$ 2.100.000
QA/Tester	$ 20.000	80	$ 1.600.000
Total estimado			**$ 19.400.000**

Fuente: CPCIBA – https://www.cpciba.org.ar

Costos Operativos e Infraestructura

El sistema será alojado en un entorno híbrido, utilizando servidores físicos en Geex y servicios cloud externos para backups y disponibilidad redundante.

Servicio	Cantidad	Costo mensual (ARS)	Total (3 meses)	Fuente
Servidor VPS (Cloud – AWS EC2 t3.medium)	1	$ 35.000	$ 105.000	aws.amazon.com

Almacenamiento AWS S3 (100 GB)	1	$ 12.000	$ 36.000	aws.amazon.com
Backup automático Rclone + GPG + SFTP	1	$ 10.000	$ 30.000	Estimación propia
Dominio + SSL Let's Encrypt	1	Gratis	$ 0	letsencrypt.org
Internet dedicada (600 Mbps simétrico)	1	$ 15.000	$ 45.000	Claro Empresas
Total estimado			**$ 216.000**	

Costos de Hardware

ArgusNet se ejecutará sobre servidores ya existentes, pero se proyecta la necesidad de una estación de desarrollo y un servidor de pruebas adicional.

Hardware	Cant.	Precio unitario (ARS)	Total (ARS)	Fuente
Servidor físico (Dell PowerEdge T140 / Ryzen / 32 GB RAM / 2TB RAID1)	1	$ 1.950.000	$ 1.950.000	https://venex.com.ar
Notebook Dev (HP i7 / 16GB / SSD)	1	$ 1.200.000	$ 1.200.000	https://compragamer.com
Switch Gigabit TP-Link 24 puertos	1	$ 180.000	$ 180.000	https://mercadolibre.com.ar
Total estimado			**$ 3.330.000**	

Resumen de Costos Totales

Categoría	Costo total estimado (ARS)
Recursos Humanos	$ 19.400.000
Servicios e Infraestructura	$ 216.000
Hardware	$ 3.330.000
TOTAL ESTIMADO	**$ 22.946.000**

Análisis de Riesgos

El desarrollo de ArgusNet, al tratarse de una herramienta crítica para la gestión de seguridad perimetral en entornos empresariales, presenta distintos factores de riesgo que podrían impactar en su ejecución y operatividad. En esta sección se identifican, categorizan y priorizan los principales riesgos del proyecto, asignándoles un nivel de probabilidad de ocurrencia, impacto estimado y acciones de contingencia. El análisis se basa en el Principio de Pareto (80/20) y la evaluación cualitativa de impacto (escala 1 a 5).

ID	Riesgo	Categoría	Probabilidad	Impacto (1-5)	Descripción / Causa
R1	Aumento no previsto en costos de infraestructura cloud	Financiero	Alta	4	Fluctuación del dólar o aumentos de tarifas en AWS/Azure.
R2	Rotación del personal clave	Recurso Humano	Intermedia	3	Pérdida de programadores o administradores durante fases críticas.
R3	Retrasos por complejidad de integraciones (firewalls multi-marca)	Técnico	Alta	4	Integrar APIs diversas (Cisco, Fortinet, Palo Alto) puede requerir más esfuerzo.
R4	Fallas en el parsing de logs	Técnico	Intermedia	3	Formatos incompatibles o eventos mal estructurados impiden ingestión de datos.
R5	Mal dimensionamiento de recursos (CPU/RAM/datos)	Operativo	Intermedia	2	Subestimación de carga real de eventos o usuarios simultáneos.
R6	Vulnerabilidad no detectada en la suite	Seguridad	Baja	5	Error en programación o configuración que expone datos o deja vectores abiertos.
R7	Cambios en requisitos por parte de la empresa	Gestión	Intermedia	3	Incorporación de funcionalidades fuera del alcance original.
R8	Fallos en respaldos automáticos o restauración fallida	Técnico	Intermedia	4	Scripts de backup mal configurados o restauración no funcional.
R9	Baja adopción por parte del equipo operativo	Organizacional	Baja	2	Resistencia al cambio, falta de capacitación o baja usabilidad.

R10	Falta de financiamiento para escalamiento	Financiero	Intermedia	3	Imposibilidad de migrar a nube o adquirir hardware por falta de presupuesto.

Plan de Contingencias

Riesgo	Plan de Contingencia
R1	Negociar instancias reservadas o free-tier con proveedores; usar herramientas de monitoreo para optimización.
R2	Documentación continua del código y tareas clave; backup interno de recursos clave para continuidad.
R3	Prototipado y pruebas tempranas con dispositivos de firewall; buffer de tiempo en cronograma.
R4	Validación con logs reales antes del despliegue productivo; fallback manual temporal.
R5	Simulación de carga previa al despliegue; escalabilidad vertical planificada.
R6	Auditorías de código; escaneo periódico con herramientas como OpenVAS y pruebas de penetración.
R7	Control de cambios; requerimientos cerrados por sprint con validación del Coordinador IT.
R8	Backups diarios cifrados + pruebas mensuales de restauración en entorno aislado.
R9	Capacitaciones internas; rediseño de UX; feedback continuo desde las mesas de monitoreo.
R10	Alternativas híbridas (on-premise + cloud gratuita); presentación a dirección para justificar retorno.

Priorización según Grado de Exposición

Riesgo	Probabilidad	Impacto	Grado de Exposición (P × I)
R3	Alta	4	4.00
R1	Alta	4	4.00
R8	Intermedia	4	3.00
R6	Baja	5	2.50
R2	Intermedia	3	2.00
R4	Intermedia	3	2.00
R7	Intermedia	3	2.00
R10	Intermedia	3	2.00
R5	Intermedia	2	1.50
R9	Baja	2	1.00

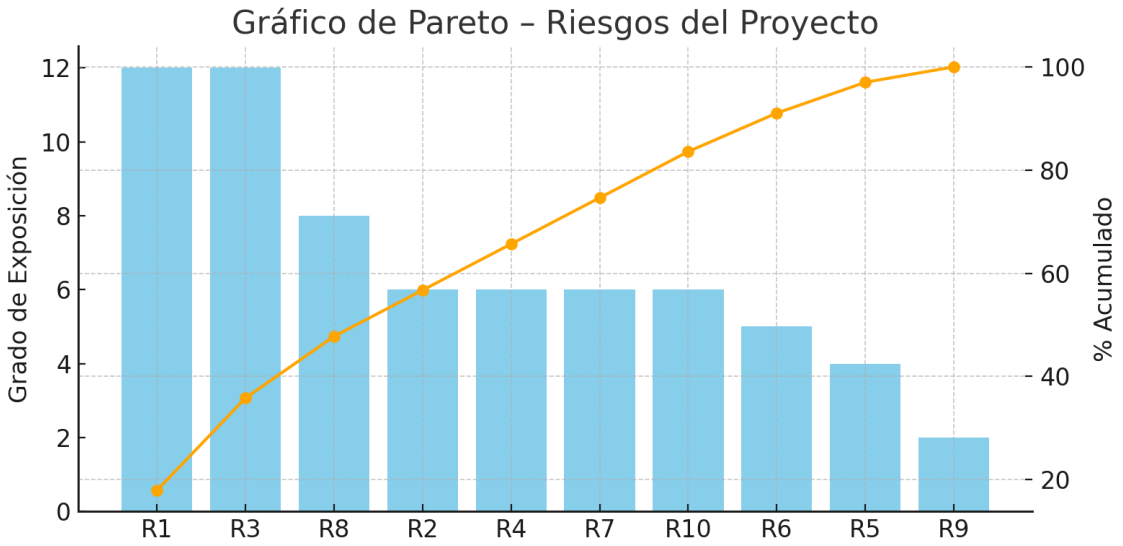


Gráfico de Pareto – Riesgos del Proyecto
Grado de Exposición
% Acumulado
0
2
4
6
8
10
12
20
40
60
80
100
R1
R3
R8
R2
R4
R7
R10
R6
R5
R9

Conclusiones

ArgusNet es un sistema diseñado para mejorar la gestión, el control y la colaboración sobre las reglas de firewall en entornos empresariales. Su desarrollo surgió a partir de una necesidad real identificada en el ámbito laboral, específicamente en empresas como Geex, donde la administración de firewalls es una tarea crítica, pero muchas veces dispersa, poco documentada y con alta dependencia de conocimientos tácitos.

El objetivo principal fue construir una plataforma colaborativa, centralizada y amigable que permita a distintos perfiles técnicos documentar, auditar, proponer y validar reglas de seguridad en múltiples marcas de firewall. A lo largo del proyecto, se lograron importantes avances: desde el diseño de interfaces hasta la definición de casos de uso, estructura de base de datos y prototipos funcionales. Se propuso un sistema extensible que integra tecnologías open source como ELK, Snort, bases relacionales y servicios web, con un enfoque moderno en seguridad y trazabilidad.

Durante el proceso de desarrollo se abordaron diversas dimensiones del proyecto: relevamiento, análisis funcional y técnico, diseño arquitectónico, políticas de seguridad, análisis de riesgos, costos y planificación. Todo ello permitió materializar una solución sólida, adaptable, y con posibilidades de evolución futura, incluyendo integración con sistemas de autenticación como Active Directory, doble factor, y backup automatizado.

Desde una perspectiva profesional, ArgusNet me permitió consolidar y aplicar competencias clave en arquitectura de sistemas, seguridad informática, administración de proyectos y desarrollo de software. Asimismo, me desafió a pensar en soluciones transversales, colaborativas y con foco en la escalabilidad y el cumplimiento normativo.

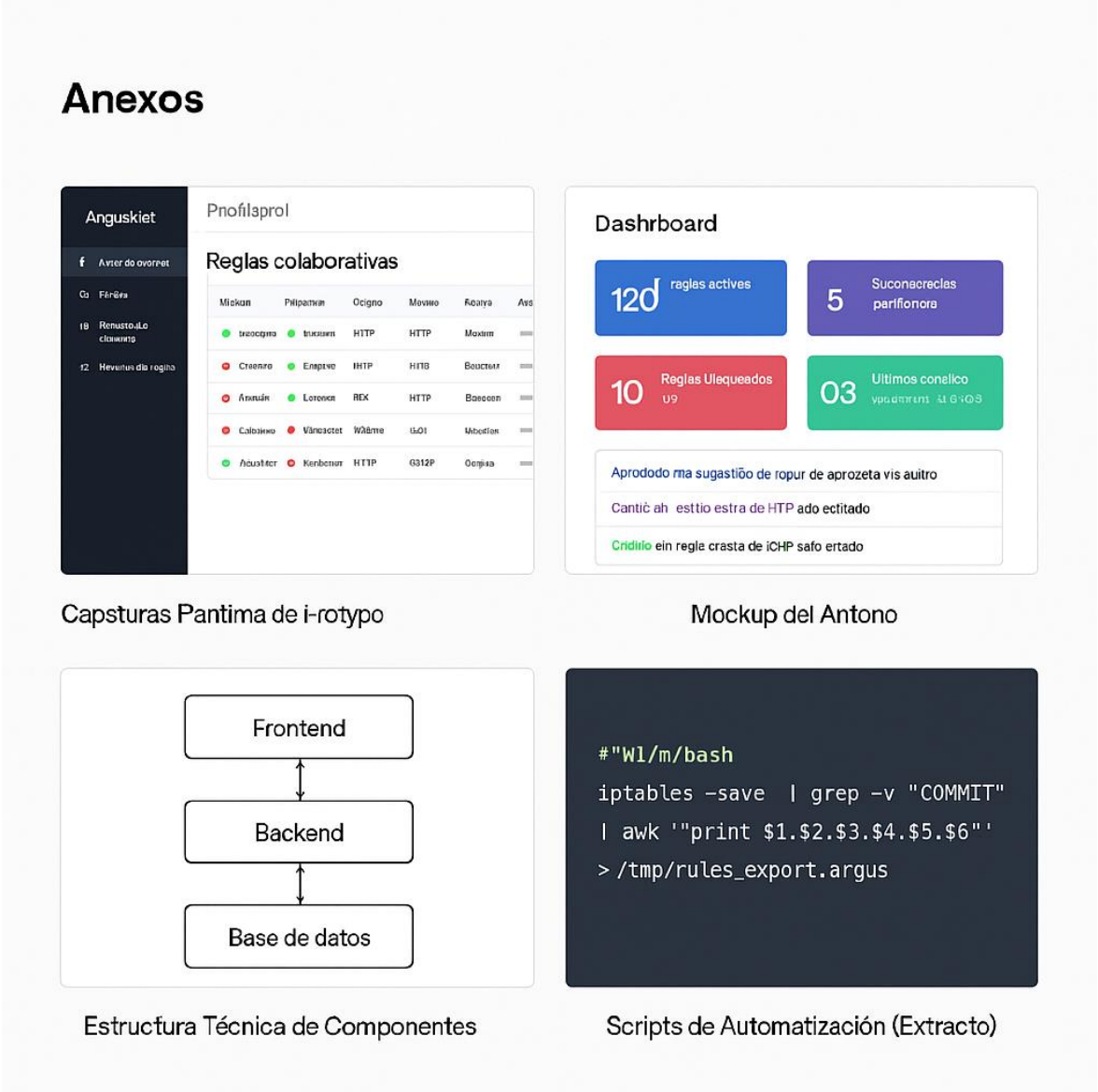
En el plano personal, fue una experiencia enriquecedora que me reafirmó el valor del diseño de soluciones que nacen desde problemas reales. Me permitió conectar mi experiencia como Coordinador de Tecnología con una propuesta académica seria, estructurada y con proyección concreta.

En fin, ArgusNet representa un aporte innovador al mundo de la administración de infraestructura crítica, proponiendo una herramienta que no solo documenta, sino que también promueve la colaboración y la gobernanza en materia de seguridad perimetral.

Anexos

1. Capturas de Pantalla del Prototipo

A continuación, se adjuntan capturas del prototipo inicial de ArgusNet, donde se puede observar:



- Panel de gestión de reglas colaborativas.
- Historial de auditoría y modificaciones.
- Panel de revisión y votación de reglas por múltiples usuarios.
- Integración con Active Directory para login seguro.

2. Mockup del Dashboard

Se incluye un esquema gráfico del dashboard principal, que ilustra la vista de estado de las reglas, sugerencias pendientes, reglas bloqueadas por seguridad y últimos eventos registrados por el sistema.

3. Estructura Técnica de Componentes

Se presenta el diagrama de arquitectura del sistema, que incluye:

- Backend en Node.js / Django
- Frontend en React
- Base de datos PostgreSQL
- Integración con LDAP/AD
- Seguridad basada en roles (RBAC)
- Backup y logging centralizado

4. Scripts de Automatización (Extracto)

Fragmento del script para la extracción automatizada de reglas IPTables y su conversión al formato unificado para revisión:

```
#!/bin/bash

iptables-save | grep -v "COMMIT" | awk '{print $1,$2,$3,$4,$5,$6}' > /tmp/rules_export.argus
```

5. Encuesta de Validación Técnica

Durante el desarrollo del proyecto, se realizó una validación técnica a través de un breve cuestionario entre colegas de IT, donde se evaluó:

- Necesidad de un sistema colaborativo de firewalls.
- Frecuencia de errores en reglas manuales.
- Viabilidad de implementación en entornos mixtos (Linux/Cisco/Mikrotik).
- Satisfacción estimada con la solución propuesta.

Demo

https://drive.google.com/drive/folders/1CIuqz5_eyK4VKalv2JrpRr8NzZdJWtCw?usp=sharing

Referencias

El desarrollo de la suite ArgusNet se basó en una combinación de conocimientos adquiridos a lo largo de la carrera de Licenciatura en Informática, experiencia profesional en infraestructura y seguridad, y el estudio de materiales académicos y técnicos relevantes. A continuación se detallan las principales fuentes teóricas, prácticas y tecnológicas que sirvieron de sustento para la elaboración del presente trabajo:

1. Formación académica y certificaciones técnicas

- **Currícula oficial del programa Cisco Networking Academy – CCNA y CCNP**. Esta formación proporcionó fundamentos sólidos en redes, seguridad perimetral, routing, switching y gestión de dispositivos Cisco ASA, aplicables directamente en el diseño y monitoreo de reglas firewall.
- **Programa de Hacking Ético – Universidad Siglo 21**. Aportó nociones de análisis de vulnerabilidades, técnicas de hardening, escaneo y detección de amenazas que nutrieron las funciones de monitoreo y respuesta ante incidentes.
- **Certificación Linux CLA – Linux Professional Institute**, fundamental para la comprensión y administración de firewalls basados en iptables en entornos Linux.
- **Capacitación en Mikrotik MTCNA**, que permitió extender la visión del manejo de dispositivos de seguridad más allá del universo Cisco.

2. Bibliografía técnica consultada

- Stallings, W. (2019). *Network Security Essentials: Applications and Standards*. Pearson.
- Pfleeger, C. P., & Pfleeger, S. L. (2018). *Security in Computing*. Pearson Education.
- Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.
- Bejtlich, R. (2013). *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. No Starch Press.
- Skoudis, E., & Liston, T. (2006). *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall.

3. Herramientas y software utilizados como referencia

- **Kiwi Syslog Server (SolarWinds)** – Referencia práctica en la recolección y almacenamiento centralizado de logs.
- **Graylog** – Plataforma open-source utilizada como inspiración para las funcionalidades de análisis y visualización de eventos de seguridad.
- **AlienVault OSSIM** – Sistema de detección de intrusos e integración de eventos (SIEM) que sirvió de benchmark para funciones de correlación de incidentes.
- **Pila ELK (Elasticsearch, Logstash, Kibana)** – Base técnica sobre la cual se estructuró la arquitectura de monitoreo y visualización en ArgusNet.
- **Snort** – Sistema IDS de referencia para detección de amenazas en tiempo real.
- **Zabbix / Nagios** – Inspiración para el diseño del sistema de alertas e indicadores de estado.

4. Documentación corporativa y normativa

- **Ley N.º 25.326 de Protección de los Datos Personales** (Argentina) y su decreto reglamentario 1558/2001, como marco legal para garantizar la seguridad, integridad y privacidad de los datos gestionados por ArgusNet.
- **Estándar ISO/IEC 27001** – Guía para la gestión de seguridad de la información, utilizada como base conceptual para los controles implementados.
- **Protocolo interno de respuesta a incidentes y documentación técnica de Geex S.A.**, utilizados en el relevamiento funcional y la validación de requerimientos.

4. **Experiencia práctica profesional**

La experiencia como Coordinador de Tecnología en Geex S.A. aportó conocimiento directo sobre las limitaciones operativas y técnicas en la gestión de firewalls multivendor, así como el uso real de plataformas como Cisco ASA, iptables en Linux, y herramientas de monitoreo de seguridad.