Universidad Norbert Wiener

FACULTAD DE INGENIERÍA
PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Trabajo de Suficiencia Profesional

Implementación de Nginx como proxy inverso para mejorar la seguridad de la infraestructura web en una empresa de servicios, Lima 2025

Para optar el Título Profesional de

Ingeniero de Sistemas e Informática

Presentado por:

Autor: Hu Urbano, Rui Qing

Código ORCID: https://orcid.org/0000-0002-8480-4991

Asesora: Dra. Díaz Reátegui, Mónica

Código ORCID: https://orcid.org/0000-0003-4506-7383

Lima – Perú

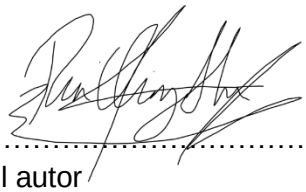
2026

Universidad Norbert Wiener	DECLARACIÓN JURADA DE AUTORIA Y DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN		
	CÓDIGO: UPNW-GRA-FOR-033	VERSIÓN: 01 REVISIÓN: 01	FECHA: 08/11/2022

Yo, Rui Qing Hu Urbano egresado de la Facultad de **Ingeniería Y Negocios** y Escuela Académica Profesional de **Ingenierías** de la Universidad privada Norbert Wiener declaro que el trabajo de investigación **"Implementación de Nginx como proxy inverso para mejorar la seguridad de la infraestructura web en una empresa de servicios, Lima 2025"** Asesorado por la docente: Dra. Mónica Díaz Reátegui DNI 09537647 ORCID 0000-0003-4506-7383 tiene un índice de similitud de **4 (cuatro) %** con código trn:oid:::14912:543829221 verificable en el reporte de originalidad del software Turnitin.

Así mismo:

1. Se ha mencionado todas las fuentes utilizadas, identificando correctamente las citas textuales o paráfrasis provenientes de otras fuentes.
2. No he utilizado ninguna otra fuente distinta de aquella señalada en el trabajo.
3. Se autoriza que el trabajo puede ser revisado en búsqueda de plagios.
4. El porcentaje señalado es el mismo que arrojó al momento de indexar, grabar o hacer el depósito en el turnitin de la universidad y,
5. Asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión en la información aportada, por lo cual nos sometemos a lo dispuesto en las normas del reglamento vigente de la universidad.



…….

Firma del autor
Rui Qing Hu Urbano
DNI: 77435349

…….

Firma
Dra. Mónica Díaz Reátegui
DNI: 09537647

Lima, 31 de diciembre del 2025

Dedicatoria

A mi padre, quien me guía desde el cielo.

Ingeniero antes que yo, y mi más grande inspiración. Tu partida dejó un vacío inmenso, pero tu esperanza en mi me dio la fuerza para llegar hasta aquí.

Sé que hoy estarías orgulloso.

Índice general

Índice de tablas

Índice de figuras

Resumen

El presente trabajo de suficiencia profesional aborda la optimización de la seguridad y la disponibilidad de la infraestructura web en una empresa de servicios en Lima, la cual enfrentaba riesgos críticos debido a la exposición directa de puertos, la falta de cifrado en comunicaciones internas y una dependencia limitante del proveedor de servicios de Internet (ISP) para la gestión de publicaciones es por esto que el objetivo principal fue implementar Nginx como proxy inverso para centralizar el tráfico y fortalecer la seguridad.

La metodología empleada fue de carácter experimental y ágil, utilizando una adaptación de SCRUM para el despliegue de la solución sobre contenedores Docker y la gestión mediante Nginx Proxy Manager. La solución estableció una arquitectura de cifrado de extremo a extremo mediante certificados Let's Encrypt para el tráfico público y una Entidad Certificadora (CA) interna para la red local.

Los resultados obtenidos validan la eficacia de la propuesta ya que se logró una reducción bastante grande en la superficie de ataque perimetral al eliminar subdominios obsoletos al igual que en el cierre de puertos expuestos. Asimismo, se recuperó la autonomía administrativa, reduciendo los tiempos de despliegue de nuevos servicios de días a minutos y eliminando los costos recurrentes por adquisición de certificados SSL. Dicho esto, se puede afirmar que la integración de un proxy inverso no solo mitiga vulnerabilidades críticas, sino que actúa como un catalizador para la eficiencia operativa y la modernización tecnológica de la institución.

Palabras clave: Proxy Inverso, Nginx, Ciberseguridad, Infraestructura Web, SSL/TLS, Docker, Let's Encrypt.

Abstract

This professional sufficiency work addresses the optimization of security and availability of the web infrastructure in a service company in Lima, which faced critical risks due to direct port exposure, lack of encryption in internal communications, and a limiting dependence on the Internet Service Provider (ISP) for publication management. Therefore, the main objective was to implement Nginx as a reverse proxy to centralize traffic and strengthen security.

The methodology employed was experimental and agile, utilizing an adaptation of SCRUM for deployment on Docker containers and management via Nginx Proxy Manager. The solution established an end-to-end encryption architecture using Let's Encrypt certificates for public traffic and an internal Certificate Authority (CA) for the local network.

The obtained results validate the efficacy of the proposal, as a significant reduction in the perimeter attack surface was achieved by eliminating obsolete subdomains as well as closing exposed ports. Likewise, administrative autonomy was recovered, reducing new service deployment times from days to minutes and eliminating recurring costs for SSL certificate acquisition. Having said that, it can be affirmed that the integration of a reverse proxy not only mitigates critical vulnerabilities but acts as a catalyst for operational efficiency and the institution's technological modernization.

Keywords: Reverse Proxy, Nginx, Cybersecurity, Web Infrastructure, SSL/TLS, Docker, Let's Encrypt.

Introducción

El presente trabajo de suficiencia profesional tiene como propósito la mejora de la seguridad y disponibilidad de la infraestructura web mediante la implementación de Nginx como proxy inverso, proyecto que será implementado en una empresa de servicios en Lima. Para ello, se definieron objetivos específicos orientados a su logro, tales como: (i) Diseñar la integración de Nginx como proxy inverso para mejorar la seguridad de la infraestructura web; y (ii) Configurar los certificados SSL en Nginx para garantizar la seguridad de las comunicaciones cliente-servidor.

Este trabajo fue posible no solo gracias a la experiencia laboral en el cargo, sino que también gracias a la aplicación de habilidades técnicas aprendidas de manera autodidacta en ciberseguridad e infraestructura, ello es importante, ya que complementa el criterio de evaluación de la suficiencia profesional.

El contenido del informe consta de tres capítulos. En el Capítulo I, se evidencia la descripción general de la organización, el planteamiento de la problemática y objetivos. En el Capítulo II, se presentan las bases teóricas que sustentan la solución. Asimismo, se desarrolla el marco conceptual sobre Nginx y la seguridad web, los antecedentes y la justificación de la metodología usada. Finalmente, en el Capítulo III, se detalla el diagnóstico de la situación problemática y la solución técnica basada en contenedores Docker y Nginx Proxy Manager.

El alcance principal de este trabajo de investigación es demostrar la suficiencia profesional, evidenciando el nivel de competencia para resolver problemas complejos de infraestructura tecnológica mediante soluciones innovadoras y eficientes.

Capítulo I: Antecedentes y descripción de la empresa

1.1. Reseña de la empresa

La empresa en estudio es una institución sin fines de lucro con más de un siglo de trayectoria, que se ha consolidado como una de las organizaciones más representativas del sector automotor y de servicios del país. Su sede central está ubicada en el distrito de Lince, en la ciudad de Lima. Actualmente, la institución cuenta con dos sedes administrativas y un club para sus asociados lejos del centro de la ciudad.

La institución está afiliada a la Federación Internacional del Automóvil (FIA), lo que le otorga un reconocimiento internacional en materia de movilidad, seguridad vial y turismo. A lo largo de los años, ha brindado servicios orientados a promover una movilidad segura y responsable, así como a satisfacer las necesidades básicas en el ámbito del hogar, desde asistencia médica hasta asistencia con equipos informáticos.

Entre sus principales actividades destacan la emisión de licencias de conducir mediante convenio con el Ministerio de Transportes y Comunicaciones (MTC), la expedición de certificados internacionales de manejo (Licencia Internacional), el servicio de asistencia mecánica en carretera (auxilio mecánico y grúa), la atención en servicios médicos y exámenes de aptitud para conductores, así como la promoción de la educación y seguridad vial en coordinación con entidades públicas y privadas. Asimismo, participa activamente en competencias automovilísticas y en la organización de eventos relacionados con el deporte automotor en el Perú.

Principales clientes

- Ministerio de Transporte y Comunicaciones (MTC)
- Pacifico Asiste S.A.C.
- Autoland S.A.
- Alese S.A.C.

En la **Figura 1**, se presentan los logotipos de algunos de los principales clientes y aliados estratégicos, con quienes mantiene fuertes relaciones comerciales para ofrecer sus servicios y otorgar beneficios adicionales a sus asociados, en ámbitos como licencias, movilidad, seguros de viaje, turismo, etc.

Figura 1

Principales clientes de la empresa.

(https://sierdgtt.mtc.gob.pe/)

(https://www.pacifico.com.pe/)

(https://www.autoland.com.pe)

(https://www.grupoalese.com/nosotros)

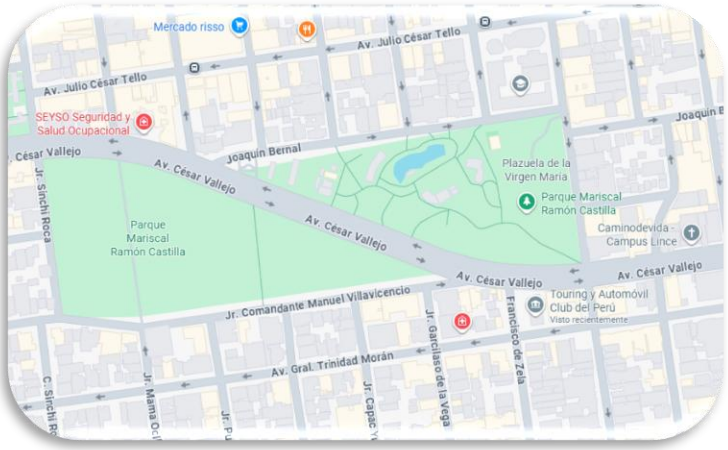
1.2. Ubicación y actividad empresarial

Ubicación

La ubicación fiscal de la empresa, en donde se encuentra su sede principal, es Av. General Trinidad Moran, distrito de Lince, Lima – Perú. En la siguiente figura se puede observar una referencia de la ubicación geográfica a través de Google Maps.

Figura 2

Croquis de la ubicación aproximada de la empresa



Nota. El croquis muestra la ubicación de la empresa en estudio a través de Google Maps. *https://maps.app.goo.gl/hDykJvji9Kt5HaJ9A*

Actividad empresarial

La actividad empresarial de esta entidad está enfocada en la prestación de servicios relacionados a la movilidad, seguridad vial y asistencia al automovilista, mediante convenios con entidades públicas y privadas, entre las que se encuentran el Ministerio de Transporte y Comunicaciones (MTC) y la Federación Internacional del Automóvil (FIA).

Los principales servicios que destacan en su página web son:

- Emisión de licencias de conducir en convenio con el Ministerio de Transportes y Comunicaciones.
- Expedición de licencias internacionales de conducir, válidas en más de 150 países.
- Asistencia mecánica y auxilio en carretera, incluyendo servicio de grúas y mecánica ligera.
- Servicios médicos básicos y servicios para el hogar.
- Capacitación y programas de educación vial, dirigidos a escolares, empresas y ciudadanía en general.
- Organización de eventos deportivos automovilísticos, en coordinación con la FIA.

Asimismo, ofrece beneficios adicionales a sus asociados mediante convenios con empresas privadas en rubros como seguros de viaje, alquiler de autos y combustibles.

En la **Figura 3** se muestra algunos servicios y beneficios más representativos que forman parte del plan integral ofertado por la institución en estudio.

Figura 3

Servicios ofrecidos por la institución: Plan integral

Nota. Imagen extraída de la página web de la institución en estudio.

1.3. Misión, visión y valores de la empresa

Misión:

Atender de manera integral las necesidades y expectativas de los asociados en ámbitos de asistencia, recreación, automovilismo, turismo, formación y seguridad vial, así como las de clientes y demás partes interesadas, ofreciendo servicios con altos niveles de calidad, transparencia y confianza, respaldados por la experiencia técnica y el compromiso de su equipo humano.

Visión:

Consolidarse como un club referente en movilidad segura y sostenible, en la promoción del automovilismo deportivo y en el impulso del turismo nacional, incorporando un enfoque innovador que aporte valor a sus asociados, clientes y a la sociedad en general.

Valores:

- **Innovación:** Promovemos la creación ágil de soluciones y mejoras en los procesos, orientados a garantizar una movilidad accesible, sostenible y segura para todos.
- **Integridad:** Mantenemos una conducta transparente en la interacción con nuestros asociados, clientes y demás partes interesadas.
- **Orientación Al Cliente:** Nos enfocamos en ofrecer y generar propuestas de valor que satisfagan a nuestros asociados y clientes.
- **Eficiencia:** Procuramos aprovechar de manera óptima los recursos disponibles, asegurando un servicio de calidad al menor costo posible.

1.4. Descripción del puesto desarrollado y su entorno

La institución se desempeña como una organización orientada a la prestación de diversos servicios, los cuales cuentan con un soporte tecnológico que respalda sus procesos y operaciones. En este contexto, la Gerencia de Tecnologías de la Información (GTI) cumple un rol estratégico, asegurando la continuidad, seguridad y eficiencia de estos servicios que soportan sus diversos procesos.

El investigador ocupa el cargo de Coordinador de Innovación y Mejora Continua, el cual se ubica directamente bajo la supervisión del Gerente de TI participando de manera activa y colaborativa con las distintas unidades que conforman el departamento de TI:

infraestructura, seguridad informática, soporte técnico, desarrollo de software y gestión de bases de datos.

Este puesto se caracteriza por una interacción transversal con todas las áreas del departamento de TI, lo cual permite tener una visión integral de los retos tecnológicos de toda la institución. A partir de esta perspectiva, se puede identificar la necesidad de implementar soluciones que fortalezcan la seguridad y disponibilidad de la infraestructura web.

Tabla 1

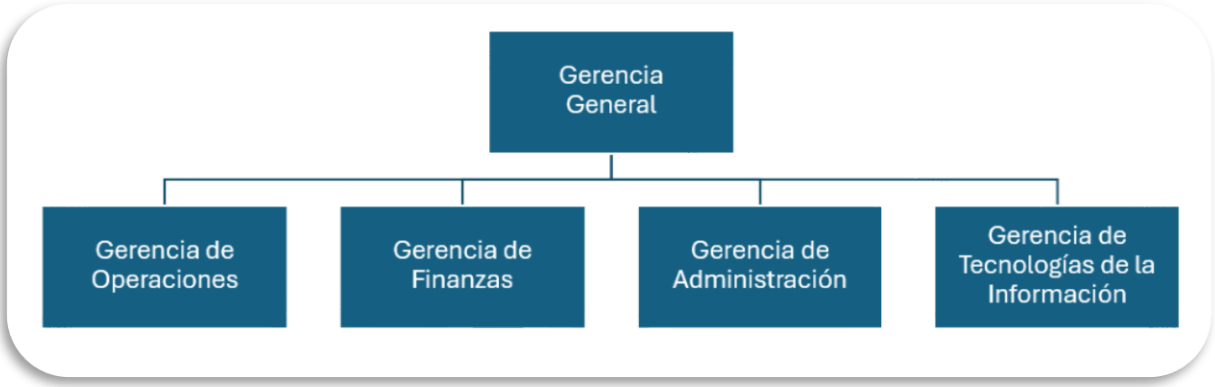
Principales empresas que compiten en el mismo nicho de mercado

Ítem	Principales empresas competidoras
1	Centros de evaluación de municipalidades provinciales
2	Rimac Seguros y Reaseguros S.A.C.
3	Pacifico Compañia de Seguros y Reaseguros S.A.C.
4	Mapfre Peru S.A.

La institución tiene actualmente más de 300 empleados registrados en su planilla. En la siguiente figura se presenta el organigrama:

Figura 4

Organigrama de la institución con las gerencias más resaltantes



Descripción del puesto: Gerente General

Función principal: Dirigir estratégicamente a la organización asegurando el cumplimiento de la misión, visión y objetivos institucionales.

Funciones específicas:

- Definir políticas generales y lineamientos estratégicos.
- Representar a la empresa ante entidades públicas, privadas e internacionales.
- Supervisar el desempeño de todas las gerencias para garantizar eficiencia y sostenibilidad.

Descripción del puesto: Gerente de Operaciones

Función principal: Gestionar los servicios principales (asistencia vehicular, seguridad vial, y servicios hogar) garantizando calidad en la atención.

Funciones específicas:

- Supervisar la idoneidad de los servicios de asistencia y servicios hogar.
- Asegurar el cumplimiento de estándares de calidad en el servicio.
- Optimizar procesos operativos para mejorar la experiencia del asociado y cliente.

Descripción del puesto: Gerente de Finanzas

Función principal: Administrar los recursos financieros de la empresa garantizando transparencia, control y sostenibilidad económica.

Funciones específicas:

- Elaborar y supervisar presupuestos anuales.
- Gestionar la liquidez y flujo de caja.
- Velar por el cumplimiento tributario y normativo financiero.

Descripción del puesto: Gerente de Administración

Función principal: Gestionar los recursos humanos, logísticos y administrativos para el adecuado soporte institucional.

Funciones específicas:

- Supervisar la gestión y funciones del personal tercerizado.

- Administrar recursos materiales, infraestructura y patrimonio institucional.
- Implementar políticas administrativas que fortalezcan la eficiencia organizacional.

Descripción del puesto: Gerente de Tecnologías de la Información

Función principal: Asegurar la innovación y sostenibilidad tecnológica de la institución, brindando soporte a los procesos de negocio y la transformación digital.

Funciones específicas:

- Dirigir la infraestructura tecnológica y de telecomunicaciones.
- Implementar proyectos de transformación digital e innovación en servicios.
- Garantizar la seguridad de la información y continuidad operativa.

1.5. Problemática y objetivos trazados

En Europa, informes especializados indican que la disponibilidad web enfrenta diversas amenazas que afectan la administración de servicios críticos, lo que legitima reforzar la seguridad con Nginx y otras herramientas (European Union Agency for Cybersecurity - ENISA, 2023). Los ataques disruptivos se intensificaron en 2023 y 2024, confirmando la urgencia de arquitecturas resilientes orientadas a continuidad operativa (European Union Agency for Cybersecurity - ENISA, 2024).

En Latinoamérica, el índice DGI (Digital Goverment Index) muestra que Perú, Colombia y Uruguay encabezaban la lista en la dimensión “Digital by Design” la cual resalta (entre otros) medidas y esfuerzos relacionados a la ciberseguridad (OECD & IDB, 2024). Esto es especialmente positivo, ya que, en un país en desarrollo, reducir la cantidad de ciberincidentes puede aumentar el PIB per cápita en un 1,5 %, y que un espacio cibernético más seguro promueve la confianza en la economía digital y protege a los sectores vulnerables (The World Bank, 2024).

En Perú, se registraron 31,5 millones de intentos de phishing entre junio de 2022 y julio de 2023, lo que lo coloca entre los países más afectados de América Latina. En cuanto a troyanos bancarios, Perú sufrió 58 mil intentos de infección, ubicándose detrás de Brasil, México y Colombia (AO Kaspersky Lab, 2023)

En Lima, en el segundo trimestre de 2024, el 91,2% de la población usuaria de Internet en Lima Metropolitana accede a través de un teléfono móvil, lo cual subraya la importancia de fortalecer las medidas de seguridad para proteger la información personal y

empresarial en un entorno cada vez más digital y móvil (Instituto Nacional de Estadística e Informática - INEI, 2024).

Mientras que en Europa los avances se traducen en una aplicación más consolidada de marcos normativos y arquitecturas de seguridad robustas, en Latinoamérica aún persiste una brecha significativa entre la planificación y la capacidad de responder a amenazas de esta índole, razón por la cual es de suma importancia contar con mecanismos tales como Nginx como proxy inverso para mejorar la seguridad de la arquitectura web de las empresas.

Desde una perspectiva crítica, el pronóstico negativo de no abordar los problemas de seguridad y disponibilidad de la infraestructura web podría perpetuar la exclusión tecnológica de sectores vulnerables e incrementar los costos operacionales para empresas locales debido a interrupciones frecuentes del servicio. Si estos problemas no se atienden, las empresas podrían perder competitividad por tener servicios expuestos a interrupciones y colapsos prolongados.

En la institución en estudio se detectaron fallas de configuración en la infraestructura web que representan un riesgo significativo para la seguridad y la disponibilidad de los sistemas. Estos aspectos fueron evidenciados mediante el uso de la herramienta de diagnóstico cuantitativo, lo que permitió dar a reconocer los siguientes problemas:

i. La exposición directa de direcciones IP reales dificulta el acceso a los servicios web para los usuarios finales internos.
ii. La falta de certificados SSL afecta la seguridad en las comunicaciones cliente-servidor debido a que la información transmitida podría ser interceptada y visualizada en texto plano.
iii. El uso de múltiples direcciones IP públicas dificulta la administración y limita la disponibilidad de nuevos servicios debido a que se incrementa la complejidad del enrutamiento y la dependencia de personal especializado para su configuración.
iv. La infraestructura descentralizada, caracterizada por configuraciones individuales y múltiples puntos de gestión, dificulta la estandarización, el mantenimiento de la estabilidad y la trazabilidad unificada de incidentes.
v. La gestión de la publicación de servicios web depende exclusivamente del Proveedor de Servicios de Internet (ISP) generando un cuello de botella operativo que restringe la agilidad del área de TI.

De no revertirse este escenario en el corto plazo, podrían presentarse las siguientes consecuencias negativas:

i. Incremento de vulnerabilidades críticas que facilitarían la ocurrencia de ciberataques exitosos.
ii. Pérdidas económicas derivadas de interrupciones en los servicios digitales.
iii. Disminución en la confianza de los clientes hacia la empresa y sus productos.
iv. Limitaciones en la capacidad de expansión tecnológica, lo que afectaría directamente la competitividad en el mercado.

Problema general

¿De qué manera la implementación de Nginx como proxy inverso mejora la seguridad de la infraestructura web en una empresa de servicios, Lima 2025?

Problemas específicos

i. ¿Cómo el diseño de la integración de Nginx como proxy inverso mejora la seguridad de la infraestructura web en una empresa de servicios, Lima 2025?
ii. ¿Cómo la configuración de los certificados SSL en Nginx como proxy inverso garantiza la seguridad de la infraestructura web en una empresa de servicios, Lima 2025?

Objetivo general

Implementar Nginx como proxy inverso para mejorar la seguridad de la infraestructura web en una empresa de servicios, Lima 2025

Objetivos específicos

i. Diseñar la integración de Nginx como proxy inverso para mejorar la seguridad de la infraestructura web en una empresa de servicios, Lima 2025
ii. Configurar los certificados SSL en Nginx para garantizar la seguridad de la infraestructura web en una empresa de servicios, Lima 2025

Capítulo II: Fundamento del Tema elegido.

2.1 Bases Teóricas

El presente trabajo de suficiencia profesional, que tiene como objetivo implementar Nginx como proxy inverso para mejorar la seguridad de la infraestructura web en una empresa de servicios, se fundamenta en un conjunto de marcos teóricos consolidados en la ingeniería de sistemas y la seguridad de la información. Las teorías que dan soporte a la variable independiente son: (i) la Teoría General de Sistemas; (ii) la Teoría de la Información; y (iii) la Teoría de la Cibernética. Para la variable dependiente, se cuenta con las teorías: (a) la Teoría de la Confiabilidad; (b) la Teoría de Juegos; y (c) la Teoría de la Disuasión.

Teoría General de Sistemas

Bertalanffy (1968) brinda un marco para comprender las entidades no como elementos separados, sino como un conjunto de componentes interconectados que constituyen una totalidad integrada. También hace una distinción entre sistemas abiertos y cerrados: los primeros intercambian energía o información con su medio ambiente, mientras que los segundos no lo hacen. Una infraestructura tecnológica es un sistema inherentemente abierto y su comportamiento colectivo o "sinergia" no puede ser capturado simplemente sumando sus partes, sino que emerge de las interacciones entre ellas y que crean propiedades que las partes individuales no poseen.

Asimismo, para Ackoff (1971), desde una perspectiva gerencial, el pensamiento sistémico es una herramienta para resolver problemas complejos en las organizaciones. El enfoque de sistemas se enfoca en la manera en que los componentes de un sistema colaboran entre sí dentro del marco de un sistema mayor, a diferencia del método analítico, que consiste en dividir un problema en partes más pequeñas y resolverlas individualmente.

Además, Boulding (1956) planteó una jerarquía de sistemas, desde los más simples y estáticos hasta los socioculturales. Esta jerarquía sirve para encuadrar la TGS como "esqueleto científico", al ofrecer un lenguaje para hablar de los principios que se aplican en las disciplinas.

En resumen, estos autores demuestran que la Teoría General de Sistemas va más allá de la perspectiva fragmentada y sugiere un enfoque integrador. Esta visión enfatiza que los

sistemas, en particular los tecnológicos y organizacionales, deben ser considerados como totalidades abiertas cuyos atributos surgen de la interacción entre sus partes. Asimismo, el pensamiento sistémico es necesario para la gestión de problemas complejos, porque posibilita abordar la interdependencia de los elementos en vez de considerarlos por separado.

Teoría de la Información

Shannon (1948), en su obra seminal, formuló esta teoría, en la que la comunicación se representa como un proceso estadístico compuesto por una fuente, un transmisor, un canal, un receptor y un destino. También incluyó una fuente de "ruido", capaz de dañar la señal. Cuantificar la información y establecer los límites esenciales para transmitirla de forma confiable a través de un canal ruidoso eran el objetivo principal de su teoría, no el significado del mensaje. Por medio de este enfoque matemático, se logró, por primera vez, considerar a la información como una cantidad que puede ser medida, normalmente en "bits".

Además, Weaver (1949) amplió la teoría al identificar tres niveles de problemas en la comunicación: el técnico (la exactitud con que se pueden transmitir los símbolos), el semántico (la exactitud con que los símbolos transmitidos comunican lo que se quiere expresar) y el de efectividad (cuán eficazmente la conducta se ve afectada por lo que se recibe). Weaver hizo esta distinción en su introducción a un libro que popularizó las ideas de Shannon.

Finalmente, Gleick (2011), desde un punto de vista contemporáneo, define la teoría de la información de Shannon como el ADN del tiempo digital. Afirma que el concepto de extraer información de su entorno físico y manejarla como una secuencia de bits fue la revolución conceptual que permitió todo, desde las computadoras hasta Internet. La teoría se aplica a la compresión de datos, así como a la transmisión, al evidenciar que es posible suprimir la redundancia en un mensaje para lograr una codificación más eficaz; esta idea es esencial hoy en día para el almacenamiento y streaming de datos.

En conclusión, la teoría de la información constituye un pilar fundamental para comprender los procesos de comunicación en la era digital. Al modelar la transmisión de mensajes como un sistema estructurado y cuantificable, se estableció la base para medir la información y enfrentar las limitaciones impuestas por el ruido en los canales. La posterior

ampliación del modelo permitió reconocer dimensiones más amplias del proceso comunicativo, vinculadas tanto al significado como a la efectividad del mensaje.

Teoría de la Cibernética

Wiener (1948), en su obra fundacional del año 1948, describió la cibernética como la investigación de la comunicación y el control tanto en máquinas como en seres vivos. La retroalimentación (feedback) es la idea principal de su teoría, y consiste en un mecanismo por el cual un sistema modifica sus acciones futuras con base en los datos sobre su desempeño previo. Este ciclo de retroalimentación posibilita que los sistemas, sean de tipo biológico, mecánico o social, conserven una condición de estabilidad o equilibrio (homeostasis) ante las alteraciones del medio ambiente.

Asi tambien, Ashby (1956), estableció la "Ley de la Variedad Requerida", que sostiene que un sistema necesita tener como mínimo la misma cantidad de variedad en sus acciones que el sistema al cual intenta regular para ejercer un control eficiente sobre él. Dicho de otro modo, cualquier buen regulador debería poder reaccionar a todas las posibles alteraciones que el sistema pueda afrontar. Esto quiere decir que la complejidad del mecanismo de control tiene que ser equivalente a la complejidad de las amenazas.

Además, Beer (1981) creó el "Modelo de Sistema Viable" (VSM) al poner en práctica varios principios dentro del entorno empresarial. Dicho modelo utiliza la cibernética para formar organizaciones que puedan adaptarse y sobrevivir en entornos cambiantes. El VSM describe múltiples componentes que un sistema viable debe incorporar, estos abarcan las funciones de control, operación, dirección y coordinación, todas vinculadas entre sí a través de ciclos de comunicación y retroalimentación para asegurar la resiliencia en la organización.

Siendo asi, la cibernética ofrece un marco para comprender cómo los sistemas naturales y/o artificiales logran mantener su estabilidad y adaptarse frente a la complejidad de su entorno. Esta ha evolucionado hasta el punto de poder aplicarse de manera practica en las organizaciones, al integrar principios como la recursividad y la variedad requerida, las empresas dejan de funcionar como jerarquías rígidas para convertirse en sistemas dinámicos que facilitan una respuesta ágil ante las incertidumbres del mercado.

Teoría de la Confiabilidad

Lewis (1996) explica que la confiabilidad de un sistema depende de su arquitectura. Un principio es la redundancia, la cual consiste en disponer los elementos en una configuración en paralelo. Ello puede tolerar fallos en sus componentes, aumentando la disponibilidad y fiabilidad del servicio. Por el contrario, en una configuración en serie, si falla un solo componente de la cadena, todo el sistema falla junto con él.

Adicionalmente, Srinath (1991) profundiza en las métricas cuantitativas de esta teoría, especificando medidas como el Tiempo Medio Entre Fallos (MTBF) y el Tiempo Medio de Reparación (MTTR). Estas métricas no solo informan sobre el pasado, sino que también se pueden usar para estimar la disponibilidad futura de un sistema. La disponibilidad (porcentaje de tiempo que un sistema está funcionando) depende de con qué frecuencia falla (MTBF) y con qué rapidez puede restaurarse (MTTR). En ese sentido, hacer más confiable un sistema es aumentar el MTBF y disminuir el MTTR.

De igual forma, O'Connor y Kleyner (2012) señalan que la fiabilidad no es una característica que se añada al final, sino que se debe incorporar desde el principio al sistema y gestionarse durante todo su ciclo de vida. Fomentan una actitud anticipatoria que incluye el diseño para tolerancia a fallos, los mantenimientos preventivos y el análisis de modos y efectos de falla (FMEA). Siendo asi, la confiabilidad es el resultado de un trabajo que busca anticiparse, evitar y reducir los fallos.

Por lo antes expuesto, la confiabilidad de un sistema es una característica que depende de su diseño y de la gestión de su ciclo de vida. La redundancia garantiza que el sistema siga funcionando, aunque fallen algunas partes, y las métricas de rendimiento, como MTBF y MTTR, son una buena manera de estimar la disponibilidad. Pero lograr alta confiabilidad requiere un enfoque integral desde el diseño del sistema, con prácticas preventivas, tolerancia a fallos y mantenimiento programado.

Teoría de Juegos

Von Neumann y Morgenstern (1944) desarrollaron la teoría de juegos y ofreciendo un modelo para examinar cómo se toman decisiones estratégicas entre entes racionales cuyos resultados varían según las elecciones de los demás. El modelo estudia "juegos" en los que los "jugadores" escogen "estrategias" con el objetivo de incrementar sus "premios". La teoría se presenta como un juego no cooperativo entre un "atacante" y un "defensor", donde cada participante intenta maximizar su premio frente a las posibles acciones del otro.

Posteriormente, Nash (1951) desarrolló el concepto de "Equilibrio de Nash", ello ocurre cuando cada jugador ha elegido la mejor estrategia posible, dadas las posibles estrategias elegidas por los demás jugadores, donde ningún participante recibirá un premio mejor si no confía en el otro. En ciberseguridad, el defensor busca establecer una configuración de seguridad que cree un equilibrio en el que la mejor respuesta del atacante sea no atacar, o como mínimo, que su ataque sea ineficaz.

De igual forma, Alpcan y Başar (2010) se apoyan en esta teoría y la aplican en la seguridad de redes, modelando la interacción en la red como un juego dinámico. En este juego el defensor debe asignar recursos limitados (capacidad de procesamiento o personal de seguridad) para protegerse de un atacante que elige sus movimientos en un ataque. La seguridad no es una acción aislada, es una acción que cambia las reglas del juego, que cambia la relación de costos y beneficios para el atacante en favor del defensor.

En síntesis, la teoría de juegos en ciberseguridad representa como un juego estratégico en donde los atacantes y defensores van moviendo sus piezas y así van alterando las posibilidades y recompensas del otro. El equilibrio es una guía para crear medidas seguras que reduzcan los motivos de un ataque o eliminen los beneficios, mostrando cómo los recursos pueden ser utilizados en contra de amenazas y cómo pueden trabajar para ti.

Teoría de la Disuasión

Schelling (1960) planteó que la disuasión no es solo un defensa, sino la capacidad de afectar la decisión del oponente con la amenaza de un costo inaceptable para él. El oponente debe creer que cualquier beneficio posible no justificará el coste de la acción. Es por ello que una disuasión exitosa y efectiva implica demostrar una capacidad de represalia y una postura defensiva firme.

De la misma manera, Davis & Jenkins (2014) adaptaron el marco de disuasión al ciberespacio, separando entre "disuasión por negación" y "disuasión por castigo". La disuasión por negación es la más importante para la seguridad de la infraestructura y busca persuadir a un atacante de que su ataque fracasará. Esto se consigue volviendo el objetivo demasiado complicado para que el ataque tenga éxito o merezca la pena. Por el otro, la disuasión por castigo intenta evitar la agresión amenazando con altos costos posteriores al ataque. Esta estrategia se apoya en la capacidad de tomar represalias legales, económicas o contraataques.

Asimismo, Kramer et al. (2009) sostienen que una postura eficaz en ciberseguridad combina aspectos técnicos y políticos para generar un efecto disuasivo fuerte. Alegan que la resiliencia de un sistema (habilidad para soportar un ataque y reponerse con rapidez) es, por sí misma, una forma de disuasión por negación. Cuando el defensor muestra que un ataque no producirá una interrupción significativa, disminuye la motivación del atacante, cuya recompensa frecuentemente está sujeta a la magnitud de daño que pueda causar.

Siendo asi, en el terreno de la ciberseguridad, se considera disuasión a la habilidad para cambiar la estrategia de un adversario reduciendo su motivación para atacar al tener que afrontar costos muy altos y beneficios muy bajos. El enfoque basado en la disuasión subraya la relevancia de tener defensas robustas, resiliencia y respuestas veloces que hagan del sistema un objetivo poco atractivo por la recompensa que pudiese obtenerse de él, más allá de la simple capacidad de represalia, sin desmerecer la efectividad de este último tampoco.

2.2 Marco conceptual

2.2.1 Nginx como proxy inverso

Nginx es una plataforma open source flexible que evolucionó de servidor web a un software versátil con funcionalidades de balanceador de carga y proxy inverso (Kazemi, 2023). Es eficiente, escalable y de arquitectura modular, lo que permite implementaciones personalizadas para cualquier necesidad relacionada con las webs modernas (Insights2TechInfo, 2023). Esto es posible ya que está estructurado con una arquitectura escalable de núcleo pequeño y módulos de alto rendimiento que se pueden acoplar (Intel Corporation, 2021). Se puede afirmar que, es una tecnología diseñada para mejorar el rendimiento, la seguridad y la escalabilidad de aplicaciones y API (F5 Inc., 2024).

La función principal de un proxy inverso es reenviar peticiones de clientes para incrementar la seguridad, el rendimiento y la fiabilidad del sistema detrás de él (Lacnic, 2023). El valor fundamental de Nginx como proxy inverso no reside en una única función, sino en la versatilidad de su arquitectura, que se traduce directamente en una capacidad superior para resolver los desafíos de rendimiento, seguridad y escalabilidad de la web moderna, especialmente su funcionalidad como proxy que ayuda a facilitar la administración cuando se usa junto a un gestor visual como NPM (Nginx Proxy Manager).

Características

Las características de Nginx determinan su flexibilidad y rendimiento elevados. Su núcleo está basado en una estructura orientada a eventos y asíncrona, lo que le posibilita manejar un amplio número de conexiones simultáneas con un consumo de recursos muy bajo. Esto posibilita la existencia de funcionalidades superiores, como los firewalls de aplicaciones web (WAF) o algoritmos de compresión actualizados, adecuándose a múltiples y diversas necesidades (Insights2TechInfo, 2023).

Adicionalmente, su diseño modular compuesto por un núcleo pequeño y simple también se puede ver en sus módulos permitiéndole añadir distintas funcionalidades específicas (Intel Corporation, 2021). Esta simplicidad facilita la gestión de hosts virtuales, permitiendo que cada uno tenga una configuración distinta, específica y aislada dentro de una misma instancia de Nginx. Sin embargo, a medida que la infraestructura crece, la gestión de múltiples instancias requiere un plano de control centralizado para aplicar políticas uniformes de seguridad y cumplimiento (F5 Inc., 2024).

Usos

Los usos de Nginx son:

i. Proxy Inverso y Servidor de Contenido Estático:
Un proxy inverso es un servidor situado en el borde de la red que recibe las peticiones de los clientes y las reenvía a uno o varios servidores de origen; suele usarse para ocultar la topología interna, mejorar la seguridad (terminación TLS, filtrado) y acelerar la entrega de activos estáticos mediante caché y offloading, liberando a los servidores de aplicación de esa carga (Reese, 2008).

ii. Balanceador de Carga:
Un balanceador de carga distribuye de forma automática las solicitudes entrantes entre un conjunto de recursos o nodos (a nivel de red o aplicación) para optimizar la utilización de recursos, evitar sobrecargas de un único servidor y mejorar la disponibilidad y tolerancia a fallos del sistema (Devi et al., 2024).

iii. Gateway de API:
Un gateway de API actúa como punto de entrada único para clientes hacia un conjunto de microservicios, centralizando funciones transversales (enrutamiento, autenticación/autorización, limitación de tasa, caching y monitoreo) y desacoplando a los consumidores de la complejidad y heterogeneidad de los servicios internos (Ochuba et al., 2021).

iv. Controlador de Ingreso en Kubernetes:
Un Ingress Controller es la implementación que observa los objetos Ingress en un clúster Kubernetes y materializa sus reglas (host/path, TLS, reescrituras) mediante un proxy inverso/load-balancer, gestionando el tráfico HTTP/S desde fuera del clúster hacia los servicios apropiados dentro del mismo (Veeri, 2024).

v. Componente de Malla de Servicios:
Una malla de servicios es una capa de infraestructura dedicada (normalmente formada por proxies ligeros desplegados junto a cada servicio) que gestiona la comunicación inter-servicios proporcionando enrutamiento avanzado, observabilidad, seguridad y mecanismos de resiliencia sin modificar el código de las aplicaciones (Nicolas-Plata et al., 2024).

Beneficios

Los beneficios que ofrece Nginx son:

i. Fortalecimiento de la Seguridad
ii. Escalabilidad y Alta Disponibilidad
iii. Flexibilidad y Consolidación de Infraestructura

2.2.2 Seguridad de la infraestructura web

La seguridad informática de la infraestructura web busca garantizar el acceso seguro y confiable a los servicios digitales (Instituto Distrital de Gestión de Riesgos y Cambio Climático, 2025). A su vez, implica definir el monitoreo y control para mantener un esquema de seguridad y alta disponibilidad en las plataformas tecnológicas (Secretaría Jurídica Distrital, 2025). Además, este término abarca la seguridad de los recursos y la seguridad física en centros de datos con estándares internacionales (Rivera, 2022).

La nueva tendencia es hacer más privada y eficiente la infraestructura de Internet con sistemas de datos descentralizados (Cheema, 2024). Sin embargo, el objetivo final sigue siendo el mismo: garantizar la integridad, disponibilidad y seguridad de los datos frente a accesos no autorizados (Rozó, 2024). En definitiva, seguridad y disponibilidad no son objetivos separados, sino que en conjunto generan la confianza en los ecosistemas digitales de hoy.

Características

Una infraestructura web segura tiene las siguientes propiedades: la utilización de centros de datos y servicios en la nube que garantizan escalabilidad y alta disponibilidad. A su vez, necesita de redes sólidas y seguras que estén diseñadas para aguantar un tráfico elevado sin interrupciones, asegurando la protección de la información y la continuidad operativa (Instituto Distrital de Gestión de Riesgos y Cambio Climático, 2025).

Otras características son la aplicación de protocolos de monitoreo y la asistencia técnica para garantizar el funcionamiento adecuado de los sistemas durante el mayor tiempo posible (Secretaría Jurídica Distrital, 2025). Además, el control de cambios y accesos a la infraestructura de red es crucial para detectar, informar y manejar incidentes de seguridad y disponibilidad de forma proactiva (Agencia Nacional Digital, 2022).

Pilares

Los pilares para la gestión de la seguridad son:

i. Seguridad Física y Perimetral de la Infraestructura:
Abarca el conjunto de barreras físicas y lógicas además de controles de acceso al borde de la infraestructura para prevenir intrusiones no autorizadas antes de que lleguen a los sistemas internos (Lohani et al., 2022).

ii. Seguridad de Redes y Comunicaciones:
Se ocupa de proteger los canales de transmisión (mediante cifrado, control de acceso, detección de amenazas y segmentación) para garantizar confidencialidad, integridad y disponibilidad frente a ataques activos o pasivos (Nayana et al., 2019).

iii. Seguridad de Aplicaciones y Servicios Web:
Trata de prevenir vulnerabilidades (como control de acceso roto, inyección, XSS) que permitan a un atacante comprometer la lógica de negocio o la integridad de los datos, aplicando controles en el nivel de aplicación, validación de entradas y defensa en profundidad (Anas et al., 2024).

iv. Gestión de Identidad y Control de Acceso:
Engloba procesos y tecnologías que permiten definir, autenticar y autorizar identidades (usuarios, servicios, dispositivos) con el principio de mínimo privilegio, revocación y gobernanza, con el fin de controlar quién puede acceder a qué recursos y bajo qué condiciones (Glöckler et al., 2023).

v. Monitoreo, Detección y Respuesta a Incidentes:
Involucra la supervisión continua de eventos y registros para detectar anomalías y amenazas (mediante sistemas de monitorización de red, SIEM, IDS/IPS) y activar mecanismos de respuesta como aislamiento, contención, análisis forense para mitigar el impacto de incidentes de seguridad (Younus & Alanezi, 2023).

Beneficios

Los beneficios que ofrece la gestión de la seguridad son:

i. Continuidad del Negocio y Operativa
ii. Integridad, Confidencialidad y Privacidad de los Datos
iii. Generación de Confianza en Clientes y Usuarios
iv. Cumplimiento de Regulaciones y Estándares
v. Resiliencia y Capacidad de Recuperación ante Ciberataques

2.3 Antecedentes

Internacionales

Peidro (2025) discutió los desafíos de la obsolescencia tecnológica y el agotamiento de las direcciones IPv4 en una empresa del sector médico global y recomendó reemplazar una infraestructura basada en NAT y Windows Server con Nginx Plus como proxy inverso. Centralizó la gestión de certificados SSL y permitió que los servidores equilibraran la carga entre sí, logrando la publicación segura de más de 250 servicios web. Los resultados obtenidos mostraron una optimización de los recursos de red y un perímetro más seguro utilizando políticas HSTS, permitiendo que el entorno empresarial sea de alta disponibilidad y también escalable.

Adicionalmente, Pezoa (2024) desarrolló una solución de gestión de vulnerabilidades web donde se requiere una arquitectura para evaluar la exposición pública con el fin de mejorar el rendimiento y la seguridad. Se implementó Nginx como servidor proxy inverso y gestor de contenido estático en un entorno de contenedores con Docker entre los usuarios y el servidor de aplicaciones Django. Esta configuración permitió que el servidor de aplicaciones "permanezca aislado" de las solicitudes, facilitando la entrega de recursos estáticos y proporcionando una capa adicional de seguridad que respalda el despliegue ágil y el monitoreo de vulnerabilidades de seguridad identificadas.

Asi tambien, Elorza (2024) creó una aplicación web de control nutricional y se enfrentó al desafío de desplegar servicios seguros y accesibles en la nube con una arquitectura de microservicios. El autor utilizó Nginx para servir como servidor web y proxy inverso para gestionar las solicitudes dirigidas al framework Flask y la base de datos MySQL, gestionada con Docker Compose. Esto facilita que el lado del servidor proporcione un certificado SSL para manejar el tráfico HTTPS y gestione adecuadamente el tráfico entrante, demostrando además que un proxy inverso es necesario para la protección y el despliegue escalable de la plataforma moderna en producción.

Asimismo, Bravo (2020) creó un entorno de prueba para mejorar la voz en la telefonía IP y utilizó Nginx como proxy inverso para asegurar la comunicación entre la plataforma Twilio y el backend desarrollado en Python mediante solicitudes WebSocket y HTTPS. Bajo esta configuración, la terminación SSL se realizaría en el proxy, transfiriendo la responsabilidad al proxy y asegurando que las grabaciones de llamadas en vivo y la clonación de llamadas fueran seguras y permanecieran confidenciales.

Además, Boettner (2022) investigó vulnerabilidades vinculadas al robo de sesiones y cookies en aplicaciones web, y sugirió un mecanismo de defensa basado en la interceptación y manipulación de encabezados HTTP. Se empleó mitmproxy (proxy local) para modificar los valores de las cookies en tránsito, desacoplando los identificadores de sesión reales de los almacenados en el navegador del cliente. Como muestra la investigación, el uso de intermediarios proxy permite crear capas de seguridad que proporcionan prevención contra ataques de Cross-Site Scripting (XSS) y secuestro de sesiones.

Nacionales

Núñez (2022) abordó el problema de la inseguridad y latencia en el monitoreo de la operación en modo remoto de una planta generadora de oxígeno y propuso el uso del servidor web como proxy inverso para separar la capa de control de la exposición pública. Este arreglo permitió cubrir la infraestructura interna de la planta y gestionar las solicitudes externas realizadas al Raspberry Pi, asegurando la integridad de los datos clave del proceso industrial mientras se habilitaba el acceso continuo al monitoreo.

De igual forma, Chambi y Huaranca (2017) investigaron la gestión descentralizada y la seguridad de la información para la organización comercial e introdujeron un Sistema de Gestión Integral en Línea. Se reconoció que la liberación directa del módulo administrativo en la red pública revelaba un riesgo de exposición a la confidencialidad de la información financiera y de inventario. Además, la solución implementó un entorno web flexible que permitió un servidor proxy inverso fuerte para el filtrado de tráfico malicioso y la gestión de sesiones de usuario, proporcionando así acceso centralizado y reduciendo en gran medida las vulnerabilidades de inyección SQL y acceso no autorizado a la base de datos.

Además, Córdova (2012) habló de los problemas de escalabilidad y seguridad con aplicaciones colaborativas alojadas "on-premise" y propuso mover la aplicación a una nube privada. Como los servicios internos se exponían directamente, había cuellos de botella y agujeros de seguridad, así que se añadió una capa intermedia: un proxy inverso para controlar el tráfico que llega a los servidores. Esto generó un único punto en el cual se aplicaron políticas de seguridad y cifrado SSL, mejorando la disponibilidad y sensación de seguridad de los usuarios.

Asimismo, Huaman (2024) se enfocó en optimizar la eficiencia y seguridad del sistema de centro de llamadas. Se determinó que la sobreexposición de los servicios de telefonía IP era una mala práctica. Para mitigarlo, se desplegó un servidor web y proxy

inverso de Nginx, aprovechando la arquitectura asíncrona y de alto rendimiento de Nginx. Esto posibilitó enmascarar la red interna y administrar los certificados de seguridad, creando así una plataforma estable que asegura la confidencialidad de las llamadas y disminuye los tiempos de respuesta del sistema.

Locales

Dávalos (2022) analizó los problemas de seguridad y escalabilidad en la infraestructura de la startup Qempo y descubrió amenazas críticas como la ejecución de procesos Node.js con permisos de administrador y la exposición directa de la base de datos a Internet. Para resolver esto, se reestructuró el servidor proxy inverso con Nginx, sirviendo certificados SSL y archivos estáticos para liberar el backend. Esta intervención eliminó un riesgo de seguridad significativo e introdujo una capa intermedia que mejoró la respuesta y redujo el riesgo de fuga de datos.

Por otro lado, Larrea y Victoria (2020) desarrollaron la plataforma tecnológica "TRecomiendo", cuya tarea era gestionar la alta disponibilidad y seguridad de un sistema de microservicios. Los autores encontraron que era absolutamente crítico tener Nginx como proxy inverso, por un lado, para salvaguardar la aplicación y, por el otro, sus servidores. Esta configuración de seguridad perimetral permitió la eficiencia del equilibrio de carga y la protección de la infraestructura contra ataques directos y, por lo tanto, mejorando la operación e integridad de la información.

Asi también, Castillo et al. (2025) en su propuesta de desarrollo "DestinarIA" en la industria del turismo pusieron los aspectos de optimización del rendimiento y seguridad de transacciones al frente del marco de arquitectura de tres capas. Nginx fue utilizado como proxy inverso, gestionando el certificado HTTPS y cifrando la comunicación de la aplicación entre capas basadas en red y capas basadas en servicios. Esta decisión introdujo una barrera de seguridad que valida la viabilidad técnica de la plataforma para procesar información sensible de los viajeros.

2.4 Justificación de la metodología elegida

Para el presente informe de suficiencia profesional se ha considerado de importancia usar la experiencia laboral en la institución para evidenciar la competencia y dominio de habilidades propias de la profesión. La justificación de este proyecto no solo se basa en la experiencia laboral, sino también en el crecimiento profesional, la aplicación de habilidades específicas y personales y éticas para una evaluación integral.

Por lo tanto, como buena práctica, se empleó parcialmente la metodología SCRUM para cumplir con los siguientes objetivos:

i. Diseñar la integración de Nginx como proxy inverso para mejorar la seguridad de la infraestructura web en una empresa de servicios, Lima 2025.
ii. Configurar los certificados SSL en Nginx para garantizar la seguridad de la infraestructura web en una empresa de servicios, Lima 2025.

Cabe destacar que, por el tamaño del equipo, se ha adaptado una versión reducida de SCRUM. Esta metodología se centró en la adaptación continua a los requerimientos y la revisión constante del trabajo. En cuanto a la colaboración, se basó en la comunicación abierta y continua entre los integrantes del equipo, con pocas formalidades y total transparencia sobre el proyecto. Esta flexibilidad hizo posible una adaptación rápida a los problemas técnicos y de gestión del proyecto.

Finalmente, al madurar el objetivo de implementar Nginx como proxy inverso para reforzar la seguridad de la infraestructura web, se obtuvieron beneficios como: seguridad, escalabilidad y alta disponibilidad; flexibilidad y consolidación de infraestructura; continuidad de negocio y operativa; integridad, confidencialidad y privacidad de los datos; generación de confianza en clientes y usuarios; cumplimiento normativo y estándares; resiliencia y recuperación ante ciberataques.

Capitulo III: Aporte y desarrollo de la experiencia

3.1 Diagnóstico de la situación problemática

La revisión inicial de la infraestructura web previo a la intervención reveló vulnerabilidades críticas en seguridad, agilidad y complejidad administrativa. Estos eran potenciales amenazas para la sostenibilidad del negocio y su habilidad para adaptarse rápidamente a los cambios necesarios.

El diagnóstico reveló que este problema se dividía principalmente en dos ramas:

La primera, operativa, era la dependencia de proveedores externos para el control de tráfico y aprovisionamiento de servicios, lo que afectaba la agilidad.

La segunda, más técnica, destapó una arquitectura de red interna y configuraciones que estaban creando agujeros de seguridad latentes.

Figura 5

Diagnóstico de la problemática

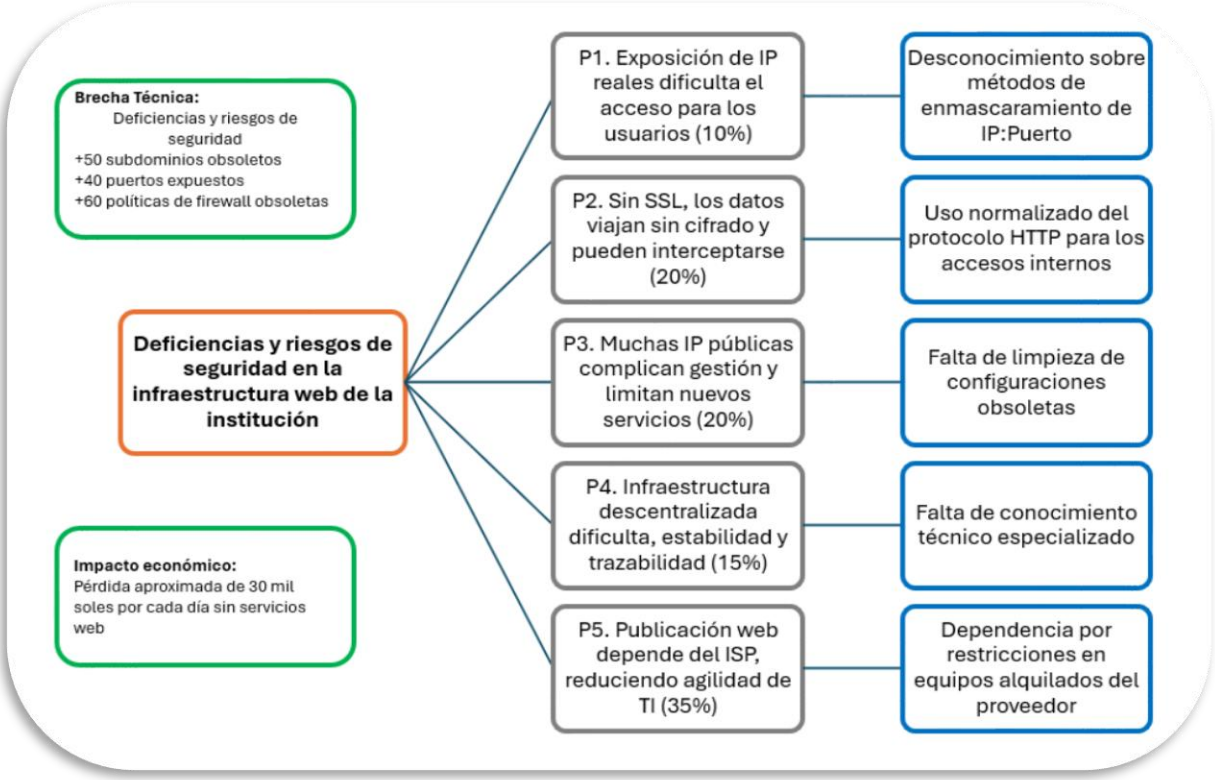
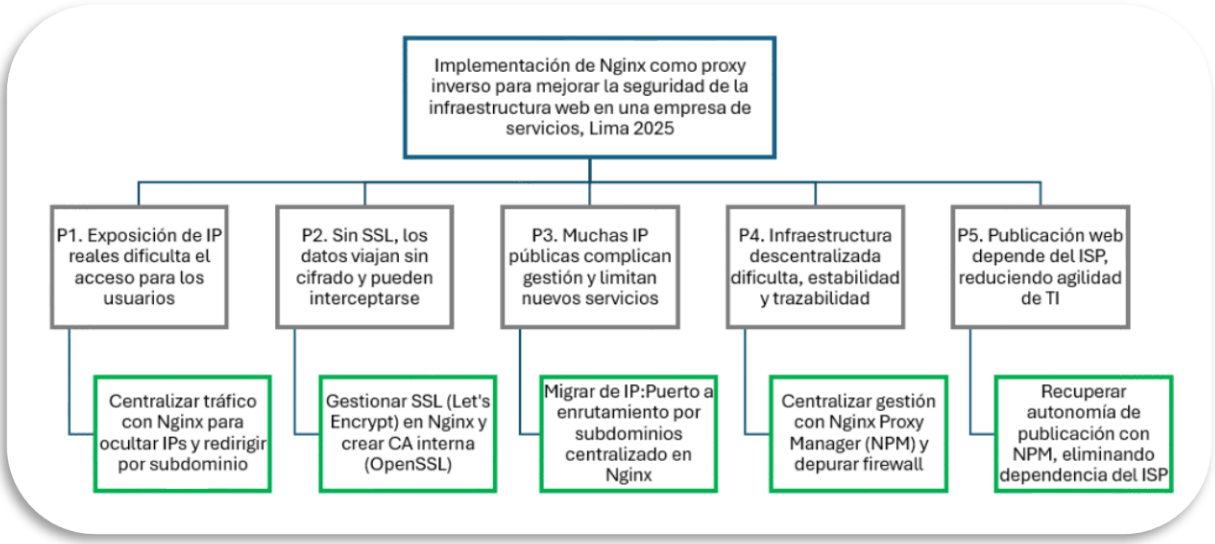


Figura 6

Diagnóstico de la solución



Dependencia Operacional y Agilidad Restringida

La arquitectura preexistente estaba basada en el uso de balanceadores físicos FortiADC y un firewall FortiGate, cuya configuración para la exposición de servicios web (tráfico inbound) generaba una dependencia crítica del proveedor de servicios de Internet (ISP), dueño del FortiADC. Para la publicación de cada nuevo subdominio o la modificación de reglas, la entidad debía solicitar intervenciones externas.

Esta dependencia se tradujo en una restricción operativa considerable y un cuello de botella en los tiempos de respuesta. Las peticiones de configuración eran frecuentemente escaladas a técnicos de primer nivel (N1), lo cual resultaba en demoras que podían extenderse por días, afectando directamente la agilidad del área de Tecnologías de la Información (TI) para lanzar nuevos servicios o corregir incidentes rápidamente.

Adicionalmente, la institución se veía obligada a comprar certificados SSL para cada web expuesta a Internet, generando un costo operativo recurrente innecesario. Esta gestión no automatizada, exigía una reconfiguración manual tras cada vencimiento, aumentando significativamente la carga operativa y el riesgo de interrupciones del servicio por errores humanos o renovaciones a destiempo.

Brechas de Seguridad y Complejidad de Administración

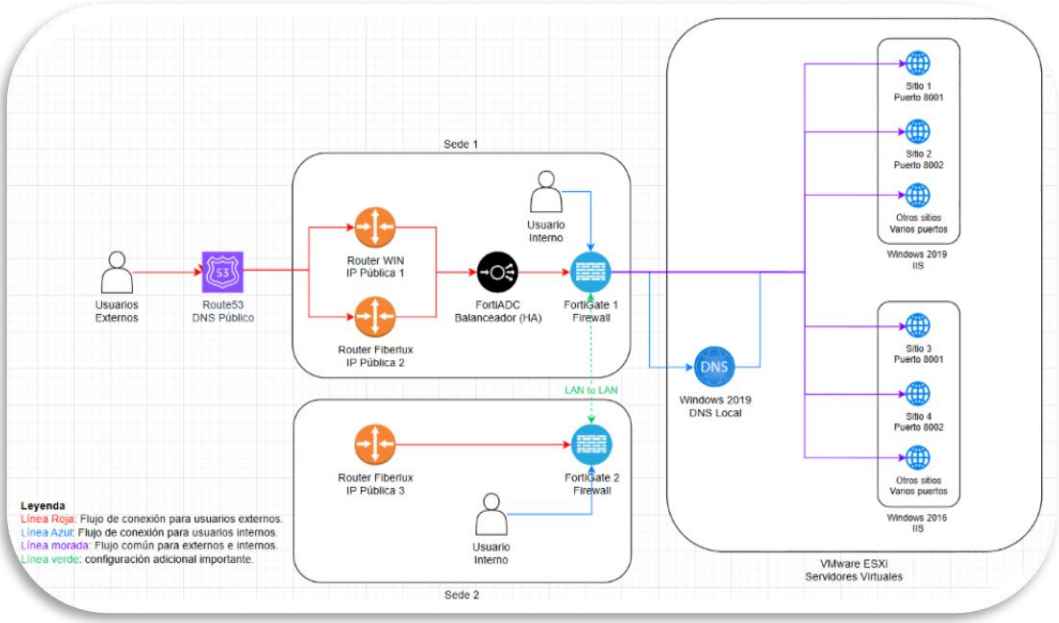
El diagnóstico identificó dos brechas de seguridad primarias asociadas a la gestión de accesos y el cifrado:

- Exposición Insegura de Servicios Internos:
  Las publicaciones y webservices internos eran accedidos por los usuarios directamente mediante la combinación de IP y Puerto (ej. 192.168.1.50:8080), utilizando el protocolo HTTP. Esta práctica hacía que las comunicaciones fuesen inherentemente inseguras, dejando la información sin cifrar y vulnerable a ataques de tipo Man-in-the-Middle.
- Alta Superficie de Ataque y Complejidad de Certificados:
  La configuración de la infraestructura requería un alto número de políticas NAT en el firewall y múltiples registros en Route53 y DNS local para gestionar el tráfico hacia los distintos puertos de los servidores IIS. Esta fragmentación de la configuración incrementaba la superficie de ataque y dificultaba la auditoría.

La convergencia de estos problemas evidenció la necesidad de implementar una solución de Proxy Inverso que recuperara el control administrativo, centralizara la gestión del tráfico y mitigara las vulnerabilidades de seguridad, adoptando una postura proactiva.

Figura 7

Diagrama de la arquitectura web AS IS



3.2 Desarrollo de la experiencia

La presente experiencia se desarrolló en un ambiente en constante evolución y mejora de su infraestructura tecnológica. Aunque las primeras labores del investigador en la institución fueron como administrador de bases de datos y de Business Intelligence (BI), el ascenso a coordinador de Innovación y Mejora Continua se logró por el buen desempeño, la consecución de resultados y el dominio transversal de áreas críticas como infraestructura y seguridad. Esta trayectoria permitió asumir un rol de Líder Técnico en el proyecto de implementación de Nginx.

Administrador de Bases de Datos y Business Intelligence

En esta época el papel del investigador se centró en velar por la integridad, disponibilidad y explotación de los datos institucionales. Principalmente administración y gestión de servidores de bases de datos como MSSQL, MySQL, MariaDB. Esto implicó no solo supervisar la actividad y el rendimiento de las instancias, sino también gestionar usuarios, perfiles y permisos para garantizar que el acceso a los datos siguiera el principio de mínimo privilegio y gobernanza de datos.

Parte de esta responsabilidad era diseñar, implementar y supervisar procesos de backup y restauración para garantizar la continuidad del negocio y la resistencia ante fallos o desastres. El investigador desarrolló herramientas de auditoría y rastreo para dar seguimiento a las transacciones y alteraciones de datos, asegurando el cumplimiento normativo interno. Además, se optimizó y corrigió código, sobre todo stored procedures (SP), jobs y código T-SQL, mejorando el rendimiento de las consultas y reduciendo los tiempos de respuesta transaccional.

En Business Intelligence se dedicó a transformar datos en información estratégica. El investigador desarrolló dashboards en Power BI utilizando ETL avanzado, modelado de datos en Power Query y creación de medidas y cálculos complejos en DAX. Se reunió con los dueños de proceso para establecer KPIs y asegurarse de que los dashboards fueran útiles y representaran la realidad de la organización. La configuración de AWS S3 para el almacenamiento también fue parte de este rol, sentando las bases para una arquitectura de datos escalable.

La transversalidad de este cargo que demandó la mejora de sistemas y entendimiento de la infraestructura on-premise y en la nube, preparó al investigador para sugerir soluciones en otras áreas críticas, como la seguridad perimetral.

Coordinador de Innovación y Mejora Continua

El cambio a Coordinador de Innovación y Mejora Continua convirtió al investigador en un impulsor de transformación, preocupado por la modernización tecnológica y la mejora de los procesos de la institución. En este rol, el investigador escaló de ser reactivo a proactivo y líder integral en la Gerencia de TI.

La labor principal es el Scouting Tecnológico, investigando y evaluando nuevas tecnologías y tendencias del mercado. Tras esto, el investigador propone mejoras en los procesos del área de TI y gestiona los proyectos que de ello se deriven. La meta es mejorar la infraestructura tecnológica, como por ejemplo la implementación de Nginx, que nació por una necesidad de modernización y seguridad.

Un objetivo principal es la identificación y eliminación de la causa de problemas repetitivos, utilizando técnicas de análisis causa-raíz. Esta función significa no sólo apagar el fuego (resolver el síntoma), sino cambiar las arquitecturas o los procesos de fondo que causan ineficiencia o riesgo. También el investigador asesora y es gestor financiero tecnológico, optimizando los gastos de otras gerencias a través de la tecnología y disminuyendo productos y servicios tecnológicos innecesarios.

Esta perspectiva de ahorro y eficiencia es una motivación permanente para los proyectos de mejora continua que el investigador dirige, para que las inversiones en TI generen el mayor valor para la institución.

El rol de evangelizador es crucial, con habilidades de comunicación, gestión del cambio y liderazgo técnico para cultivar la cultura de innovación en el equipo. Este ambiente es el que llevó al investigador a implementar Nginx y solucionar problemas de gestión y seguridad que iban más allá de su función inicial.

Contexto Operacional

El investigador fue responsable del proyecto desde la idea hasta la ejecución. El proyecto se manejó con un equipo pequeño, pero con la participación en momentos críticos de todo el equipo de TI, usando una forma modificada y ligera de SCRUM, donde los valores de comunicación directa, transparencia total y adaptación continua fueron esenciales para la velocidad y el éxito del desarrollo.

La principal causa fue reconocer una dependencia del ISP para publicar contenido web y tener un agujero de seguridad interno. La arquitectura anterior usaba FortiADC (balanceadores físicos en HA) y un firewall FortiGate, con configuraciones complejas de NAT y port forwarding para exponer cada subdominio y puerto interno a la red pública. Esta estructura la gestionaba el ISP con tiempos lentos de respuesta, lo que limitaba la capacidad de la empresa para sacar nuevas publicaciones.

Planificación y Justificación de la Solución

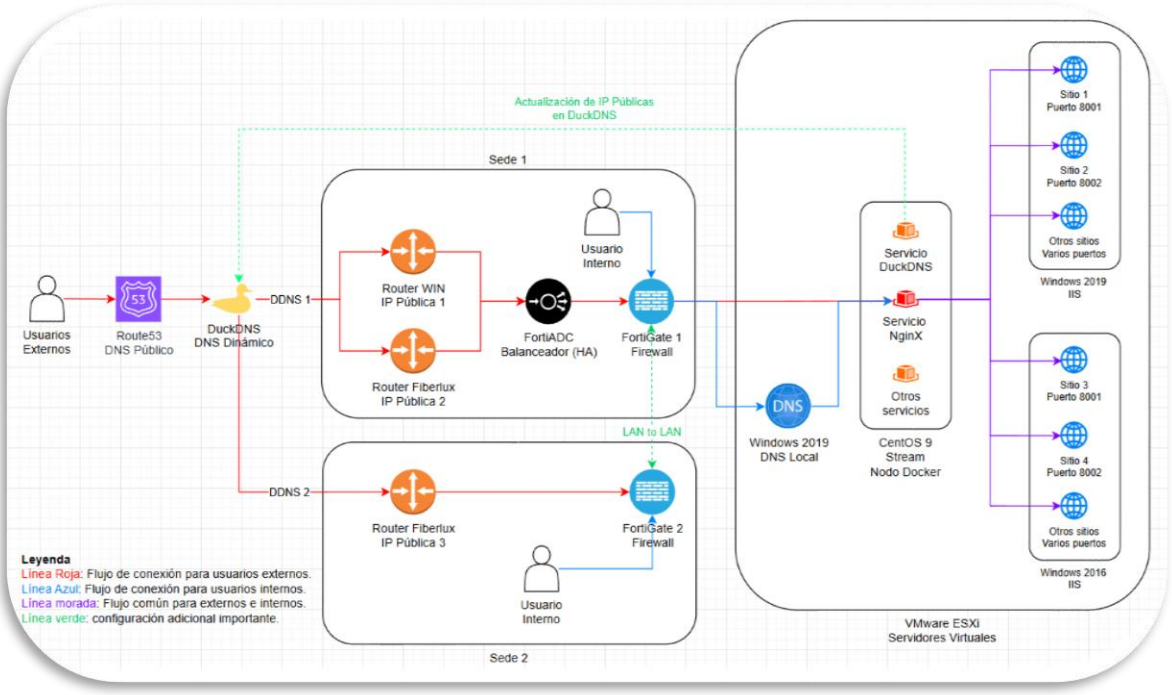
Se eligió el software Nginx (como reverse proxy) por los siguientes criterios:

- Implementación rápida y flexible:
  Se decidió por desplegar Nginx Proxy Manager (NPM) en Docker. Esto dotó al equipo de mucha más agilidad, pudiendo levantar y modificar el servicio en las fases de prueba y minimizando los riesgos en producción.
- Facilidad en la gestión:
  NPM (proyecto open-source con interfaz gráfica) es de curva de aprendizaje casi nula por lo intuitiva que es su interfaz. Esto sirvió para centralizar la administración y que el personal de TI administrara los registros host sin depender del proveedor.
- Seguridad Centralizada:
  Nginx podría centralizar el manejo de tráfico y certificados SSL, cerrando además puertos que antes quedaban expuestos directamente a la red por las antiguas configuraciones de Firewall y Balanceador.

El hito principal de esta etapa fue la entrega de un Diagrama de Red Propuesto que evidenciaba la recuperación del control sobre las publicaciones de Internet, simplificando radicalmente el proceso de exposición de nuevos sitios y centralizando la administración del tráfico en Nginx, mitigando la dependencia del proveedor para realizar configuraciones en el balanceador FortiADC, dicho diagrama es el que se muestra a continuación:

Figura 8

Diagrama de la arquitectura web TO BE



3.3 Modelado de la propuesta o solución

La solución se modeló en torno a la implementación de Nginx como Reverse Proxy centralizador, buscando establecer una capa de control y seguridad que separara la infraestructura de publicaciones internas de la exposición directa a Internet y la red local.

Arquitectura Lógica de la Solución

La propuesta consistió en interponer un nuevo servidor Nginx, desplegado de manera ágil y flexible mediante Docker y administrado a través de Nginx Proxy Manager (NPM), entre el firewall (FortiGate) y los servidores de publicaciones (IIS).

El diseño lógico se enfocó en:

- Centralización del Tráfico:
  Se coordinó con el proveedor para que la IP pública del servidor Nginx fuese el único punto de exposición a Internet. Nginx, a su vez, actuaría como el único gestor de las redirecciones internas.

- Enrutamiento por Subdominio:
  El modelo de enrutamiento se migró de la dependencia IP:Puerto a la dependencia Subdominio. Mediante la funcionalidad Proxy Host de NPM, Nginx escucha un subdominio específico y lo redirige internamente a la dirección IP y puerto delweb server, eliminando la necesidad de que el usuario final acceda a través de un puerto.
- Recuperación del Control:
  Al centralizar toda la administración de hosts en NPM (que cuenta con una interfaz gráfica y una curva de aprendizaje mínima), el equipo de TI recuperó la autonomía total sobre la publicación de nuevos sitios, sin depender de terceros.

Modelo de Cifrado y Certificación SSL

Un componente fundamental del modelado fue la adopción de una estrategia de cifrado end-to-end (cifrado de extremo a extremo) tanto para el tráfico externo como interno:

- Publicaciones Externas:
  Se utilizó Certbot y Let's Encrypt implementado en NPM. Se configuró Nginx para que gestionara automáticamente la generación, instalación, y renovación de los certificados SSL. Esta metodología garantiza que el tráfico externo se maneje exclusivamente bajo HTTPS, al mismo tiempo que elimina los costos recurrentes asociados a la adquisición y mantenimiento manual de certificados.
- Publicaciones Internas:
  Para asegurar el cifrado interno, donde servicios como Let's Encrypt no son aplicables, se modeló la creación de una Entidad Certificadora (CA) interna utilizando OpenSSL. Los certificados raíz generados, con una vigencia de diez años, se distribuyeron e instalaron masivamente en todos los endpoints (servidores y clientes) a través de la Política de Grupo (GPO). Esto estableció la confianza necesaria para el acceso cifrado mediante subdominios (HTTPS) dentro de la red local.

Este modelo de solución permitió la simplificación drástica de la infraestructura, minimizando la cantidad de configuraciones críticas en el firewall y consolidando la seguridad en un único punto, eficiente y de fácil administración.

3.4 Resultados

La implementación de Nginx como reverse proxy y su enfoque en la seguridad de la infraestructura web, guiada por los objetivos estratégicos, generó un impacto directo en la seguridad, eficiencia operativa y gestión de costos, logrando mitigar las principales problemáticas identificadas.

Resultados de Seguridad y Reducción de la Superficie de Ataque

- Mitigación de Vulnerabilidades Perimetrales:
  Se logró una reducción del 76% de los subdominios que antes apuntaban a reglas de firewall o balanceador. De igual forma, se eliminó el 60% de los puertos expuestos en las IP's públicas, con un potencial de reducción adicional del 25% tras la eliminación de configuraciones residuales.
- Limpieza de Políticas Obsoletas:
  La centralización del tráfico permitió eliminar 63 políticas de firewall (FW) que se habían acumulado de forma obsoleta, reduciendo la complejidad del FortiGate y disminuyendo la probabilidad de errores de configuración.
- Cifrado de Comunicaciones (HTTPS):
  Se cumplió con el objetivo de configurar certificados SSL mediante la migración total de los servicios externos a Let's Encrypt (gestión automática a través de Nginx). Además, se encriptaron el 75% de los accesos a servicios internos que previamente utilizaban el protocolo inseguro HTTP, utilizando una CA propia con OpenSSL para garantizar la privacidad de los datos en la red local.

Resultados en la Eficiencia Operacional y Autonomía Administrativa

- Autonomía y Agilidad de Despliegue:
  Se eliminó la dependencia del ISP para exponer nuevos servicios web. El tiempo promedio para lanzar una nueva aplicación a producción se redujo de días (o semanas) a minutos, permitiendo a la entidad responder con mayor agilidad a los requerimientos de negocio.
- Reducción de Costos Operacionales:
  Se eliminó la necesidad de la compra recurrente de certificados SSL individuales, generando un ahorro directo en el presupuesto de licenciamiento del área de TI, al consolidar la gestión SSL en la solución gratuita de Let's Encrypt.

- Simplificación de la Gestión:
  Se redujo la complejidad de la gestión, migrando a una administración centralizada y con interfaz gráfica a través de Nginx Proxy Manager (NPM). Esta centralización facilita la detección y corrección de incidentes de enrutamiento web (controlando un único punto en lugar de depender de registros descentralizados).

Impacto en la Usabilidad y Adopción por el Usuario

- Usabilidad Mejorada:
  Se eliminó la necesidad de que los usuarios internos accedieran a las aplicaciones mediante la combinación de IP y Puerto. Se estandarizó el acceso a través de subdominios amigables y cifrados (HTTPS), lo que facilitó el uso frecuente de las herramientas internas.
- Adopción de Buenas Prácticas:
  Se mitigaron brechas de seguridad sin que fuese la función principal del investigador y se logró que el equipo técnico adoptara una perspectiva de seguridad más robusta y general, al comprender la magnitud de la exposición que se había normalizado.

Solución de Desafíos y Lecciones Aprendidas

El mayor desafío fue entender cómo funcionaba el balanceador de carga físico que teníamos en "caja negra". Este problema se solucionó comunicándose continuamente con el proveedor, el cual proporcionó una credencial de lectura. Esto sirvió para desarrollar nuevas configuraciones paralelas a las actuales que, eventualmente, las sustituirían, garantizando una transición lo más fluida posible.

La migración de páginas en producción que procesan transacciones críticas, como las de pago, fue otro desafío. Se resolvió creando subdominios alternativos y configuraciones paralelas para realizar pruebas separadas en caso de que el servicio se cayera en producción.

De este proyecto se aprendió como enseñanza profesional que la comunicación y un equipo que aprecia aprender e investigar son la clave para resolver problemas de manera rápida y flexible. Se implementó con éxito en un ambiente complejo y sin documentación previa, solucionando vulnerabilidades críticas de seguridad y facilitando el acceso a usuarios a través de subdominios legibles.

Conclusiones

La implementación de Nginx como proxy inverso permitió una mejora importante en la seguridad al mitigar significativamente la exposición de la infraestructura web. Al centralizar el tráfico de los servicios webs, se reconfiguró el 76% de los subdominios configurados en el balanceador FortiADC que apuntaban directamente a reglas del firewall y se cerró el 60% de los puertos que se encontraban sin uso en FortiGate, demostrando que una capa adicional de tipo proxy inverso es una estrategia efectiva para ocultar la infraestructura interna y reducir la superficie de ataque.

Asimismo, la solución transformó el modelo de gestión de TI optimizando la eficiencia operativa y devolviendo la autonomía al equipo técnico. La eliminación de la dependencia crítica del ISP para la publicación de servicios y la transición hacia la autogestión con Nginx Proxy Manager redujeron los tiempos de puesta en producción de nuevos servicios de días a cuestión de minutos, confirmando que la modernización de la arquitectura impacta directamente en la capacidad de respuesta del negocio.

Por otro lado, se garantizó la confidencialidad mediante un modelo de cifrado híbrido, logrando asegurar las comunicaciones cliente-servidor a través de la gestión automatizada de certificados con Let's Encrypt para el entorno público y una Entidad Certificadora (CA) interna basada en OpenSSL para la red local, cifrando así la totalidad del tráfico externo y gran parte del tráfico interno que operaba previamente en protocolo inseguro HTTP.

Finalmente, este proyecto evidenció que la reducción de costos y la simplificación operativa también son beneficios derivados de la correcta implementación de medidas de seguridad en la infraestructura tecnológica. Además, facilitó la gestión y el mantenimiento, lo que repercute directa y positivamente en el ámbito financiero, generando ahorros y evitando sobrecostos.

Recomendaciones

Se recomienda a la Gerencia de TI evolucionar la arquitectura actual hacia una de Alta Disponibilidad (HA) para asegurar la continuidad del negocio. Como Nginx se ha vuelto el único punto de entrada a los servicios críticos, es conveniente usar Kubernetes para replicar los nuevos contenedores y configurarlos para que mantengan el servicio de Nginx en caso de fallos.

Se sugiere a la Gerencia de TI mejorar la gobernanza de seguridad con auditorías regulares de registros y actualizaciones; mantener actualizadas las imágenes de los contenedores ayudará a defenderse de nuevas vulnerabilidades.

Se recomienda a la Gerencia de TI combinar la solución con un sistema de monitoreo como Prometheus + Grafana, herramientas de observabilidad que permitirán visualizar patrones de tráfico en tiempo real y recibir alertas tempranas ante problemas de latencia o errores, aumentando el control sobre la infraestructura.

Finalmente, se recomienda establecer un programa de capacitación permanente para el equipo de infraestructura y soporte, creando una cultura de "seguridad por diseño" para garantizar que cualquier despliegue o cambio futuro se conciba desde el principio con una arquitectura segura, evitando prácticas como el bypass del proxy inverso o el uso de protocolos inseguros.

Referencias Bibliográficas

Ackoff, R. L. (1971). Russell L. Ackoff. *Towards a System of Systems Concepts, 17*(11), 671. https://doi.org/10.1287/mnsc.17.11.661

Agencia Nacional Digital. (2022). *Política de Seguridad de la Información.* Agencia Nacional Digital. Obtenido de https://and.gov.co/sites/default/files/2022-09/Politica-de-Seguridad-de-la-Informacion-V2.pdf

Alpcan, T., & Başar, T. (2010). *Network Security: A Decision and Game-Theoretic Approach.* Cambridge University Press.

Anas, A., Elgamal, S., & Youssef, B. (2024). Survey on detecting and preventing web application broken access control attacks. *International Journal of Electrical and Computer Engineering (IJECE), 14*(1), 10. https://doi.org/10.11591/ijece.v14i1.pp772-781

AO Kaspersky Lab. (23 de agosto de 2023). *kaspersky Daily*. Obtenido de kaspersky Daily: https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/

Ashby, W. R. (1956). *An Introduction to Cybernetics.* Chapman & Hall.

Beer, S. (1981). *Brain of the Firm.* Allen Lane.

Bertalanffy, L. v. (1968). *General System Theory: Foundations, Development, Applications.* George Braziller, Incorporated.

Boettner, F. (2022). *Mejoras en la seguridad web del usuario mediante el uso de un proxy local.*

Boulding, K. E. (1956). General Systems Theory—The Skeleton of Science. *Management Science, 2*(3), 208. https://doi.org/10.1287/mnsc.2.3.197

Bravo Mendoza, M. (2020). *Sistema de pruebas para el realce del habla en VoIP sobre SIP.*

Chambi Llica, W., & Huaranca Rodríguez, R. (2017). *Sistema Integrado de Administración Online de la Empresa Compunegocios International S.A.C. Puno 2015.*

Cheema, A. (2024). *AI x Crypto Primer.* Obtenido de https://alexcheema.github.io/AIxCryptoPrimer.pdf

Córdova Solís, R. (2012). *Migración De Aplicaciones Colaborativas In House A Unentorno Virtual Basado En La Nube Para Mejorar El Servicio Del Espacio Colaborativo Integrado De Investigación En El Centro Internacional De La Papa.*

DAVALOS LOO, G. (2022). *Desafíos En El Soporte Tecnológico A Un Emprendimiento: El Caso Qempo.*

Dávila Morales, M., Ramírez Rodríguez, E., & Peña Espinoza, G. (2025). *Modelo Prolab: Solución Digital Inteligente "DestinarIA": Turismo Informado, Personalizado y Sostenible.*

Davis, P., & Jenkins, B. (2014). *Deterrence and Influence in Cyberspace.* RAND Corporation.

Devi, N., Dalal, S., Solanki, K., Dalal, S., Lilhore, U. K., Simaiya, S., & Nuristani, N. (2024). A systematic literature review for load balancing and task scheduling techniques in cloud computing. *Springer, 57*(276), 63. https://doi.org/https://doi.org/10.1007/s10462-024-10925-w

Elorza Gabilondo, D. (2024). *VeganMania: App para Controlar tu Alimentación.*

European Union Agency for Cybersecurity - ENISA. (2023). ENISA Threat Landscape 2023. *ENISA*, 1-161. https://doi.org/10.2824/782573

European Union Agency for Cybersecurity - ENISA. (2024). ENISA Threat Landscape 2024. *ENISA*, 1-131. https://doi.org/10.2824/0710888

F5 Inc. (2024). *NGINX One: One NGINX for all your apps and APIs.* F5 Inc. Obtenido de https://www.f5.com/pdf/solution-overview/f5-nginx-one-solution-overview.pdf

Gleick, J. (2011). *The Information: A History, a Theory, a Flood.* Pantheon Books.

Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2023). A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. *Springer, 66*(1), 440. https://doi.org/https://doi.org/10.1007/s12599-023-00830-x

Huaman Gamero, M. (2024). *Desarrollo de un sistema de call center integrando Asterisk ARI y ReactJS para optimizar el registro de llamadas en una empresa privada en Lima, 2024.*

Insights2TechInfo. (2023). *CSIM: Comprehensive guide to NGINX and its modules.* Insights2TechInfo. Obtenido de https://insights2techinfo.com/wp-content/uploads/2023/11/CSIM_Comprehensive-Guide-to-NGINX-and-its-Modules.pdf

Instituto Distrital de Gestión de Riesgos y Cambio Climático. (2025). *Plan Estratégico de Tecnologías de la Información y las Comunicaciones.* Instituto Distrital de Gestión de Riesgos y Cambio Climático - IDIGER. Obtenido de https://www.idiger.gov.co/documents/d/portal/plan-estrategico-de-tecnologias-de-la-informacion-y-las-comunicaciones

Instituto Nacional de Estadística e Informática - INEI. (2024). *Estadisticas de las Tecnologías de la Información y Comunicación en los hogares.* Instituto Nacional de Estadística e Informática - INEI. Obtenido de https://www.inei.gob.pe/media/MenuRecursivo/boletines/boletin_tic_iit24.pdf

Intel Corporation. (2021). *Nginx HTTPs with Crypto-NI tuning guide on 3rd generation Intel® Xeon® scalable processors.* Intel Corporation. Obtenido de https://cdrdv2-public.intel.com/686423/Nginx-HTTPs-with-Crypto-NI-Tuning-Guide-on-3rd-Generation-Intel-Xeon-Scalable-Processors.pdf

Kazemi, M. (2023). *Comparative analysis of NGINX and.* Alma Mater Studiorum - Università di Bologna. Obtenido de https://amslaurea.unibo.it/id/eprint/33906/1/Final-Mahsakazemi.pdf

Kramer, F., Starr, S., & Wentz, L. (2009). *Cyberpower and National Security.* Potomac Books.

Lacnic. (2023). *Efficient web connectivity: Offering dual-stack web access to an IPv6-only server farm using NGINX.* Lacnic. Obtenido de https://www.lacnic.net/innovaportal/file/6687/1/lacnic-efficient_web_connectivity.pdf

Larrea Cardozo, A. (2020). *Implementación De La Plataforma Tecnológica De Recomendación Como Caso De Estudio De Mejora En La Empresa Debug S.A.C.*

Lewis, E. E. (1996). *Introduction to Reliability Engineering.* John Wiley & Sons.

Lohani, D., Crispim-Junior, C., Barthélemy, Q., Bertrand, S., Robinault, L., & Rodet, L. T. (2022). Perimeter Intrusion Detection by Video Surveillance A Survey. *Sensors, 22*(3601), 28. https://doi.org/https://doi.org/10.3390/s22093601

Nash, J. (1951). Non-Cooperative Games. *Annals of Mathematics, 54*(2), 286–295.

Nayana, R., Harish, G., & Asharani, R. (2019). A comprehensive survey of modern network security techniques and challenges. *World Journal of Advanced Research and Reviews, 03*(02), 110. https://doi.org/https://doi.org/10.30574/wjarr.2019.3.2.0069

Nicolas-Plata, A., Gonzalez-Compean, J. L., & Sosa-Sosa, V. J. (2024). A service mesh approach to integrate processing patterns into microservices applications. *Springer, 27*(1), 7438. Obtenido de https://link.springer.com/article/10.1007/s10586-024-04342-5

Núñez Melgar Obregón, J. (2022). *Diseño E Implementación De Un Prototipo De "Digital Twin" Aplicado A Una Planta Psa Generadora De Oxígeno, Con El Uso De Internet De Las Cosas.*

Ochuba, N. A., Kisina, D., Owoade, S., Uzoka, A. C., Gbenle, T. P., & Adanigbo, O. S. (2021). Systematic Review of API Gateway Patterns for Scalable and Secure Application. *Journal of Frontiers in Multidisciplinary Research, 02*(01), 100. https://doi.org/https://doi.org/10.54660/.IJFMR.2021.2.1.94-100

O'Connor, P., & Kleyner, A. (2012). *Practical Reliability Engineering (5th ed.).* John Wiley & Sons.

OECD & IDB. (2024). 2023 OECD/IDB Digital Government Index of Latin America and the Caribbean. *OECD Public Governance Policy Papers*, 37. https://doi.org/10.1787/10b82c83-en

Pezoa Vergara, B. (2024). *Plataforma Para El Seguimiento De Vulnerabilidades En Aplicaciones Web.*

Prieto Vega , M. (2025). *Implantación de un proxy inverso en un entorno empresarial.*

Reese, W. (2008). Nginx: the High-Performance Web Server and Reverse Proxy. *Linux Journal*. Obtenido de https://www.linuxjournal.com/article/10108

Rivera, E. M. (2022). *Plan de seguridad y privacidad de la información para la Alcaldía de San José de Cúcuta, basado en el modelo de seguridad y privacidad del MinTIC.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/55076/emriverame.pdf?sequence=1&isAllowed=y

Rozó, O. (2024). *Propuesta de un sistema de información para la gestión de historias clínicas veterinarias, basado en tecnología Blockchain.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/63157/odrozog.pdf?sequence=1&isAllowed=y

Schelling, T. (1960). *The Strategy of Conflict.* Harvard University Press.

Secretaría Jurídica Distrital. (2025). *Plan Estratégico de Tecnologías de la Información - PETI.* Secretaría Jurídica Distrital. Obtenido de https://www.secretariajuridica.gov.co/sites/default/files/2025-02/Plan%20Estrat%C3%A9gico%20de%20Tecnolog%C3%ADas%20de%20la%20Informaci%C3%B3n%20-%20PETI_V6%2016-12-24%20VF.pdf

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal, 27*(3), 423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

Shannon, C., & Weaver, W. (1949). *The Mathematical Theory of Communication.* University of Illinois Press.

Srinath, L. (1991). *Reliability Engineering.* Affiliated East-West Press.

The World Bank. (2024). Cybersecurity Economics For Emerging Markets. *World Bank Group*, 132. https://doi.org/10.1596/978-1-4648-2120-2

Veeri, V. (2024). Modern Kubernetes Ingress Solutions: An In depth Comparison of Contour and Istio Architectures. *International Journal for Multidisciplinary Research, 6*(6), 12. Obtenido de https://www.ijfmr.com/papers/2024/6/30753.pdf

Von Neumann, J., & Morgenstern, O. (1944). *Theory of Games and Economic Behavior.* Princeton University Press.

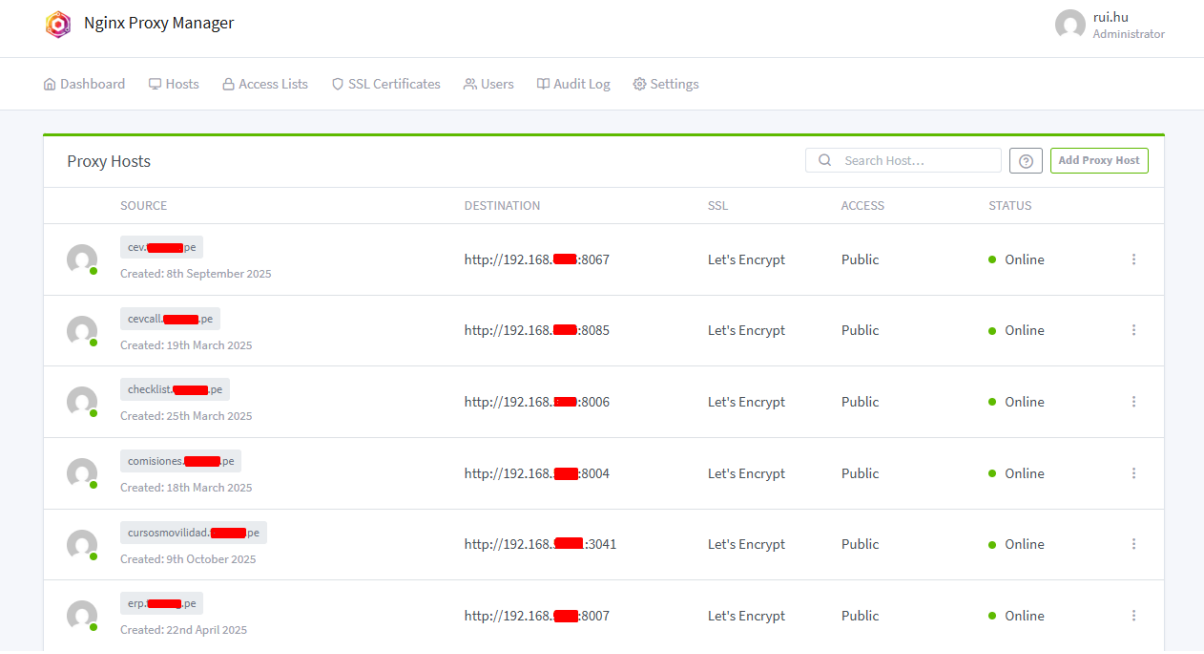
Wiener, N. (1948). *Cybernetics: Or Control and Communication in the Animal and the Machine.* The MIT Press.

Younus, Z., & Alanezi, M. (2023). A Survey on Network Security Monitoring: Tools and Functionalities. *Mustansiriyah Journal of Pure and Applied Sciences, 1*(2), 86. https://doi.org/https://doi.org/10.47831/mjpas.v1i2.33

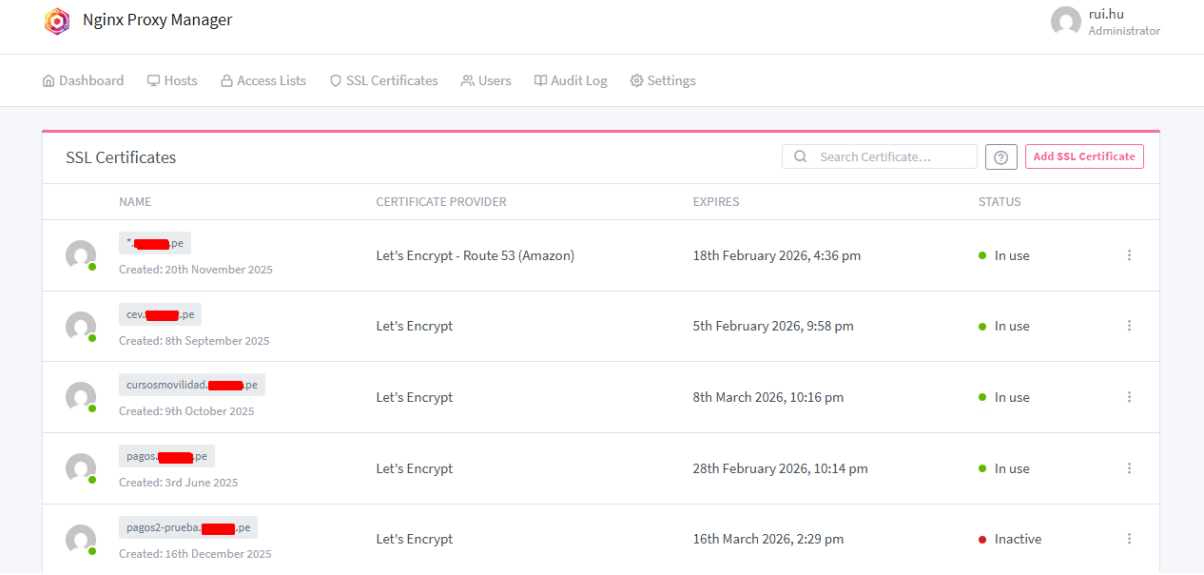
Anexos

Anexo 1: Interfaz gráfica de NPM

Configuración de subdominios

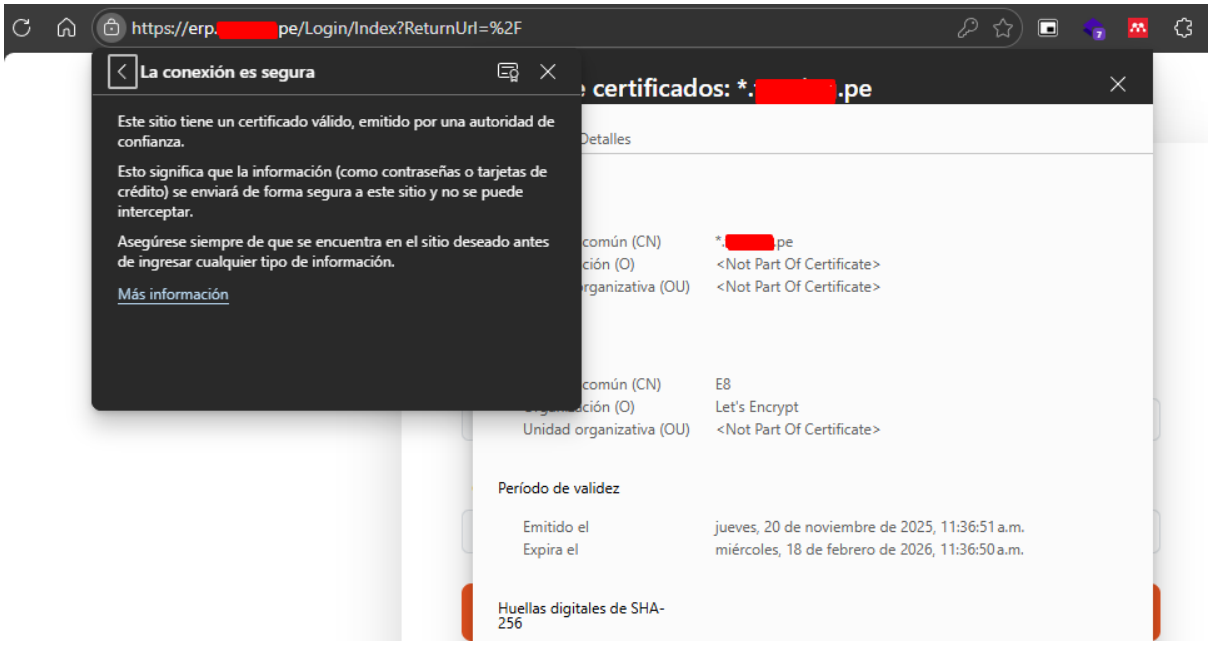


Configuración de certificados SSL

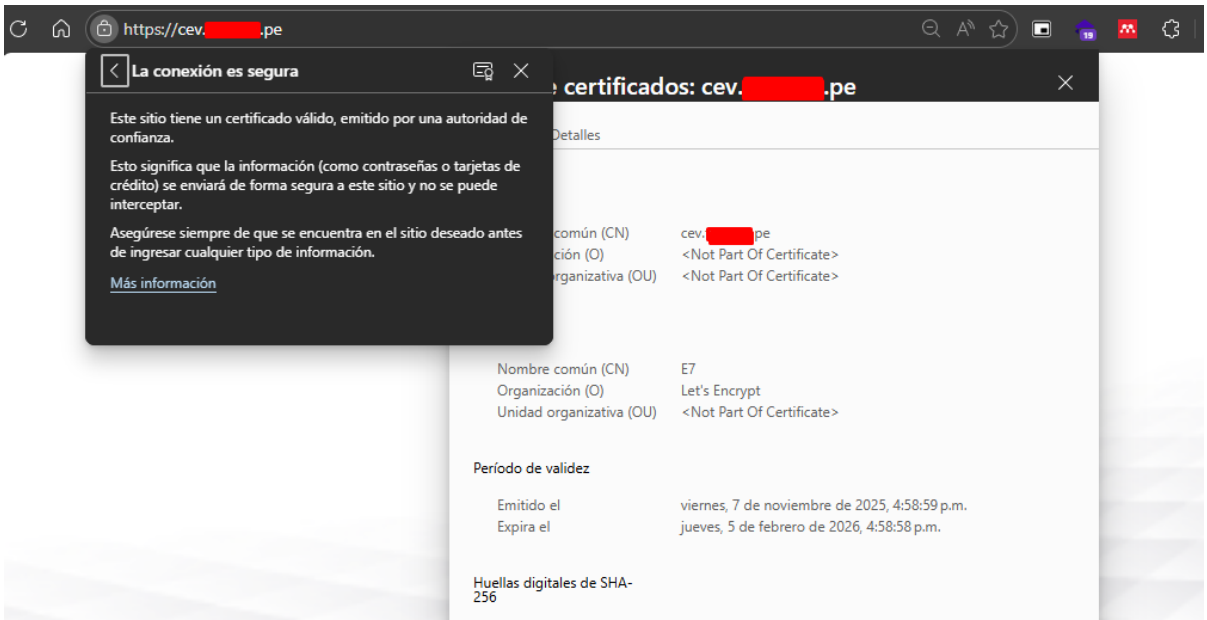


Anexo 2: Conexión HTTPS

Certificado SSL (wildcard) emitido por Let’s Encrypt



Certificado SSL (Single-Domain) emitido por Let’s Encrypt



Anexo 3: Configuración de contenedores Docker

Contenedor NPM (Nginx)

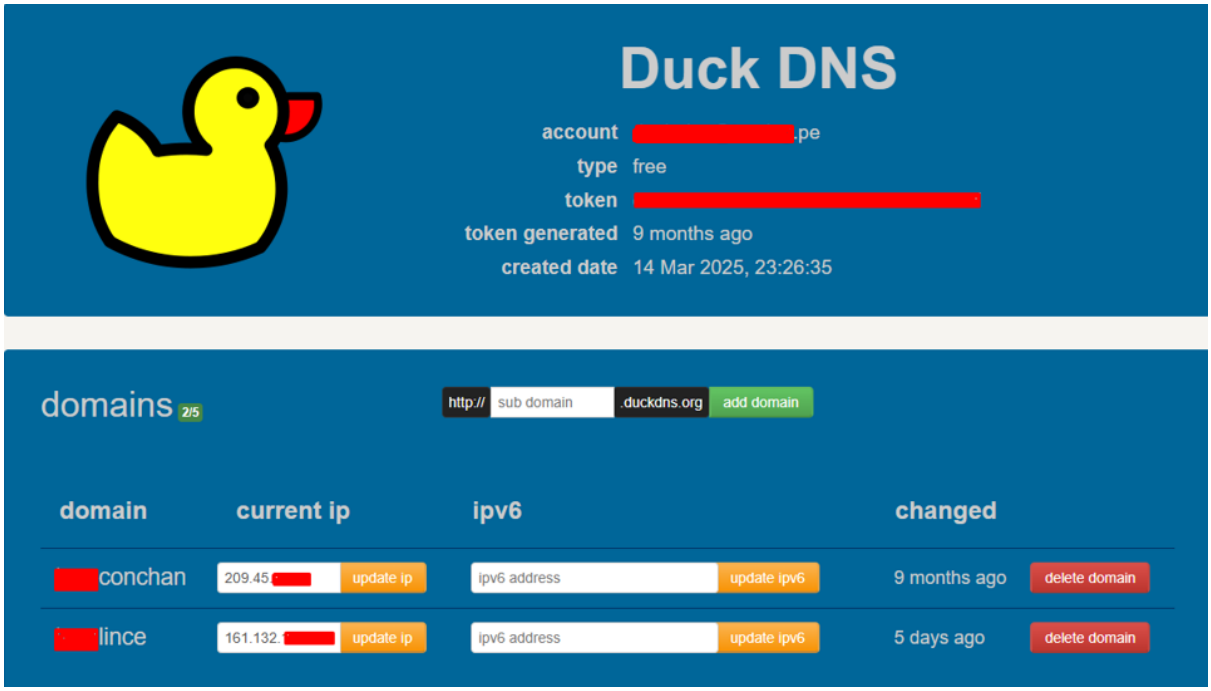
```yaml
networks:
  net_nginx_npm:
    driver: bridge

services:
  nginx_npm:
    container_name: nginx_npm
    image: jc21/nginx-proxy-manager:2.12.6
    ports:
      - '80:80' # Escucha http
      - '81:81' # Interfaz grafica
      - '443:443' # Escucha https
    volumes:
      - /etc/localtime:/etc/localtime:ro # Sincroniza la hora con el servidor
      - ./nginx/npm/data:/data
      - ./nginx/npm/letsencrypt:/etc/letsencrypt
    restart: unless-stopped
    mem_limit: 4g
    cpus: 3.0
    networks:
      - net_nginx_npm
```

Contenedor DuckDNS

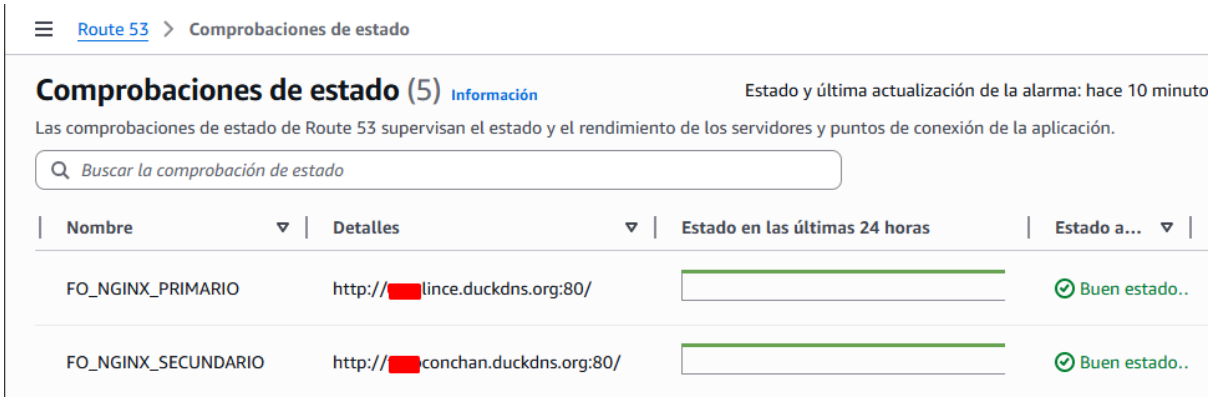
```yaml
networks:
  net_duckdns:
    driver: bridge

services:
  duckdnslince:
    image: lscr.io/linuxserver/duckdns:d1f23212-ls63
    container_name: duckdns
    environment:
      - SUBDOMAINS=lince
      - TOKEN=*ADD_YOUR_TOKEN*
      - LOG_FILE=true
    volumes:
      - ./duckdns/config:/config
    restart: unless-stopped
    cpus: 0.5
    networks:
      - net_duckdns
```

Anexo 4: Configuración High Availability

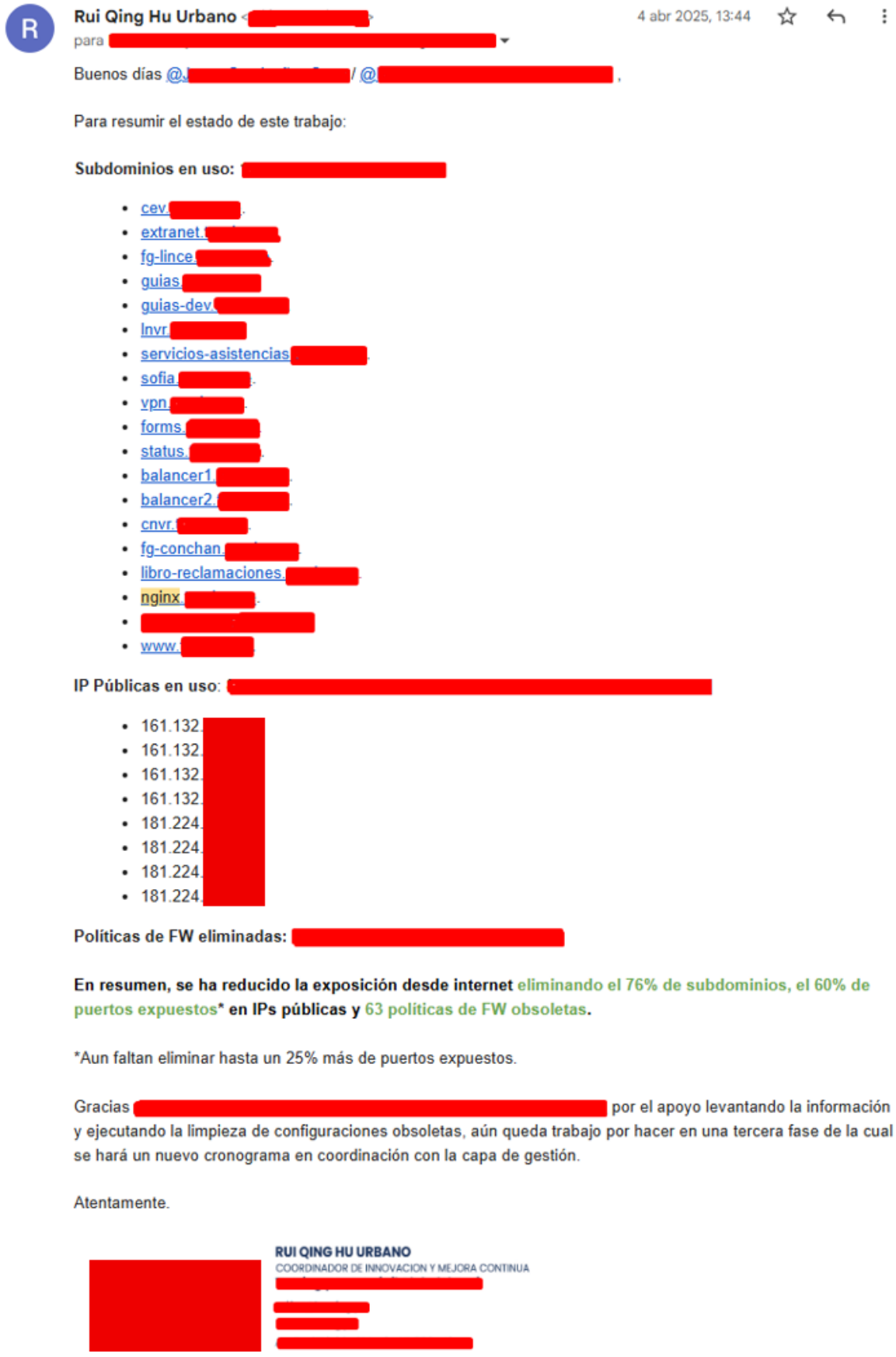
DNS Dinámico gratuito



Failover en AWS Route53



Anexo 5: Correo informativo para el Gerente de TI



Rui Qing Hu Urbano <[redacted]>
4 abr 2025, 13:44
para [redacted]

Buenos días @[redacted] / @[redacted],

Para resumir el estado de este trabajo:

Subdominios en uso: [redacted]

- cev.[redacted].
- extranet.[redacted].
- fg-lince.[redacted].
- guias.[redacted]
- guias-dev.[redacted]
- lnvr.[redacted]
- servicios-asistencias.[redacted].
- sofia.[redacted].
- vpn.[redacted].
- forms.[redacted]
- status.[redacted].
- balancer1.[redacted].
- balancer2.[redacted].
- cnvr.[redacted].
- fg-conchan.[redacted].
- libro-reclamaciones.[redacted].
- nginx.[redacted].
- [redacted]
- www.[redacted]

IP Públicas en uso: [redacted]

- 161.132.[redacted]
- 161.132.[redacted]
- 161.132.[redacted]
- 161.132.[redacted]
- 181.224.[redacted]
- 181.224.[redacted]
- 181.224.[redacted]
- 181.224.[redacted]

Políticas de FW eliminadas: [redacted]

En resumen, se ha reducido la exposición desde internet eliminando el 76% de subdominios, el 60% de puertos expuestos* **en IPs públicas y** 63 políticas de FW obsoletas**.**

*Aun faltan eliminar hasta un 25% más de puertos expuestos.

Gracias [redacted] por el apoyo levantando la información y ejecutando la limpieza de configuraciones obsoletas, aún queda trabajo por hacer en una tercera fase de la cual se hará un nuevo cronograma en coordinación con la capa de gestión.

Atentamente.

[redacted]
RUI QING HU URBANO
COORDINADOR DE INNOVACION Y MEJORA CONTINUA
[redacted]

Anexo 6: Correo de reconocimiento del Gerente de TI

Henrry Eduardo Gomez Barbaran [redacted] 4 abr 2025, 13:59

para mí, [redacted]

Equipo,

¡Felicitaciones por este gran avance!

Quiero reconocer el esfuerzo y compromiso de todos los involucrados en este importante trabajo de ordenamiento y fortalecimiento de nuestra infraestructura. Reducir el 76% de subdominios, el 60% de puertos expuestos y eliminar 63 políticas de firewall obsoletas no solo demuestra un trabajo técnico, sino también una clara orientación a la mejora continua, la seguridad y la eficiencia operativa.

Gracias a [redacted] por su ejecución en campo, y a todo el equipo por el trabajo coordinado. Este es un claro ejemplo de cómo el trabajo colaborativo y el enfoque a objetivos concretos generan resultados que aportan valor al negocio.

Aún queda camino por recorrer con la siguiente fase, pero lo logrado hasta ahora marca una base sólida sobre la cual seguiremos construyendo.

¡Vamos por más!

saludos,

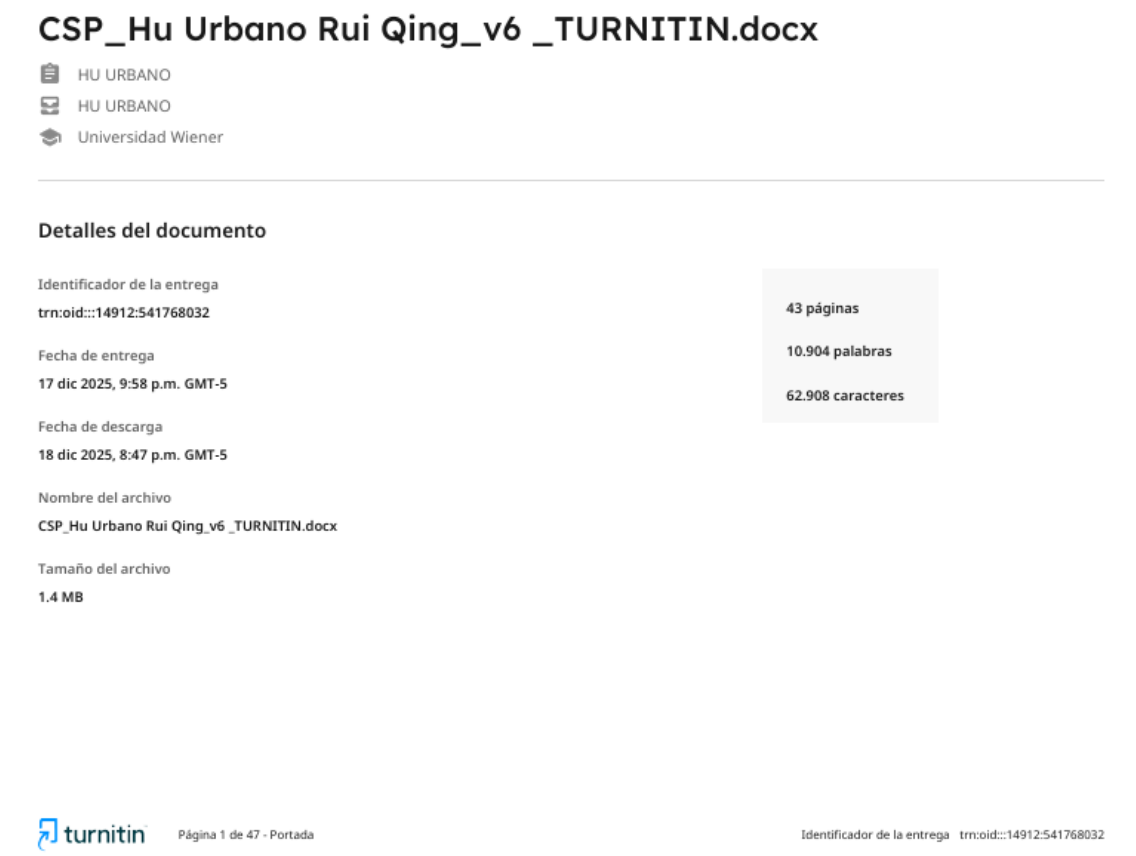
[redacted]

HENRRY EDUARDO GOMEZ BARBARAN
GERENTE DE TECNOLOGÍA DE INFORMACIÓN

[redacted]

Empresa certificada por:
AENOR

Anexo 7: Informe de similitud Turnitin



CSP_Hu Urbano Rui Qing_v6 _TURNITIN.docx

HU URBANO

HU URBANO

Universidad Wiener

Detalles del documento

Identificador de la entrega
trn:oid:::14912:541768032

Fecha de entrega
17 dic 2025, 9:58 p.m. GMT-5

Fecha de descarga
18 dic 2025, 8:47 p.m. GMT-5

Nombre del archivo
CSP_Hu Urbano Rui Qing_v6 _TURNITIN.docx

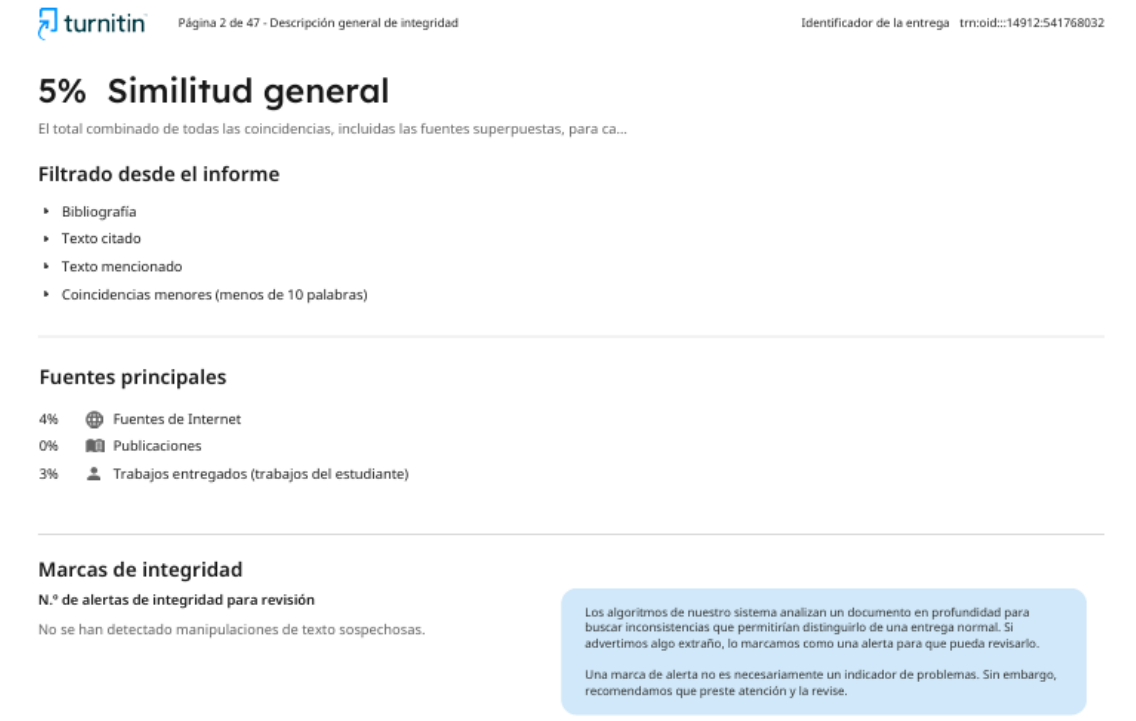
Tamaño del archivo
1.4 MB

43 páginas

10.904 palabras

62.908 caracteres

turnitin Página 1 de 47 - Portada Identificador de la entrega trn:oid:::14912:541768032



turnitin Página 2 de 47 - Descripción general de integridad Identificador de la entrega trn:oid:::14912:541768032

5% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 10 palabras)

Fuentes principales

4% Fuentes de Internet
0% Publicaciones
3% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Anexo 8: Constancia de autorización de investigación

TOURING
AUTOMÓVIL CLUB DEL PERÚ

MIEMBRO DE FIA

CONSTANCIA DE AUTORIZACIÓN

Yo, Henrry Eduardo Gómez Barbaran, identificado con DNI N.° 44131491, en mi calidad de Gerente de TI de la Empresa Touring y Automóvil Club del Perú, con RUC 20100091896, ubicado en Av. Las Palmeras 268, La Molina-Lima, otorgo la siguiente autorización:

Al señor Rui Qing Hu Urbano, identificado con DNI N.° 77435349 de la Carrera Profesional de Ingeniería de Sistemas e Informática de la Universidad Privada Norbert Wiener que realiza la investigación titulada "Implementación de Nginx como proxy inverso para mejorar la seguridad de la infraestructura web en una empresa de servicios, Lima 2025", para que se le proporcione la información necesaria y se autorice la difusión de los resultados obtenidos, con la finalidad de desarrollar su investigación con fines académicos.

TD-225-11018

Indicar si el representante autoriza:

(X) Mantener en reserva el nombre o cualquier distintivo de la institución o

( ) Mencionar el nombre de la institución.

Lima, 25 de Julio de 2025

GERENTE DE TECNOLOGÍA DE INFORMACIÓN
V° B°
HENRRY GÓMEZ BARBARAN
T.A.C.P.

Henrry Eduardo Gómez Barbaran

AENOR ER Empresa Registrada ISO 9001
ER-0877/2008
Norma de calidad ISO 9001:2015

AENOR ER Seguridad Vial ISO 39001
SV-2018/0018
Norma de Seguridad Vial 39001:2012

Av. Trinidad Morán 698, Lince - Lima
T. (511) 614-9999 - Touring.pe

4% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 10 palabras)

Fuentes principales

4%	Fuentes de Internet
0%	Publicaciones
3%	Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Fuentes principales

4% Fuentes de Internet
0% Publicaciones
3% Trabajos entregados (trabajos del estudiante)

Fuentes principales

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1 Internet
repositorio.uwiener.edu.pe 2%

2 Trabajos entregados
uwiener on 2023-09-11 <1%

3 Trabajos entregados
Universidad Internacional de la Rioja on 2024-07-22 <1%

4 Trabajos entregados
uwiener on 2024-05-21 <1%

5 Trabajos entregados
Universidad Nacional Abierta y a Distancia, UNAD,UNAD on 2025-12-05 <1%

6 Internet
www.datosabiertos.gob.pe <1%

7 Internet
www.coursehero.com <1%

8 Trabajos entregados
Submitted on 1691793895511 <1%

9 Internet
www.universiaargentina.com.ar <1%

10 Trabajos entregados
Universidad Cesar Vallejo on 2025-12-04 <1%

11 Trabajos entregados
Universidad Wiener on 2025-12-18 <1%