UPN
UNIVERSIDAD PRIVADA DEL NORTE

# FACULTAD DE INGENIERÍA

**Carrera de Ingeniería de Sistemas Computacionales**

# “IMPLEMENTACIÓN DE UN SISTEMA AUTOMATIZADO DE MONITOREO Y ANÁLISIS DE ACCESOS A SERVIDORES EN LA EMPRESA ORION PERU S.A.C.”

**Trabajo de suficiencia profesional para optar al título profesional de:**

**Ingeniero de Sistemas Computacionales**


Autores:

Jose Alexander Leiva Alcedo

Alvaro Rodrigo Torres Cavero

**Asesor:**

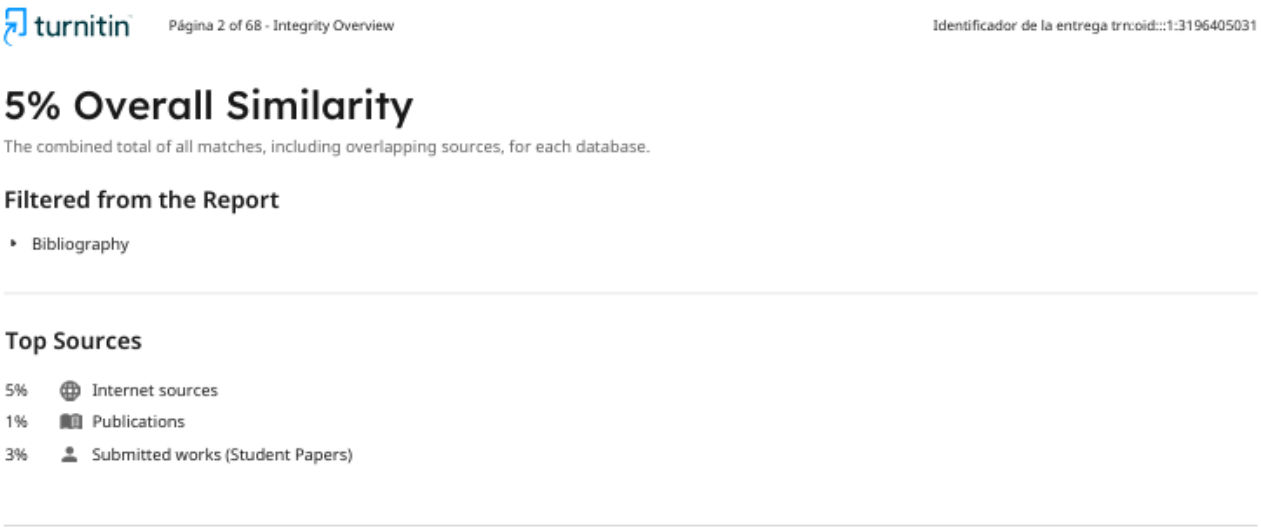
Mg. Lic. Roberto Elias Montero Flores

**0000-0003-2519-3083**


Lima - **Perú**

**2025**

# Informe de Similitud



turnitin Página 2 of 68 - Integrity Overview Identificador de la entrega trn:oid:::1:3196405031

## 5% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

### Filtered from the Report

- Bibliography

### Top Sources

5% Internet sources
1% Publications
3% Submitted works (Student Papers)

## Dedicatoria

Dedicamos este trabajo a nuestras familias, por su apoyo incondicional y por ser nuestra mayor fuente de motivación a lo largo de nuestra formación profesional. También a nuestros compañeros y amigos, quienes nos acompañaron en este camino, brindándonos su apoyo y compartiendo momentos de aprendizaje y superación.

## Agradecimiento

Agradecemos a ORION PERU S.A.C. por brindarnos la oportunidad de desarrollar este proyecto, permitiéndonos aplicar y fortalecer nuestros conocimientos en un entorno profesional real. Asimismo, expresamos nuestro profundo agradecimiento a nuestro asesor del taller, Roberto, por su dedicación y guía durante todo el proceso, brindándonos valiosas recomendaciones que fueron fundamentales para la culminación de este trabajo. Finalmente, a nuestro equipo de trabajo, cuya colaboración y esfuerzo hicieron posible este logro.

## Tabla de contenido

Informe de Similitud ..... 2

Dedicatoria ..... 3

Agradecimiento ..... 4

Tabla de contenido ..... 5

Índice de tablas ..... 7

Índice de Figuras ..... 8

RESUMEN EJECUTIVO ..... 9

CAPÍTULO I. INTRODUCCIÓN ..... 10

1.1. Información de la Empresa ..... 11
1.1.1 Datos de la Empresa ..... 11
1.1.2 Misión ..... 11
1.1.3 Visión ..... 11
1.1.4 Valores ..... 11
1.1.5 Logotipo ..... 12
1.1.6 Organigrama ..... 12

CAPÍTULO II. MARCO TEÓRICO ..... 14

2.1. Fundamento de la Ciberseguridad ..... 14
2.2. Análisis de IPs Maliciosas ..... 14
2.3. Herramientas de Automatización ..... 15
2.3.1. Uipath ..... 15
2.3.2. Kibana ..... 16
2.3.3. Elasticsearch ..... 17
2.3.4. Webhooks ..... 17
2.4. Metodologías Ágiles ..... 18
2.5. Software de programación ..... 19

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA ..... 20

3.1. Descripción del proyecto desarrollado ..... 22

CAPÍTULO IV. RESULTADOS ..... 53

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES..... 58

REFERENCIAS ..... 62

ANEXOS ..... 65

**Índice de tablas**

## Índice de tablas

Tabla 1 ..... 26

Tabla 2 ..... 27

Tabla 3 ..... 35

Tabla 4 ..... 35

Tabla 5 ..... 36

Tabla 6 ..... 41

Tabla 7 ..... 42

Tabla 7 ..... 43

Tabla 8 ..... 45

Tabla 9 ..... 46

Tabla 10 ..... 47

Tabla 11 ..... 49

Tabla 12 ..... 50

Tabla 13 ..... 53

Tabla 14 ..... 54

Tabla 15 ..... 56

Tabla 16 ..... 57

**Índice de Figuras**

## Índice de Figuras

Figura 1 ..... 12

Figura 2 ..... 12

Figura 3 ..... 42

Figura 4 ..... 43

Figura 5 ..... 45

Figura 6 ..... 45

Figura 7 ..... 46

Figura 8 ..... 46

Figura 9 ..... 48

Figura 10 ..... 48

Figura 11 ..... 51

Figura 12 ..... 51

Figura 13 ..... 52

Figura 14 ..... 57

## RESUMEN EJECUTIVO

El presente trabajo de suficiencia profesional se desarrolló en ORION PERU S.A.C., una empresa dedicada a la consultoría en Tecnologías de la Información (TI), especializada en transformación digital, infraestructura en la nube y ciberseguridad. Durante la experiencia laboral, se identificó una deficiencia crítica en el monitoreo de intrusiones en servidores, ya que este proceso se realizaba manualmente, lo que ocasionaba demoras en la detección de amenazas, errores en la clasificación de direcciones IP sospechosas y una carga operativa excesiva para el equipo de seguridad informática.

Para abordar esta problemática, se diseñó e implementó un sistema automatizado de monitoreo de intrusiones, empleando herramientas como UiPath, Kibana, AppScript y Google Sheets, además de aplicar la metodología ágil Scrum para gestionar el desarrollo del proyecto. Gracias a esta solución, se optimizó la recopilación y el análisis de datos, reduciendo el tiempo de procesamiento de 55 a 5 minutos y mejorando la precisión en la identificación de accesos no autorizados.

Las competencias profesionales aplicadas incluyeron automatización de procesos, gestión de infraestructuras tecnológicas y análisis de grandes volúmenes de datos. En conclusión, el proyecto fortaleció la seguridad operativa de la empresa, minimizó la necesidad de intervención manual y mejoró significativamente la capacidad de respuesta ante incidentes cibernéticos.

# CAPÍTULO I. INTRODUCCIÓN

El presente trabajo de suficiencia profesional se llevó a cabo en la empresa ORION PERU S.A.C., dedicada a la consultoría en el sector de Tecnologías de la Información (TI). Este sector se especializa en el desarrollo e implementación de soluciones tecnológicas orientadas a la transformación digital, modernización de infraestructuras en la nube, productividad digital, inteligencia artificial (IA) y ciberseguridad. En el contexto actual, el sector de TI en Perú ha experimentado un crecimiento significativo, impulsado por la digitalización de las empresas y la necesidad de fortalecer sus sistemas de seguridad. Según un informe de IDC, uno de los cambios más significativos en TI es la expansión de la entrega de tecnología como servicio: software, hardware y servicios, logrando que sea más necesario el uso de herramientas de control avanzadas que permitan mejorar la resiliencia de negocios digitales, reduciendo la sobrecarga operativa. En este marco, ORION PERU S.A.C. ofrece servicios especializados como consultoría en transformación digital, implementación de infraestructuras seguras y análisis de datos mediante herramientas avanzadas como Kibana y Elasticsearch, lo que permite mejorar la gestión de riesgos y la protección de la información empresarial.

El presente trabajo de suficiencia profesional se enfoca en la mejora del proceso de monitoreo, análisis y notificación de posibles intrusiones en los servidores de la empresa. Actualmente, ORION PERU S.A.C. realiza la descarga y validación de direcciones IP tres veces al día con el fin de detectar posibles amenazas cibernéticas. Este procedimiento implica la recopilación de datos a través de Kibana, una plataforma de análisis que permite visualizar el tráfico en los servidores monitoreados, seguida de la verificación de la reputación de cada IPv4 en la web para identificar accesos no autorizados. En caso de detectar una amenaza, se notifica al usuario final para que tome las medidas pertinentes. No obstante, este proceso se realiza manualmente, lo que lo hace susceptible a errores y demanda un tiempo considerable, afectando la capacidad de respuesta ante incidentes de seguridad.

La presente investigación surge ante la necesidad de automatizar este proceso, con el objetivo de mejorar el tiempo de ejecución y ampliar el análisis de intrusiones en los servidores. La solución propuesta busca optimizar la detección de accesos no autorizados mediante un sistema automatizado que reduzca la intervención manual, agilice la identificación de amenazas y minimice el margen de error. Con esta automatización, se espera fortalecer la seguridad informática de la empresa, mejorando la eficiencia operativa y alineándose con las tendencias actuales del sector TI en ciberseguridad.

## 1.1. Información de la Empresa

### 1.1.1 Datos de la Empresa

- Año de Fundación: 2000
- Ubicación: Cal.Los Alcanfores Nro. 140 Int. 701 Urb. Cercado De Miraflores (Oficina 701 7mo Piso) Lima - Lima - Miraflores
- Razón Social: ORION PERU S.A.C
- Actividad Económica: Consultoría De Informática Y Gestión De Instalaciones Informáticas
- WEB: https://orion.global/

### 1.1.2 Misión

Nuestro propósito es “evolucionar las capacidades de personas, organizaciones y la sociedad en la era digital”.

### 1.1.3 Visión

Orión es el partner digital que resuelve los desafíos críticos del negocio, a través de servicios y soluciones contables y de vanguardia.

### 1.1.4 Valores

- Empieza por la Integridad
- Eleva los Estándares
- Trabaja en equipo, siempre

- Impulsa el Optimismo
- Adáptate y Evoluciona

### 1.1.5 Logotipo

La Figura 1 muestra el logotipo oficial de Orión Perú, un símbolo distintivo que representa a la empresa.

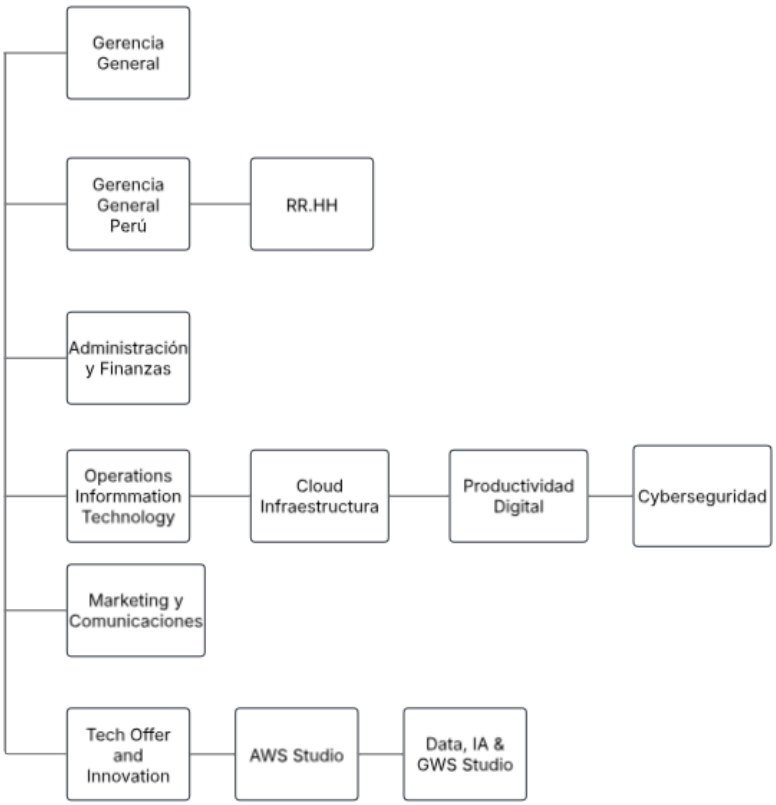
**Figura 1**

*Logotipo Orión Perú*


### 1.1.6 Organigrama

**Figura 2**

Organigrama


Gerencia General
Gerencia General Perú
RR.HH
Administración y Finanzas
Operations Informmation Technology
Cloud Infraestructura
Productividad Digital
Cyberseguridad
Marketing y Comunicaciones
Tech Offer and Innovation
AWS Studio
Data, IA & GWS Studio

# CAPÍTULO II. MARCO TEÓRICO

## 2.1. Fundamento de la Ciberseguridad

Según Sanchez Garcia et al. (2024), “la etapa de monitoreo y revisión de riesgos de ciberseguridad incluye el monitoreo regular de los riesgos y contramedidas definidas en las etapas de evaluación y tratamiento de riesgos.”, Por lo mencionado, una de las etapas en la ciberseguridad es el monitoreo constante y continuo la cual es requerida en toda la vida ya sea de una gran empresa o de una pequeña empresa que se está realizando. Asimismo, Clara-Luz (2022) indica lo siguiente, “los ciber incidentes son aquellos que causan interrupción, acceso no autorizado o cualquier falla que afecte a las redes servicios, equipos e instalaciones asociados o vinculados a activos de tecnologías de la información y comunicaciones, pudiendo o no tener un origen en un ciberataque.”

## 2.2. Análisis de IPs Maliciosas

El análisis de direcciones IP maliciosas es una tarea esencial en ciberseguridad, ya que permite detectar y bloquear actividades sospechosas en la red, salvaguardando sistemas y datos sensibles. Como menciona Wang et al.(2024) la detección de direcciones de dudosa procedencia es la primera línea de defensa contra los atacantes cibernéticos que puedan inyectar phishing, botnets, spam, malware, etc. Para una mayor seguridad se hace uso de listas negras así como indica explica Imperva(sf), “La creación de listas negras de direcciones IP es un método que se utiliza para filtrar direcciones IP ilegítimas o maliciosas que impiden el acceso a sus redes . Las listas negras son listas que contienen rangos de direcciones IP individuales que desea bloquear. Puede utilizar estas listas en combinación con

firewalls, sistemas de prevención de intrusiones (IPS) y otras herramientas de filtrado de tráfico.”

## 2.3. Herramientas de Automatización

Las herramientas de automatización han revolucionado la gestión de infraestructuras tecnológicas al minimizar la intervención manual y mejorar la eficiencia en procesos clave, como el monitoreo de servidores y la gestión de accesos. Según Montoya et al.(2024), menciona que los monitoreos constantes en la vida de la empresa se llevaban a cabo de una mejor manera usando herramientas de automatización como el RPA(Automatización Robótica de Procesos). Para hacer uso de forma básica de las herramientas RPA no es necesario tener un conocimiento profundo en la programación, asi como menciona IBM (sf.) “La RPA no requiere necesariamente la configuración de un desarrollador; las características de arrastrar y soltar en las interfaces de usuario facilitan la incorporación de personal no técnico.” Y en una empresa en crecimiento ayudaría en gran medida ya que no sería necesario un trabajador especializado en esta área.

### 2.3.1. Uipath

Uipath es una de las herramientas más populares en el campo de la Automatización Robótica de Procesos (RPA, por sus siglas en inglés), ya que facilita la automatización de tareas repetitivas al imitar la interacción humana con los sistemas informáticos y como explica Ribeiro et al.(2021), “las herramientas RPA corresponden a un conjunto de técnicas que tienen como objetivo mejorar el trabajo reduciendo el número de tareas repetitivas, automatizándolas”,

### 2.3.2 Google Apps Script

Google Apps Script es una plataforma de desarrollo en la nube diseñada para automatizar tareas y crear aplicaciones empresariales dentro del entorno de Google Workspace. Según la documentación oficial de Google (2024), “es una plataforma de desarrollo de aplicaciones rápida que permite crear aplicaciones empresariales con rapidez y facilidad que se integran con Google Workspace”. Pero esto tambien puede traer consecuencias asi como explica Kissflow (sf.) “Apps Script es suficiente para integraciones de flujo de datos simples, pero ni siquiera es de gran ayuda cuando se trata de crear un flujo de trabajo centrado en el ser humano.” Es por ello que para llegar a un producto final de un proyecto es necesaria la implementación de herramientas adicionales fuera del Appscript.

### 2.3.2. Kibana

Kibana es una herramienta que facilita la exploración y análisis de datos dentro de Elastic Stack, permitiendo a los usuarios buscar, visualizar y proteger la información de manera eficiente. Además, ofrece diversas opciones de representación gráfica, como mapas e indicadores, para facilitar la interpretación de datos. También permite la gestión y monitoreo del estado del clúster, así como el control de acceso de los usuarios a diferentes funciones (Elastic, s.f.). La herramienta Kibana se desprende del acrónimo ELK, como indica AWS (s.f.) “La pila ELK es un acrónimo utilizado para describir una pila que se compone de tres proyectos conocidos: Elasticsearch, Logstash y Kibana. A menudo conocida como Elasticsearch, la pila ELK le ofrece la posibilidad de agregar registros de todos sus sistemas y aplicaciones, analizar estos registros y crear visualizaciones para la supervisión de las aplicaciones y la infraestructura, una solución de problemas más rápida, análisis de seguridad y mucho más.” Como se explica Kibana se puede

integrar con más herramientas para un mayor seguridad y monitoreo de sus equipos.

### 2.3.3. Elasticsearch

Elasticsearch es una solución altamente escalable que permite indexar y buscar grandes volúmenes de datos en tiempo real, facilitando su integración con diversas aplicaciones de análisis. Segun Amazon Web Services. (s.f.). “Elasticsearch es un motor de búsqueda y análisis distribuido basado en Apache Lucene. Desde su lanzamiento en 2010, Elasticsearch se ha convertido rápidamente en el motor de búsqueda más popular y se utiliza habitualmente para análisis de registros, búsqueda de texto completo, inteligencia de seguridad, análisis empresarial y casos de uso de inteligencia operativa”. Debido a su gran integración con varias herramientas también se puede usar en el sector salud como lo explica LNM Sales et.al. (2024), se hizo uso de esta herramienta para poder realizar el análisis de sangre de una gran cantidad de voluntarios para procesar la data y generar los resultados finales.

### 2.3.4. Webhooks

Un webhook es una comunicación que facilita la integración y automatización de procesos al enviar notificaciones en tiempo real cuando se produce un evento específico en una aplicación. Según Red Hat (2024), "Un webhook consiste en una comunicación ligera basada en eventos que envía datos automáticamente entre las aplicaciones a través del protocolo HTTP. Los webhooks, que se activan por eventos específicos, automatizan la comunicación entre las interfaces de programación de aplicaciones (API) y se pueden utilizar para ejecutar flujos de trabajo, como en los entornos de GitOps." Complementando esta descripción, como

indica GitHub (s.f.), “Los webhooks permiten suscribirse a eventos que se producen en un sistema de software y recibir automáticamente una entrega de datos al servidor cada vez que se produzcan esos eventos.” Para poder realizar las pruebas correspondientes se hace uso de herramientas para poder visualizar si los webhooks envían o reciben los datos como se esperan.

## 2.4. Metodologías Ágiles

Las metodologías ágiles hoy en día nos ayudan a como se encaminara un proyecto, como lo explica Atlassian(s.f.), “La metodología ágil es un concepto de gestión de proyectos que implica dividir el proyecto en fases y hace hincapié en la colaboración y la mejora continuas. Los equipos siguen un ciclo de planificación, ejecución y evaluación.” Asimismo uno de los puntos fuertes de usar metodologías ágiles para Filippo Lanfranchi (s.f.), “Además, la importancia de la metodología ágil radica en su capacidad para fomentar la innovación y gestionar la incertidumbre de forma eficiente. Permite a los equipos responder con prontitud a los cambios del mercado o a las oportunidades emergentes adaptando rápidamente sus procesos de desarrollo.”

### 2.4.1. SCRUM

Scrum es una metodología ágil muy utilizada en la gestión y desarrollo de proyectos, particularmente en el sector del software. Su estructura se apoya en ciclos iterativos llamados sprints, en los cuales los equipos se enfocan en objetivos concretos para optimizar tiempos, mejorar la flexibilidad y asegurar una entrega constante de valor. Según Muñoz et al.(2024) “Scrum es una de las metodologías ágiles más ampliamente adoptadas en el desarrollo de software, ha experimentado

un notable aumento en su uso en los últimos años. Se basa en el trabajo colaborativo entre los miembros del equipo para lograr los objetivos del proyecto, puesto que, se espera que los miembros del equipo trabajen juntos de forma colaborativa para lograr estos objetivos." Asimismo, como indica Alnanih R.(2024), "Scrum, a diferencia de las metodologías tradicionales, ofrece un enfoque ágil, iterativo y centrado en el cliente para la ingeniería de software. Hace hincapié en la participación frecuente del cliente, la adaptabilidad a los requisitos cambiantes y la mitigación temprana de riesgos, fomentando un entorno de desarrollo dinámico y receptivo."

## 2.5. Software de programación

### 2.5.1. Python

Python es un lenguaje de programación de alto nivel, destacado por su facilidad de uso y su flexibilidad en múltiples aplicaciones tecnológicas. Según Amazon Web Services. (s.f.). "Python es un lenguaje de programación ampliamente utilizado en las aplicaciones web, el desarrollo de software, la ciencia de datos y el machine learning (ML). Los desarrolladores utilizan Python porque es eficiente y fácil de aprender, además de que se puede ejecutar en muchas plataformas diferentes. El software Python se puede descargar gratis, se integra bien a todos los tipos de sistemas y aumenta la velocidad del desarrollo." Este lenguaje a ser de codigo abierto permite a los usuarios poder crear sus propias bibliotecas para poder implementarlas en diferentes trabajos, como indica Garrido-Labrador J. et. al(2025), "SSLearn es una biblioteca de código abierto basada en Python que promueve el aprendizaje semisupervisado con un enfoque en algoritmos de envoltura y clasificación de conjuntos restringidos, un paradigma novedoso.

Fomenta la innovación al permitir que los investigadores modifiquen métodos o creen otros nuevos, lo que facilita el acceso a algoritmos de última generación y estudios comparativos.”

## CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA

Ingresamos a Orion Perú a través de un contrato de prácticas profesionales, luego de superar un exigente proceso de selección. Desde el inicio, fuimos asignados al área de automatización, donde realizamos estudios y prácticas enfocadas en la optimización de pequeños procesos mediante Apps Script.

Una vez adquiridos los conocimientos esenciales, comenzamos a identificar procesos susceptibles de automatización y ampliamos nuestro aprendizaje con herramientas como Terraform y Ansible. Para ello, mantuvimos reuniones con los responsables de cada área con el fin de realizar un análisis detallado antes de desarrollar las soluciones.

Posteriormente, llevamos a cabo diversas automatizaciones, las cuales fueron sometidas a revisión y validación por parte de los encargados correspondientes. Durante este proceso, realizamos ajustes y mejoras para garantizar la funcionalidad y eficiencia de cada solución implementada.

Tras la culminación de estos proyectos, la empresa nos ofreció un contrato como parte del equipo de *Service Operation Specialist*. Esta oportunidad nos permitió encargarnos del mantenimiento de las automatizaciones existentes y del desarrollo de nuevas soluciones orientadas a optimizar los distintos flujos de trabajo dentro de la organización.

Además de nuestras funciones en automatización, asumimos responsabilidades como la

elaboración de informes mensuales, la prestación de soporte de TI a diversas carteras de clientes y la gestión de incidencias diarias. También nos encargamos del análisis de procesos internos para identificar oportunidades de automatización, siempre considerando los objetivos estratégicos y presupuestarios de la empresa.

Este crecimiento dentro de la organización nos permitió adquirir un conocimiento profundo sobre su infraestructura tecnológica y los desafíos operativos que enfrentaba. En este contexto, identificamos múltiples oportunidades de mejora, especialmente en la reducción de tareas manuales repetitivas que afectaban la eficiencia operativa.

En el desarrollo de este proyecto, los autores desempeñaron el rol de *Service Operation Specialist*, una posición estratégica en la gestión de infraestructura en la nube, administración de bases de datos y automatización de procesos dentro de la empresa. Su primer contacto con la organización se dio a través de las prácticas profesionales, lo que les permitió comprender a fondo su funcionamiento y detectar diversas oportunidades de mejora en los procesos internos.

Uno de los principales desafíos identificados fue la ejecución manual de tareas rutinarias, las cuales demandaban una gran cantidad de horas de trabajo y representaban una carga operativa considerable. Además, esta dependencia de la intervención humana aumentaba la probabilidad de errores y omisiones, afectando directamente la productividad del usuario final y el rendimiento de las operaciones diarias.

Durante su labor, los autores detectaron un procedimiento crítico que generaba constantes inconvenientes: el monitoreo, análisis y notificación de posibles intrusiones en servidores. Al depender exclusivamente de la intervención manual, este proceso presentaba múltiples

desafíos, como retrasos en la detección de accesos no autorizados, errores en la clasificación de amenazas y una sobrecarga operativa para el equipo de seguridad informática.

Ante esta problemática, se determinó la necesidad de desarrollar e implementar una solución automatizada que optimizará la gestión de intrusiones en los servidores. Esta automatización permite reducir los tiempos de análisis, mejorar la precisión en la identificación de amenazas y agilizar la notificación a los responsables de seguridad, logrando así una gestión más eficiente de la infraestructura tecnológica. Tras un análisis detallado y la presentación del proyecto a la empresa, la propuesta fue aprobada y ejecutada con éxito.

## 3.1. Descripción del proyecto desarrollado

### 3.1.1. Identificación del problema

En el campo de la ciberseguridad, la detección temprana de accesos no autorizados a los servidores es fundamental para prevenir ataques y mantener la integridad de los sistemas. No obstante, en ORION PERU S.A.C., este procedimiento se llevaba a cabo manualmente, lo que generaba problemas en términos de eficiencia, precisión y tiempo de respuesta.

El equipo de seguridad informática debía examinar uno por uno los registros de acceso en cada servidor, identificar posibles intentos de intrusión, recopilar direcciones IP sospechosas y analizarlas para determinar si representaban una amenaza. Debido a su dependencia total de la intervención humana, este método presentaba diversas desventajas operativas:

- **Retraso en la detección de amenazas:** La revisión manual requería demasiado tiempo, lo que dificulta una respuesta rápida ante posibles ataques.

- **Mayor margen de error:** El proceso manual de recopilación y análisis podía dar lugar a omisiones o clasificaciones incorrectas de direcciones IP.

- **Ausencia de alertas en tiempo real:** No existía un sistema automatizado que notificará inmediatamente sobre intentos de intrusión.

- **Desgaste del equipo de seguridad:** El personal debía invertir una cantidad significativa de tiempo en tareas repetitivas, reduciendo su capacidad de enfocarse en estrategias más avanzadas de protección.

Ante estas limitaciones, se hacía indispensable optimizar el monitoreo de accesos no autorizados, minimizando los tiempos de respuesta y reduciendo los errores. Para ello, se implementó un sistema automatizado que permitió mejorar la eficiencia de la seguridad y generar alertas en tiempo real.

### 3.1.2. Objetivos del proyecto

#### 3.1.2.1.Objetivo Principal

Desarrollar e implementar una automatización para el monitoreo de intrusiones en los servidores de ORION PERU S.A.C., con el fin de optimizar la detección de accesos no autorizados, reducir los tiempos de análisis, minimizar errores en la identificación de amenazas y generar notificaciones automáticas en tiempo real para el equipo de seguridad informática.

#### 3.1.2.2.Objetivos Específicos

- Automatizar la recopilación de direcciones IP sospechosas para optimizar la

detección de intrusiones a los servidores.

- Disminuir el tiempo de análisis y registro de la reputación de direcciones IP sospechosas.
- Implementar un sistema de filtrado y clasificación de eventos para reducir el tiempo de análisis y facilitar la identificación de amenazas.
- Reducir la intervención manual en el proceso de monitoreo mediante la implementación de un flujo de trabajo completamente automatizado.

### 3.1.3. Alcance del proyecto:

Este proyecto comprende el diseño, desarrollo e implementación de un sistema automatizado para el monitoreo de intrusiones en servidores.

Los aspectos clave considerados para el desarrollo del sistema son los siguientes:

- Implementación de un sistema automatizado para la detección y análisis de accesos no autorizados.
- Centralización del almacenamiento de datos en un repositorio en la nube.
- Generación de reportes automáticos con información detallada sobre direcciones IP maliciosas.
- Envío de notificaciones en tiempo real mediante correos electrónicos y canales de chat.

### 3.1.4. Limitaciones del proyecto

El desarrollo del proyecto de automatización para el monitoreo de intrusiones en servidores enfrentó diversas limitaciones que impactaron su implementación. A continuación, se presentan los principales desafíos identificados durante su ejecución:

- **Falta de un servidor en la nube**: No se contó con un servidor virtual en la nube para ejecutar las automatizaciones, lo que obligó a replantear la infraestructura inicial y a buscar alternativas dentro de los recursos disponibles en la empresa.
- **Uso de equipo físico**: Ante la imposibilidad de acceder a un servidor en la nube, la automatización se implementó en una laptop en desuso dentro de la organización. Esto requirió ajustes en el RPA para adaptarlo a las capacidades y restricciones del equipo.
- **Limitaciones presupuestarias**: La falta de inversión en infraestructura tecnológica generó retrasos en la implementación y demandó la optimización del desarrollo con las herramientas y plataformas disponibles.
- **Tiempo de desarrollo ajustado**: Debido a las modificaciones necesarias para adecuar el proyecto al entorno disponible, fue preciso reajustar los tiempos de trabajo, redistribuyendo tareas en los *sprints* para cumplir con los plazos establecidos.

### 3.1.5. Estrategias de desarrollo

Para el desarrollo del proyecto, se adoptó la metodología ágil Scrum, lo que permitió una gestión estructurada y eficiente del proceso, favoreciendo la colaboración del equipo y la adaptación a los cambios de manera ágil.

### 3.1.6. Implementación y desarrollo de la solución

#### 3.1.6.1. Metodología del desarrollo

##### 3.1.6.1.1. Elección de la Metodología

Se optó por la metodología SCRUM, ya que permite gestionar proyectos de forma flexible, entregando valor de manera continua mediante ciclos cortos llamados sprints. Y uno de sus puntos más fuertes es mejorar la calidad del producto y reducir riesgos al permitir ajustes constantes según las necesidades del cliente.

3.1.6.1.2. Equipo Scrum

**Tabla 1**

Equipo Scrum

| Persona | Cargo | Rol |
|---|---|---|
| Carlos Iglesias | SOC Senior Specialist | Product Owner |
| Victor Bohorquez | Service Operation Lead | Scrum Master |
| Jose Leiva | Service Operation | Development team |
| Alvaro Torres | Service Operation | Development team |

3.1.6.1.2.1. Responsabilidades del equipo Scrum

I. Product owner

- Es el responsable de definir los requerimientos del producto o servicio.
- Prioriza las tareas en el Product Backlog para que el equipo trabaje en lo más importante primero.
- Representa las necesidades del cliente o la empresa.

II. Scrum Máster

- Actúa como facilitador del equipo y se asegura de que se sigan las reglas de Scrum.
- Elimina bloqueos o impedimentos que frenen al equipo.
- Ayuda a mejorar los procesos de trabajo y fomenta la colaboración.

III. Development team

- Son los encargados de desarrollar el producto o servicio.
- Trabajan en los Sprints entregando incrementos funcionales.
- Se auto-organizan para cumplir los objetivos sin necesidad de una supervisión

constante.

3.1.6.1.3. Ambiente de desarrollo

**Tabla 2**

Ambiente de desarrollo

| | |
|---|---|
| Sistema Operativo | Windows 10 Pro |
| Sitio Web | Kibana |
| RPA | Uipath |
| Editor de Código Fuente | Appscript |
| Lenguaje de Programación | Java Script |

3.1.6.2. Requerimientos del Sistema

3.1.6.2.1. REQUERIMIENTOS FUNCIONALES

RF-01: El sistema debe acceder automáticamente a la web de Kibana - ElasticSearch.

RF-02: El sistema debe autenticarse con credenciales seguras y acceder al dashboard "AWS WAF".

RF-03: El sistema debe seleccionar automáticamente el rango de horas predefinido para cada automatización.

RF-04: El sistema debe aplicar filtros específicos para seleccionar los eventos relevantes.

RF-05: El sistema debe descargar el reporte en el formato requerido.

RF-06: El sistema debe convertir el reporte al formato adecuado (CSV, Excel, etc.).

RF-07: El sistema debe extraer y filtrar las columnas necesarias para el análisis.

RF-08: El sistema debe subir los datos procesados a un primer repositorio en la nube.

RF-09: El sistema debe crear un backup automático de la hoja actual y renombrarlo con la fecha del día anterior.

RF-10: El sistema debe limpiar las columnas predefinidas antes de pegar la nueva información.

RF-11: El sistema debe insertar los datos en las ubicaciones correctas dentro del repositorio.

RF-12: El sistema debe extraer únicamente direcciones IPv4 de la columna "IP Origen".

RF-13: El sistema debe consultar automáticamente cada IP en la web ABUSE IP mediante una API.

RF-14: El sistema debe extraer el estado de reputación de cada IP y agregarlo al Excel.

RF-15: El sistema debe repetir este proceso para todas las IPs listadas.

RF-16: El sistema debe concatenar la información en una columna llamada "ip/pais".

RF-17: El sistema debe copiar los valores de la columna "ip/pais" y asignar cada registro en un segundo archivo Excel, según el tipo de evento.

RF-18: El sistema debe identificar la pestaña correcta dentro del segundo Excel y pegar los datos correspondientes.

RF-19: El sistema debe enviar automáticamente un correo a los responsables de cada tipo de evento.

RF-20: El sistema debe publicar una notificación en Google Space con un resumen de los eventos detectados.

3.1.6.2.2. REQUERIMIENTOS NO FUNCIONALES

RNF-01: El sistema debe ejecutar la automatización sin intervención manual del usuario.

RNF-02: La autenticación debe cumplir con estándares de seguridad, utilizando cifrado y solo permitiendo el acceso a los usuarios autorizados.

RNF-03: El tiempo total de ejecución del proceso no debe superar los 10 minutos.

RNF-04: El sistema debe ser compatible con los navegadores Google Chrome y Mozilla

Firefox.

RNF-05: El formato del reporte descargado debe ser compatible con herramientas de análisis de datos (Excel, CSV, JSON).

RNF-06: La información procesada debe almacenarse en la nube con un esquema de seguridad que garantice confidencialidad e integridad.

RNF-07: La búsqueda y filtrado de eventos debe realizarse en menos de 20 segundos.

RNF-08: La API de consulta de reputación de IP debe tener una disponibilidad mínima del 99.5%.

RNF-09: El almacenamiento en la nube debe contar con respaldo automático para evitar la pérdida de información.

RNF-10: El sistema debe permitir la configuración de los destinatarios de los correos electrónicos sin modificar el código fuente.

RNF-11: Las notificaciones en Google Space deben enviarse en formato estructurado y con información clave resaltada.

3.1.6.2.3. REQUERIMIENTOS TÉCNICOS

RT-01: El sistema debe desarrollarse en Python como lenguaje de programación principal.

RT-02: La automatización debe implementarse utilizando UiPath como herramienta RPA.

RT-03: El entorno de desarrollo debe ejecutarse en una computadora Lenovo Ideapad S340 con las siguientes especificaciones:

- Procesador: Intel Core i5-1035G4 a 1.10GHz
- Memoria RAM: 12 GB
- Almacenamiento: SSD NVMe de 500 GB

RT-04: La herramienta de almacenamiento y procesamiento de datos principal será Microsoft Excel y Google Sheets.

RT-05: La comunicación con la API de ABUSE IP debe realizarse mediante solicitudes HTTPS con autenticación segura.

RT-06: El sistema debe integrarse con Google Space y servicios de correo electrónico a través de API o webhooks.

3.1.6.3. Historias de Usuario

**Historia de Usuario N°1**

**Prioridad: 5**

**Tiempo Estimado: 7d**

**Condiciones:**

- El sistema debe acceder automáticamente a la web de Kibana - ElasticSearch.
- El sistema debe autenticarse con credenciales seguras y acceder al dashboard "AWS WAF".
- El sistema debe seleccionar automáticamente el rango de horas predefinido para cada automatización.
- El sistema debe aplicar filtros específicos para seleccionar los eventos relevantes.
- El sistema debe descargar el reporte en el formato requerido.

**Restricciones:**

- El sistema debe garantizar la autenticación segura mediante credenciales encriptadas.
- Solo los usuarios autorizados podrán acceder y extraer datos del dashboard "AWS WAF".
- La selección del rango de horas debe ser acorde a los parámetros establecidos

previamente.

- Los filtros deben aplicarse correctamente para evitar la extracción de datos innecesarios.
- El formato del reporte descargado debe ser compatible con las herramientas de análisis establecidas.

**Historia de Usuario N°2**

**Prioridad: 5**

**Tiempo Estimado: 10d**

**Condiciones:**

- El sistema debe convertir el reporte al formato adecuado (CSV, Excel, etc.).
- El sistema debe extraer y filtrar las columnas necesarias para el análisis.
- El sistema debe subir los datos procesados a un primer repositorio en la nube.
- El sistema debe crear un backup automático de la hoja actual y renombrarlo con la fecha del día anterior.
- El sistema debe limpiar las columnas predefinidas antes de pegar la nueva información.
- El sistema debe insertar los datos en las ubicaciones correctas dentro del repositorio.

**Restricciones:**

- El sistema debe garantizar la conversión del reporte sin pérdida de datos o errores de formato.
- Solo se deben extraer y filtrar las columnas necesarias para el análisis, evitando datos irrelevantes.
- La subida de datos a la nube debe realizarse con protocolos de seguridad para

evitar accesos no autorizados.

- El backup debe generarse automáticamente sin intervención del usuario y con un nombre que incluya la fecha anterior.
- La limpieza de las columnas debe ser precisa para evitar la eliminación de información relevante.
- Los datos deben ser insertados correctamente en su ubicación dentro del repositorio sin alterar otros registros.

**Historia de Usuario N°3**

**Prioridad: 5**

**Tiempo Estimado: 8d**

**Condiciones:**

- El sistema debe extraer únicamente direcciones IPv4 de la columna "IP Origen".
- El sistema debe consultar automáticamente cada IP en la web ABUSE IP mediante una API.
- El sistema debe extraer el estado de reputación de cada IP y agregarlo al Excel.
- El sistema debe repetir este proceso para todas las IPs listadas.

**Restricciones:**

- El sistema debe asegurarse de que solo se extraigan direcciones IPv4, evitando otros formatos de IP o datos irrelevantes.
- La consulta a la API de ABUSE IP debe realizarse de manera eficiente, respetando los límites de solicitudes.
- La información de reputación de cada IP debe agregarse correctamente en la columna correspondiente del Excel.
- El proceso debe repetirse automáticamente para todas las IPs sin intervención

manual del usuario.

- El tiempo total del análisis de IPs no debe afectar el rendimiento del sistema ni superar el tiempo de ejecución definido.

**Historia de Usuario N°4**

**Prioridad: 4**

**Tiempo Estimado: 5d**

**Condiciones:**

- El sistema debe concatenar la información en una columna llamada "ip/pais".
- El sistema debe copiar los valores de la columna "ip/pais" y asignar cada registro en un segundo archivo Excel, según el tipo de evento.
- El sistema debe identificar la pestaña correcta dentro del segundo Excel y pegar los datos correspondientes.

**Restricciones:**

- La información en la columna "ip/pais" debe formatearse correctamente para evitar errores en el procesamiento.
- La asignación de registros en el segundo archivo Excel debe realizarse según reglas predefinidas y sin intervención manual.
- El sistema debe asegurarse de que los datos se peguen en la pestaña correcta dentro del segundo Excel.
- No debe haber pérdida de datos ni duplicación en el proceso de transferencia entre archivos.
- La operación debe completarse en un tiempo óptimo sin afectar el rendimiento del sistema.

**Historia de Usuario N°5**

**Prioridad: 4**

**Tiempo Estimado: 4d**

**Condiciones:**

- El sistema debe enviar automáticamente un correo a los responsables de cada tipo de evento.
- El sistema debe publicar una notificación en Google Space con un resumen de los eventos detectados.

**Restricciones:**

- Los correos deben enviarse únicamente a los destinatarios configurados en el sistema.
- El formato del correo debe ser estructurado y contener la información clave del evento.
- La notificación en Google Space debe enviarse en un formato claro y fácil de entender.
- No debe haber duplicación en el envío de correos o notificaciones.
- La operación debe realizarse en menos de 1 minuto tras la finalización del procesamiento de datos.

3.1.6.4. Matriz de Impacto

**Tabla 3**

Matriz de Impacto

| PRIORIDAD | |
|---|---|
| MUY ALTA | 5 |
| ALTA | 4 |
| MEDIA | 3 |
| BAJA | 2 |
| MUY BAJA | 1 |

3.1.6.5. Product Backlog

El producto backlog se muestra a continuación, el cual muestra los requerimientos funcionales, especificando su número de historia, tiempo estimado, y prioridad.

**Tabla 4**

Product Backlog

| REQUERIMIENTO FUNCIONAL | Historia | T.E. | PRIORIDAD |
|---|---|---|---|
| RF-01: El sistema debe acceder automáticamente a la web de Kibana - ElasticSearch. | 1 | 2 | 5 |
| RF-02: El sistema debe autenticarse con credenciales seguras y acceder al dashboard "AWS WAF". | 1 | 1 | 5 |
| RF-03: El sistema debe seleccionar automáticamente el rango de horas predefinido para cada automatización. | 1 | 1 | 5 |
| RF-04: El sistema debe aplicar filtros específicos para seleccionar los eventos relevantes. | 1 | 2 | 5 |
| RF-05: El sistema debe descargar el reporte en el formato requerido. | 1 | 1 | 5 |
| RF-06: El sistema debe convertir el reporte al formato adecuado (CSV, Excel, etc.). | 2 | 1 | 5 |
| RF-07: El sistema debe extraer y filtrar las columnas necesarias para el análisis. | 2 | 2 | 5 |
| RF-08: El sistema debe subir los datos procesados a un primer repositorio en la nube. | 2 | 2 | 5 |
| RF-09: El sistema debe crear un backup automático de la hoja actual y renombrarlo con la fecha del día anterior. | 2 | 1 | 5 |

| | | | |
|---|---|---|---|
| RF-10: El sistema debe limpiar las columnas predefinidas antes de pegar la nueva información. | 2 | 2 | 5 |
| RF-11: El sistema debe insertar los datos en las ubicaciones correctas dentro del repositorio. | 2 | 2 | 5 |
| RF-12: El sistema debe extraer únicamente direcciones IPv4 de la columna "IP Origen". | 3 | 1 | 5 |
| RF-13: El sistema debe consultar automáticamente cada IP en la web ABUSE IP mediante una API. | 3 | 3 | 5 |
| RF-14: El sistema debe extraer el estado de reputación de cada IP y agregarlo al Excel. | 3 | 2 | 5 |
| RF-15: El sistema debe repetir este proceso para todas las IPs listadas. | 3 | 2 | 5 |
| RF-16: El sistema debe concatenar la información en una columna llamada "ip/pais". | 4 | 1 | 4 |
| RF-17: El sistema debe copiar los valores de la columna "ip/pais" y asignar cada registro en un segundo archivo Excel, según el tipo de evento. | 4 | 2 | 4 |
| RF-18: El sistema debe identificar la pestaña correcta dentro del segundo Excel y pegar los datos correspondientes. | 4 | 2 | 4 |
| RF-19: El sistema debe enviar automáticamente un correo a los responsables de cada tipo de evento. | 5 | 2 | 4 |
| RF-20: El sistema debe publicar una notificación en Google Space con un resumen de los eventos detectados. | 5 | 2 | 4 |

3.1.6.6..Plan de trabajo

**Tabla 5**

Plan de trabajo

| Nro | Nombre de la tarea | Duracion | Comienzo | Fin |
|---|---|---|---|---|
| | Desarrollo de la aplicación | 40d | ago-5 | sep-19 |
| | Sprint 1 | 6d | ago-5 | ago-12 |
| RF-01 | El sistema debe acceder automáticamente a la web de Kibana - ElasticSearch. | 2d | ago-5 | ago-6 |
| | Análisis | 0.5d | ago-5 | ago-5 |

| | | | | |
|---|---|---|---|---|
| | Diseño | 0.5d | ago-5 | ago-5 |
| | Implementación | 1d | ago-6 | ago-6 |
| RF-02 | El sistema debe autenticarse con credenciales seguras y acceder al dashboard "AWS WAF". | 1d | ago-7 | ago-7 |
| | Análisis | 0.3d | ago-7 | ago-7 |
| | Diseño | 0.3d | ago-7 | ago-7 |
| | Implementación | 0.4d | ago-7 | ago-7 |
| RF-03 | El sistema debe seleccionar automáticamente el rango de horas predefinido para cada automatización. | 1d | ago-8 | ago-8 |
| | Análisis | 0.3d | ago-8 | ago-8 |
| | Diseño | 0.3d | ago-8 | ago-8 |
| | Implementación | 0.4d | ago-8 | ago-8 |
| RF-04 | El sistema debe aplicar filtros específicos para seleccionar los eventos relevantes. | 2d | ago-9 | ago-12 |
| | Análisis | 0.5d | ago-9 | ago-9 |
| | Diseño | 0.5d | ago-9 | ago-9 |
| | Implementación | 1d | ago-12 | ago-12 |
| | Sprint 2 | 13d | ago-13 | ago-27 |
| RF-05 | El sistema debe descargar el reporte en el formato requerido. | 1d | ago-13 | ago-13 |
| | Análisis | 0.3d | ago-13 | ago-13 |
| | Diseño | 0.3d | ago-13 | ago-13 |
| | Implementación | 0.4d | ago-13 | ago-13 |
| RF-06 | El sistema debe convertir el reporte al formato adecuado | 1d | ago-14 | ago-14 |

| | | | | |
|---|---|---|---|---|
| | (CSV, Excel, etc.). | | | |
| | Análisis | 0.3d | ago-14 | ago-14 |
| | Diseño | 0.3d | ago-14 | ago-14 |
| | Implementación | 0.4d | ago-14 | ago-14 |
| RF-07 | El sistema debe extraer y filtrar las columnas necesarias para el análisis. | 2d | ago-15 | ago-16 |
| | Análisis | 0.5d | ago-15 | ago-15 |
| | Diseño | 0.5d | ago-15 | ago-15 |
| | Implementación | 1d | ago-16 | ago-16 |
| RF-08 | El sistema debe subir los datos procesados a un primer repositorio en la nube. | 2d | ago-19 | ago-20 |
| | Análisis | 0.5d | ago-19 | ago-19 |
| | Diseño | 0.5d | ago-19 | ago-19 |
| | Implementación | 1d | ago-20 | ago-20 |
| RF-09 | El sistema debe crear un backup automático de la hoja actual y renombrarlo con la fecha del día anterior. | 1d | ago-21 | ago-21 |
| | Análisis | 0.3d | ago-21 | ago-21 |
| | Diseño | 0.3d | ago-21 | ago-21 |
| | Implementación | 0.4d | ago-21 | ago-21 |
| RF-10 | El sistema debe limpiar las columnas predefinidas antes de pegar la nueva información. | 2d | ago-22 | ago-23 |
| | Análisis | 0.5d | ago-22 | ago-22 |
| | Diseño | 0.5d | ago-22 | ago-22 |
| | Implementación | 1d | ago-23 | ago-23 |

| | | | | |
|---|---|---|---|---|
| RF-11 | El sistema debe insertar los datos en las ubicaciones correctas dentro del repositorio. | 2d | ago-26 | ago-27 |
| | Análisis | 0.5d | ago-26 | ago-26 |
| | Diseño | 0.5d | ago-26 | ago-26 |
| | Implementación | 1d | ago-27 | ago-27 |
| | Sprint 3 | 8d | ago-28 | sep-6 |
| RF-12 | El sistema debe extraer únicamente direcciones IPv4 de la columna "IP Origen". | 1d | ago-28 | ago-28 |
| | Análisis | 0.3d | ago-28 | ago-28 |
| | Diseño | 0.3d | ago-28 | ago-28 |
| | Implementación | 0.4d | ago-28 | ago-28 |
| RF-13 | El sistema debe consultar automáticamente cada IP en la web ABUSE IP mediante una API. | 3d | ago-29 | sep-2 |
| | Análisis | 1d | ago-29 | ago-29 |
| | Diseño | 1d | ago-30 | ago-30 |
| | Implementación | 1d | sep-2 | sep-2 |
| RF-14 | El sistema debe extraer el estado de reputación de cada IP y agregarlo al Excel. | 2d | sep-3 | sep-4 |
| | Análisis | 0.5d | sep-3 | sep-3 |
| | Diseño | 0.5d | sep-3 | sep-3 |
| | Implementación | 1d | sep-4 | sep-4 |
| RF-15 | El sistema debe repetir este proceso para todas las IPs listadas. | 2d | sep-5 | sep-6 |
| | Análisis | 0.5d | sep-5 | sep-5 |

| | | | | |
|---|---|---|---|---|
| | Diseño | 0.5d | sep-5 | sep-5 |
| | Implementación | 1d | sep-6 | sep-6 |
| | Sprint 4 | 9d | sep-9 | sep-19 |
| RF-16 | El sistema debe concatenar la información en una columna llamada "ip/pais". | 1d | sep-9 | sep-9 |
| | Análisis | 0.3d | sep-9 | sep-9 |
| | Diseño | 0.3d | sep-9 | sep-9 |
| | Implementación | 0.4d | sep-9 | sep-9 |
| RF-17 | El sistema debe copiar los valores de la columna "ip/pais" y asignar cada registro en un segundo archivo Excel, según el tipo de evento. | 2d | sep-10 | sep-11 |
| | Análisis | 0.5d | sep-10 | sep-10 |
| | Diseño | 0.5d | sep-10 | sep-10 |
| | Implementación | 1d | sep-11 | sep-11 |
| RF-18 | El sistema debe identificar la pestaña correcta dentro del segundo Excel y pegar los datos correspondientes. | 2d | sep-12 | sep-13 |
| | Análisis | 0.5d | sep-12 | sep-12 |
| | Diseño | 0.5d | sep-12 | sep-12 |
| | Implementación | 1d | sep-13 | sep-13 |
| RF-19 | El sistema debe enviar automáticamente un correo a los responsables de cada tipo de evento. | 2d | sep-16 | sep-17 |
| | Análisis | 0.5d | sep-16 | sep-16 |
| | Diseño | 0.5d | sep-16 | sep-16 |
| | Implementación | 1d | sep-17 | sep-17 |

| | | | | |
|---|---|---|---|---|
| RF-20 | El sistema debe publicar una notificación en Google Space con un resumen de los eventos detectados. | 2d | sep-18 | sep-19 |
| | Análisis | 0.5d | sep-18 | sep-18 |
| | Diseño | 0.5d | sep-18 | sep-18 |
| | Implementación | 1d | sep-19 | sep-19 |

3.1.6.7. Story Point

3.1.6.7.1. SPRINT Nº1

**Tabla 6**

SPRINT Nº1

| SPRINT | REQUERIMIENTO FUNCIONAL | Historia | T. E. | PRIORIDAD |
|---|---|---|---|---|
| SPRINT 1 | **RF-01:** El sistema debe acceder automáticamente a la web de Kibana - ElasticSearch. | 1 | 2 | 5 |
| | **RF-02:** El sistema debe autenticarse con credenciales seguras y acceder al dashboard "AWS WAF". | 1 | 1 | 5 |
| | **RF-03:** El sistema debe seleccionar automáticamente el rango de horas predefinido para cada automatización. | 1 | 1 | 5 |
| | **RF-04:** El sistema debe aplicar filtros específicos para seleccionar los eventos relevantes. | 1 | 2 | 5 |

**REQUERIMIENTOS**

- **Análisis**

El sistema iniciará autenticándose en la web con credenciales preconfiguradas, luego seleccionará automáticamente uno de los tres rangos de tiempo definidos según la hora en la que se ejecute el proceso y aplicará los filtros correspondientes para obtener los eventos específicos que serán analizados.

- **Pruebas del sistema**

Las pruebas se realizaron en un entorno controlado, donde se pudo ejecutar esta sección

las veces necesarias sin causar problemas o bloqueos en la cuenta de usuario. Se llevaron a cabo de forma diaria en diferentes lapsos de tiempo para validar que los tiempos de respuesta fueran los correctos y que no hubiera errores al acceder, seleccionar el rango de tiempo o aplicar los filtros. Además, se verificó que la autenticación con credenciales preconfiguradas se realizara sin inconvenientes y que los filtros extrajeran únicamente los eventos específicos requeridos. Durante las pruebas, se identificó un problema en la selección del rango de tiempo, el cual fue corregido ajustando la lógica de asignación según la hora del sistema.

- **Revisión del sprint Nº1**

**Tabla 7**

Revisión del sprint Nº1

| Nº | Requerimiento | Estado |
|---|---|---|
| 1 | **RF-01:** El sistema debe acceder automáticamente a la web de Kibana - ElasticSearch. | Cumplido |
| 2 | **RF-02:** El sistema debe autenticarse con credenciales seguras y acceder al dashboard "AWS WAF". | Cumplido |
| 3 | **RF-03:** El sistema debe seleccionar automáticamente el rango de horas predefinido para cada automatización. | Cumplido |
| 4 | **RF-04:** El sistema debe aplicar filtros específicos para seleccionar los eventos relevantes. | Cumplido |

- Implementación

**Figura 3**

Logueo a Kibana - ElasticSearch

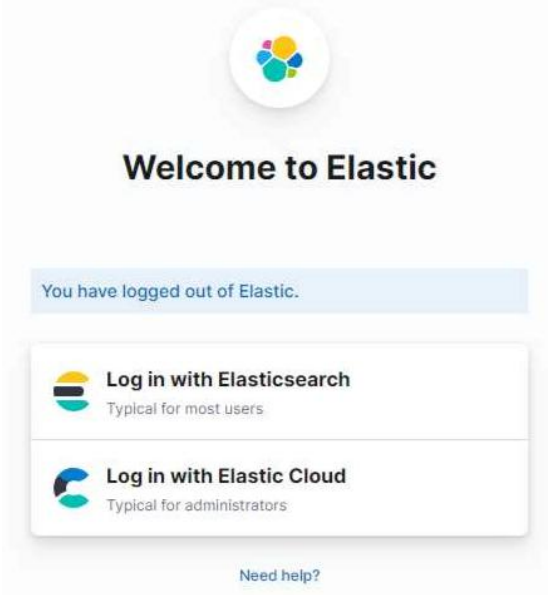
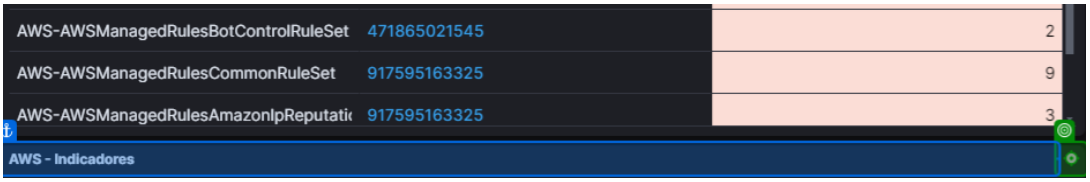



**Figura 4**

RF-04




### 3.1.6.7.2. SPRINT Nº2

**Tabla 7**

SPRINT Nº2

| SPRINT | REQUERIMIENTO FUNCIONAL | Historia | T. E. | PRIORIDAD |
|---|---|---|---|---|
| SPRINT 2 | **RF-05:** El sistema debe descargar el reporte en el formato requerido. | 1 | 1 | 5 |
| | **RF-06:** El sistema debe convertir el reporte al formato adecuado (CSV, Excel, etc.). | 2 | 1 | 5 |
| | **RF-07:** El sistema debe extraer y filtrar las columnas necesarias para el análisis. | 2 | 2 | 5 |
| | **RF-08:** El sistema debe subir los datos procesados a un primer repositorio en la nube. | 2 | 2 | 5 |
| | **RF-09:** El sistema debe crear un backup automático de la hoja actual y renombrarlo con la fecha del día | 2 | 1 | 5 |

| | | | | |
|---|---|---|---|---|
| | anterior. | | | |
| | **RF-10:** El sistema debe limpiar las columnas predefinidas antes de pegar la nueva información. | 2 | 2 | 5 |
| | **RF-11:** El sistema debe insertar los datos en las ubicaciones correctas dentro del repositorio. | 2 | 2 | 5 |

**REQUERIMIENTOS**

- **Análisis**

El sistema descargará el reporte en el formato preconfigurado para su correcta lectura. Luego, leerá y filtrará solo las columnas necesarias y cargará la información en un repositorio en la nube. Antes de esta carga, el sistema hará una copia de la hoja actual, la cual contiene la data extraída del día anterior, y la guardará como backup con la fecha de ayer. Como resultado, habrá dos hojas: una de backup y otra con la información del día anterior. En esta última, el sistema limpiará los datos para eliminar la información antigua y reemplazarla con la data correspondiente al día en curso.

- **Pruebas del sistema**

Las pruebas se realizaron en un entorno controlado, permitiendo ejecutar cada proceso repetidamente sin afectar la integridad de los datos. Se validó que el sistema descargara el reporte en el formato preconfigurado y que la conversión se realizará correctamente sin pérdida de información.

Asimismo, se probó que la extracción y filtrado de columnas fueran precisos, asegurando que solo se seleccionara la información necesaria. Se verificó que la carga de datos al repositorio en la nube se realizara sin errores y que el backup de la hoja actual se generara correctamente con la fecha del día anterior. Además, se comprobó que la hoja principal se limpiara antes de insertar la nueva data, evitando duplicaciones o inconsistencias.

Durante las pruebas, se identificó un problema en el renombrado del archivo de backup,

el cual fue corregido ajustando el formato de fecha para garantizar su correcta generación.

- **Revisión del sprint Nº2**

**Tabla 8**

Revisión del sprint Nº2

| Nº | Requerimiento | Estado |
|---|---|---|
| 5 | **RF-05:** El sistema debe descargar el reporte en el formato requerido. | Cumplido |
| 6 | **RF-06:** El sistema debe convertir el reporte al formato adecuado (CSV, Excel, etc.). | Cumplido |
| 7 | **RF-07:** El sistema debe extraer y filtrar las columnas necesarias para el análisis. | Cumplido |
| 8 | **RF-08:** El sistema debe subir los datos procesados a un primer repositorio en la nube. | Cumplido |
| 9 | **RF-09:** El sistema debe crear un backup automático de la hoja actual y renombrarlo con la fecha del día anterior. | Cumplido |
| 10 | **RF-10:** El sistema debe limpiar las columnas predefinidas antes de pegar la nueva información. | Cumplido |
| 11 | **RF-11:** El sistema debe insertar los datos en las ubicaciones correctas dentro del repositorio. | Cumplido |

- Implementación

**Figura 5**

RF-05


**Figura 6**

RF-07

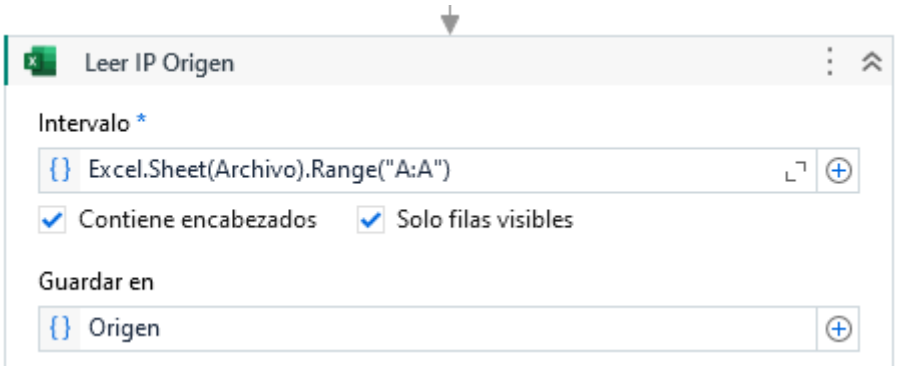



**Figura 7**

RF-10

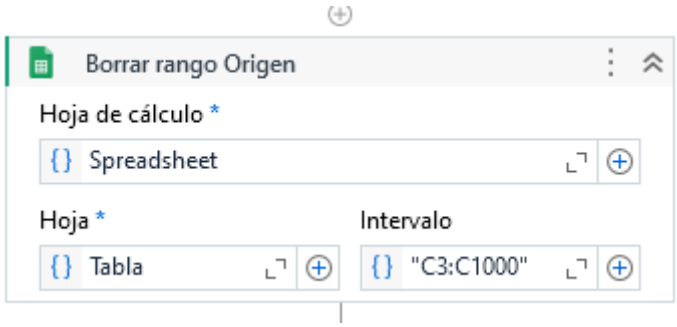
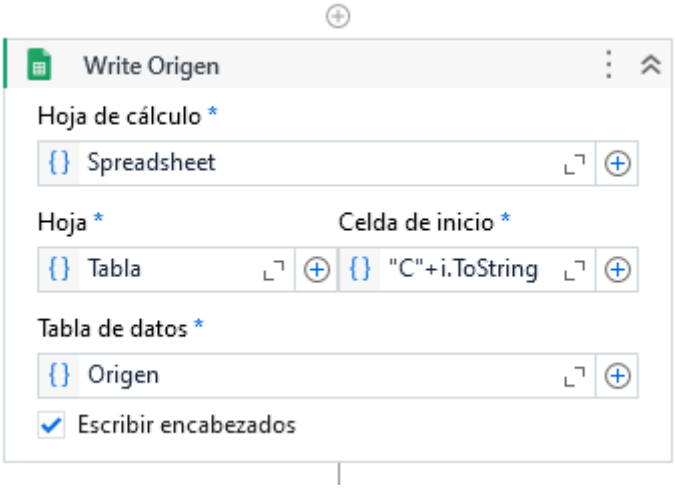



**Figura 8**

RF-11




3.1.6.7.3. SPRINT Nº3

**Tabla 9**

SPRINT Nº3

| SPRINT | REQUERIMIENTO FUNCIONAL | Historia | T. E. | PRIORIDAD |
|---|---|---|---|---|
| SPRINT 3 | **RF-12:** El sistema debe extraer únicamente direcciones IPv4 de la columna "IP Origen". | 3 | 1 | 5 |
| | **RF-13:** El sistema debe consultar automáticamente cada IP en la web ABUSE IP mediante una API. | 3 | 3 | 5 |
| | **RF-14:** El sistema debe extraer el estado de reputación de cada IP y agregarlo al Excel. | 3 | 2 | 5 |
| | **RF-15:** El sistema debe repetir este proceso para todas las IPs listadas. | 3 | 2 | 5 |

## REQUERIMIENTOS

- **Análisis**

El sistema extraerá las direcciones IPv4 de la columna correspondiente y consultará automáticamente cada una en ABUSE IP mediante una API. Luego, registrará el estado de reputación en el Excel y repetirá este proceso hasta analizar todas las IPs listadas.

- **Pruebas del sistema**

Las pruebas se realizaron en un entorno controlado, ejecutando el proceso varias veces para validar que solo se extrajeran direcciones IPv4 y que no se incluyeran datos incorrectos. Se verificó que las consultas a la API de ABUSE IP se realizaran sin errores y que el estado de reputación de cada IP se registrara correctamente en el Excel. Además, se comprobó que el sistema completara el análisis de todas las IPs sin interrupciones ni necesidad de intervención manual. Durante las pruebas, se detectó un problema con la velocidad de consulta a la API, el cual se solucionó optimizando el manejo de solicitudes.

- **Revisión del sprint Nº3**

**Tabla 10**

Revisión del sprint Nº3

| Nº | Requerimiento | Estado |
|---|---|---|

| | | |
|---|---|---|
| 12 | **RF-12:** El sistema debe extraer únicamente direcciones IPv4 de la columna "IP Origen". | Cumplido |
| 13 | **RF-13:** El sistema debe consultar automáticamente cada IP en la web ABUSE IP mediante una API. | Cumplido |
| 14 | **RF-14:** El sistema debe extraer el estado de reputación de cada IP y agregarlo al Excel. | Cumplido |
| 15 | **RF-15:** El sistema debe repetir este proceso para todas las IPs listadas. | Cumplido |

- Implementación

**Figura 9**

RF-12

```
// Obtener los datos de la hoja de cálculo
var datos = hoja.getRange("C3:C").getValues();

// Recorrer los datos y buscar direcciones IP válidas
for (var i = 0; i < datos.length; i++) {
  var ip = datos[i][0]; // Suponiendo que la dirección IP está en la primera columna de la hoja de cálculo

  // Verificar si la dirección IP es de tipo IPv4 y pública
  if (esIPv4(ip) && esDireccionIPPublica(ip)) {
    // Realizar la búsqueda utilizando la función buscarIPenAbuseIPDB
    var resultado = buscarIPenAbuseIPDB(ip);
    // Escribir el ISP en la columna E
    hoja.getRange("E" + (i + 3)).setValue(resultado.isp);
    var puntaje = resultado.abuse;
    var etiqueta;
    if (puntaje === 0) {
      etiqueta = "Good";
    } else if (puntaje >= 1 && puntaje <= 15) {
      etiqueta = "Neutral";
    } else {
      etiqueta = "Poor";
    }
    hoja.getRange("F" + (i + 3)).setValue(etiqueta);
  }
}
filtrarYGuardarTabla();
//enviarDatosPorCorreo();
}
```

**Figura 10**

RF-13

```
//buscarIPenVirusTotal("IPv4");

function usarAPI() {
  var ahora = new Date();
  var horaActual = ahora.getHours();

  var apiKey1 = "b717746d2b92d10fe7a89f413eb70
  var apiKey2 = "c6aee9d2bed252b5cd1c1adc8ef40

  if (horaActual >= 5 && horaActual <= 18) {
    // Usar apiKey1
    return apiKey1;
  } else {
    // Usar apiKey2
    return apiKey2;
  }
}
```

3.1.6.7.4. SPRINT Nº4

**Tabla 11**

SPRINT Nº4

| SPRINT | REQUERIMIENTO FUNCIONAL | Historia | T.E. | PRIORIDAD |
|---|---|---|---|---|
| SPRINT 4 | **RF-16:** El sistema debe concatenar la información en una columna llamada "ip/pais". | 4 | 1 | 4 |
| | **RF-17:** El sistema debe copiar los valores de la columna "ip/pais" y asignar cada registro en un segundo archivo Excel, según el tipo de evento. | 4 | 2 | 4 |
| | **RF-18:** El sistema debe identificar la pestaña correcta dentro del segundo Excel y pegar los datos correspondientes. | 4 | 2 | 4 |
| | **RF-19:** El sistema debe enviar automáticamente un correo a los responsables de cada tipo de evento. | 5 | 2 | 4 |
| | **RF-20:** El sistema debe publicar una notificación en Google Space con un resumen de los eventos detectados. | 5 | 2 | 4 |

**REQUERIMIENTOS**

- **Análisis**

El sistema combinará información como la IP, su reputación y otros datos en la columna

"ip/pais". Luego, copiará estos valores y los trasladará a otra plantilla de Excel, organizándose según el tipo de evento. Antes de agregar los nuevos datos, limpiará las casillas correspondientes y los pegará en la pestaña adecuada dentro del archivo.

Una vez organizada la información, el sistema enviará un correo automático a los responsables de cada evento con los detalles recopilados. Además, notificará en canales internos mediante una conexión webhook para que los equipos puedan dar seguimiento a los incidentes detectados.

- **Pruebas del sistema**

Las pruebas se realizaron en un entorno controlado para validar que el sistema concatenara correctamente la información en la columna "ip/país" y la organizara en la plantilla de Excel según el tipo de evento. Se verificó que las casillas se limpiarán antes de insertar los nuevos datos y que cada registro se ubicará en la pestaña correspondiente. También se probó el envío de correos automáticos a los responsables asignados, asegurando que la información fuera clara y precisa. Finalmente, se validó la integración con la conexión webhook, confirmando que las notificaciones en canales internos se enviaran sin errores. Durante las pruebas, se detectó un problema en la asignación de eventos a las pestañas del Excel, el cual fue corregido ajustando la lógica de clasificación.

- **Revisión del sprint Nº4**

**Tabla 12**

Revisión del sprint Nº4

| Nº | Requerimiento | Estado |
|---|---|---|
| 16 | **RF-16:** El sistema debe concatenar la información en una columna llamada "ip/país". | Cumplido |
| 17 | **RF-17:** El sistema debe copiar los valores de la columna "ip/pais" y asignar cada registro en un segundo archivo Excel, según el tipo de evento. | Cumplido |

| | | |
|---|---|---|
| 18 | **RF-18:** El sistema debe identificar la pestaña correcta dentro del segundo Excel y pegar los datos correspondientes. | Cumplido |
| 19 | **RF-19:** El sistema debe enviar automáticamente un correo a los responsables de cada tipo de evento. | Cumplido |
| 20 | **RF-20:** El sistema debe publicar una notificación en Google Space con un resumen de los eventos detectados. | Cumplido |

- **Implementación**

**Figura 11**

RF-16

| IP Origen | País de origen | ISP | RE | Hits | IP / PAÍS | N° DE CONEXIONES |
|---|---|---|---|---|---|---|
| [redacted] | Chile | CTC. Corp S.A. | Good | 1,480 | [redacted]18.173.11 \| Chile \| CTC. Corp S.A. \| Good | 1,480 |
| | Chile | CTC. Corp S.A. | Good | 431 | [redacted]18.173.11 \| Chile \| CTC. Corp S.A. \| Good | 431 |
| | Chile | Telmex Chile Internet S.A. | Good | 1,404 | [redacted].108 \| Chile \| Telmex Chile Internet S.A. \| Good | 1,404 |
| | Chile | Telmex Chile Internet S.A. | Good | 416 | [redacted].108 \| Chile \| Telmex Chile Internet S.A. \| Good | 416 |
| | Chile | Entel Chile S.A. | Good | 1,347 | [redacted]42.3.62 \| Chile \| Entel Chile S.A. \| Good | 1,347 |
| | Chile | Entel Chile S.A. | Good | 416 | [redacted]42.3.62 \| Chile \| Entel Chile S.A. \| Good | 416 |
| | Chile | GTD Internet S.A. | Good | 1,325 | [redacted]0.26.50 \| Chile \| GTD Internet S.A. \| Good | 1,325 |
| | Chile | GTD Internet S.A. | Good | 403 | [redacted]0.26.50 \| Chile \| GTD Internet S.A. \| Good | 403 |
| | Chile | Telefonica Movil de Chile S.A. | Good | 2 | [redacted]73 \| Chile \| Telefonica Movil de Chile S.A. \| Good | 2 |
| | United States | Hotwire Fision | Good | 2 | [redacted]7.247 \| United States \| Hotwire Fision \| Good | 2 |
| | Chile | | | 2 | [redacted]60:128:d54:3022:8f6a:c1d:4310 \| Chile \| \| | 2 |
| | Canada | Dmytro Ahrefs Pte Ltd | Poor | 1 | [redacted]3.17 \| Canada \| Dmytro Ahrefs Pte Ltd \| Poor | 1 |
| | Hong Kong | Chang Way Technologies Co. Limited | Poor | 1 | [redacted]ong Kong \| Chang Way Technologies Co. Limited \| Poor | 1 |
| | Chile | Starlink Chile SpA | Good | 1 | [redacted].33.166 \| Chile \| Starlink Chile SpA \| Good | 1 |
| | Chile | Artec Telecomunicaciones Limitada | Good | 1 | [redacted]\| Chile \| Artec Telecomunicaciones Limitada \| Good | 1 |
| | Chile | GTD Internet S.A. | Good | 1 | [redacted].184.136 \| Chile \| GTD Internet S.A. \| Good | 1 |
| | United States | DigitalOcean LLC | Good | 1 | [redacted]211 \| United States \| DigitalOcean LLC \| Good | 1 |

Nota: Por razones de confidencialidad, las direcciones IP que ingresaron a la base de datos no se muestran en la Figura 11.

**Figura 12**

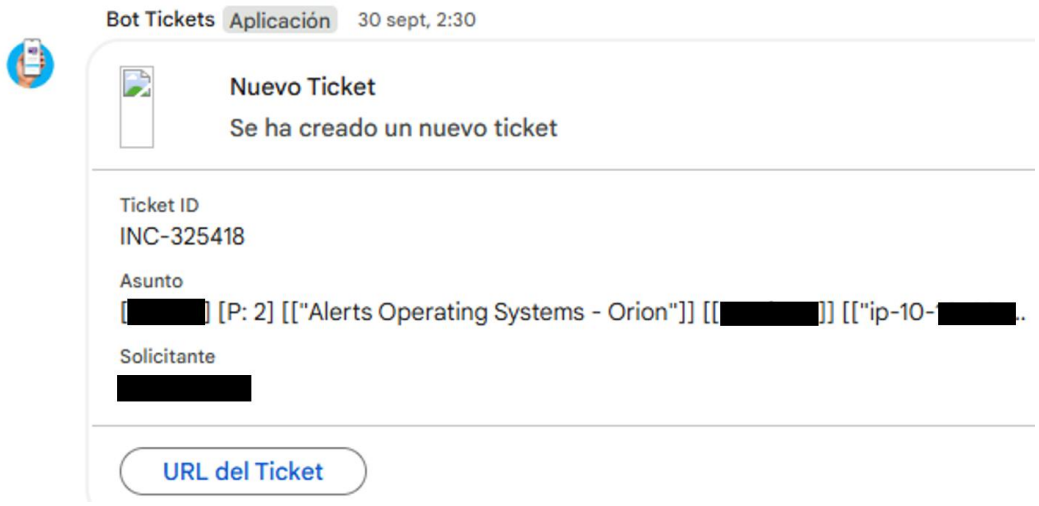
RF-18

| Regla | AWS-AWSManagedRulesBotControlRuleSet | | |
|---|---|---|---|
| | Dirección IP / País / Proveedor / Reputación | N° de Conexiones | Destino |
| Origen de Ofensa | [redacted]173 \| Chile \| Telefonica Movil de Chile S.A. \| Good | 2 | clave.w.sii.cl |
| | [redacted]47 \| United States \| Hotwire Fision \| Good | 2 | clave.w.sii.cl |
| | [redacted]:d54:3022:8f6a:c1d:4310 \| Chile \| \| | 2 | bcm2.sii.cl |
| | [redacted]0 \| Hong Kong \| Chang Way Technologies Co. Limited \| Poor | 1 | bcm2.sii.cl |
| | [redacted]6 \| Chile \| Starlink Chile SpA \| Good | 1 | clave.w.sii.cl |
| | [redacted]39 \| Chile \| Artec Telecomunicaciones Limitada \| Good | 1 | clave.w.sii.cl |
| | [redacted]136 \| Chile \| GTD Internet S.A. \| Good | 1 | bcm2.sii.cl |
| | [redacted] Chile \| Telefonica Chile S.A. \| Good | 1 | clave.w.sii.cl |
| | [redacted] \| Chile \| Pacifico Cable SPA. \| Good | 1 | clave.w.sii.cl |
| | [redacted]16 \| Chile \| Telefonica Chile S.A. \| Good | 1 | clave.w.sii.cl |
| | [redacted] \| Chile \| Entel PCS Telecomunicaciones S.A. \| Good | 1 | clave.w.sii.cl |
| | [redacted]76 \| Chile \| Telefonica Chile S.A. \| Good | 1 | clave.w.sii.cl |
| | [redacted]106 \| Chile \| Telefonica Chile S.A. \| Good | 1 | clave.w.sii.cl |
| | [redacted]190 \| Chile \| Telefonica Chile S.A. \| Good | 1 | clave.w.sii.cl |
| | [redacted]247 \| Chile \| Telefonica Chile S.A. \| Good | 1 | clave.w.sii.cl |
| | [redacted] \| Chile \| Pacifico Cable SPA. \| Good | 1 | bcm2.sii.cl |
| | [redacted] \| Chile \| Pacifico Cable SPA. \| Good | 1 | clave.w.sii.cl |
| | [redacted]17 \| Chile \| VTR Banda Ancha S.A. \| Good | 1 | clave.w.sii.cl |
| | [redacted]88 \| Chile \| GTD Internet S.A. \| Good | 1 | clave.w.sii.cl |
| | [redacted]:2790:4431:d6ff:39ff:24a2 \| Chile \| \| | 1 | clave.w.sii.cl |
| | [redacted]:d27:f476:9c63:cf81:c645 \| Chile \| \| | 1 | clave.w.sii.cl |
| | [redacted]:e2a:a42d:b47f:c3f2:acf7 \| Chile \| \| | 1 | clave.w.sii.cl |
| | [redacted]3:b680:513f:a24:a35e:4a3 \| Chile \| \| | 1 | clave.w.sii.cl |
| | [redacted]1:c9a0:7d24:948f:2182:2919 \| Chile \| \| | 1 | clave.w.sii.cl |
| | [redacted]12:be97:c09a:cbab:f5d6:3bf2 \| Chile \| \| | 1 | clave.w.sii.cl |
| | [redacted]ff:70::face:b00c \| United States \| \| | 1 | bcm2.sii.cl |
| Acción | Block | | |
| Descripción | AWS WAF Bot Control ofrece protección contra bots automatizados que pueden consumir recursos en exceso, sesgar las métricas comerciales, causar tiempo de inactividad o realizar actividades maliciosas. Bot Control brinda visibilidad adicional a través de Amazon CloudWatch y genera etiquetas que puede usar para controlar el tráfico de bots a sus aplicaciones. | | |
| Análisis | Los eventos detectados por esté grupo de reglas, se genera por la identificación de BOT, los cuales, se van dirigidos a los sitio web y/o aplicaciones. Dichos BOT, generalmente realizan escaneos o consultas a través de internet, web scraping, búsqueda de enlaces rotos, etc. | | |
| Recomendación | Validar si el tráfico de estos BOT es válido para la entidad del SII, caso contrario proceder con el bloqueo | | |

Nota: Por razones de confidencialidad, las direcciones IP que ingresaron a la base de datos no se muestran en la Figura 11.

**Figura 13**

RF-20




## CAPÍTULO IV. RESULTADOS

En este capítulo se demostrará la eficacia de implementar una automatización al monitoreo de intrusiones en los servidores de ORION PERU S.A.C.

El primer criterio que se tomó para evaluar fue la eficacia en la recopilación de direcciones IP sospechosas. Anteriormente, este proceso se realizaba manualmente, lo que implicaba descargar la data sin una selección precisa de eventos, ocasionando que en algunos casos se incluyeran registros irrelevantes o se omitieron eventos importantes. Esto generaba errores en la identificación de amenazas, aumentando la cantidad de falsos positivos y falsos negativos en los reportes de seguridad.

A continuación, se comparará la eficiencia con la que anteriormente se realizaba esta tarea con el sistema automatizado implementado, evaluando su impacto en la detección de accesos no autorizados.

**Tabla 13**

Eficacia en la recopilación de direcciones IP sospechosas

| Eficacia en la recopilación de direcciones IP sospechosas | |
|---|---|
| Manual | 75% |
| Sistema | 100% |

Como se puede observar en la Tabla 13, la recopilación manual de direcciones IP presentó un margen de error del 25%, causado por la inclusión de eventos incorrectos o la omisión de registros que no fueron descargados completamente. Este margen de error afectaba la precisión del análisis y aumentaba el riesgo de interpretar información incompleta o errónea. En contraste, con la implementación del sistema automatizado, el margen de error se redujo a 0%, ya que el proceso fue programado para aplicar las reglas de filtrado adecuadas, asegurando la descarga exacta de los eventos requeridos para el análisis.

El segundo criterio a evaluar es la diferencia en el tiempo de búsqueda y registro de la reputación de las direcciones IPv4 que han accedido al servidor. Anteriormente, este proceso se realizaba de forma manual, donde el operador debía analizar cada IP individualmente, consultar su reputación en fuentes externas y registrar la información obtenida en los reportes. Debido a la gran cantidad de accesos diarios, este método requería un tiempo considerable, ya que cada consulta debía realizarse de manera secuencial, prolongando el análisis y aumentando la carga de trabajo del personal.

A continuación, se comparará el tiempo de análisis y registro de IPs antes y después de la implementación del sistema automatizado, evaluando su impacto en la optimización de este proceso.

**Tabla 14**

Eficiencia de evaluación de reputación

| Eficiencia de evaluación de reputación | |
|---|---|
| Manual | 30 minutos |
| Sistema | 2 minutos |

Como se observa en la Tabla 14, el proceso manual de búsqueda y registro de la reputación de cada dirección IPv4 tomaba aproximadamente 60 minutos, dependiendo de la cantidad de registros a analizar. Dado que cada consulta debía realizarse de forma individual y secuencial, el tiempo total aumentaba proporcionalmente a la cantidad de direcciones IP registradas, generando una carga de trabajo considerable para el personal.

En contraste, con la implementación del sistema automatizado, el tiempo de análisis y registro de reputación se redujo drásticamente a 0.10 minutos, sin importar si existen 10, 100 o más direcciones IPv4. Esto se debe a que el sistema consulta y procesa la información en segundos, optimizando el análisis y reduciendo significativamente el tiempo requerido para esta tarea.

El tercer criterio a evaluar es el tiempo de filtrado y clasificación de las direcciones IP según el evento registrado. Anteriormente, este proceso se realizaba manualmente, lo que implicaba que el operador debía revisar cada registro individualmente, aplicar los filtros correspondientes y asignarlo a su categoría según el tipo de evento. Debido a la gran cantidad de registros diarios, esta tarea demandaba un alto consumo de tiempo y recursos, retrasando la identificación de amenazas y aumentando el margen de error en la clasificación.

A continuación, se comparará el tiempo promedio de clasificación de eventos entre el método manual y el sistema automatizado, analizando las diferencias en eficiencia y tiempos de procesamiento.

**Tabla 15**

Eficiencia de filtrado y clasificación de eventos

| Eficiencia de filtrado y clasificación de eventos | |
|---|---|
| Manual | 10 minutos |
| Sistema | 1 minuto |

Como se observa en la Tabla 15, el proceso manual de filtrado y clasificación de eventos requería aproximadamente 10 minutos, debido a la gran cantidad de datos que el operador debía revisar y categorizar individualmente. Este método, además de consumir tiempo, incrementaba el riesgo de errores en la clasificación, lo que podía afectar la identificación precisa de amenazas.

En contraste, con la implementación del sistema automatizado, el tiempo de clasificación se redujo a 1 minuto, lo que representa una disminución significativa de 9 minutos en promedio. Gracias a esta optimización, el sistema puede procesar grandes volúmenes de datos de manera más rápida y eficiente, permitiendo una respuesta más ágil ante posibles incidentes de seguridad

El cuarto criterio a evaluar es la reducción de la intervención manual en el proceso de monitoreo mediante la automatización del flujo de trabajo. Anteriormente, todo el proceso se realizaba de forma manual, lo que requería que el personal ejecuta cada tarea

de manera individual, desde la recopilación y análisis de direcciones IP hasta la clasificación de eventos y el envío de notificaciones. Este método consumía una gran cantidad de tiempo y aumentaba la posibilidad de errores humanos, afectando la eficiencia en la detección y respuesta ante incidentes de seguridad.

A continuación, se comparará el tiempo total invertido en monitoreo entre el método manual y el sistema automatizado, evaluando la diferencia en los tiempos de ejecución dentro de todo el proceso.

**Figura 14**

Comparativa en minutos

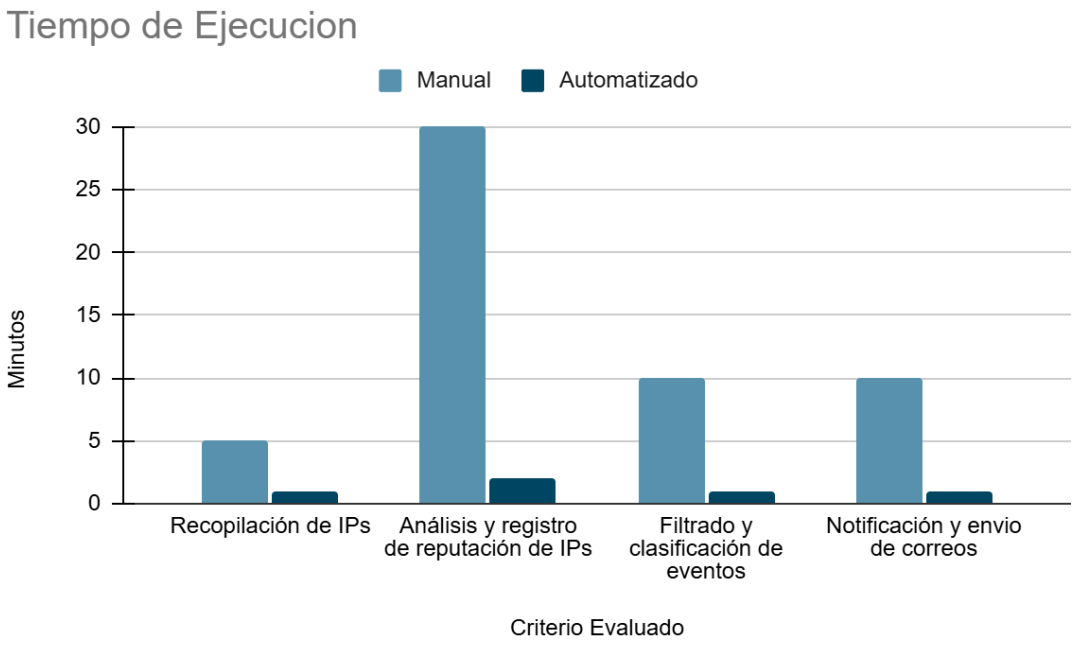



**Tabla 16**

Tiempo de Ejecución

| Criterio Evaluado | Manual | Automatizado |
|---|---|---|
| Recopilación de IPs | 5 | 1 |

| | | |
|---|---|---|
| Análisis y registro de reputación de IPs | 30 | 2 |
| Filtrado y clasificación de eventos | 10 | 1 |
| Notificación y envío de correos | 10 | 1 |
| Tiempo total de monitoreo | 55 | 5 |

Según la Figura 13, la implementación del sistema automatizado permitió reducir significativamente el tiempo de ejecución de cada proceso. Mientras que el método manual requería 55 minutos para completar el monitoreo, con la automatización este tiempo se redujo a solo 5 minutos, optimizando de manera considerable la eficiencia operativa, como se muestra en la Tabla 16.

Cada tarea analizada, desde la recopilación de direcciones IP hasta la notificación y el envío de correos, experimentó una reducción notable en su tiempo de ejecución, agilizando el procesamiento y minimizando la necesidad de intervención manual por parte del personal.

# CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

## Conclusiones

A partir del análisis del desarrollo y los resultados obtenidos en este proyecto, se puede concluir que la implementación de un sistema automatizado para el monitoreo de intrusiones en servidores ha representado una mejora significativa en la seguridad informática y la eficiencia operativa de ORION PERU S.A.C. La solución desarrollada optimizó el proceso de detección de accesos no autorizados, reduciendo los tiempos de análisis y minimizando la posibilidad de errores humanos en la clasificación de amenazas.

La automatización permitió reemplazar un proceso manual que demandaba una alta inversión de tiempo y recursos humanos, lo que generaba demoras y riesgos en la gestión de incidentes de seguridad. Con la incorporación de un flujo de trabajo automatizado, la identificación de direcciones IP sospechosas, el análisis de reputación y la clasificación de eventos se realizan ahora de manera más eficiente, logrando una reducción drástica en los tiempos de respuesta y una mayor precisión en la detección de amenazas.

Otro de los impactos relevantes de este proyecto fue la disminución de la carga operativa del equipo de seguridad informática, ya que la intervención manual en tareas repetitivas se redujo significativamente. Esto permitió que el personal pudiera enfocarse en actividades de mayor valor estratégico, como la optimización de infraestructuras de seguridad, la actualización y configuración de firewalls, el fortalecimiento de políticas de acceso y autenticación, la implementación de nuevas estrategias de detección de amenazas avanzadas, y la revisión periódica de vulnerabilidades en los sistemas críticos de la empresa.

Desde una perspectiva profesional, la experiencia adquirida en este proyecto permitió aplicar y reforzar conocimientos en automatización de procesos, gestión de infraestructuras tecnológicas y análisis y procesamiento de grandes volúmenes de datos. La formación académica en estas áreas proporcionó las bases necesarias para identificar la problemática, diseñar una solución viable e implementarla de manera eficiente dentro del entorno empresarial.

En conclusión, el desarrollo de esta solución tecnológica no solo mejoró los procesos internos de la empresa, sino que también demostró el valor de la automatización en la seguridad informática. La combinación de conocimientos teóricos adquiridos en la formación universitaria con la experiencia práctica en ORION PERU S.A.C. permitió llevar a cabo un proyecto alineado con los requerimientos del sector TI, destacando la importancia de la innovación y la optimización de procesos en entornos empresariales.

**Recomendaciones**

A partir de las lecciones aprendidas durante el desarrollo de este proyecto, se plantean las siguientes recomendaciones con el objetivo de mejorar el sistema implementado, optimizar aún más los procesos y explorar nuevas tecnologías que permitan fortalecer la seguridad informática y la eficiencia operativa en ORION PERU S.A.C.

1. **Ampliar la infraestructura tecnológica para mejorar el rendimiento del sistema**

   Se recomienda la implementación de un **servidor en la nube** dedicado exclusivamente a la ejecución del sistema automatizado. Esto permitiría una mayor estabilidad, escalabilidad y disponibilidad del proceso, eliminando la dependencia de un equipo físico dentro de la empresa.

2. **Integrar herramientas avanzadas de análisis de amenazas**

   Se sugiere complementar el sistema con soluciones como **Splunk, Graylog o Wazuh**, las cuales ofrecen capacidades avanzadas de análisis de registros y correlación de eventos en tiempo real, mejorando la detección de posibles ataques.

3. **Automatizar la respuesta ante incidentes**

   Como una mejora adicional, se podría integrar una funcionalidad que permita la **respuesta automática** ante ciertas amenazas detectadas. Por ejemplo, mediante la configuración de reglas en **firewalls o sistemas IDS/IPS**, se podrían **bloquear direcciones IP sospechosas** de manera inmediata sin intervención humana.

4. **Optimizar la consulta de reputación de IPs con múltiples fuentes de información**

   Para mejorar la precisión en la clasificación de amenazas, se recomienda utilizar varias **APIs de reputación de IPs**, como **VirusTotal, IBM X-Force Exchange o Cisco Talos**, en lugar de depender de una sola fuente. Esto permitiría una validación cruzada de la información, reduciendo el margen de error.

5. **Implementar inteligencia artificial y aprendizaje automático para mejorar la detección de amenazas**

   Se propone explorar el uso de **modelos de machine learning** que permitan identificar patrones de comportamiento sospechoso en los accesos a los servidores. Herramientas como **TensorFlow o Scikit-learn** podrían entrenarse con datos históricos para predecir posibles ataques y generar alertas antes de que ocurran.

6. **Desarrollar un dashboard interactivo para la visualización de datos en tiempo real**

Para mejorar la toma de decisiones, se recomienda integrar un **panel de control interactivo** utilizando herramientas como **Grafana o Power BI**, que permita visualizar métricas clave en tiempo real, facilitando la supervisión del sistema y la identificación de tendencias en los intentos de intrusión.

7. **Capacitar al personal en el uso y supervisión del sistema automatizado**

   Es fundamental que el equipo de seguridad informática reciba **formación continua** en el uso de la herramienta y en nuevas estrategias de ciberseguridad. Esto garantizará una **gestión eficiente del sistema** y permitirá que el personal pueda adaptarse a futuras mejoras o actualizaciones tecnológicas.

## REFERENCIAS

Álvarez, C. L. (2022). Estándar para activar la obligación de comunicar sobre ciberincidentes relevantes en instituciones públicas. Revista Chilena de Derecho y Tecnología, 11(2), 183–210. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842022000200183&lang=es

*A partir de 2024, empresas de TI de Latinoamérica tendrán un crecimiento más estable que las de EEUU, según IDC - IDC*. (2023, December 6). https://www.idc.com/getdoc.jsp?containerId=prLA51751624

Acerca de webhooks - Documentación de GitHub. (n.d.). Retrieved March 22, 2025, from https://docs.github.com/es/webhooks/about-webhooks

Alnanih, R. (2024). Enhancing Usability: A Grounded Theory Approach-based Scrum Framework for Mobile Application Design. Procedia Computer Science, 241, 162–170. https://www.sciencedirect.com/science/article/pii/S1877050924017344?via%3Dihub

Descripción general de Google Apps Script | Google Workspace
. (n.d.). Retrieved March 22, 2025, from https://developers.google.com/apps-script/overview?hl=es-419

Garrido-Labrador, J. L., Maudes-Raedo, J. M., Rodríguez, J. J., & García-Osorio, C. I. (2025). SSLearn: A Semi-Supervised Learning library for Python. SoftwareX, 29, 102024. https://www.sciencedirect.com/science/article/pii/S2352711024003947

*IDC FutureScape: Latin America IT Industry - IDC*. (2023, December 13). https://www.idclatin.com/2023/Events/13_Dec_LA/FutureScapeLA2024.pdf

Introduction To Agile Methodology And Its Importance – B2E Consulting. (n.d.). Retrieved March 22, 2025, from https://www.b2econsulting.com/introduction-to-agile-methodology-and-its-importance/

Kibana—your window into Elastic | Kibana Guide [8.17] | Elastic. (n.d.). Retrieved March 22, 2025, from https://www.elastic.co/guide/en/kibana/current/introduction.html

Montoya, M., Rojas, J. A., Aguirre, Y. A., Montoya, M., Rojas, J. A., & Aguirre, Y. A. (2024). Dashboard para el monitoreo de gestión RPA - Automatización Robótica de Procesos: un estudio en la Pyme manufacturera. Entre Ciencia e Ingeniería, 18(35), 59–66. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-83672024000100059&lng=en&nrm=iso&tlng=es

Muñoz, I. C., Collazos, C. A., & Hurtado, J. A. (2024). Desafíos de colaboración en la adopción de Scrum: un estudio en equipos de desarrollo de software del departamento del Cauca, Colombia. TecnoLógicas, 27(59), e2881. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-77992024000100202&lng=en&nrm=iso&tlng=es

*¿Qué es Elasticsearch? - AWS*. (n.d.). Retrieved March 22, 2025, from

https://aws.amazon.com/es/what-is/elasticsearch/

¿Qué es la automatización robótica de procesos (RPA)? | IBM. (n.d.). Retrieved March 22, 2025, from https://www.ibm.com/mx-es/topics/rpa

*¿Qué es la pila ELK? - AWS*. (n.d.). Retrieved March 22, 2025, from https://aws.amazon.com/what-is/elk-stack/

*¿Qué es un webhook? - Red Hat*. (2024, February 1). https://www.redhat.com/es/topics/automation-and-management/que-es-un-webhook

Ribeiro, J., Lima, R., Eckhardt, T., & Paiva, S. (2021). Robotic Process Automation and Artificial Intelligence in Industry 4.0 – A Literature review. Procedia Computer Science, 181, 51–58. https://www.sciencedirect.com/science/article/pii/S1877050921001393?via%3Dihub

Sales, L., Ormenese, A., & Pereira, F. (2024). APLICAÇÃO DA FERRAMENTA ELASTICSEARCH NO MONITORAMENTO DE INDICADORES DO SETOR DE COLETA DE SANGUE DO HEMOCENTRO UNICAMP: GARANTINDO EFICIÊNCIA E SEGURANÇA. Hematology, Transfusion and Cell Therapy, 46, S727–S728. https://www.sciencedirect.com/science/article/pii/S2531137924015566?via%3Dihub

Sanchez-Garcia, I. D., Rea-Guaman, A. M., Feliu, T. S., & Calvo-Manzano, J. A. (2024). Auditoría de riesgos de ciberseguridad: Revisión de Literatura, propuesta y aplicación. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *2024*(53), 69–87. https://scielo.pt/scielo.php?script=sci_arttext&pid=S1646-989520240001000

Wang, Y., Xiao, R., Sun, J., & Jin, S. (2024). MC-Det: Multi-channel representation fusion for malicious domain name detection. Computer Networks, 255, 110847. https://www.sciencedirect.com/science/article/abs/pii/S1389128624006790?via%3Dihub

*What is IP Blacklist - Imperva*. (n.d.). Retrieved March 22, 2025, from https://www.imperva.com/learn/application-security/ip-blacklist/

*Why Apps Script isn't the Best Solution for Workflow Management in G Suite (Google Apps) - Kissflow*. (2025, February 14). https://kissflow.com/workflow/google-apps/why-apps-script-isnt-the-solution-for-workflow-in-google-apps/

## ANEXOS

En los anexos colocar sólo aquellos complementos que signifique evidencias o procedimientos realizados en la investigación de manera pertinente y suficiente. (Evitar excesos innecesarios)

Cada evidencia en los anexos va en hoja independiente.
Cada hoja que contenga un anexo debe ser numerada: ANEXO N° 1. Título del anexo.

Cuando el informe de Suficiencia Profesional, según requerimiento enmarcado en el Código de Ética de la UPN, cuenta con la Carta de autorización del Comité Institucional de Ética en Investigación (CIEI), ésta debe insertarse como Anexo N°1 (con carácter de obligatorio).

ANEXO N° 1