

**IMPLEMENTACIÓN DE IDS PARA FUNCIONARIOS QUE TRABAJAN DE
FORMA REMOTA Y DISEÑO DE POLÍTICAS DLP PARA LA CORPORACIÓN
UNIVERSITARIA AUTÓNOMA DEL CAUCA**



JULIÁN ALBERTO MOLANO MOLANO

**CORPORACIÓN UNIVERSITARIA AUTÓNOMA DEL CAUCA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS
POPAYÁN CAUCA**

2021

**IMPLEMENTACIÓN DE IDS PARA FUNCIONARIOS QUE TRABAJAN DE
FORMA REMOTA Y DISEÑO DE POLÍTICAS DLP PARA LA CORPORACIÓN
UNIVERSITARIA AUTÓNOMA DEL CAUCA**

**Trabajo de grado para optar por el título profesional en Ingeniería de
sistemas**

JULIAN ALBERTO MOLANO MOLANO

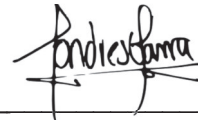
Director:

RODRIGO ARTURO CARREÑO VALLEJO

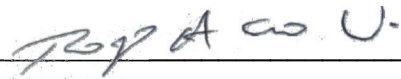
**CORPORACIÓN UNIVERSITARIA AUTÓNOMA DEL CAUCA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS
POPAYÁN CAUCA**

2021

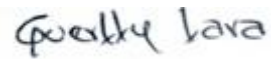
Nota de Aceptación



Ing Fabian Andrés Ibarra F.
Coordinador de seguridad de la información



Ing Rodrigo Arturo Carreño V.
Director Pasantía



MG José Guerlly Lara A.
Jurado



Ing Carlos Antonio Flórez
Jurado

Popayán, 09 de septiembre de 2022

AGRADECIMIENTOS

Este trabajo de grado se lo quisiera agradecer a Dios por guiar mi camino, a la CORPORACIÓN UNIVERSITARIA AUTÓNOMA DEL CAUCA por abrirme las puertas de su claustro y ser un profesional.

A mi director de trabajo de grado, Ing. Rodrigo Arturo Carreño V. y a los profesores de la corporación Universidad Autónoma del Cauca por brindar el conocimiento en mi formación como ingeniero, al coordinador del área de T.I el Ing. Fabian Ibarra, por la colaboración y disponibilidad que siempre mostro.

Por último y no menos importante a mi familia, mis padres, Bolívar Molano, Amparo Molano, mi hermana Patricia Molano, que siempre me brindaron un apoyo incondicional, queriendo siempre brindarme lo mejor; A mi hijo Sergio Molano que con su llegada marcó un cambio en mi vida dándole un impulso para seguir adelante y culminar mi carrera.

Tabla de contenido

| | |
|---|-----------|
| TABLA DE CONTENIDO | 5 |
| LISTA DE FIGURAS | 8 |
| LISTA DE TABLAS | 9 |
| RESUMEN | 9 |
| ABSTRACT | 10 |
| INTRODUCCIÓN | 11 |
| 1. CAPITULO I | 12 |
| 1.1 Problema/Oportunidad | 12 |
| 1.2 Hipótesis O Idea Inicial de Trabajo | 13 |
| 1.3 Objetivos | 13 |
| 1.3.1 Objetivo general | 13 |
| 1.3.2 Objetivos específicos | 14 |
| 2. CAPITULO II..... | 14 |
| 2.1 Aspectos teóricos | 14 |
| 2.1.1 Seguridad Informática..... | 14 |
| 2.1.1.1 Activos..... | 14 |
| 2.1.2 Políticas Seguridad | 15 |
| 2.1.2.1 Vulnerabilidad..... | 15 |
| 2.1.2.2 Amenazas | 15 |
| 2.1.2.2.1 Tipos de Amenazas..... | 15 |
| 2.1.2.3 Ataques | 16 |

| | |
|---|-----------|
| 3. CAPITULO III | 18 |
| 3.1 Metodología | 18 |
| 3.2 Estado inicial del proyecto | 19 |
| 3.2.1 Sophos..... | 19 |
| 3.2.1 Endpoint Protection | 20 |
| 3.2.1 Server Protection. | 21 |
| 3.2.1 Suricata..... | 21 |
| | |
| 4. CAPITULO IV | 20 |
| 4.1 Requerimientos funcionales | 22 |
| 4.2 Requerimientos no funcionales | 23 |
| 4.3 Historias de usuario | 24 |
| 4.4 Estado inicial del proyecto | 25 |
| 4.5 Marco de Trabajo Scrum | 21 |
| 4.6 Sprint 1 | 21 |
| 4.6.1 Análisis de reglas para políticas DLP | 20 |
| 4.6.2 Análisis de reglas para IDS | 20 |
| 4.6.3 Problemas encontrados | 20 |
| 4.7 Sprint 2 | 22 |
| 4.7.1 Modelado de reglas para políticas DLP | 20 |
| 4.7.2 Modelado de IDS | 20 |

| | |
|---------------------------------|----|
| 4.7.3 Diseño políticas DLP..... | 20 |
| 4.7.4 Diseño de IDS..... | 20 |
| 4.8 Sprint 3 | 22 |
| 4.9 Sprint 4 | 22 |

INDICE DE FIGURAS

| | |
|---|-----------|
| <i>Figura 1. Panel central Sophos</i> | <i>22</i> |
| <i>Figura 2. Panel de control Endpoint Protection</i> | <i>22</i> |
| <i>Figura 3. Panel de control Server Protection</i> | <i>23</i> |
| <i>Figura 4. Logo suricata</i> | <i>24</i> |
| <i>Figura 5. Instalación Suricata-6.0.3-1-64bit.msi</i> | <i>26</i> |
| <i>Figura 6. Reportes eve.json</i> | <i>27</i> |
| <i>Figura 7. Un reporte JSON.</i> | <i>27</i> |
| <i>Figura 8. Reporte JSON.</i> | <i>28</i> |
| <i>Figura 9. Implementación políticas DLP Endpoint Protection.</i> | <i>29</i> |
| <i>Figura 10. Reglas dentro de la política DLP Endpoint Protection</i> | <i>29</i> |
| <i>Figura 11. Configuración políticas DLP Endpoint Protection. Reglas de archivo documento.</i> | <i>30</i> |
| <i>Figura 12. Configuración políticas DLP Endpoint Protection. Reglas de archivo imagen</i> | <i>30</i> |
| <i>Figura 13. Implementación políticas DLP Server Protection</i> | <i>31</i> |
| <i>Figura 14. Reglas dentro de la política DLP Server Protection</i> | <i>31</i> |
| <i>Figura 15. Configuración políticas DLP Server Protection. Reglas de archivo Datos</i> | <i>32</i> |
| <i>Figura 16. Configuración políticas DLP Server Protection. Reglas de archivo Documentos</i> | <i>32</i> |
| <i>Figura 17. Configuración políticas DLP Server Protection. Reglas de archivo imágenes</i> | <i>33</i> |
| <i>Figura 18. Server Protection - Registro de eventos de prevención de pérdida de datos</i> | <i>34</i> |
| <i>Figura 19. Endpoint Protection - Registro de eventos de prevención de pérdida de datos</i> | <i>35</i> |

TABLA DE GRAFICOS

Gráfico 1 Equipos que más descargan o envían documentos

33

RESUMEN

El presente informe de pasantía se basa en la implementación de políticas DLP y de la implementación de una herramienta IDS para mejorar la seguridad de la Corporación Universitaria Autónoma del Cauca, se realizó un diseño de políticas tratando de mejorar el control de documentos, imágenes, información personal que podría tomarse como una pérdida de datos.

En lo referente a la herramienta IDS se tomó en consideración las de tipo de código abierto, teniendo en cuenta su funcionabilidad, con un buen rendimiento.

ABSTRACT

This internship report is based on the implementation of DLP policies and the implementation of an IDS tool to improve the security of the Autonomous University Corporation of Cauca, a policy design was carried out trying to improve the control of documents, images, personal information that could be taken as a data loss.

Regarding the IDS tool, those of the open source type were taken into consideration, taking into account their functionality, with good performance.

INTRODUCCIÓN

Los continuos avances tecnológicos, dan pie para una globalización en la economía, la marcada necesidad de poseer la mayor cantidad de información y consigo los sistemas que la suministran, llevan consigo una fragilidad con una inmensa visión para amenazas. Las amenazas a las que más se tendrían son las cibernéticas.

Esto nos lleva a mejoras con controles que se le deben efectuar a la red, estos controles se inician principalmente en el diagnóstico y revisión de la manera que tiene la empresa actualmente los sistemas; que tan buen manejo tiene de sus políticas, con esto teniendo la posibilidad de disminuir la posibilidad de un ataque cibernético.

Las instituciones como empresa tienen la necesidad que mejorar, y la parte tecnológica es de las más importantes, ya que, con el constante crecimiento de nuevas tecnologías, hace las instituciones se conviertan en blancos fáciles y vulnerables.

CAPÍTULO I

1.1 PROBLEMA/ OPORTUNIDAD:

Se han visto en estos días diversos ataques realizados a diferentes entidades tanto públicas como privadas, con esto vemos que nadie está completamente bien resguardado de los ataques de hackers. Una de la forma de controlar estos ataques es implementar un Firewall que ayude a cerrar diferentes puertos que no estén en uso. Lastimosamente esto no es suficiente ya que el Firewall restringe servicios no autorizados, pero permite el paso de aquellos que el o los usuarios detrás del Firewall necesita usar. El problema se encuentra en ese punto. Aunque se utilice para servicios hipotéticamente seguros, no obstante, se encuentran vulnerabilidades que se pueden aprovechar, por lo que el Firewall queda sin poder hacer nada (servicio autorizado, lo deja pasar).

Un IDS puede convertirse en una excelente herramienta para optimizar la protección de los sistemas. En algunos casos el Firewall puede llegar a estar comprometido, es preciso disponer de un sistema que ayude a descubrir este hecho.

De los problemas más críticos que puede presentar una empresa o institución, es no solo la pérdida, también: alteración, secuestro, indisponibilidad, ya que estos datos son considerados como un activo muy valioso para la institución: (La información hace parte de un activo). Los cuales están propensos a ser divulgados por diferentes medios digitales: Así abarcas todos no solo correos o copias de discos locales.

La Corporación Autónoma del Cauca tiene alto manejo de información los cuales sin un adecuado manejo puede generar una serie de inconvenientes en la gestión de la información, comprometiendo principios de integridad, disponibilidad y confiabilidad de la información.

1.2 HIPÓTESIS O IDEA INICIAL DE TRABAJO:

Con el aumento de las tecnologías de la información, se ha incrementado las intrusiones para estos sistemas. Por esto las instituciones buscan reforzar sus líneas de defensa empleando los IDS (*Intrusion Detection System*), la finalidad de esta herramienta es descubrir, determinar e identificar cualquier uso no autorizado, duplicación, alteración y destrucción de información del sistema.

Los IDS (*Intrusion Detection System*) Hacen parte de los módulos de un Firewall al igual que los Módulos de Control de Accesos, Endpoint NAC, Módulo Antivirus / Antispyware, cuando estos han sido vulnerados por algún atacante, el cortafuegos filtra los datos y el IDS posteriormente los analiza de acuerdo con los criterios de firmas. Con esto se determina si pasaron paquetes maliciosos que puedan comprometer la seguridad de la información.

La información que maneja una institución hace parte muy importante en los activos, ya que esta da una ventaja para quien la posee, esto también interfiere en el éxito de una empresa. Con más frecuencia se conocen noticias de fugas de información. Por estas razones para una empresa es importante contar con un protocolo de seguridad para cuidar su información.

1.3 OBJETIVOS:

1.3.1 GENERAL:

- Implementar un sistema IDS y configurar las políticas DLP que complementen y fortalezcan el sistema de seguridad con el que actualmente cuenta la Corporación Universitaria Autónoma del Cauca.

1.3.2 ESPECÍFICOS:

- Estimar un sistema que complemente el Firewall con el que actualmente cuenta la Universidad para afianzar la seguridad de los usuarios.

- Recomendar unas políticas de DLP para el tratamiento de la información.
- Analizar diferentes soluciones IDS que existen en el mercado para resolver los problemas de intrusión.

CAPÍTULO II

2.1 ASPECTOS TEÓRICOS:

2.1.1 Seguridad Informática

La seguridad informática es basada en la defensa contra los daños ocasionados o padecidos por sistema informático y realizados por el acto intencional y de mala fe de una persona,

Los recursos informáticos hacen parte muy importante de la empresa, ya que al estar conectadas en la red de redes estas pueden sufrir irrupciones para con sus datos. Por esto se hace importante la seguridad informática, ya que esta consiste en implementar métodos para proteger la información de la empresa. Así como despliegue de antivirus, firewall, detección de intrusos, detección de anomalías, corrección de eventos, atención e incidentes.

2.1.1.1 Activos

Tomando como base la información recopilada, los activos son los diferentes componentes que la seguridad informática tiene como finalidad proteger, dichos componentes son:

- **Información:** es el componente con mayor importancia en una organización. Esto implica tener una mayor prioridad en el instante que se deba proteger.
- **Dispositivos:** hacen parte de él las herramientas tanto como hardware, como las herramientas software, además de los componentes estructurales que brindan servicio.
- **Usuarios:** el personal que tiene a disposición la infraestructura dispuesta para la administración de la información, con el fin de originar mayor competencia con dicha información.

2.1.2 Políticas de seguridad.

Las políticas de seguridad se deben encaminar a conservar un estado fiable, con esto se concluye que es conveniente una adecuada implementación de reglas y así definir las responsabilidades de los que tienen incidencia sobre el manejo de la información. Esto para así proteger el acceso a la información de la empresa.

2.1.2.1 Vulnerabilidad: Esta palabra da entender que la empresa tiene algún tipo de debilidad con el cual puede sufrir posibles ataques contra sus sistemas de información, ya que los ciberdelincuentes buscan beneficiarse entrando para robar la información sensible o bloquear su funcionamiento, generando contratiempos para la empresa.

2.1.2.2 Amenazas: Estas amenazas suelen confundirse de manera errónea con vulnerabilidades. La amenaza no es un problema de debilidad que tenga la empresa, no obstante, es algo que puede quebrantar la seguridad de la empresa. Al tener alguna vulnerabilidad estas pueden ser aprovechadas para un ataque convirtiéndose en una amenaza.

Las amenazas son de carácter continuo ya que pueden suceder en el momento menos esperado

2.1.2.2.1 Tipos de Amenazas

- **Amenazas Físicas:** Estas amenazas están relacionadas con las instalaciones donde se está manejando el almacenamiento de la información.
 - Instalaciones poco adecuadas
- **Amenazas Naturales:** Este tipo de amenazas está relacionado con los desastres naturales que lleguen a poner en peligro la información.
 - Instalaciones que puedan verse afectadas con terremotos, tormentas,

- Incendios, instalaciones con poca protección contra este.
- Inundaciones, con instalaciones cerca de caudales de ríos.
- **Amenazas de Hardware:** Esta amenaza se basa en la falla de los equipos por fallos en fabricación o en una manera adecuada en su utilización. Convirtiéndose en una vulnerabilidad facilitando los ataques.
 - La falta de actualizaciones
 - El mal manejo de los equipos.
 - La poca configuración de respaldos o equipos de contingencia
- **Amenazas Software:** la instalación de programas clandestinos los cuales pueden conllevar a infiltraciones o accesos de personas inescrupulosas.
 - Programas para la automatización de procesos.
 - Editores de texto que facilitan la ejecución de virus de macro etc.

2.1.2.2.2 Ataques:

- **Ataque fuerza bruta:** Este método consiste en experimentar todas las posibles combinaciones hasta detectar la combinación correcta.
- **Ataque combinado:** de los ataques puede ser uno de los más ofensivos, ya que combinan diferentes virus informáticos (gusanos, troyanos y códigos maliciosos). Este aprovecha vulnerabilidades para propagarse rápidamente y así ocasionar la mayor cantidad de daños.

- **Ataque de repetición:** La forma para protegerse de este tipo de ataques es necesario tomar medidas como implementar un control de identificación.

CAPÍTULO III

3.1 ASPECTOS METODOLÓGICOS

La metodología usada en esta investigación fue la de tipo: "Aplicada", ya que se implementó una tecnología, probada y aceptada en la industria para realizar el intercambio de información entre aplicativos de software.

Con el paso del tiempo las técnicas de penetración y seguridad informática han brindado infinidad de herramientas que permiten realizar ataques y monitoreo para los diferentes sistemas de información. En este proyecto se emplearán cuatro fases: Análisis, Diseño, implementación y pruebas.

En la primera fase se hará la toma de requerimientos y datos útiles para la toma de decisiones. En la segunda fase se procederá a diseñar la arquitectura del sistema de detección de intrusiones. En la tercera fase se dará paso a implementar el sistema. Por último, se harán validaciones y pruebas del producto.

Para la elaboración de este proyecto, se optó por el uso del marco de referencia ágil, específicamente el que brinda apoyo en la gestión de proyectos, en este caso el marco de referencia será SCRUM, el cual se caracteriza por la flexibilidad y facilidad para la gestión de proyectos en equipos pequeños, que trabajen en proyectos donde los requisitos cambien rápidamente.

Scrum, es un marco de trabajo basado en los métodos ágiles, que tiene como objetivo el control continuo sobre el estado actual de las tareas, en el cual el cliente establece las prioridades y el equipo Scrum se auto-organiza para determinar la mejor forma de entregar resultados.

El marco de trabajo SCRUM usa tres roles y unos elementos que implementaremos en nuestro desarrollo:

Roles.

- Product Owner: Representa a todos los interesados en el producto final que en este caso sería la división de TI y medios Educativos de la corporación universitaria autónoma del Cauca.

- Scrum Master: Ayuda al grupo del producto a aprender y aplicar scrum para conseguir valor de negocio. El scrum master hace todo lo que sea necesario para ayudar a que el equipo tenga éxito.
- Team: Equipo de trabajo. Responsable de transformar el Backlog en un incremento funcional, es decir, convertir el “product backlog” en un producto entregable.

3.2 Estado inicial del proyecto

Al iniciar este proyecto se hace un estudio de la condición de las políticas DLP y IDS. Definiendo que la Corporación Universidad Autónoma del Cauca, dispone de un software (SOPHOS), para implementar las políticas DLP. Mas no se dispone de un motor IDS, se busca un programa código abierto que sea eficiente, entre las opciones se encuentran: suricata y zeek. Para escoger cual, de los dos, se tendrá en cuenta el consumo de recursos.

3.2.1 Sophos

Sophos sintetiza la tarea de la protección de los ordenadores de escritorio, ordenadores portátiles, dispositivos móviles y servidores de archivos, contra amenazas conocidas y desconocidas, además de proteger la institución contra la pérdida accidental de datos.

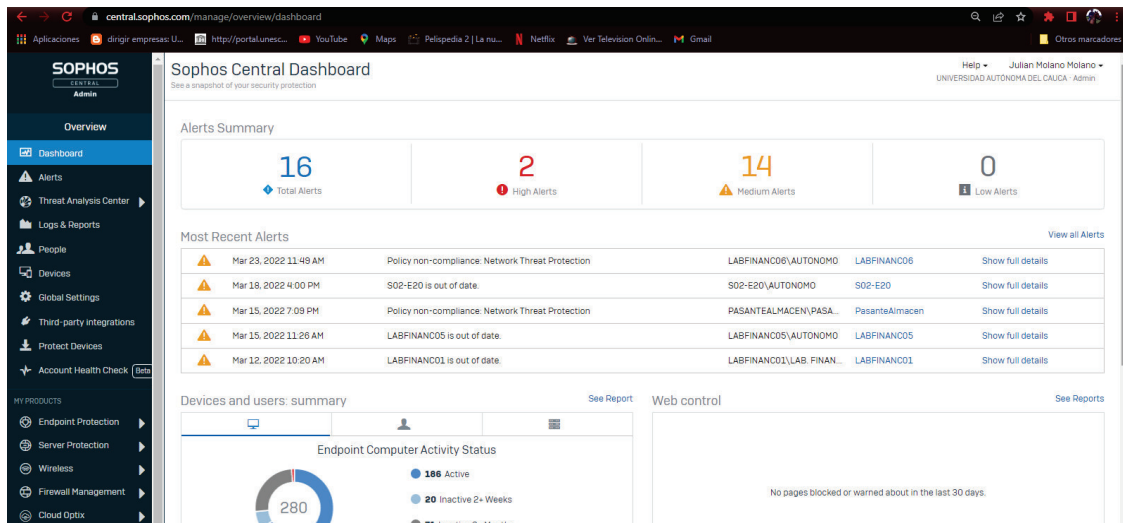


Figura 1 Panel central Sophos

- **Endpoint Protection.**

Permite salvaguardar a los usuarios y dispositivos contra software maliciosos, tipos de archivo y sitios web peligrosos y tráfico de red malicioso.

Las políticas se utilizan para aplicar protección a usuarios y dispositivos.

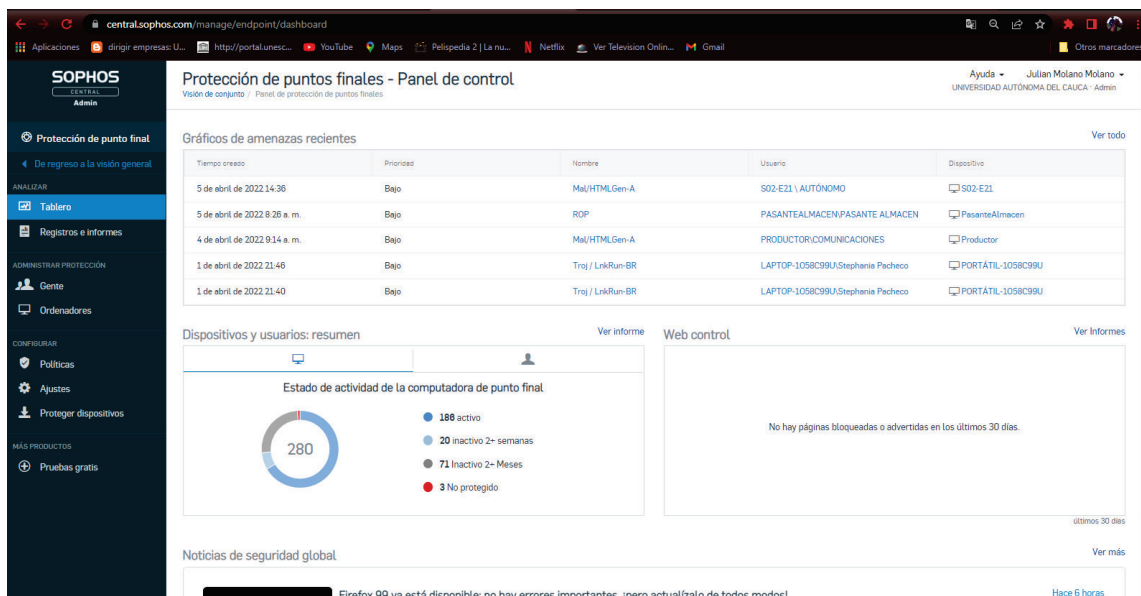


Figura 2 Panel de control Endpoint Protection

- **Server Protection.**

Protege los servidores contra programas maliciosos, tipos de archivo y sitios web peligrosos y tráfico de red malicioso. También ofrece control de periféricos, control web y bloqueo de servidor, lo que le permite controlar el software que ejecuta en sus servidores.

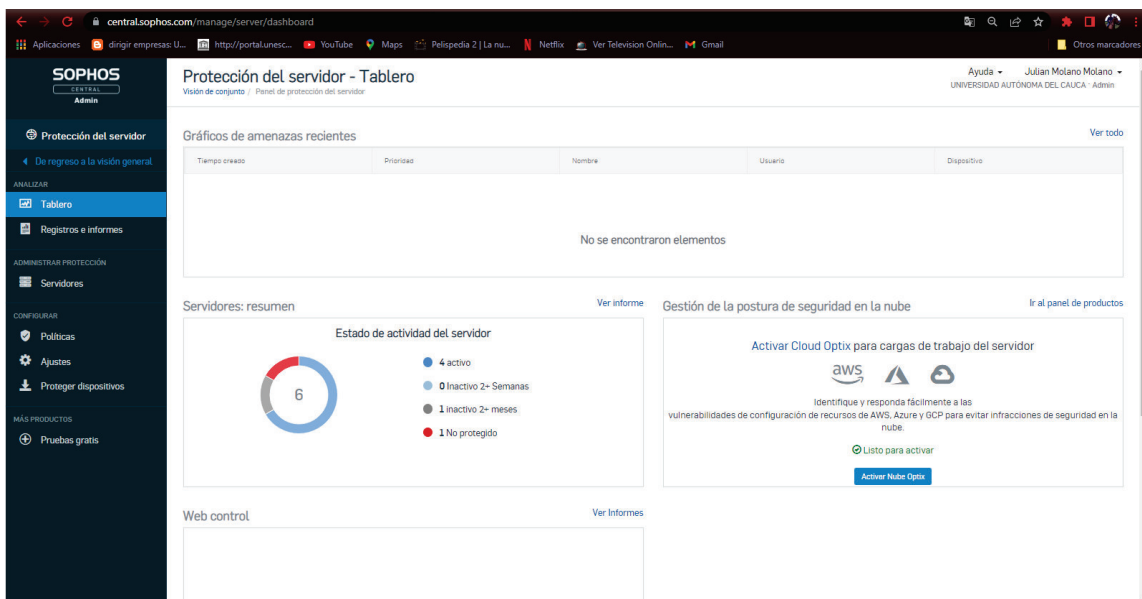


Figura 3 Panel de control Server Protection

3.2.2 Suricata IDS

Tomando en cuenta las opciones con las que se disponía en la escogencia de la herramienta IDS, se encontró una opción muy interesante: El motor Suricata IDS que se basa en código abierto para la seguridad en la red, El cual tiene una gran superioridad respecto a las demás herramientas IDS más modernos, y es que se favorece de otras reglas ya creadas durante años.



Figura 4 Logo suricata <https://suricata.io/download/>

CAPÍTULO IV

4.1 Marco de trabajo scrum

Se crea la lista priorizada de productos (prioritized product backlog) la cual debe contener:

Documentación funcionamiento de software tipo IDS para UAC.

4.1.1 Sprint 1 (2 semanas)

- a. Planificación del sprint (Sprint planning meeting)
- b. Sprint backlog
 - i. Análisis de servicios y servidores a monitorear.
 - ii. Análisis de alertas que debe generar el IDS.
- c. Reunión diaria (Daily Meeting)
 - i. Evidencia progreso diario
- d. Entregables
 - i. Arquitectura IDS y modelo monitoreo, alertas y notificaciones.

Se instalará un IDS, evidenciará el proceso para emparejar los datos de netflow de un sistema con los procesos de Windows que crearon cada flujo.
 - ii. Lista de servicios a monitorear.

Se realizaron estudios de los IDS que daban mejor rendimiento para la realización del proyecto. Se documentará para una adecuada instalación, Se encontraron impedimentos, como la versión adecuada de suricata y determinar si se podía instalar en Windows o era necesaria una máquina virtual.

4.1.2 Sprint 2 (2 semanas)

- a. Planificación del sprint (Sprint planning meeting)
- b. Sprint backlog

i. Implementación de la arquitectura IDS.

La arquitectura IDS que se implementará es SURICATA. El cual es un motor para monitorear la seguridad, IPS e IDS de red con un alto rendimiento. Es de código abierto desarrollada por OISF.

ii. Instalación del IDS. Se realizó la instalación de Suricata-6.0.3-1-64bit.msi con la versión Npcap 1.60 para Windows.

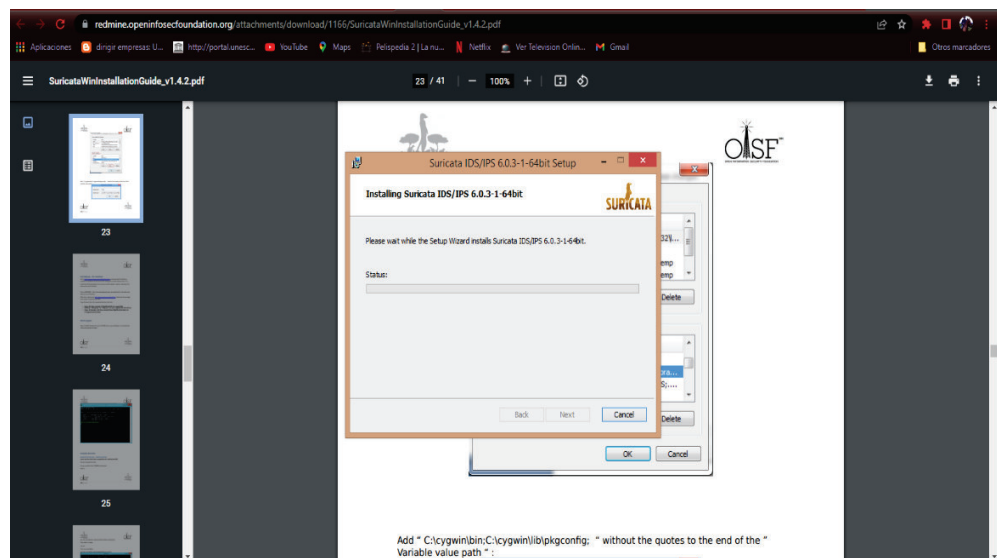


Figura 5 Instalación Suricata-6.0.3-1-64bit.msi

iii. Garantizar la comunicación con los servidores

c. Reunión diaria (Daily Standup)

i. Evidencia progreso diario

ii. Identifican problemas

d. Entregables

i. Diseño de la arquitectura IDS.

4.1.3 Sprint 3 (2 semanas)

a. Planificación del sprint (Sprint planning meeting)

b. Sprint backlog

i. Diseñar reportes (como medir la eficacia del IDS)

Los ficheros son guardados por defecto en un formato JSON por cada evento generado se crea una nueva línea.

ii. Generar Reportes.

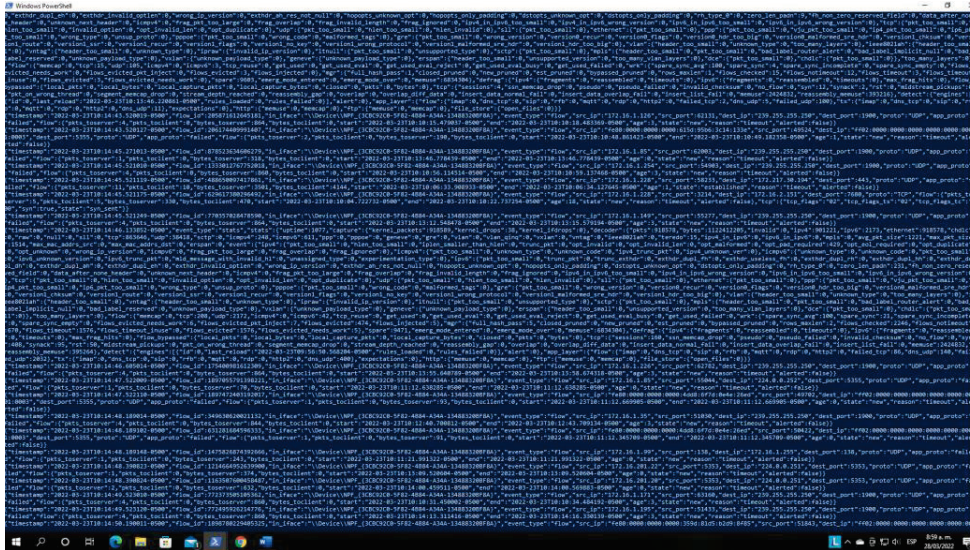


Figura 6 Reportes eve.json

iii. Publicar Reportes.

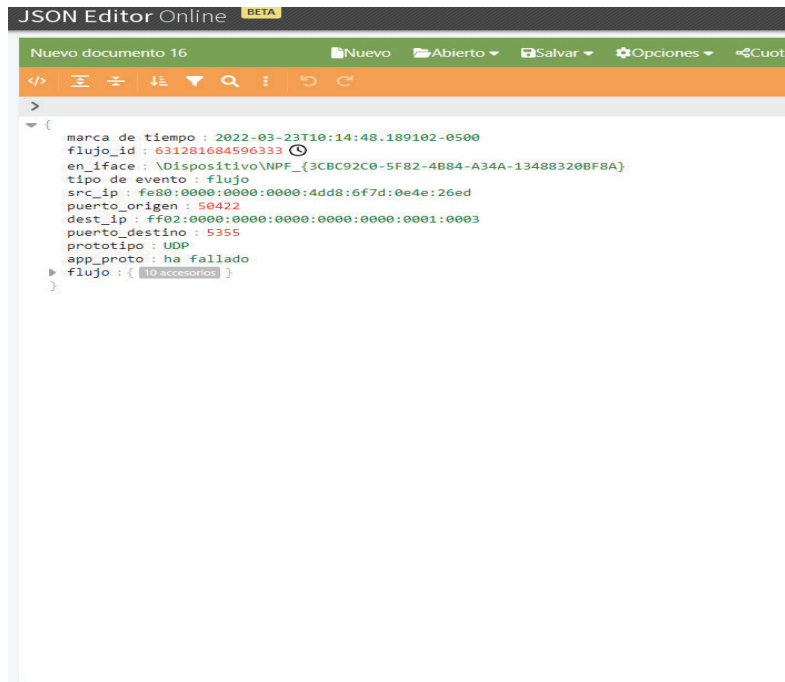


Figura 7 Un reporte JSON

```
{
  "marca de tiempo": "2022-03-23T10:14:45.521175-0500",
  "flujo_id": "629617380296492",
  "en_iface": "\\Dispositivo\\NPF_{3CBC92C0-5F82-4B84-A34A-13488320BF8A}",
  "tipo de evento": "flujo",
  "src_ip": "172.16.1.228",
  "puerto_origen": "3214",
  "dest_ip": "172.16.2.151",
  "puerto_destino": "7680",
  "prototipo": "TCP",
  "flujo": {
    "10 accesorios": {}
  },
  "tcp": {
    "5 accesorios": {}
  }
}
```

Figura 8 reporte JSON

- c. Reunión diaria (Daily Standup)
 - i. Evidencia progreso diario

4.1.4 Sprint 4 (4 semanas) DLP

- a. Planificación del sprint (Sprint planning meeting)
- b. Sprint backlog
 - i. Sophos DLP documentación y soporte
 - ii. Diseño de políticas para el DLP
 - iii. Implementación políticas

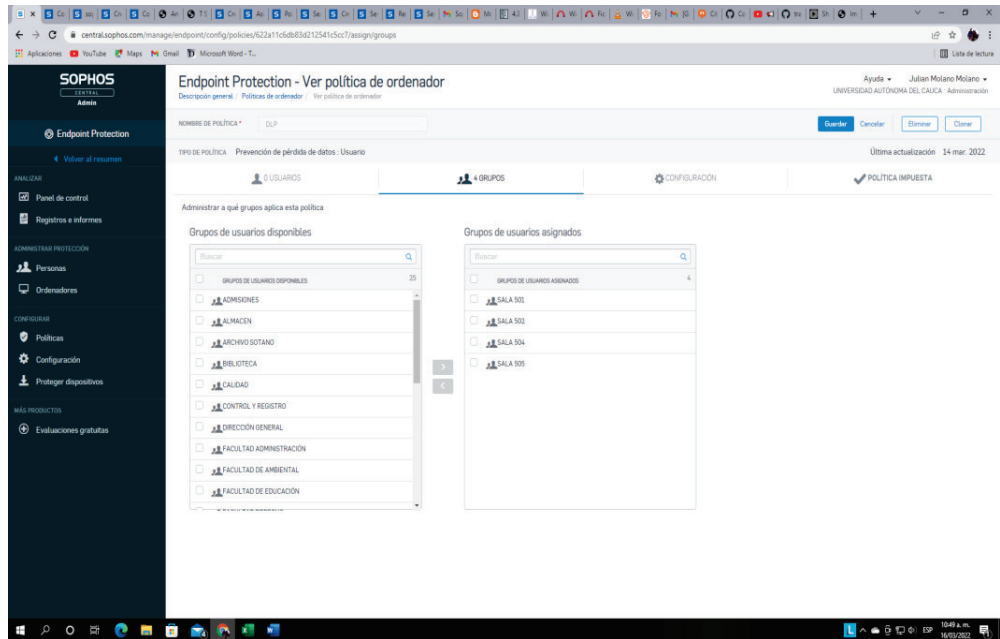


Figura 9 Implementación políticas DLP Endpoint Protection

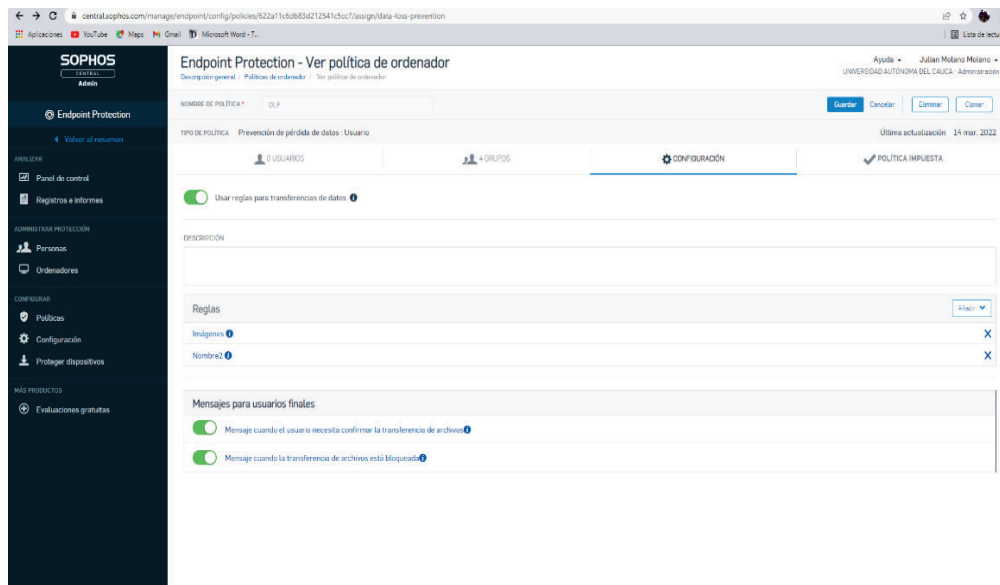


Figura 10 Reglas dentro de la política DLP Endpoint Protection

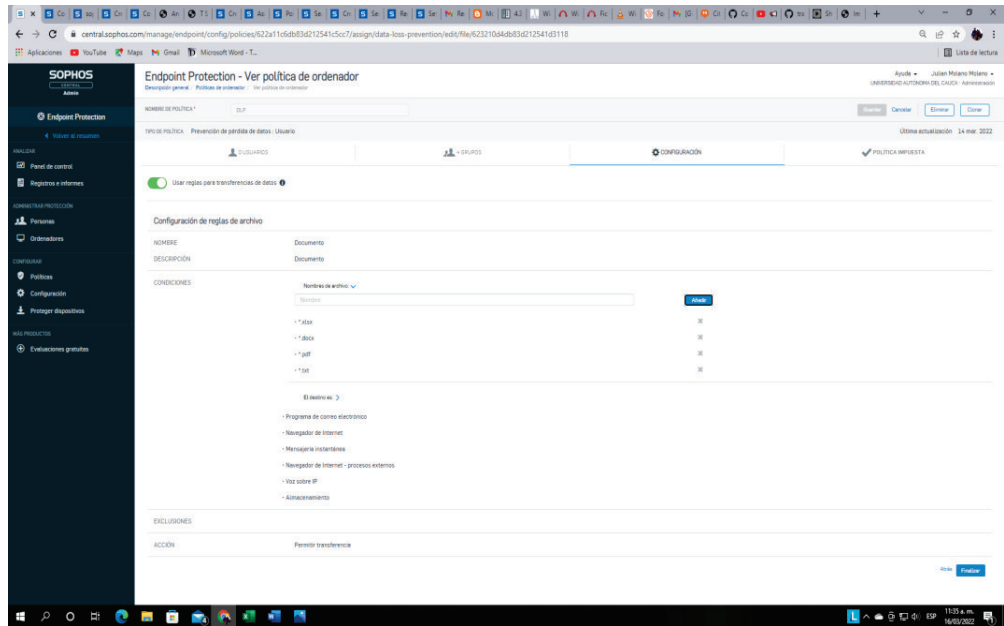


Figura 11 Configuración políticas DLP Endpoint Protection. Reglas de archivo documento

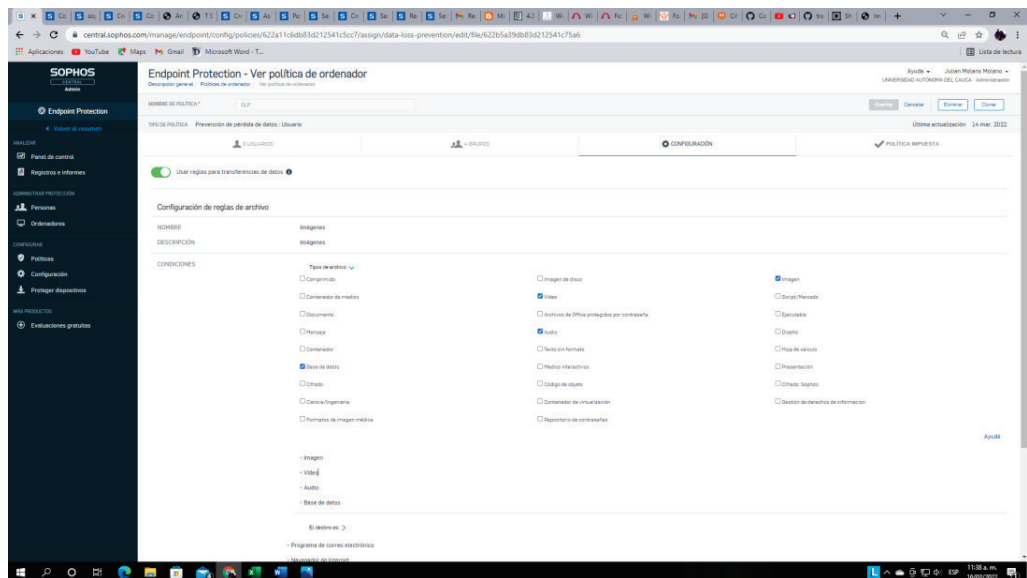


Figura 12 Configuración políticas DLP Endpoint Protection. Reglas de archivo imagen

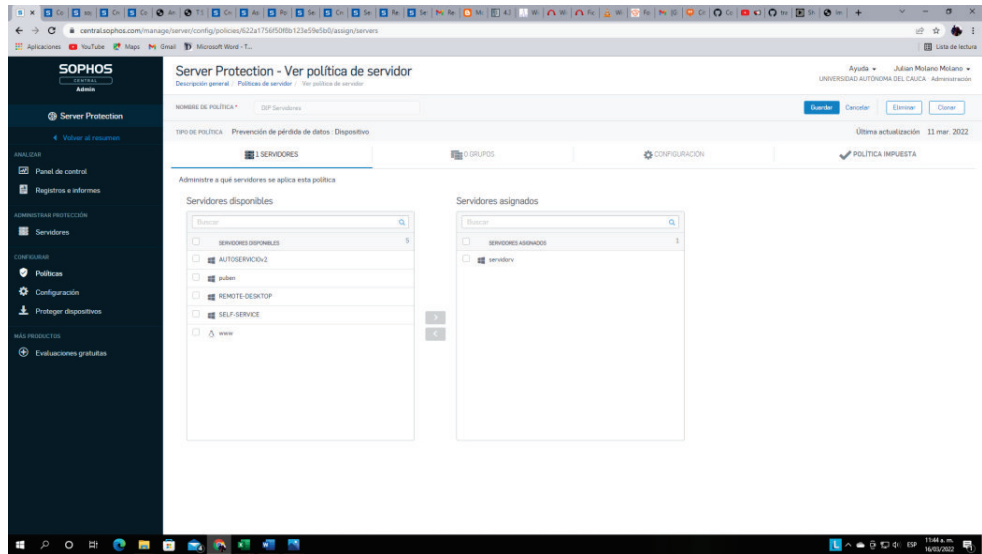


Figura 13 Implementación políticas DLP Server Protection.

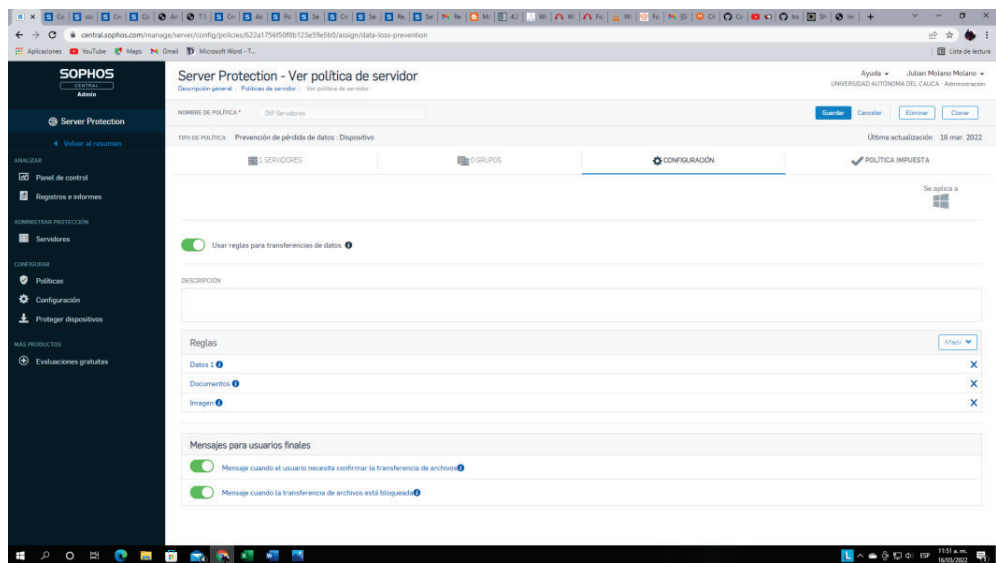


Figura 14 Reglas dentro de la política DLP Server Protection.

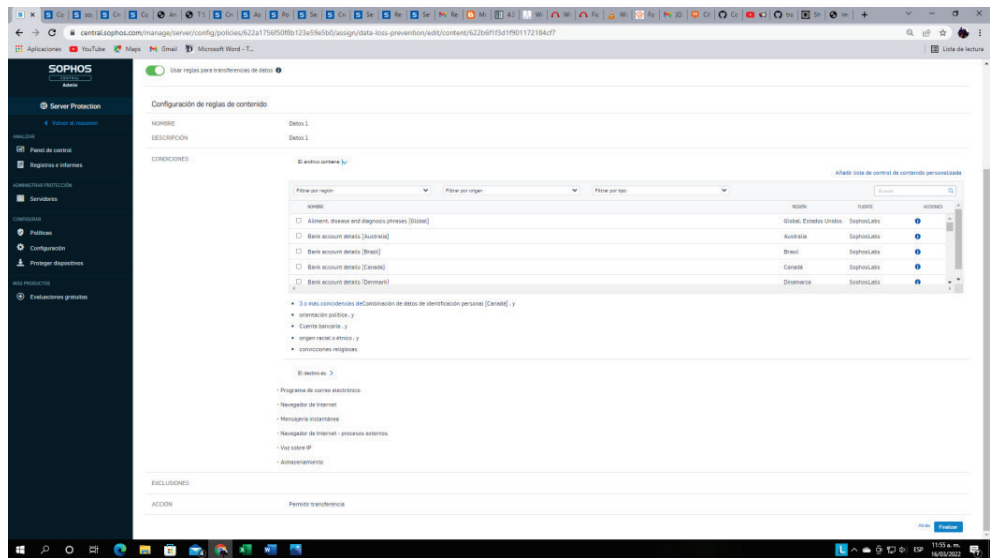


Figura 15 Configuración políticas DLP Server Protection. Reglas de archivo Datos

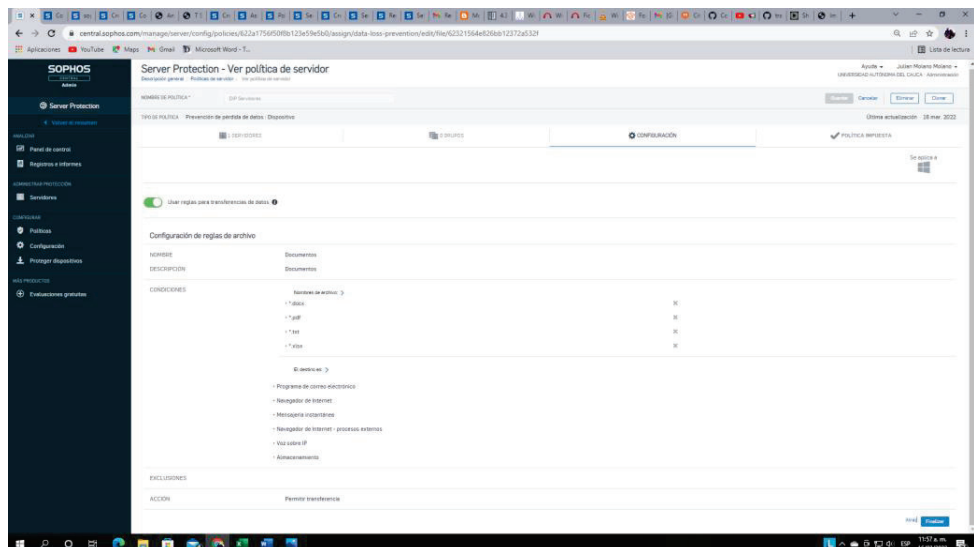


Figura 16 Configuración políticas DLP Server Protection. Reglas de archivo Documentos

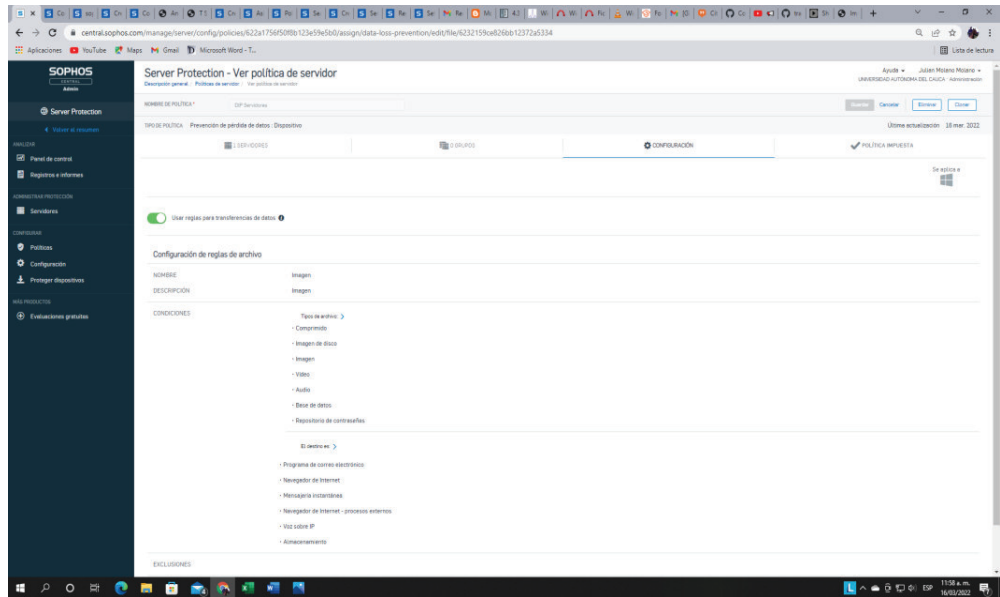


Figura 17 Configuración políticas DLP Server Protection. Reglas de archivo imágenes

iv. Pruebas políticas DLP



Gráfico 1 Equipos que más descargan o envían documentos

c. Reunión diaria (Daily Standup)

- i. Evidencia progreso diario
 - d. Entregables
 - i. Guía implementación de políticas de protección DLP en el software SOPHOS.
 - ii. Políticas implementadas en SOPHOS.
- Las políticas DLP creadas en Sophos son para detectar la salida o descarga de documentos, imágenes, tanto en los Endpoint Protection y los Server Protection.
- Envío de información relevante como convicciones religiosas, grupo étnico, cuenta bancaria.
- Con destino a correo electrónico, navegador internet, mensajería instantánea, navegador internet (procesos externos), Voz IP, almacenamiento.
- iii. Reporte cumplimiento o no de la política.

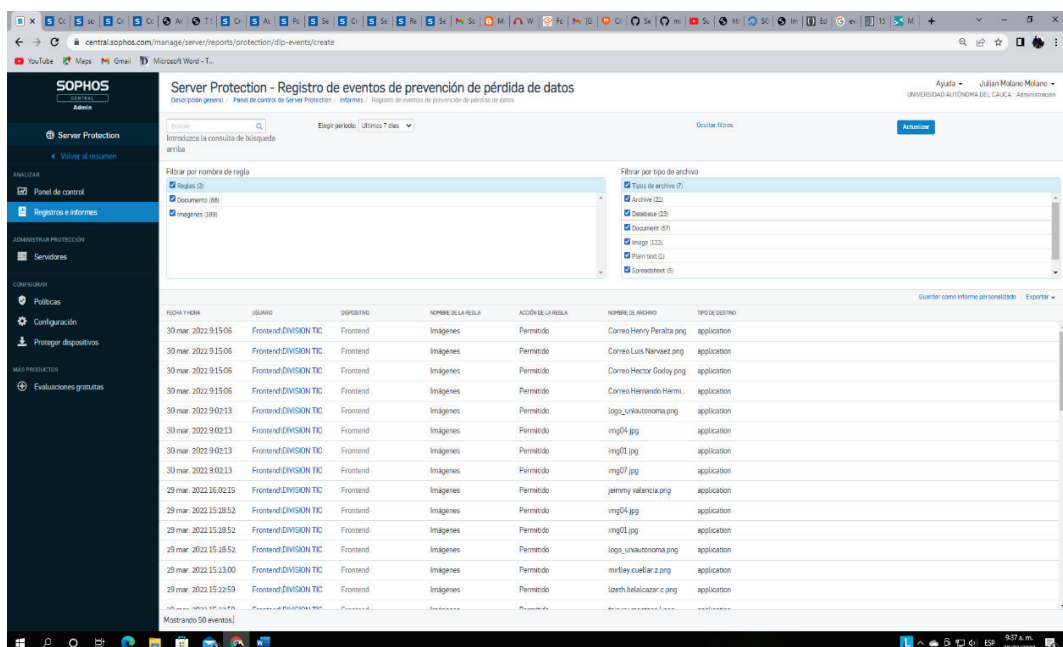


Figura 18 Server Protection - Registro de eventos de prevención de pérdida de datos

Endpoint Protection - Registro de eventos de prevención de pérdida de datos

Descripción general Panel de control de Endpoint Protection Informes Registro de eventos de prevención de pérdida de datos

Introduzca la consulta de búsqueda de reglas

Filtrar por nombre de regla

- Reglas (2)
- Excepciones (0)
- Indicados (20)

Filtrar por tipo de archivo

- Tipo de archivo (2)
- Imagen (2)
- Documento (2)
- Hoja (2)
- Plantilla (2)
- ScreenShot (2)

| FECHA Y HORA | USUARIO | SISTEMA | NOMBRE DE LA REGLA | ACCION DE LA REGLA | NOMBRE DE APLICACION | TIPO DE APLICACION |
|-----------------------|-----------------------|----------|--------------------|--------------------|--------------------------|--------------------|
| 30 mar. 2022 8:15:00 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | Correo Henry Penales.png | application |
| 30 mar. 2022 8:15:00 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | Correo Luis Navarret.png | application |
| 30 mar. 2022 8:15:00 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | Correo Hector Godoy.png | application |
| 30 mar. 2022 8:15:00 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | Correo Hernandez Herm... | application |
| 30 mar. 2022 8:02:13 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | loginextension.png | application |
| 30 mar. 2022 8:02:13 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | img01.jpg | application |
| 30 mar. 2022 8:02:13 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | img07.jpg | application |
| 29 mar. 2022 18:03:35 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | jeremy.valencia.png | application |
| 29 mar. 2022 18:28:52 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | img04.jpg | application |
| 29 mar. 2022 18:28:52 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | img05.jpg | application |
| 29 mar. 2022 18:28:52 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | loginextension.png | application |
| 29 mar. 2022 18:23:00 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | marley.ouellar.x.png | application |
| 29 mar. 2022 18:22:59 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | lorth.babalocar.x.png | application |
| 29 mar. 2022 18:22:59 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | tecury.montero.x.png | application |
| 29 mar. 2022 18:22:58 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | claudia.villegas.x.png | application |
| 29 mar. 2022 18:22:36 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | img04.jpg | application |
| 29 mar. 2022 18:22:36 | Frontend DIVISION TIC | Frontend | Imágenes | Permitido | img05.jpg | application |

Mostrando 180 eventos.

Figura 19 Endpoint Protection - Registro de eventos de prevención de pérdida de datos

CONCLUSIONES Y RECOMENDACIONES

Se implementaron con éxito las políticas DLP en la plataforma Sophos, lo cual permite tener un mejor control de los datos.

Se planteó una herramienta que permita mitigar la problemática de pérdida de información sensible para la Uniautónoma, la cual se basó en software libre como lo es Suricata IDS u mediante políticas DLP en la plataforma Sophos.

La implementación de las políticas DLP ayuda a bajar la fuga de información más se está lejos de tener un 100% de efectividad por esto es recomendable en tener controles.

BIBLIOGRAFÍA

1. Aguilar G., Martínez A., Morales V. (2007) Sistema Detección De Intrusos Para Una Red Inalámbrica De Una PyME. Tesis MG Becerril H., ING Ángeles W. Instituto Politécnico Nacional Escuela Superior De Ingeniería Mecánica Y Eléctrica de México, FAC ING
2. Reyes C. (2016) Diseño, Optimización E Implementación De Un Sistema De Detección De Intrusiones Híbrido. Tesis Malonnek R., González A. Universidad Técnica Federico Santa María de Chile. FAC ING.
3. Rendón M. (2014) Prevención Y Minimización De Fuga De Información Implementando DLP (Data Loss Prevention). Tesis ING Aguilar F. Universidad del Azuay de Ecuador. FAC CIEN ADMIN.
4. El Título De: Ingeniero En Informática Presenta: QPHC." Importancia de la seguridad en informática" [Internet]. Edu.mx. [citado el 24 de agosto de 2021]. Disponible en:
<http://repositorio.upsin.edu.mx/formatos/182016030052BastidasMorenoJosephRaul8495.pdf>
5. Marco teórico seguridad informática y de la información - El rincon del hacking etico [Internet]. Google.com. [citado el 24 de agosto de 2021]. Disponible en:
<https://sites.google.com/site/elrincondelhackingetico/marco-teorico-seguridad-informatica-y-de-la-informacion>.
6. Incibe.es. [citado el 25 de agosto de 2021]. Disponible en:
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf
7. Entradas VM. 5.3- Amenazas y Vulnerabilidades [Internet]. Adolfoaraujo.com. 2008 [cited 2021 Aug 25]. Available from:
<https://adolfoaraujo.com/2008/11/18/53-amenazas-y-vulnerabilidades/>

8. (N.d.). Gov.Co. Retrieved September 16, 2021, from <http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf>
9. (Dakota del Norte). Edu.Co. Recuperado el 24 de septiembre de 2021 de <http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2511/0058A811.pdf?sequence=1&isAllowed=y>
10. *Ataque de fuerza bruta (Ciberseguridad)*. (2018, 30 marzo). Glosarios especializados. <https://glosarios.servidor-alicante.com/ciberseguridad/ataque-de-fuerza-bruta>
11. Sánchez, N. R. (2017, 10 enero). *Vulnerabilidades en redes*. TechClub Tajamar. <https://techclub.tajamar.es/vulnerabilidades-en-redes/>
12. (Dakota del Norte). Edu.Co. Obtenido el 26 de octubre de 2021 de <https://repository.udistrital.edu.co/bitstream/handle/11349/4258/MaciasMendezXiomaraMayerli2015.pdf%3Bjsessionid%3D3653429B8E6D9BB8C65076EC12EDFDCA?sequence=9>
13. Business News Daily Editor. (2013, August 26). *What is agile scrum methodology?* Businessnewsdaily.Com; [businessnewsdaily.com. https://www.businessnewsdaily.com/4987-what-is-agile-scrum-methodology.html](https://www.businessnewsdaily.com/4987-what-is-agile-scrum-methodology.html)
14. Fowler, F. M. (2019). What is scrum? In *Navigating Hybrid Scrum Environments* (pp. 3–8). Apress.
15. Blokdyk, G. (2020). *Data loss prevention A complete guide - 2020 edition*. 5starcooks.
16. *Data Loss Prevention Policy*. (2021). (C) Copyright 2021. <https://docs.sophos.com/central/Customer/help/en-us/central/Customer/concepts/datalossprevention.html>
17. Chalá Ibarra, E. R. C. I. (2020, septiembre). *Propuesta de un modelo de seguridad para la prevención de pérdida de Información Sensible Dirigido a La Asamblea Nacional*. Universidad Internacional Sek Digital School.

18. *Endpoint Protection*. (2022, 23 febrero). Docs.sophos.com.
<https://docs.sophos.com/central/Customer/help/en-us/central/Customer/concepts/EndpointProtection.html>
19. *Endpoint Protection*. (2022, 23 febrero). Docs.sophos.com.
<https://docs.sophos.com/central/Customer/help/en-us/central/Customer/concepts/EndpointProtection.html>
- 20.1. *What is Suricata — Suricata 6.0.0 documentation*. (2019). Guía Del Usuario de Suricata. Recuperado 28 de marzo de 2022, de <https://suricata.readthedocs.io/en/suricata-6.0.0/what-is-suricata.html>
21. C. (2020, 9 mayo). GitHub - Compiler-Error/Netstat-Suricata-ProcessName. GitHub. Recuperado 30 de marzo de 2022, de <https://github.com/Compiler-Error/Netstat-Suricata-ProcessName>