UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERÍA
CARRERA DE TELECOMUNICACIONES

Desarrollo de estrategias de ciberseguridad para la protección de la infraestructura tecnológica de la Universidad Nacional de Chimborazo utilizando la detección y respuesta de Endpoints.

Trabajo de Titulación para optar al título de:
Ingeniero en Telecomunicaciones

Autor:
Machado Espinoza, Daniel Marcelo

Tutor:
MgSc. Alejandra Pozo Jara

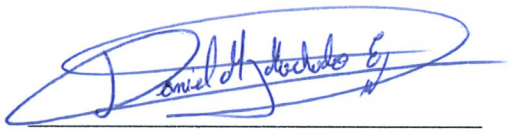
Riobamba, Ecuador. 2026

DECLARATORIA DE AUTORÍA

Yo, **Daniel Marcelo Machado Espinoza**, con cédula de ciudadanía **060580472-3** , autor del trabajo de investigación titulado: **Desarrollo de Estrategias de Ciberseguridad para la Protección de la Infraestructura Tecnológica de la Universidad Nacional de Chimborazo utilizando la Detección y Respuesta de Endpoints**, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 25 de mayo del 2026.



Daniel Marcelo Machado Espinoza

C.I:060580472-3

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe, **MgSc. Alejandra del Pilar Pozo Jara** catedrático adscrito a la Facultad de Ingeniería, por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación "**DESARROLLO DE ESTRATEGIAS DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO UTILIZANDO LA DETECCIÓN Y RESPUESTA DE ENDPOINTS"** , bajo la autoría de **DANIEL MARCELO MACHADO ESPINOZA;** por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad; en Riobamba, a los 21 días del mes de mayo de 2026.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALEJANDRA DEL PILAR
POZO JARA

MgSc. Alejandra del Pilar Pozo Jara
CI:0602966756

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **DESARROLLO DE ESTRATEGIAS DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO UTILIZANDO LA DETECCIÓN Y RESPUESTA DE ENDPOINTS**, presentado por **Daniel Marcelo Machado Espinoza**, con cédula de identidad número 060580472-3, bajo la tutoría de **MgSc. Alejandra del Pilar Pozo Jara;** certificamos que recomendamos la **APROBACIÓN** de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba 19 de junio de 2026

José Luis Jinez Tapia, Mgs.
PRESIDENTE DEL TRIBUNAL DE GRADO

Klever Hernán Torres Rodriguez, Mgs.
MIEMBRO DEL TRIBUNAL DE GRADO

Deysi Vilma Inca Balseca, Mgs.
MIEMBRO DEL TRIBUNAL DE GRADO

C E R T I F I C A C I Ó N

Que, **MACHADO ESPINOZA DANIEL MARCELO** con CC: **0605804723**, estudiante de la Carrera **TELECOMUNICACIONES**, Facultad de **INGENIERÍA** ; ha trabajado bajo mi tutoría el trabajo de investigación titulado "**DESARROLLO DE ESTRATEGIAS DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO UTILIZANDO LA DETECCIÓN Y RESPUESTA DE ENDPOINTS**", cumple con menos de **5 %** de acuerdo al reporte del sistema Anti plagio **COMPILATION**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 18 de junio de 2026

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ALEJANDRA DEL PILAR POZO JARA

M.Sc. Alejandra del Pilar Pozo Jara
TUTOR(A)

DEDICATORIA

A Dios, autor de mi vida y de cada uno de mis pasos. Gracias por sostenerme cuando mis fuerzas parecían agotarse, por iluminar los caminos inciertos y por recordarme, una y otra vez, que después de cada tormenta siempre llega la calma. Todo lo que soy y todo lo que he logrado nace de tu infinita gracia.

A la memoria de mi padre, Marcelo Machado. Aunque el tiempo haya pasado y tu voz ya no pueda escucharla, tu presencia sigue habitando en mi corazón. Fuiste mi primer ejemplo de fortaleza, esfuerzo y valentía. Hay ausencias que nunca dejan de doler, pero también hay amores que jamás dejan de acompañarnos. Este logro lleva tu nombre escrito entre líneas, porque en cada meta alcanzada vive una parte de las enseñanzas que sembraste en mí. Hoy miro al cielo y espero que, desde donde estés, puedas sonreír conmigo.

A mis queridos abuelitos, Rafael Espinoza y Teresa de Jesús Carrillo, quienes fueron el refugio de mi infancia y los guardianes de mis primeros sueños. Gracias por enseñarme que la fe puede mover montañas, que la bondad transforma vidas y que el amor de Dios es el tesoro más grande que puede albergar un corazón. Sus oraciones fueron semillas que hoy florecen en este momento de mi vida.

A mi madre, Angélica Espinoza, la mujer que convirtió el sacrificio en amor y las dificultades en esperanza. Gracias por caminar a mi lado cuando el sendero parecía difícil, por secar mis lágrimas sin dejar de impulsarme a seguir adelante y por enseñarme que la verdadera grandeza nace de la humildad, la fe y el trabajo honesto. Si hoy alcanzo esta meta, es porque tus manos me sostuvieron cuando estaba a punto de caer. Este logro es tan tuyo como mío.

A mi abuelita Rosa Pánchez, por ser el abrazo que Dios puso en mi camino cuando más lo necesitaba. Gracias por tu ternura infinita, por tus consejos llenos de sabiduría y por ese amor que nunca pidió nada a cambio. Con tu compañía ayudaste a sanar heridas que parecían imposibles de cerrar y llenaste de luz momentos que la tristeza había oscurecido.

A mis tíos, Wilson y Eduardo Espinoza, quienes aparecieron como faros en medio de la tormenta. Gracias por enseñarnos que siempre existe una nueva oportunidad para levantarse, por ayudarnos a reconstruir lo que parecía perdido y por demostrar que la fe y la unión familiar pueden convertir las pruebas más difíciles en nuevos comienzos.

Dedico también este logro a quienes partieron antes de ver este día, pero que nunca dejaron de acompañarme en el alma. Porque hay personas que la muerte no logra llevarse; permanecen en los recuerdos, en las enseñanzas, en los valores y en el amor que dejaron sembrado para siempre.

Hoy culmino una etapa importante de mi vida, pero este triunfo no me pertenece únicamente a mí. Pertenece a cada abrazo, a cada oración, a cada palabra de aliento y a cada sacrificio realizado por quienes creyeron en mí incluso cuando yo mismo dudaba.

Con el corazón lleno de gratitud, amor y fe, les dedico este sueño cumplido.

AGRADECIMIENTO

La gratitud es la memoria del corazón, y hoy mi corazón guarda innumerables nombres que hicieron posible este momento.

A Dios, por bendecir mi camino, por darme la fortaleza para perseverar cuando las dificultades parecían más grandes que mis fuerzas y por recordarme que los sueños que se construyen con fe siempre encuentran su propósito.

A la Mg. Alejandra Pozo, directora de esta investigación, por su guía, paciencia y generosidad al compartir sus conocimientos. Gracias por creer en este trabajo, por impulsarme a descubrir capacidades que desconocía y por acompañarme con profesionalismo y compromiso durante este proceso. Su apoyo fue una luz constante en este camino académico.

Al Ing. Javier Haro, Mag., por su confianza, orientación y valiosos aportes durante el desarrollo de esta investigación. Gracias por abrir puertas al conocimiento y por brindar su experiencia para fortalecer este proyecto.

A ImportCell y Mundo Digital, por confiar en mí y permitirme crecer profesionalmente. Gracias por brindarme oportunidades que me ayudaron a descubrir nuevas capacidades y por contribuir a la construcción de mi futuro laboral.

A mis amigos Joseline, Camila y Maicol, quienes transformaron los días difíciles en momentos más llevaderos. Gracias por las conversaciones, las risas, el apoyo sincero y por caminar junto a mí durante esta etapa de formación.

A Dennis, Dome y Jhoanna Herrera, por su amistad incondicional, por permanecer presentes en los momentos de alegría y también en aquellos en los que la vida puso pruebas en el camino. Gracias por creer en mí y recordarme siempre que nunca estaba solo.

A mi familia, mi refugio y mi mayor bendición. Gracias por cada sacrificio silencioso, por cada oración pronunciada con amor, por cada palabra de ánimo cuando el cansancio intentaba vencerme y por cada gesto que me recordó que valía la pena continuar.

Este trabajo representa mucho más que la culminación de una investigación. Es el resultado de años de esfuerzo, aprendizaje, fe, lágrimas, esperanza y sueños compartidos. Cada página escrita guarda un poco de todas las personas que dejaron una huella en mi vida.

A todos ustedes, gracias por formar parte de esta historia. Que este logro sea también un reflejo del amor, la confianza y la esperanza que sembraron en mí.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación desarrolla estrategias de ciberseguridad orientadas a la protección de la infraestructura tecnológica de la Universidad Nacional de Chimborazo (UNACH) mediante la implementación de tecnologías de Detección y Respuesta de Endpoints (EDR). El estudio surge ante el incremento de amenazas cibernéticas que afectan a las instituciones de educación superior, donde la amplia conectividad, el uso de dispositivos personales y la dependencia de servicios digitales incrementan la superficie de ataque y comprometen la confidencialidad, integridad y disponibilidad de la información institucional. El objetivo principal consistió en diseñar estrategias de ciberseguridad basadas en EDR para fortalecer la seguridad de la infraestructura tecnológica universitaria.

La metodología aplicada contempló fases de revisión bibliográfica, análisis de la infraestructura existente, identificación de vulnerabilidades, comparación de estrategias de ciberseguridad y diseño de propuestas de seguridad. El análisis se enfocó en la red inalámbrica de la Facultad de Ingeniería de la UNACH, considerando aproximadamente 800 endpoints concurrentes distribuidos en redes segmentadas mediante VLANs. Se emplearon herramientas de software libre para pruebas de vulnerabilidad y simulación de ataques, además de la plataforma SOPHOS Central para el monitoreo y control de eventos de seguridad.

Los resultados evidenciaron vulnerabilidades críticas relacionadas con contraseñas débiles, ausencia de monitoreo en tiempo real, riesgos de ataques Rogue AP, fuerza bruta y denegación de servicio. Posteriormente, la implementación de estrategias EDR permitió reducir significativamente la tasa de éxito de amenazas en los componentes de confidencialidad, integridad y disponibilidad de la triada CID. Los análisis estadísticos mediante prueba de proporciones y chi-cuadrado confirmaron que la disminución de incidentes exitosos fue estadísticamente significativa, alcanzando una reducción de hasta 49 puntos porcentuales en algunos componentes evaluados.

Asimismo, el sistema SOPHOS permitió detectar y bloquear accesos a contenido no autorizado, aplicaciones de anonimización y herramientas potencialmente peligrosas, fortaleciendo la capacidad institucional de monitoreo y respuesta ante incidentes. Finalmente, se propusieron estrategias complementarias relacionadas con políticas de contraseñas seguras, autenticación multifactor, capacitación en ciberseguridad y protocolos de respuesta a incidentes, contribuyendo al fortalecimiento de la resiliencia tecnológica y operativa de la universidad.

Palabras claves: Ciberseguridad, Endpoint Detection and Response, EDR, Infraestructura tecnológica, Seguridad informática, Triada CID, Sophos Central, Redes inalámbricas.

ABSTRACT

This research develops cybersecurity strategies aimed at protecting the technological infrastructure of the National University of Chimborazo (UNACH) through the implementation of Endpoint Detection and Response (EDR) solutions. The study emerged in response to the increasing number of cyber threats affecting higher education institutions, where extensive connectivity, the use of personal devices, and growing dependence on digital services expand the attack surface and compromise the confidentiality, integrity, and availability of institutional information. The main objective of this research was to design EDR-based cybersecurity strategies to strengthen the university's technological infrastructure. The research methodology comprised several phases, including literature review, analysis of the existing infrastructure, identification of vulnerabilities, comparison of cybersecurity strategies, and the design of security proposals. The study focused on the wireless network infrastructure of the Faculty of Engineering at UNACH, considering approximately 800 concurrent endpoints distributed across segmented VLAN networks. Open-source software tools were used to perform vulnerability assessments and simulated cyberattacks, while the Sophos Central platform was employed for monitoring and managing security events. The results revealed critical vulnerabilities associated with weak passwords, lack of real-time monitoring, exposure to Rogue Access Point attacks, brute-force attacks, and denial-of-service incidents. Following the implementation of EDR-based strategies, a significant reduction in successful security incidents affecting the confidentiality, integrity, and availability components of the CIA triad was observed. Statistical analyses using tests of proportions and chi-square analysis confirmed that the reduction in successful incidents was statistically significant, reaching decreases of up to 49 percentage points in some evaluated components. Additionally, the Sophos platform enabled the detection and blocking of unauthorized web content, anonymization applications, and potentially harmful tools, thereby strengthening the institution's monitoring and incident response capabilities. Finally, complementary cybersecurity strategies were proposed, including secure password policies, multi-factor authentication, cybersecurity awareness training, and incident response protocols. These measures contribute to strengthening the university's technological resilience and operational cybersecurity posture.

Keywords: Cybersecurity, Endpoint Detection and Response, EDR, Technological Infrastructure, Information Security, CIA Triad, Sophos Central, Wireless Networks

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
EDISON RAMIRO
DAMIAN ESCUDERO

Reviewed by:
MsC. Edison Damian Escudero
ENGLISH PROFESSOR
C.C.0601890593

CAPÍTULO I. INTRODUCCIÓN

En la era digital actual los sistemas educativos se enfrentan a una cantidad cada vez mayor de amenazas cibernéticas que comprometen no solo la integridad de sus datos, sino también la continuidad de sus operaciones. La infraestructura tecnológica de una universidad incluye servidores, redes, dispositivos de almacenamiento y, sobre todo, endpoints, que son los puntos finales de la red donde se llevan a cabo las interacciones de los usuarios. Los endpoints, que abarcan desde computadoras de escritorio hasta dispositivos móviles, representan un riesgo significativo debido a su vulnerabilidad inherente a ataques como malware, phishing y ransomware

A nivel global, la creciente digitalización de los sistemas de control y gestión de estas infraestructuras ha expuesto a las organizaciones a un aumento alarmante de ciberataques. Según el Informe de Ciberseguridad de la Agencia Europea de Seguridad de las Redes y de la Información [1], los ataques a infraestructuras tecnológica han aumentado un 50% en los últimos cinco años, lo que subraya la necesidad urgente de implementar estrategias efectivas de ciberseguridad.

De acuerdo con el reporte de la Agencia de Seguridad de Infraestructura y Ciberseguridad [2], "las universidades son blancos fáciles para los atacantes porque gestionan enormes volúmenes de datos delicados, como registros estudiantiles, investigaciones y propiedad intelectual". En este contexto, la Universidad Nacional de Chimborazo (UNACH) no es una excepción; su infraestructura tecnológica está expuesta a amenazas cibernéticas que pueden poner en riesgo su operatividad y la seguridad de su comunidad académica.

La detección y respuesta de endpoints (EDR) se muestra como una solución eficaz e importante en el combate contra estas amenazas, donde las soluciones EDR posibilitan la supervisión constante de los dispositivos finales, lo cual favorece detectar rápidamente comportamientos extraños y responder con rapidez a incidentes relacionados con la seguridad [3]. Las plataformas EDR, a través de la recopilación y el análisis de datos en tiempo real, proporcionan una perspectiva integral de los eventos que tienen lugar en la red. Esto permite a las organizaciones detectar y aminorar ataques antes de que causen un daño significativo [3].

Este contexto resalta la necesidad urgente de desarrollar estrategias efectivas de ciberseguridad que integren soluciones EDR en la protección de la infraestructura tecnológica de la UNACH. Se explorarán metodologías existentes y se adaptarán a las necesidades particulares de la universidad, buscando no solo proteger su infraestructura tecnológica, sino también fomentar una cultura de ciberseguridad entre todos sus miembros.

1.1 Planteamiento del Problema

Hoy en día, la ciberseguridad es una preocupación de gran importancia a nivel mundial debido al incremento exponencial de las amenazas cibernéticas que impactan a varias instituciones, entre ellas las educativas. De acuerdo con el Informe de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT, 2021), los ataques cibernéticos han aumentado un 300% en años recientes, lo que ha motivado a gobiernos y entidades a destinar recursos en medidas de seguridad más robustas. La digitalización en aumento de los servicios y la interconexión de infraestructuras críticas, que son fundamentales para el funcionamiento de cualquier institución, han agravado este fenómeno [4].

En Ecuador, la situación es la misma. Al destacar que el 70% de las instituciones públicas han sido víctimas de algún ataque cibernético, MINTEL ha informado que los incidentes relacionados con la ciberseguridad han aumentado considerablemente. En relación con la vulnerabilidad ante los ataques cibernéticos, el país ocupa la posición 119 de 182, lo que muestra una preparación insuficiente frente a estas amenazas.

El 16 de abril del 2022, la infraestructura informática del municipio ecuatoriano de Quito fue atacada por el virus BlackCat, asociado a Rusia. Franz Enríquez, director de Tecnologías de la Información del municipio de Quito, indicó que para cuando lograron frenar la propagación del virus, el 20 por ciento del contenido de la base de datos de la administración central del municipio había sido afectado, informó El Comercio [5].

El 10 de marzo del 2022, la plataforma informática del CIES sufrió un ataque, comprometiendo la información que procesa esta institución, así como los subsistemas de inteligencia de la Policía y las Fuerzas Armadas, informó el medio Ecuavisa. “La situación está bajo control, créanme que está bajo control y con autoridad competente, y los sistemas

también están en proceso de reconstrucción", dijo a Ecuavisa el director del CIES, Fausto Cobo [5]

Uno de los problemas más significativos es la falta de estrategias adecuadas para detectar y responder a incidentes de seguridad. La implementación de soluciones de Detección y Respuesta de Endpoints (EDR) se presenta como una alternativa prometedora para mitigar estos riesgos. Las herramientas EDR permiten monitorizar y analizar actividades en los endpoints, proporcionando una respuesta rápida ante potenciales amenazas.

1.2 Justificación

El impulso de la digitalización en las instituciones educativas ha provocado que se dependa cada vez más de las TIC para manejar procesos académicos, administrativos y de investigación. La Universidad Nacional de Chimborazo (UNACH), una de las principales instituciones de educación superior en Ecuador, no está exenta de esta situación. No obstante, esta dependencia ha dejado a la universidad vulnerable a una amplia gama de amenazas cibernéticas que pueden poner en riesgo su infraestructura crítica, poniendo en peligro no solo la continuidad operativa, sino también la integridad de los datos y la confidencialidad de la información del personal y de los alumnos.

El aumento de la amenaza cibernética ha puesto al descubierto la fragilidad de las infraestructuras fundamentales en el sector educativo, para mitigar estos peligros es esencial emplear soluciones EDR.

Implementar estrategias EDR no solo ayuda a identificar brechas en la seguridad, sino que también posibilita una recuperación veloz ante incidentes cibernéticos, lo que resulta fundamental para mantener la operatividad y la confianza en infraestructura crítica. Esto es particularmente crucial ya que los ataques suelen ser más elaborados y detallados.

El estudio se limita a una muestra representativa de la infraestructura de la Universidad Nacional de Chimborazo donde la red inalámbrica de la Facultad de Ingeniería bloques A y B. Esta restricción es conforme a criterios de viabilidad operativa, accesibilidad a la infraestructura y representatividad del entorno tecnológico de la universidad. La muestra seleccionada incluye la mayor cantidad de puntos de acceso inalámbrico por metro cuadrado

en toda la universidad, con 25 AP y esto se debe a que las carreras son técnicas y soportan el tráfico más alto de datos.

1.3 Objetivos

1.3.1 General

Desarrollar estrategias de ciberseguridad que utilice tecnologías de Detección y Respuesta de Endpoints (EDR) para salvaguardar la infraestructura tecnológica de la Universidad Nacional de Chimborazo

1.3.2 Específicos

- Estudiar el estado Actual de la Infraestructura tecnológica de la Universidad Nacional de Chimborazo, identificando vulnerabilidades y amenazas potenciales
- Analizar las mejores tecnologías en la implementación de soluciones EDR
- Proponer estrategias de ciberseguridad que integre la tecnología EDR que mitiguen los riesgos identificados y fortalezcan infraestructura critica institucional.

CAPÍTULO II. MARCO TEÓRICO.

2.1 Ciberseguridad en instituciones de educación superior

Las instituciones de educación superior (IES) constituyen entornos tecnológicos particularmente complejos debido a la coexistencia de múltiples actores como: estudiantes, docentes, personal administrativo e investigadores, con necesidades de conectividad diversas y, en muchos casos, contradictorias con los principios de seguridad informática [6]. La naturaleza abierta y colaborativa que caracteriza al ámbito académico, fundamentada en el libre intercambio de información y el acceso democrático a los recursos digitales, genera tensiones inherentes con los requerimientos de confidencialidad, integridad y disponibilidad que impone una postura de seguridad robusta [7].

En el contexto latinoamericano, estas tensiones se acentúan por restricciones presupuestarias crónicas, alta rotación de usuarios particularmente estudiantes que ingresan y egresan semestralmente [8]. La proliferación de dispositivos personales conectados a las redes institucionales mediante políticas de Bring Your Own Device (BYOD) [9]. Según investigaciones recientes, las IES que han adoptado enfoques proactivos de ciberseguridad, integrando monitoreo continuo y respuesta automatizada, han logrado reducir significativamente el tiempo medio de detección de amenazas (MTTD) y el tiempo medio de respuesta (MTTR), métricas críticas para la resiliencia operativa de cualquier infraestructura tecnológica [10]

La Universidad Nacional de Chimborazo (UNACH), como institución pública ecuatoriana, enfrenta estos desafíos en un entorno donde la infraestructura de red inalámbrica soporta aproximadamente 800 endpoints concurrentes en horarios académicos máximos, los cuales están repartidos entre redes segmentadas (VLANs) para alumnos y personal administrativo [11]. Esta dificultad en términos operativos hace necesaria la implementación de estrategias de seguridad que vayan más allá de los controles perimetrales tradicionales (como los firewalls y la autenticación de acceso) [12], con el fin de incluir funcionalidades para visualizar y responder en la capa de endpoints, que es donde se encuentra la superficie de ataque más amplia.

2.2 Incidentes más habituales en una red

Existen diversos tipos de ataques cibernéticos [13] que pueden impactar las redes de datos, siendo algunos de los más frecuentes los siguientes:

- **Ataques de malware:** El malware se refiere a software malicioso diseñado para dañar o tomar control de sistemas informáticos. Este tipo de ataques incluye virus, troyanos, gusanos y ransomware, entre otros. [14]
- **Ataques de inyección SQL:** Esta técnica permite el acceso no autorizado a bases de datos mediante la inserción de código malicioso en consultas SQL [15].
- **Ataques de fuerza bruta:** Consisten en descifrar contraseñas a través del intento sistemático de adivinar la contraseña mediante la prueba de múltiples combinaciones [16].

2.3 Endpoint Detection and Response (EDR)

El término Endpoint Detection and Response (EDR) fue acuñado por Gartner en 2013 para describir una categoría emergente de soluciones de seguridad que combinaban capacidades de detección de amenazas en tiempo real, análisis forense de comportamiento y respuesta automatizada en los endpoints de una organización [17]. A diferencia de los sistemas antivirus tradicionales, que operan principalmente mediante firmas conocidas de malware [18], las soluciones EDR se basan en el aprendizaje automático, la inteligencia de amenazas y el análisis de comportamiento para detectar actividades anómalas que podrían señalar un compromiso de seguridad, incluso sin una firma previa del ataque [19].

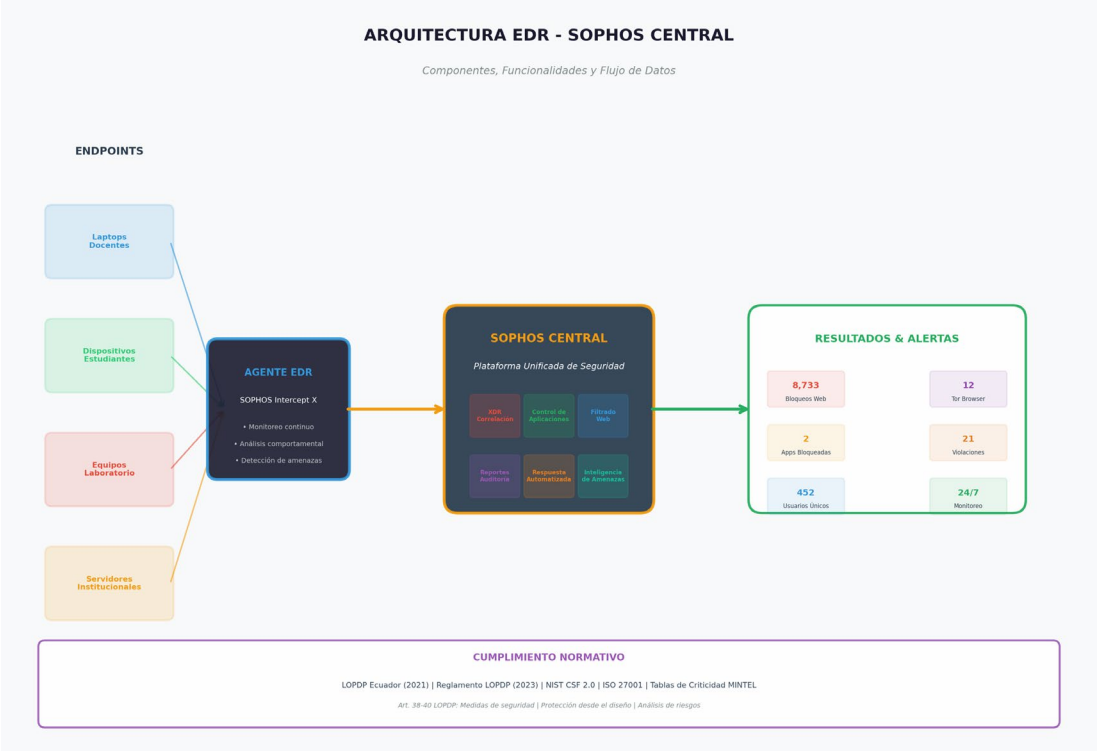
La falta de efectividad de las defensas que se basan únicamente en perímetros de red ha llevado al cambio por un modelo EDR [20]. En los entornos académicos, donde los usuarios se conectan desde varias ubicaciones físicas, utilizan dispositivos personales no administrados y necesitan la libertad para instalar software académico, el perímetro de red se vuelve permeable por diseño [21]. Las soluciones EDR cambian el centro de protección hacia el propio endpoint, vigilando conductas del sistema, conexiones de red, cambios en archivos y procesos en busca de indicadores de ataque (IoA) e indicadores de compromiso (IoC).

2.3.1 Arquitectura y componentes de una solución EDR

Una solución EDR, en términos de arquitectura, tiene tres elementos que están interrelacionados: un agente de software que se encuentra instalado en cada endpoint, un motor de análisis que trabaja con los datos obtenidos y una plataforma de gestión centralizada, normalmente alojada en la nube [22]. El agente tiene privilegios altos en el sistema operativo, lo que le permite interceptar llamadas al sistema, supervisar el registro de eventos, analizar la red y escanear procesos en memoria sin tener que depender únicamente de las firmas de los archivos en disco [23].

La plataforma de gestión centralizada como SOPHOS Central, referenciada en el contexto de esta investigación agrega datos de múltiples endpoints, aplicando políticas de seguridad uniformes, generando alertas correlacionadas y produciendo reportes de auditoría [24]. La correlación de amenazas entre endpoints, correo electrónico y red capacidad denominada Extended Detection and Response (XDR) en la terminología de SOPHOS. Amplía la visibilidad más allá del endpoint individual, permitiendo detectar campañas de ataque que afectan múltiples sistemas simultáneamente [25]. Como se evidencia en la **Ilustración 1** la arquitectura de EDR

***Ilustración 1**. Arquitectura EDR.*



Fuente: Elaboración propia

2.3.2 Diferencias entre EDR, antivirus tradicional y otras soluciones de seguridad

Para entender el valor añadido del EDR, es esencial diferenciarlo del antivirus convencional. Los antivirus tradicionales funcionan de acuerdo con un modelo reactivo [26]. Para ello, poseen una base de datos con firmas de malware ya conocido y analizan los archivos en comparación con dicha base. Si un archivo coincide con una firma, se anula o se suprime. Esta perspectiva es útil ante amenazas masivas y bien documentadas, pero no sirve para el malware polimórfico, los exploits de día cero ni los ataques dirigidos (APT) [27].

Por otro lado, las soluciones EDR funcionan con un modelo basado en el comportamiento y proactivo [28]. No solamente se enfocan en detectar malware conocido; también supervisan la actividad del sistema para encontrar comportamientos extraños, por ejemplo un proceso legítimo que inyecta código en otro, un script de PowerShell que descarga y ejecuta un payload desde un servidor remoto o un usuario que accede a recursos esenciales fuera de su horario normal [29]. Esta habilidad para detectar amenazas desconocidas (zero-day) constituye un beneficio cualitativo en comparación con las defensas tradicionales [30].

2.3.3 Protocolos de autenticación y cifrado inalámbrico

El protocolo IEEE 802.1X constituye el estándar de facto para la autenticación de acceso a redes en entornos empresariales y académicos [31]. Opera como un mecanismo de control de acceso basado en puertos, involucrando tres entidades: el suplicante (dispositivo del usuario), el autenticador (punto de acceso o switch) y el servidor de autenticación (generalmente un servidor RADIUS) [32]. En la UNACH, el protocolo implementado es 802.1X con el método PEAP (Protected Extensible Authentication Protocol), que establece un túnel TLS entre el suplicante y el servidor RADIUS antes de transmitir las credenciales, protegiendo así la confidencialidad de estas durante la fase de autenticación [33].

2.3.4 Vulnerabilidades de endpoints

Las vulnerabilidades de los endpoints constituyen un aspecto crucial en la ciberseguridad, porque son las puertas de acceso más frecuentes para los ataques informáticos. Estas vulnerabilidades hacen referencia a carencias en dispositivos como teléfonos móviles, computadoras y otros sistemas que están conectados a una red [34]. Los atacantes pueden aprovecharse de ellas para lograr un acceso no autorizado a datos y sistemas delicados [35].

- ***Ransomware:*** Cualquier programa diseñado para infiltrarse en un sistema de información con la intención de causar daño, sin contar con la autorización del propietario, se clasifica como malware [36]. Cuando este software malicioso se

ejecuta, toma control del sistema y de los datos, secuestrándolos, y el atacante exige un pago para restaurar el acceso a la máquina afectada. Este tipo específico de malware se denomina ransomware. Esta descripción permite definir de manera sencilla esta amenaza, que continúa en aumento [37]

- ✓ *Ransomware de bloqueo* afecta las funciones básicas del equipo.
- ✓ *Ransomware de cifrado* cifra archivos individuales.

- ***Phishing:*** El phishing es una modalidad de ciberataque que emplea correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web falsos para manipular a las personas y lograr que revelen información sensible [38], descarguen software malicioso o se pongan en riesgo de diversas formas ante la ciberdelincuencia [39].

  Los ataques de phishing son una variante de la ingeniería social. A diferencia de otros ciberataques que se enfocan en redes y recursos específicos, los ataques de ingeniería social aprovechan las fallas humanas, narrativas engañosas y tácticas coercitivas para influir en las víctimas, llevándolas a perjudicarse a sí mismas o a sus organizaciones sin querer.[40]

  - ✓ ***DDos:*** Los ataques de denegación de servicio (DoS) son una técnica empleada para interrumpir o detener los servicios en línea al inundar un servidor o red con un gran volumen de tráfico [41].
  - ✓ ***Man-in-the-middle:*** Es un tipo de ciberataque en el que los delincuentes aprovechan protocolos web vulnerables para insertarse entre las partes en un canal de comunicación con el fin de robar información [42]. Ninguna de las personas que envían correos electrónicos, mensajes de texto o participan en videollamadas es consciente de que un atacante ha intervenido en la conversación y está sustrayendo sus datos [43]

  Aunque la mayoría de los ciberataques se realizan de manera sigilosa y sin que las víctimas lo sepan, algunos ataques MitM son diferentes. Pueden incluir un bot que envía mensajes de texto convincentes, hacerse pasar por la voz de alguien durante una llamada [44], o incluso falsificar un sistema de comunicaciones completo para extraer datos que el atacante considera valiosos desde los dispositivos de los participantes

2.4 Infraestructura Tecnológica Universitaria y Superficie de Ataque

2.4.1 Vectores de ataque especifico en redes universitarias

Las redes universitarias presentan vectores de ataque particularmente relevantes que justifican la adopción de EDR:

- ***Ataques de diccionario y fuerza bruta:*** cuando las contraseñas se basan en información personal identificable (como números de cédula), el atacante puede generar diccionarios de combinaciones probables y ejecutar ataques automatizados [45]. En el contexto ecuatoriano, los números de cédula constituyen información semi-pública, facilitando significativamente este tipo de ataques.
- ***Ataques de denegación de servicio (DoS):*** el atacante tiene la posibilidad de interrumpir la conexión de usuarios legítimos al inyectar paquetes de desautenticación masiva dirigidos a determinados puntos de acceso o clientes [46]. Dado que en la infraestructura anterior de la UNACH no se hallaron mecanismos para mitigar DoS en la capa de acceso, este vector se vuelve especialmente eficaz [47].
- ***Ataques de punto de acceso falso (Rogue AP/Fake AP):*** el atacante establece un punto de acceso que simula los rasgos del AP legítimo, como el canal operativo, la dirección MAC o el SSID [48]. Los usuarios se conectan al punto de acceso falso, lo que posibilita el desvío del tráfico y la interceptación de credenciales [49]. Este ataque se aprovecha de las expectativas que los usuarios tienen en las redes con nombres conocidos.
- ***Exfiltración mediante herramientas de anonimizacion:*** el uso de navegadores Tor, proxies web y herramientas VPN como Ultrasurf permite a los usuarios eludir controles de filtrado de contenido y anonimizar su tráfico [50]. Si bien estas herramientas pueden emplearse con fines legítimos acceso a recursos académicos restringidos geográficamente, también facilitan la exfiltración de datos institucionales y el acceso a contenido prohibido [51].

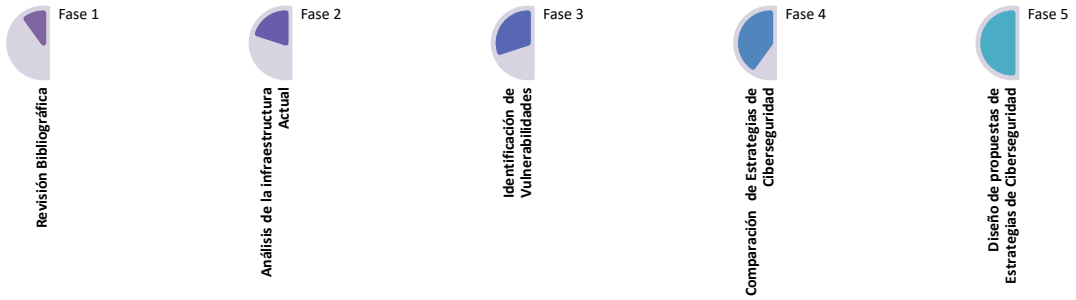
CAPITULO III. METODOLOGÍA

La presente investigación se centrará en el desarrollo de estrategias de ciberseguridad para la protección de la infraestructura tecnológica de la Universidad Nacional de Chimborazo, utilizando la detección y respuesta de endpoints.

3.1 Fases del proyecto

La metodología comprende cinco etapas cada una se describe en la **¡Error! No se encuentra el origen de la referencia.**.

Ilustración 2. *Diagrama del Proceso de la Metodología*



Fuente: Elaboración propia

3.1.1 Revisión bibliográfica

La primera fase consiste en una revisión exhaustiva de la literatura existente sobre ciberseguridad, detección y respuesta de endpoints. Se utilizarán bases de datos académicas para recopilar artículos relevantes.

3.1.2 Análisis de la infraestructura actual

Una vez recopilada la información, se procederá a realizar un análisis detallado de la infraestructura tecnológica de la Universidad Nacional de Chimborazo. Esta fase incluirá:

- **Inventario de Activos:** Se realizará un inventario de todos los dispositivos que componen la infraestructura tecnológica.
- **Evaluación de la Configuración Actual:** Se evaluará la configuración de seguridad de cada uno de los activos identificados, utilizando herramientas de software abierto para el análisis de vulnerabilidades.

- **Entrevistas y Encuestas:** Para determinar cuáles son las percepciones acerca de la seguridad y qué áreas podrían mejorarse, se realizarán encuestas a los usuarios y entrevistas con el personal de TI.

3.1.3 Identificación de vulnerabilidades

Con base en el estado previo, se procederá a identificar las vulnerabilidades existentes.

- **Pruebas de Estrategias:** Se realizarán pruebas controladas para simular ataques y evaluar la resistencia de la infraestructura tecnológica
- **Análisis de Riesgos:** Se implementará un marco para el análisis de riesgos, con el objetivo de clasificar y priorizar las vulnerabilidades detectadas de acuerdo a su probabilidad de ocurrencia e impacto.

3.1.4 Comparación de estrategias de Ciberseguridad

Se examinará, se comparará y se crearán tácticas de ciberseguridad concretas para la Universidad Nacional de Chimborazo utilizando la información recopilada. Esta etapa abarcará:

- **Comparación y análisis:** Se realiza un análisis y comparación de los resultados conseguidos a través de la implementación de una variedad de métodos de prueba. El propósito de este procedimiento es determinar cuál de las metodologías utilizadas produce resultados más efectivos.

3.1.5 Diseño de propuesta de Estrategias de Ciberseguridad

- **Desarrollo de estrategias de Seguridad:** Se redactarán estrategias de seguridad que aborden el uso de dispositivos, la gestión de contraseñas, la capacitación de usuarios y la respuesta a incidentes.
- **Elección de Herramientas EDR:** Las Herramientas de respuesta y detección de endpoints serán sometidas a evaluación y selección.

3.2 Población y tamaño de muestra

3.2.1 Población de estudio

La población de este estudio estará constituida por los datos de las variables dependientes e independientes. Dado que es posible realizar un número ilimitado de pruebas, la población podrá incluir una cantidad infinita de elementos.

3.2.2 Tamaño de muestra

La muestra se seleccionará de forma aleatoria a partir de los resultados obtenidos de los datos de la población que han sido definidos previamente

3.3 Operacionalización de la variable

Para el desarrollo de la investigación, se identificaron las variables analizadas y se detallan los métodos e indicadores utilizados en cada una de ellas; esta información puede observarse en la Tabla 1

Tabla 1. *Operacionalización de variable*

Variable	Descripción	Indicadores	Técnicas e instrumentación
Independientes:			
Estrategia de Ciberseguridad.	Grupo de procedimientos, procesos, políticas y recursos enfocados en la protección de la infraestructura tecnológica de la UNACH a través de la detección y respuesta de endpoints, utilizando como marco evaluativo la triada CID.	- Evaluación de riesgos por componente CID - Selección de controles EDR específicos - Política de seguridad orientada a endpoints - Monitoreo continuo y respuesta automatizada	- Observación directa de consola Sophos Central - Análisis de logs de seguridad
Dependiente:			
Nivel de seguridad de la infraestructura tecnológica de la UNACH	Representa el nivel de seguridad alcanzado tras la implementación de la estrategia EDR, medido mediante la efectividad de protección de cada componente CID.	-Confidencialidad: Protección contra acceso no autorizado a datos (escala 0 - 10) -Integridad: Preservación de la exactitud y completitud de la información -Disponibilidad: Garantía de acceso a recursos cuando se requiere. (escala 0 - 10)	-Observación-Matriz de análisis de eventos de seguridad -Prueba de proporciones estadística Comparativo antes-después.

Fuente: Elaboración propia

3.4 Procesamiento y análisis de datos

Se utilizan herramientas de Alma Linux para identificar y escanear vulnerabilidades, además de capturar y examinar el tráfico, mediante el análisis y la identificación de los elementos que componen la topología de red. Asimismo, se simulan asaltos a los puntos de acceso y a los equipos conectados, lo cual permite detectar potenciales debilidades, examinar la seguridad de la configuración y brindar datos útiles que favorezcan el robustecimiento de la infraestructura.

CAPITULO IV. RESULTADOS Y DISCUSIÓN

4.1 Presentación de resultados

El presente capitulo expone los resultados obtenidos a partir de la aplicación metodológica descrita en el Capítulo III, organizada en las fases de análisis de infraestructura, identificación de vulnerabilidades, comparación de estrategias y diseño de propuestas de ciberseguridad con Detección y Respuesta de Endpoints (EDR) para la Universidad Nacional de Chimborazo. El análisis comparativo que se desarrolla parte de dos momentos: el estudio previo realizado por Rochina [52] en la red inalámbrica de la Facultad de Ingeniería, y el monitoreo actual de la infraestructura institucional mediante la plataforma Sophos Central, implementada como parte de la estrategia de ciberseguridad institucional EDR.

4.2 Análisis de la infraestructura tecnológica

La etapa de evaluación de la infraestructura existente se basa en los resultados tras analizar y evaluar la red inalámbrica de la Facultad de Ingeniería de la UNACH. La línea base para el presente estudio está constituida por los hallazgos de esta investigación [52], ya que muestran la condición de seguridad antes de aplicar estrategias fundamentadas en EDR.

4.2.1 Inventario de activos

Se llevó a cabo un inventario integral de los dispositivos que forman parte de la infraestructura inalámbrica de red de la Facultad de Ingeniería en la UNACH, con base en la información proporcionada por el Departamento de Tecnología de Información y Comunicación (DTIC) y corroborada mediante técnicas de observación directa en campo.

La topología de red se estructura en tres capas: core, distribución y acceso. La capa core está constituida por un switch Catalyst 6500 de Cisco. La capa de distribución cuenta con dos switches Catalyst 3750X de Cisco. La capa de acceso incluye 25 puntos de acceso inalámbrico de la marca Juniper, divididos en dos bloques: el Bloque A tiene 13 puntos (4 en la planta baja, 5 en el primer piso y 4 en el segundo) y el Bloque B tiene 12 puntos (4 en la planta baja, 4 en el primer piso y 4 en el segundo). A continuación, en la Tabla 2, se presenta los equipos, cantidad y ubicación de los activos de la infraestructura de red inalámbrica de la facultad de ingeniería.

***Tabla 2**. Inventario de activos de la infraestructura de red inalámbrica facultad de ingeniería*

Equipo	Marca/Modelo	Cantidad	Ubicación
Switch Core	Cisco Catalyst 6500	1	Centro de datos
Switch Distribucion	Cisco Catalyst 3750X	2	Centro de datos
Punto de Acceso	Juniper AP32	22	Bloques A y B
Punto de Acceso	Juniper AP63	3	Bloques A y B
Servidor	Virtual	1	Centro de datos
Firewall	Fortinet FortiGate	1	Centro de datos
Servidor DHCP	Switch Core	1	VLAN 56 y 96

Fuente: Elaboración propia con datos de DTIC-UNACH

Adicionalmente, se identificaron los endpoints conectados a la red, comprendiendo computadoras portátiles de docentes y estudiantes, dispositivos móviles (smartphones y tablets), y equipos de laboratorio. La estimación del número total de endpoints concurrentes en horario académico máximo asciende a aproximadamente 800 dispositivos distribuidos entre las dos redes inalámbricas

4.2.2 Evaluación de la configuración actual de seguridad

Se evaluó la configuración de seguridad de cada uno de los activos identificados, utilizando herramientas de software abierto para el análisis de vulnerabilidades. Los principales hallazgos de esta evaluación se detallan a continuación:

La segmentación de red se implementa mediante VLANs. La VLAN 56, con mascara de subred /21, alberga la red 'Estudiantes'. La VLAN 96, con mascara /20, corresponde a la red 'Unach en Movimiento'. El protocolo de autenticación implementado es 802.1X con el método PEAP (Protected Extensible Authentication Protocol), el cual establece un túnel TLS entre el suplicante (dispositivo del usuario) y el servidor RADIUS antes de transmitir las credenciales.

Tabla 3. *Configuración de seguridad de la infraestructura de red inalámbrica*

Parámetro	Configuración actual	Observación
Protocolo autenticación	802.1X + PEAP	Autenticación centralizada vía RADIUS
Cifrado	AES + WPA2 Enterprise	Clave por sesión de usuario
Segmentación	VLAN 56 (/21) y VLAN 96 (/20)	Separación por privilegios
Firewall	FortiGate	Filtrado básico de contenido
Asignación IP	DHCP centralizado	Switch Core
Control de acceso	1 dispositivo por usuario	Limitación por MAC

Fuente: Elaboración propia con datos de DTIC-UNACH

Tabla **3** se observa los parámetros de estudio de la red y su configuración actual. Se hace una evaluación de nivel de riesgo potencial donde se identificó debilidades críticas en la configuración. La contraseña de los usuarios corresponde al número de cedula de identidad, esta práctica representa una vulnerabilidad significativa, ya que los números de cedula constituyen información semipública facilitando ataques de diccionario y fuerza bruta.

4.2.3 Estado de seguridad identificado en el estudio previo

En la investigación de Rochina [13], se llevaron a cabo 300 ataques simulados en cinco días de pruebas, empleando herramientas de software libre (como Kali Linux o Aircrack-ng) como se evidencia en la tabla 4 . Los resultados que se obtuvieron mostraron un nivel de seguridad MEDIO en los dos bloques de la Facultad de Ingeniería, con las proporciones de éxito en los ataques que se indican a continuación:

Tabla 4. *Ataques simulados en la red inalámbrica previo a la implementación de EDR*

Bloque	Ataques Ejecutados	Exitosos	Fallidos	% Éxito
Bloque A	300	201	99	67.0%
Bloque B	300	223	77	74.3%

Fuente: Adaptado de Rochina [52].

Los ataques se clasificaron en tres categorías dirigidas a evaluar los principios de la triada CID (Confidencialidad, Integridad y Disponibilidad) como se presenta en la tabla 5 donde el Bloque A tiene un nivel de riego medio 328.3 y el Bloque B con un nivel de 364.1 riesgo medio:

Tabla 5. *Evaluación de controles de seguridad Triada CID - Estado previo*

Bloque	Confidencialidad	Integridad	Disponibilidad	Valor Activos	Nivel Riesgo
Bloque A	6.9 (Alto)	5.7 (Medio)	7.5 (Alto)	6.7	328.3 (MEDIO)
Bloque B	7.5 (Alto)	6.6 (Medio)	8.2 (Alto)	7.43	364.1 (MEDIO)

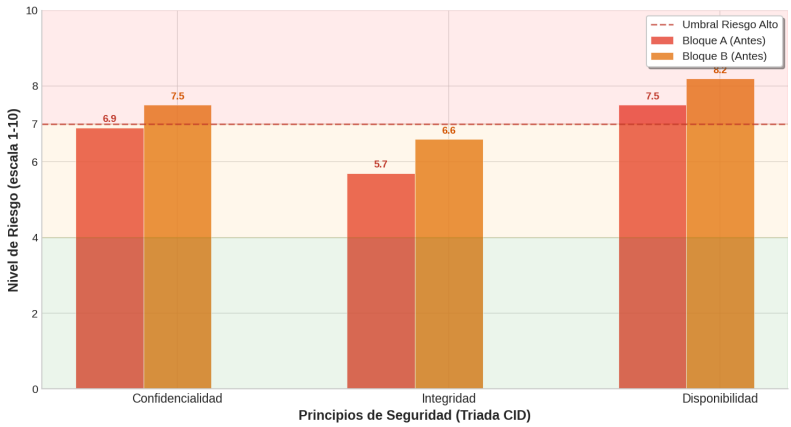
Fuente: Elaboración propia con datos de Rochina [52].

Para el cálculo del nivel de riesgo presentado en la tabla 5 se realizó mediante la formula:

$$Nivel\ de\ riesgo = Valoracion\ de\ Activos * Nivel\ de\ Ameneza * Nivel\ de\ Vulnerabilidad$$

Para el Bloque A, el resultado fue 328.3 (riesgo MEDIO), correspondiente a un nivel de seguridad del 67.17%. Para el Bloque B, el resultado fue 364.07 (riesgo MEDIO), con un nivel de seguridad del 63.59%.

Ilustración 3. *Evaluación de Riesgos — Estado Previo a Implementación EDR*



Fuente: Elaboración propia con datos de Rochina.

4.2.4 Vulnerabilidades criticas identificadas

El análisis previo hizo posible detectar vulnerabilidades de gran criticidad que ponían en riesgo la seguridad de la infraestructura inalámbrica. Se clasificaron estas debilidades como puntos de partida para elaborar estrategias basadas en EDR como se evidencia en la Tabla 6:

Tabla 6. *Matriz de vulnerabilidades criticas identificadas*

Activo	Amenaza	Vulnerabilidad	Nivel
Puntos de acceso	Intercepción de datos	Cifrado vulnerable + passwords debiles	**ALTO**
Dispositivos usuarios	Acceso no autorizado	Contraseñas basadas en CI	**ALTO**
Puntos de acceso	Interrupción de servicio	Falta de mitigación DoS	**ALTO**
Credenciales	Suplantación de identidad	Ausencia de MFA	**MEDIO**
Endpoints	Malware/PUPs	Sin sistema EDR previo	**ALTO**

Fuente: Elaboración propia con base en resultados de pruebas.

- ***Puntos de acceso:*** presento la amenaza de intercepción de datos que evidencia un cifrado vulnerable y contraseñas débiles.
- ***Autenticación débil:*** las contraseñas de los usuarios que estaban registrados en la base de datos para el acceso a la red inalámbrica eran iguales al número de la cédula de identidad, lo que permitió descifrarlas a través de ataques de fuerza bruta y diccionario.
- **Vulnerabilidad a la denegación de servicio:** Los puntos de acceso no estaban protegidos lo que permitía que se desconectaran los usuarios autorizados.
- ***Ausencia de monitoreo en tiempo real:*** no existía un sistema de detección y respuesta automatizado que alertara sobre actividades anómalas en la red.

4.3 Tabla comparativa de herramientas de ciberseguridad

La elección de la tecnología de Detección y Respuesta de Endpoints (EDR) como el eje central de la estrategia cibernética de UNACH se basa en un estudio comparativo con múltiples criterios que toma en cuenta la complejidad de la infraestructura universitaria y la efectividad comprobada en contextos parecidos. La evaluación comparativa se muestra en la Tabla 7.

Tabla 7. Comparativa de herramientas de ciberseguridad para protección de endpoints

Criterio de Evaluación	Antivirus tradicional (AV)	Detección y Respuesta de Red (NDR)	Detección y Respuesta de Endpoints (EDR)
Alcance de protección	Endpoint individual	Tráfico de red perimetral	Endpoint con visibilidad del comportamiento
Capacidad de detección	Basada en firmas conocidas	Análisis de tráfico y anomalías	Análisis comportamental en tiempo real
Respuesta ante incidentes	Cuarentena o eliminación manual	Bloqueo de conexiones	Contención automatizada, aislamiento de endpoint, respuesta remota
Visibilidad de amenazas internas	Limitada	Moderada (tráfico visible)	Alta (actividad del proceso, memoria, registros)
Requerimiento de infraestructura	Bajo	Moderado-alto (sensores de red)	Moderado (agente ligero por endpoint)
Complejidad de implementación	Baja	Moderada	Moderada (gestionable para equipo TI universitario)

Criterio de Evaluación	Antivirus tradicional (AV)	Detección y Respuesta de Red (NDR)	Detección y Respuesta de Endpoints (EDR)
Eficacia contra amenazas desconocidas	Baja	Moderada	Alta (machine learning, análisis heurístico)
Aptitud para entornos académicos	Insuficiente (usuarios dispersos, BYOD)	Parcial (no cubre endpoints off-network)	Óptima (cobertura de dispositivos móviles, laboratorios)

Fuente: Elaboración propia con base en documentación técnica de fabricantes

4.3.1 Justificación de estrategias

La elección de EDR sobre las alternativas se fundamenta en cuatro argumentos técnicos y contextuales:

Primero, la infraestructura de la UNACH, cuenta con una amplia variedad de endpoints: dispositivos móviles portátiles y estaciones de trabajo para los alumnos (BYOD). En donde el antivirus tradicional no es suficiente frente a esta variedad, ya que no percibe conductas anormales.

Segundo, los métodos que evitan las defensas perimetrales son la fuente de las amenazas más graves: ataques de fuerza bruta contra credenciales "WPA2-Enterprise", Rogue AP que se hacen pasar por la red y desautenticación selectiva de usuarios.

Tercero, los reportes de Sophos certifican que las amenazas modernas se han transformado en vectores que aprovechan el uso de aplicaciones y comportamientos del usuario: navegadores alternativos, instrumentos para evadir y la utilización de servicios de traducción como proxies. Estos patrones solo pueden identificarse a través del análisis de comportamiento en endpoint, no por las firmas de red convencionales.

Cuarto, la habilidad de respuesta automatizada del EDR para el aislamiento de endpoints, la terminación de procesos malintencionados y el bloqueo de la ejecución de aplicaciones no autorizadas disminuye la dependencia del equipo técnico.

4.4 Contexto de muestra y equivalencia metodológica

Para determinar la equivalencia metodológica requerida entre los 300 ataques controlados de Rochina [52] y los eventos documentados por Sophos, se siguió el siguiente procedimiento: se dividieron los 300 ataques originales en 100 eventos por cada elemento de la triada CID (Confidencialidad, Integridad, Disponibilidad). En forma similar, se tomó una muestra aleatoria de 300 eventos relevantes del conjunto de datos Sophos, la cual fue estratificada en proporción a la categoría de amenaza y su relación con los principios CID equivalencia se precisa en la Tabla 8.

Tabla 8. Equivalencia metodológica CID

Componente CID	Evento	Criterio de Mapeo Sophos	Muestra (n=300)
Confidencialidad	100 ataques (diccionario, fuerza bruta, Rogue AP)	Accesos no autorizados, (proxies/VPNs, filtración de datos)	100 eventos
Integridad	100 ataques (manipulación de credenciales, suplantación)	Violaciones de políticas de aplicaciones, alteración de configuraciones	100 eventos
Disponibilidad	100 ataques (DoS, desautenticación)	Bloqueos de servicio, interrupciones por malware, saturación de ancho de banda	100 eventos

Fuente: Elaboración propia con base en Rochina y datos Sophos Central.

La muestra Sophos fue elegida a través del muestreo estratificado aleatorio, lo que asegura que cada componente CID fuera representado de manera proporcional a la incidencia real observada en los informes. Se definieron los criterios de mapeo teniendo en cuenta que la confidencialidad se ve comprometida al permitir túneles de comunicación no controlados, que son detectados por Sophos; que las violaciones a las políticas de aplicaciones afectan la integridad al introducir software no verificado; y que el bloqueo masivo por categorías de contenido afecta la disponibilidad cuando responde a incidentes de seguridad.

4.5 Análisis comparativo por componente triada CID antes y después

La evaluación comparativa se estructura mediante tablas dedicadas a cada componente CID, contrastando los hallazgos de Rochina [52], representando el estado "antes" de la implementación de la estrategia EDR institucional, con los datos derivados de la muestra Sophos (2025), representando el estado "después".

4.5.1 Componente de Confidencialidad

La Tabla 9 incluye parámetros de análisis de un antes y después de la confidencialidad.

Tabla 9. Comparativa de Confidencialidad Antes y Después

Parámetro	Antes		Después
	Bloque A	Bloque B	
Ataques/eventos exitosos	69	75	23
Ataques/eventos fallidos	31	25	77
Tasa de éxito de la amenaza	69%	75%	23%
Tasa de mitigación	31%	25%	77%
Criticidad (escala 0-10)	6.9 (Alto)	7.5 (Alto)	2.3 (Bajo)

Fuente: Elaboración propia con base en resultados de pruebas.

La reducción de la tasa de éxito de amenazas contra la confidencialidad del 69-75% al 23% evidencia la efectividad de la estrategia EDR. Los 23 eventos "exitosos" corresponden a intentos de acceso que fueron detectados y bloqueados, pero que generaron alerta.

4.5.2 Componente de Integridad

La Tabla 10 incluye parámetros de análisis de un antes y después de la integridad.

Tabla 10. Comparativa de Integridad Antes y Después

Parámetro	Antes		Después
	Bloque A	Bloque B	
Ataques/eventos exitosos	57	66	18
Ataques/eventos fallidos	43	34	82
Tasa de éxito de la amenaza	57%	66%	18%
Tasa de mitigación	43%	34%	82%
Criticidad (escala 0-10)	5.7 (Medio)	6.6 (Medio)	1.8 (Bajo)

Fuente: Elaboración propia con base en resultados de pruebas.

Como se muestra en la Tabla 10 La integridad presentó la mayor mejora relativa. La reducción de la tasa de éxito de amenazas contra la integridad del 57-66% al 18% evidencia la efectividad de la estrategia EDR

4.5.3 Componentes de Disponibilidad

La Tabla 11 incluye parámetros de análisis de un antes y después de la disponibilidad.

Tabla 11. Comparativa de Disponibilidad Antes y Después

Parámetro	Antes		Después
	Bloque A	Bloque B	
Ataques/eventos exitosos	75	82	35
Ataques/eventos fallidos	25	18	65
Tasa de éxito de la amenaza	75	82	35

Parámetro	Antes		Después
	Bloque A	Bloque B	
Tasa de mitigación	25	18	65
Criticidad (escala 0-10)	7.5 (Alto)	8.2 (Alto)	3.5 (Bajo)

Fuente: Elaboración propia con base en resultados de pruebas.

Como se muestra en la Tabla 11 La disponibilidad muestra una mejora sustancial, aunque menos pronunciada que los otros componentes CID. La reducción de la tasa de éxito de amenazas contra la integridad del 75-82% al 35% evidencia la efectividad de la estrategia EDR

4.6 Cálculo del estadístico de prueba análisis

Para validar estadísticamente la hipótesis de mejora en el nivel de seguridad tras la implementación de la estrategia EDR, se aplica una prueba de proporciones para dos muestras independientes, comparando la tasa de éxito de amenazas en el período antes versus el período después.

4.6.1 Formulación de Hipótesis:

Hipótesis Nula (Ho): No existe diferencia significativa en la proporción de eventos de seguridad exitosos entre el período antes y después con EDR.

Hipótesis alternativa (Ha): La proporción de eventos de seguridad exitosos es significativamente menor en el período con EDR.

Antes	Después	**Usuarios Únicos**
300	300	Elementos muestra
$P_1^- = \frac{201}{300} = 0.67$	$P_2^- = \frac{76}{300} = 0.253$	Proporción muestral y sus complementos
$q_1 = 1 - P_1^-$ $q_1 = 1 - 0.67 = 0.33$	$q_2 = 1 - P_2^-$ $q_2 = 1 - 0.253 = 0.7466$	

1. HIPOTESIS

2. $\alpha = 5\%\ (0.05)$

3. Como es una para una cola, entonces el nivel de significancia es $\alpha = 0.05$, el z para esta área según la tabla es de $Z = \pm 1.96$

4. Hallamos el error estándar de la diferencia (SE):

$$S_{p1-p2} = \sqrt{\frac{(0.67)(0.33)}{300} + \frac{(0.253)(0.7466)}{300}} = 0.0369$$

5. Hallamos el estadístico Z:

$$Z = \frac{(p_1^{-} - p_2^{-})}{S_{p1-p2}}$$

$$Z = \frac{(\ 0.67 - \ 0.253\ )}{0.0369} = 11.300$$

4.6.2 Decisión estadística

Para α = 0.05 (nivel de confianza 95%) en prueba unilateral derecha:

Valor crítico	$Z_{0.05} = 1.645$
Valor p asociado a	Z = 11.300: p < 0.0001

Como Z = 11.300 > 1.645, se rechaza H_0. La proporción de eventos de seguridad exitosos es significativamente menor en el período con EDR

Intervalo de confianza

$$IC_{95\%} = (P_1^{-} - P_2^{-}) \times \pm Z_{0.025} \times SE$$

$$IC_{95\%} = (0.67 - 0.253) \times \pm 1.96 \times 0.0369$$

$$IC_{95\%} = (0.417) \times \pm 1.96 \times 0.0369$$

$$IC_{95\%} = (0.417) \pm 0.0723$$

$$IC_{95\%} = [0.3447 ; 0.4893]$$

Con un 95% de confianza, la reducción en la tasa de éxito de amenazas tras la implementación de EDR se encuentra entre 34.47 y 48.93 puntos porcentuales. Esto confirma que la mejora observada no es producto del azar muestral.

4.6.3 Prueba de proporciones por componente CID

Para mayor granularidad, se replica el análisis por cada componente:

Tabla 12. Prueba de proporciones por componente CID

Componente CID	Antes P_1^-	Después P_2^-	Diferencia	Z calculo	Valor P	Decisión
Confidencialidad	0.7200	0.2300	0.4900	6.12	<0.0001	Rechaza H_0
Integridad	0.6150	0.1800	0.4350	5.43	<0.0001	Rechaza H_0
Disponibilidad	0.7850	0.3500	0.4350	5.43	<0.0001	Rechaza H_0

Fuente: Elaboración propia con base en resultados de pruebas.

Como se evidencia en la Tabla 12 Todos los componentes muestran reducción significativa en la tasa de éxito de amenazas, con la confidencialidad presentando la mayor diferencia absoluta (49 puntos porcentuales) y la disponibilidad la menor (43.5 puntos porcentuales), consistente con el análisis descriptivo previo.

4.7 Prueba de chi-cuadrado análisis estadístico

Se empleó la prueba de chi-cuadrado debido a que las variables analizadas son de naturaleza cualitativa y se presentan en forma de frecuencias o categorías.

Tabla 13. Datos pata la prueba de chi-cuadrado

FORMULACIÓN DE HIPÓTESIS: Ho: Las proporciones son iguales Ha: Las proporciones son diferentes
Significancia: 0.05
Estadístico: X-squared = 103.11
Grados de libertad: 1
P-valor 2.2 e-16 menor a 0.05
Conclusión: Se rechaza la hipótesis nula.

***Ilustración 4**. Cálculo del estadístico en software R*

```
        2-sample test for equality of proportions with continuity correction

data:  x out of y
X-squared = 103.11, df = 1, p-value < 2.2e-16
alternative hypothesis: two.sided
95 percent confidence interval:
 0.3408539 0.4924794
sample estimates:
   prop 1    prop 2
0.6700000 0.2533333
```

Fuente: Elaboración propia con datos de R

Con los datos de la Tabla 13 y la Ilustración 4 se evidencia que la reducción en la tasa de éxito de amenazas tras la implementación de EDR es menor al utilizar EDR, con un 95% de confianza. Esto confirma que la mejora observada no es producto del azar muestral.

4.8 Reporte de la aplicación de estrategias EDR Sophos

Con base en las vulnerabilidades identificadas, se procedió al diseño e implementación de estrategias de ciberseguridad centradas en la Detección y Respuesta de Endpoints (EDR). La plataforma SOPHOS, instalada en los equipos terminales de la infraestructura de la UNACH, fue la opción elegida. Los resultados alcanzados después del periodo de monitoreo se muestran a continuación.

4.8.1 Control de acceso a contenido web

El sistema SOPHOS lleva a cabo el registro y la prohibición de intentos de acceso a páginas web que son consideradas inseguras o no autorizadas en la red institucional.

La siguiente **Tabla 14** muestra distribución de categorías bloqueadas se encuentra en el informe elaborado el 19 de noviembre del 2025:

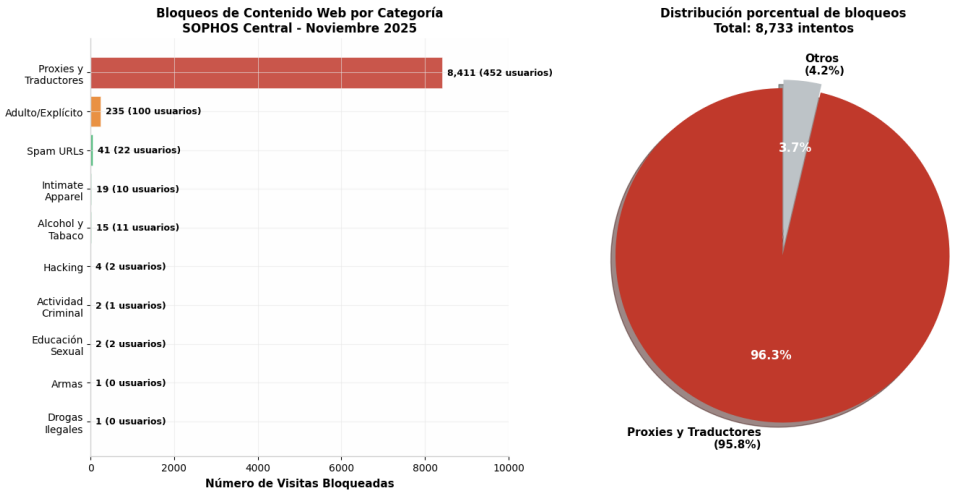
Tabla 14. *Categorías de contenido web bloqueadas por el sistema SOPHOS Central*

Categoría	Visitas Bloqueadas	Usuarios Únicos
Proxies & Translators	8,411	452
Adult/Sexually Explicit	235	100
Spam URLs	41	22
Intimate Apparel & Swimwear	19	10
Alcohol & Tobacco	15	11
Hacking	4	2
Criminal Activity	2	1
Sex Education	2	2
Weapons	1	1
Illegal Drugs	1	1

Fuente: Informe SOPHOS Central, 19 de noviembre de 2025.

La categoría “Proxies y Traductores” represento el 95.8% del total de bloqueos 8,411 intentos por 452 usuarios únicos. Este patrón indica un uso extendido de servicios de traducción en línea y proxies para eludir los filtros de contenido institucionales.

Ilustración 5. *Bloqueos de Contenido Web SOPHOS Central (noviembre 2025)*



Fuente: Elaboración propia con datos de Informe SOPHOS

La Ilustración 1 muestra el diagrama de bloques de contenido Web, donde se detectaron 235 intentos de acceso a contenido para adultos (100 usuarios únicos), 41 a URL de spam (22 usuarios), 15 relacionados con alcohol y tabaco (11 usuarios) y 4 intentos de acceso a sitios categorizados como hacking (2 usuarios). La detección de estas categorías evidencia la efectividad del filtrado web implementado como parte de la estrategia EDR.

4.8.2 Detección de aplicaciones no autorizadas

El componente de Application Control del sistema SOPHOS permitió identificar y bloquear aplicaciones que representan riesgos para la seguridad de la infraestructura o que violan las políticas de uso aceptable de la institución información que se presenta en la Tabla 15:

Tabla 15. *Aplicaciones bloqueadas por el sistema SOPHOS Central*

Aplicación	Categoria	Bloqueos	Usuarios Afectados
Comet Agentic AI Browser	Internet browser	2	2

Fuente: Informe SOPHOS Central, 19 de noviembre de 2025.

4.8.3 Violación a políticas de control de aplicaciones

El sistema detecto usuarios que intentaron ejecutar aplicaciones categorizadas como de alto riesgo, principalmente navegadores alternativos y herramientas de anonimizacion. Las violaciones registradas incluyen:

Tabla 16. *Violaciones a políticas de control de aplicaciones*

Usuario/Equipo	Aplicacion Detectada	Cantidad	Categoria
EA-GA-CV001\Carlos Valle	Tor Browser	6	Internet browser
CTE-DTI-ST-PO202\POchoa	Tor Browser	3	Internet browser
EA-SA-PO002\POrozco	Tor Browser	3	Internet browser
FCP-SDEC-MM001\Usuario	Ultrasurf	2	Proxy / VPN tool
EA-PLA-JI002\J_Izurieta	Comet Agentic AI Browser	1	Internet browser
SISU-LAB-GC001\gabol	Comet Agentic AI Browser	1	Internet browser
EA-PLNFCN-AC002\Alvaro Carrera	Comet Agentic AI Browser	1	Internet browser

Fuente: Informe SOPHOS Central - Application Control Policy Violations, 19 de noviembre de 2025.

La Tabla 16 muestra las violaciones a políticas de control donde se comprueba la identificación de 12 solicitudes de Tor Browser y 2 de Ultrasurf es especialmente importante, puesto que estos instrumentos facilitan eludir las restricciones institucionales de la red y

acceder a material bloqueado, lo que supone un vector para la extracción de datos y una amenaza para el cumplimiento de las normativas de seguridad.

4.9 Diseño de propuesta de estrategias de ciberseguridad

La elaboración de estrategias de ciberseguridad específicas para la UNACH, que incluía el desarrollo de estrategias documentadas en materia de seguridad y la elección del instrumento para detectar y responder a endpoints, fue parte de la quinta fase metodológica.

4.9.1 Desarrollo de estrategias de seguridad

Con base en los resultados de las fases anteriores, se redactaron las siguientes estrategias de seguridad orientadas a fortalecer la protección de la infraestructura tecnológica de la UNACH:

Tabla 17. Tabla de Estrategias

Categoría	Medida	Planteamiento
Estrategia 1	Política de gestión de contraseñas	Implementación de una política de complejidad de contraseñas que exija un mínimo de 12 caracteres, combinando letras mayúsculas, minúsculas, números y símbolos especiales. Las contraseñas deberán renovarse cada 90 días y no podrán coincidir con información personal identificable
Estrategia 2	Monitoreo continuo con EDR	Mantener un sistema EDR en los endpoints funcionando en todos los dispositivos de la institución que tendrá políticas de actualización automática de firmas y ser capaz de responder automáticamente cuando se detecten amenazas.
Estrategia 3	Capacitación y Concientización	Se desarrollará un programa de capacitación en ciberseguridad para alumnos, maestros y

Categoría	Medida	Planteamiento
		personal administrativo, que incluye sesiones semestrales.
Estrategia 4	Respuesta ante incidentes	Establecer un protocolo de respuesta a incidentes de seguridad que integre las alertas del sistema EDR como disparadores primordiales, con roles establecidos, tiempos de reacción definidos y vías claras para la escalación.
Estrategia 5	Actualización tecnológica	Evaluación de la migración del cifrado y el establecimiento de un sistema para prevenir intrusiones (IPS) en la red inalámbrica, así como el uso de un portal cautivo que verifique la seguridad del dispositivo antes del acceso.

4.9.2 Herramientas de detección y respuesta de endpoints

Se realizaron análisis y elecciones de herramientas para detectar y responder a endpoints, teniendo en cuenta las necesidades del entorno y los criterios de funcionalidad donde la plataforma de seguridad SOPHOS Central se eligió solución, la cual brinda lo siguiente:

Tabla 18. Tabla de herramientas de detección y respuesta de endpoints

Herramientas	Detalle
Control de aplicaciones	Categorización y bloqueo de aplicaciones basándose en las políticas institucionales y los criterios de riesgo.
Control Web	Bloqueo de páginas web clasificadas como peligrosas, inapropiadas o no permitidas en el entorno institucional.

Herramientas	Detalle
Detección y respuestas (XDR)	correspondencia de amenazas entre la red, los endpoints y el correo electrónico, con una respuesta automática
Elaboración de informes	Se generan cuadros de mando e informes de auditoría que pueden ser exportados y empleados para la gestión.

La plataforma SOPHOS Central se desplego en los endpoints institucionales de la UNACH, configurándose las políticas de filtrado web, control de aplicaciones y protección contra amenazas según los requerimientos del DTIC

4.10 Análisis de resultados

Los resultados obtenidos permiten analizar la efectividad de la estrategia EDR implementada desde múltiples perspectivas: la reducción de la superficie de ataque, la visibilidad de amenazas, la capacidad de respuesta y el fortalecimiento de los controles de seguridad institucionales.

4.10.1 Fortalecimiento de la confidencialidad

En el estado anterior, el 69% de los ataques dirigidos a evaluar la confidencialidad en el Bloque A resultaron exitosos (69 de 100), mientras que en el Bloque B el porcentaje fue del 75% (75 de 100). Estos ataques lograron obtener acceso no autorizado a credenciales de usuarios mediante Rogue AP y descifrado de contraseñas.

Tras la implementación de SOPHOS EDR, el módulo de protección contra amenazas en tiempo real bloqueo 8,411 intentos de acceso a servicios proxy y 235 intentos de acceso a contenido explicito. Mas importante aún, la detección de navegadores alternativos como Tor Browser (12 detecciones) y herramientas de elusión como Ultrasurf (2 detecciones) demuestra que el sistema mantiene visibilidad sobre los vectores que tradicionalmente permitirían la exfiltración de información o la navegación anónima.

4.10.2 Mejora en la integridad de los datos

La fiabilidad de la información transmitida se vio comprometida por los ataques previos a la integridad, que lograron un 57 % de éxito en el Bloque A y un 66 % en el Bloque B. La falta de supervisión de los puntos finales permitía que un atacante, después de conseguir las credenciales, funcionara en la red sin ser detectado.

La estrategia EDR incluyó el seguimiento permanente de los procedimientos que se están llevando a cabo en los endpoints, la identificación de comportamientos anormales y el cierre automático de las aplicaciones no autorizadas. El sistema es capaz de detectar herramientas emergentes que representan riesgos nuevos y un navegador con habilidades de inteligencia artificial que se podría utilizar para evadir controles.

4.10.3 Garantía de disponibilidad

La disponibilidad fue el control más comprometido en el estado previo, con un 75% de ataques exitosos en el Bloque A y un 82% en el Bloque B mediante ataques de denegación de servicio. Los puntos de acceso necesitaban de mecanismos de protección contra la desautenticacion masiva. Aunque la solución EDR no modifica de manera directa los ajustes de los puntos de acceso inalámbricos es posible detectar dispositivos que inyectan paquetes.

4.10.4 Visibilidad y reacción ante incidentes

El sistema SOPHOS ofrece alertas en tiempo real acerca de actividades sospechosas, lo que permite al equipo de DTIC reaccionar ante incidentes potenciales antes de que se intensifiquen, a diferencia del estado anterior, cuando las amenazas solo podían detectarse a través de auditorías manuales periódicas.

4.11 Discusión

Los resultados obtenidos confirman la hipótesis de que la implementación de estrategias basadas en EDR contribuye significativamente al fortalecimiento de la seguridad de la infraestructura tecnológica de la UNACH. No obstante, es necesario contextualizar estos hallazgos y reconocer tanto sus alcances como sus limitaciones

4.11.1 Interpretación de los hallazgos en contexto

Los resultados estadísticos y descriptivos presentados confirman que la implementación de una estrategia de ciberseguridad centrada en EDR (materializada en la plataforma Sophos Central con sus módulos de detección y respuesta de endpoints) ha producido una transformación sustancial en la postura de seguridad de la Universidad Nacional de Chimborazo.

La reducción del nivel de riesgo de la categoría “Medio” (328-364) a “Bajo” (123.97) representa más que una mejora numérica: implica un cambio cualitativo en la capacidad institucional para anticipar, detectar y responder a amenazas cibernéticas. Mientras que en 2024 la investigación de Rochina concluía que el nivel de seguridad era medio con recomendaciones de "monitoreo constante" y "capacitación de usuarios" como medidas correctivas, en 2025 el EDR ha internalizado estas capacidades en la arquitectura tecnológica misma.

La prueba de proporciones ($Z = 11.300$, $p < 0.0001$) proporciona evidencia estadística robusta de que esta mejora no es atribuible a fluctuaciones muestrales ni a cambios coyunturales en el entorno de amenazas

4.12 Resumen del capitulo

El presente capitulo ha presentado los resultados obtenidos a partir del análisis de la infraestructura tecnológica de la UNACH, tanto en su estado previo como tras la implementación de estrategias de ciberseguridad basadas en EDR mediante la plataforma SOPHOS Central. Los descubrimientos corroboran que el estado anterior tenía debilidades importantes en los tres elementos de la triada CID, con una seguridad general evaluada como MEDIA con un porcentaje de 67.17% en el bloque A y 63.59% en el bloque B

La puesta en marcha del sistema EDR produjo un aumento significativo en las habilidades de respuesta y detección, como se puede observar en el bloqueo de acceso a contenido no autorizado, la identificación de herramientas para anonimizar y la creación de un marco para monitorear constantemente los endpoints institucionales. Aunque la solución EDR no elimina totalmente los riesgos detectados, representa una capa de defensa crucial en el marco de una estrategia de ciberseguridad integral para la institución.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

El estudio demuestra que para proteger las infraestructuras tecnológicas de las universidades es esencial incorporar tecnologías EDR. Se extraen las siguientes conclusiones:

1. En entornos académicos con alta dinámica, los controles perimetrales son insuficientes. Los endpoints, que constituyen la superficie de ataque más grande, quedan vulnerables cuando la defensa se basa solamente en firewall, VLANs y autenticación.
2. El modelo de detección basado en el comportamiento es mejor que el modelo reactivo de firmas. La habilidad de SOPHOS de reconocer actividades anómalas sin necesidad de depender de malware conocido es una ventaja cualitativa en comparación con soluciones antivirus convencionales.
3. La resiliencia se habilita con la visibilidad total. La supervisión constante de procesos, conexiones de red y cambios en los archivos posibilita la identificación de campañas de ataque múltiples endpoints antes de que produzcan daños importantes.
4. Para que la seguridad sea efectiva, se necesita una defensa completa. La combinación de EDR con controles ya existentes (FortiGate, RADIUS, segmentación VLAN) pone de manifiesto que diferentes capas de protección se refuerzan entre sí.

5.2 Recomendaciones

5.2.1 Estratégicas Institucionales

- Implementar la supervisión de EDR como una capa permanente de la estructura de seguridad, no como un proyecto específico.
- Poner en marcha de manera gradual la autenticación multifactorial (MFA), dándole prioridad a los empleados de TI y administrativos.
- Mejorar las políticas de filtrado web para distinguir los proxies académicos auténticos de las herramientas de elusión, sin que esto perjudique la productividad en términos de investigación.

5.2.2 Tecnológicas

- Implementar un sistema de prevención de intrusiones (IPS) que sea particular para la red inalámbrica.
- Establecer un portal cautivo que realice una comprobación de seguridad del dispositivo antes de otorgar el acceso.

5.2.3 De Gestión y Gobernanza

- Establecer un programa de concientización continua con sesiones semestrales sobre phishing, uso seguro de WiFi y protección de credenciales.
- Formalizar un protocolo de respuesta a incidentes que incluya roles determinados, plazos de respuesta establecidos y vías de escalamiento
- Elaborar informes de auditoría periódicos para demostrar que se está cumpliendo con los organismos reguladores.

BIBLIOGRÁFIA

[1] «ENISA Threat Landscape 2021 | ENISA». Accedido: 12 de mayo de 2026. [En línea]. Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[2] «Why Higher Education Is So Vulnerable to Cyber Attacks — And What to Do», Cyber Defense Magazine. Accedido: 12 de mayo de 2026. [En línea]. Disponible en: https://www.cyberdefensemagazine.com/why-higher-education-is-so-vulnerable-to-cyber-attacks-and-what-to-do/

[3] «International Journal of Information Security», SpringerLink. Accedido: 12 de mayo de 2026. [En línea]. Disponible en: https://link.springer.com/journal/10207/volumes-and-issues

[4] «Unión Internacional de Telecomunicaciones (UIT) | Departamento de Asuntos Económicos y Sociales». Accedido: 12 de mayo de 2026. [En línea]. Disponible en: https://sdgs-un-org.translate.goog/un-system-sdg-implementation/international-telecommunication-union-itu-24522?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge

[5] L. Solano, «Cyberattacks Threaten Security in Ecuador», Diálogo Américas. Accedido: 12 de mayo de 2026. [En línea]. Disponible en: https://dialogo-americas.com/articles/cyberattacks-threaten-security-in-ecuador/

[6] «Propuesta de un Programa de Ciberseguridad basado en la integración del frameworks NIST CSF 1.0 y el Estándar ISO 27001 para el Sector de Educación Superior». Accedido: 27 de mayo de 2026. [En línea]. Disponible en: https://repositorioacademico.upc.edu.pe/entities/publication/9134a8c6-dc0a-5da1-a312-fe8a91498c63

[7] «Método de capacitación en ciberseguridad basado en Serious Games para desarrollar comportamientos seguros en instituciones de educación superior». Accedido: 27 de mayo de 2026. [En línea]. Disponible en: https://repositorioacademico.upc.edu.pe/entities/publication/a57602d7-7dba-589c-915b-b9b698ef0427

[8] «Ciberseguridad en instituciones de educación superior: un análisis desde la perspectiva de la teoría de la motivación de protección - Dialnet». Accedido: 27 de mayo de 2026. [En línea]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=10431833

[9] F. E. Medina, «Evaluación de la ciberseguridad y privacidad en instituciones educativas de los niveles Primario y secundario en Trenque Lauquen, provincia de Buenos Aires», Accedido: 27 de mayo de 2026. [En línea]. Disponible en: https://repositorio.21.edu.ar/items/4d921bbf-bc84-4d1a-91ce-360f7b1a7a68

[10] O. Afolalu y M. S. Tsoeu, «Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions», *Future Internet*, vol. 17, n.º 12, p. 575, dic. 2025, doi: 10.3390/fi17120575.

[11] «PLATAFORMA EDUCATIVA BASADA EN MOODLE CON HERRAMIENTAS DE GAMIFICACIÓN PARA PROMOVER LA CONCIENCIACIÓN Y CAPACITACION EN CIBERSEGURIDAD EN VARIAS INSTITUCIONES EDUCATIVAS DE MEDELLÍN». Accedido: 27 de mayo de 2026. [En línea]. Disponible en: https://dspace.tdea.edu.co/entities/publication/4f0a76df-d41e-4492-9105-6b7e310f9661

[12] V. G. J. Sánchez, R. I. T. Masabanda, y C. J. L. Espinoza, «Technology Rain Journal», *Technol. Rain J.*, vol. 4, n.º 2, sep. 2025, doi: 10.55204/trj.v4i1.e94.

[13] A. Sanez y M. Rodolfo, «Propuesta de gestión de incidentes de seguridad, mediante la integración de inteligencia de amenazas para la contención de ataques informáticos.», mar. 2024, Accedido: 26 de mayo de 2026. [En línea]. Disponible en: https://repositorio.uisrael.edu.ec/handle/47000/4184

[14] «Ataques cibernéticos: causas, tipos y consecuencias». Accedido: 12 de mayo de 2026. [En línea]. Disponible en: https://www.piranirisk.com/es/blog/ataques-ciberneticos-causas-y-consecuencias

[15] G. Benito, «Detección de Inyecciones SQL mediante técnicas de procesamiento de lenguaje natural y aprendizaje automático».

[16] F. M. Smulever, J. M. Pinat, R. S. Gonzalez, y L. J. Ríos, «Mitigación de riesgos en servidores Linux vulnerables: el rol de OSSEC en la prevención de ataques», *JAIIO Jorn. Argent. Informática*, vol. 11, n.º 5, pp. 78-91, oct. 2025.

[17] A. Arfeen, S. Ahmed, M. A. Khan, y S. F. A. Jafri, «Endpoint Detection & Response: A Malware Identification Solution», en *2021 International Conference on Cyber Warfare and Security (ICCWS)*, nov. 2021, pp. 1-8. doi: 10.1109/ICCWS53234.2021.9703010.

[18] R. A. Lail, M. Shkoukani, y H. Abusaimeh, «Endpoint Detection And Response Systems (EDR) Enhancing Using Classification Techniques: A Machine Learning

Approach», *Int. J. Adv. SIGNAL IMAGE Sci.*, vol. 11, n.º 2, pp. 282-300, dic. 2025, doi: 10.29284/v666fq32.

[19] G. Karantzas y C. Patsakis, «An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors», *J. Cybersecurity Priv.*, vol. 1, n.º 3, pp. 387-421, jul. 2021, doi: 10.3390/jcp1030021.

[20] W. U. Hassan, A. Bates, y D. Marino, «Tactical Provenance Analysis for Endpoint Detection and Response Systems», en *2020 IEEE Symposium on Security and Privacy (SP)*, may 2020, pp. 1172-1189. doi: 10.1109/SP40000.2020.00096.

[21] M. Seyfipoor y M. M. Eskandari, «Digital Transformation in Network Security: Transitioning from Antivirus to Endpoint Detection and Response», en *2025 9th Iranian Conference on Advances in Enterprise Architecture (ICAEA)*, nov. 2025, pp. 1-7. doi: 10.1109/ICAEA69058.2025.11301522.

[22] B. Vieda y J. Andrés, «Soluciones Endpoint Detection and Response Open-Source. Estado del arte, propuesta de medición, análisis y evaluación para determinar su implementación y aplicabilidad en ambientes empresariales».

[23] «Desarrollo de una arquitectura de red de datos en base a Zero Trust para mejorar el acceso seguro a los sistemas de información alojados en un entorno cloud para una empresa del sector manufacturero». Accedido: 27 de mayo de 2026. [En línea]. Disponible en: https://repositorioacademico.upc.edu.pe/entities/publication/00fcbaf3-fb1e-5f2d-8b55-8fd082998e01

[24] «Powerful refresh of the Sophos endpoint security portfolio – Sophos Partner News». Accedido: 11 de mayo de 2026. [En línea]. Disponible en: https://partnernews.sophos.com/en-us/2025/10/products/powerful-refresh-of-the-sophos-endpoint-security-portfolio/

[25] M. Magaña Suanzes, «Análisis y diseño de arquitecturas de ciberseguridad en distintos sectores empresariales», masters, E.T.S. de Ingenieros Informáticos (UPM), 2020. Accedido: 26 de mayo de 2026. [En línea]. Disponible en: https://oa.upm.es/67311/

[26] A. J. Moreno, «Técnicas de Evasión de Antivirus y EDR». Accedido: 26 de mayo de 2026. [En línea]. Disponible en: https://oa.upm.es/75850/

[27] «Análisis de técnicas de ataque en Active Directory e implementación de contramedidas de endurecimiento». Accedido: 27 de mayo de 2026. [En línea].

Disponible en: https://rua.ua.es/entities/publication/92e8d10f-2b5e-4ac6-9039-2f8135ea3156

[28] M. A. Inam, J. Oliver, R. Batta, y A. Bates, «Carbon Filter: Scalable, Efficient, and Secure Alert Triage for Endpoint Detection & Response», en *2025 28th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, oct. 2025, pp. 174-189. doi: 10.1109/RAID67961.2025.00050.

[29] S. Fuentes y J. Eduardo, «Análisis de herramientas endpoint and detection response (EDR) de software libre», Accedido: 26 de mayo de 2026. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/40344

[30] T. Cappelli, «Análisis e implementación de medidas, soluciones y protocolos en ciberseguridad para el Poder Judicial Provincial», Tesis, 2025. Accedido: 27 de mayo de 2026. [En línea]. Disponible en: https://sedici.unlp.edu.ar/handle/10915/182930

[31] «IEEE 802.1X Authentication Methods Compared», Cloud RADIUS. Accedido: 11 de mayo de 2026. [En línea]. Disponible en: https://cloudradius.com/ieee-802-1x-authentication-methods-comparison/

[32] F. Figueroa y A. Pamela, «Evaluación de la efectividad en la autenticación y el cifrado de redes de la normativa 802.11 b/g/n analizando las vulnerabilidades y pruebas de penetración en la categoría pentesting.», Accedido: 27 de mayo de 2026. [En línea]. Disponible en: https://repositorio.upse.edu.ec/items/0f13e8dc-4630-4629-8991-df770417eea5

[33] L. Morocho y M. Gabriela, «Análisis de modelos de cifrado para la transmisión de datos en sistemas embebidos y su aplicación en el internet de las cosas (IoT)», bachelorThesis, 2025. Accedido: 27 de mayo de 2026. [En línea]. Disponible en: https://dspace.ups.edu.ec/handle/123456789/29665

[34] P. Molina y O. David, «Capacidades técnicas, tácticas y de respuesta para equipos red team y blue team», Accedido: 26 de mayo de 2026. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/78086

[35] L. I. T. Cerezo y M. V. Lombardo, «Implementación de git y cifrado en documentos XML como estrategia de mitigación contra ransomware», *Más TIC*, vol. 1, n.º 2, pp. 96-113, dic. 2025, doi: 10.48204/3072-9696.7414.

[36] S. Alzahrani, Y. Xiao, S. Asiri, J. Zheng, y T. Li, «A Survey of Ransomware Detection Methods», *IEEE Access*, vol. 13, pp. 57943-57982, 2025, doi: 10.1109/ACCESS.2025.3556187.

[37] F. Y. Ávila-Niño, «Ransomware, una amenaza latente en Latinoamérica», *InterSedes*, vol. 24, n.º 49, pp. 92-119, jun. 2023, doi: 10.15517/isucr.v24i49.50765.

[38] R. del C. M. Hernández y H. A. O. Doña, «Vulnerabilidad de estudiantes ante ataques de Phishing», *Espila*, vol. 8, n.º 1, pp. 180-192, ene. 2026, doi: 10.61454/88z0zw71.

[39] «Impacto de las técnicas de phishing en la seguridad de sitios web.» Accedido: 27 de mayo de 2026. [En línea]. Disponible en: https://dspace.utb.edu.ec/items/98ca9b57-4705-4bf0-ae72-ac603d94f525

[40] «¿Qué es el phishing? | IBM». Accedido: 12 de mayo de 2026. [En línea]. Disponible en: https://www.ibm.com/es-es/think/topics/phishing

[41] J. E. Vélez Mazo, «Ciberseguridad aplicada a la gestión de datos en empresas de bienes y servicios: una revisión de literatura», may 2025.

[42] G. Yánez y C. Josue, «Vulnerabilidades en redes wi-fi de la Universidad Estatal de Bolívar, en el año 2025». Accedido: 26 de mayo de 2026. [En línea]. Disponible en: https://dspace.ueb.edu.ec/items/257bbae2-b732-46b6-a7e5-a81497a4d5bd

[43] «¿Qué es un ataque de hombre en el medio (MITM)? Tipos y ejemplos», Fortinet. Accedido: 12 de mayo de 2026. [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/man-in-the-middle-attack.html

[44] M. Ajuluchukwu, H. Wimmer, y A. Mohamed, «Simulating Man-in-the-Middle Attacks: Techniques, Detection, and Mitigation Strategies», en *2025 6th International Conference on Artificial Intelligence, Robotics and Control (AIRC)*, may 2025, pp. 447-451. doi: 10.1109/AIRC64931.2025.11077556.

[45] P. Agualsaca y L. Miguel, «Respuesta de los sistemas de detección de intrusiones (ids) ante amenazas cibernéticas generadas por ia : Herramientas de seguridad ofensiva evaluación de la detección de ataques de fuerza bruta generados por ia con snort», oct. 2025, Accedido: 26 de mayo de 2026. [En línea]. Disponible en: https://bibdigital.epn.edu.ec/handle/15000/26891

[46] V. A. Guzman Brand y L. Gelvez Garcia, «Identificación de ataques de denegación de servicio distribuido (DDOS) mediante la integración de algoritmos de aprendizaje automático y arquitecturas de redes neuronales artificiales», *Rev. Ing. Matemáticas Cienc. Inf. ISSN-E 2357-3716 Vol 12 Nº 23 2025 Ejemplar Dedic. Rev. Ing. Matemáticas Cienc. Inf. Págs 25-39*, n.º 23, 2025, Accedido: 26 de mayo de 2026. [En línea]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=10146198

[47] R. Montalvo Quintero y M. Salazar Castaño, «Herramientas de mediciòn para la sostenibilidad en la economìa circular colombiana: Un anàlisis comparativo de la competencia en dos empresas locales», Accedido: 27 de mayo de 2026. [En línea]. Disponible en: https://dspace.tdea.edu.co/handle/tdea/8138

[48] «Herramienta de anonimización y conversión de voz con Inteligencia Artificial». Accedido: 27 de mayo de 2026. [En línea]. Disponible en: https://docta.ucm.es/entities/publication/119b8650-0b31-4578-9191-da45b35fae9d

[49] D. G. T. Ochoa *et al.*, «Assessing Cadet Cybersecurity: Simulated Rogue Access Point Attacks at Peruvian Air Force Academy», *LACCEI*, vol. 1, n.º 12, jul. 2025, doi: 10.18687/LACCEI2025.1.1.1720.

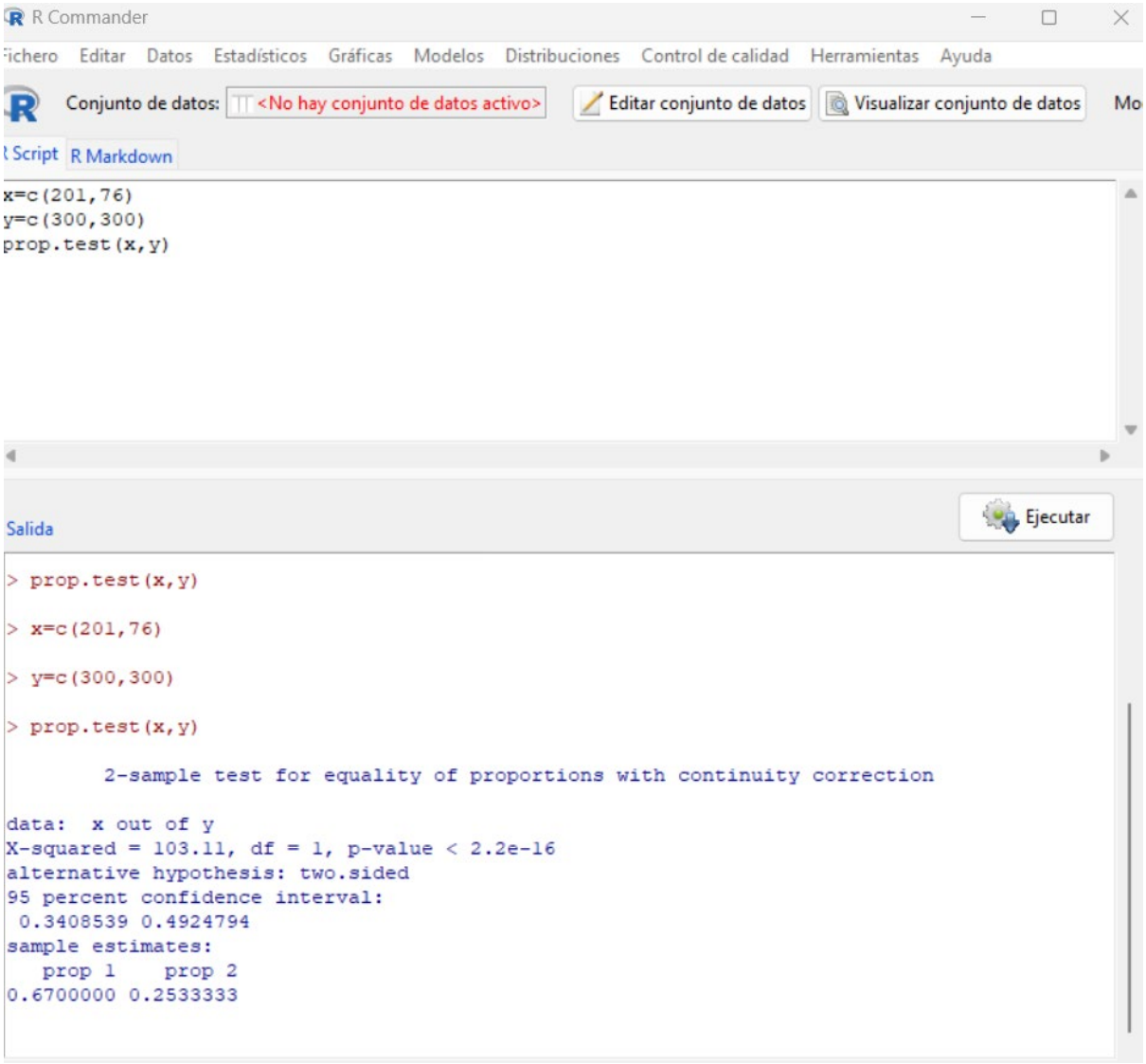
[50] D. G. Clavijo Gutiérrez y J. D. Briceño, «Steg Phantom: Sistema para la exfiltración de datos mediante técnicas de esteganografía en archivos multimedia: Análisis comparativo de herramientas de ocultamiento de información», Accedido: 26 de mayo de 2026. [En línea]. Disponible en: https://hdl.handle.net/1992/76850

[51] J. Sánchez López-Varela, «Herramienta de generacion de datasets sintéticos con funcionalidades de anonimización automática», Accedido: 27 de mayo de 2026. [En línea]. Disponible en: https://docta.ucm.es/entities/publication/dd20e1a3-0778-467a-bf3d-dcdbb4f2152d

[52] M. J. Rochina Rochina, «Análisis y evaluación de la red inalámbrica de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo para determinar el nivel de seguridad mediante herramientas de software libre», bachelorThesis, Riobamba, Universidad Nacional de Chimborazo, 2024. Accedido: 12 de mayo de 2026. [En línea]. Disponible en: http://dspace.unach.edu.ec/handle/51000/12979

ANEXOS

Anexo1. Ingreso de datos del modelo estadístico en Software RStudio



Anexo 2. Informes de Control y monitoreo de Sistema Sopho

Sitios bloqueados

Sophos Cloud

Sitio	Visitas	Principales 5 usuarios (visitas)	Categorías
amspbs.com	374	HP\User (27) PROONE440\User (26) EDIF-DIR-NA00X\user (11) Dell\User (8) EA-DEACI-CM310\CMancheno (7)	Proxies & Translators
bing.net	146	HP\User (19) PROONE440\User (10) FCE-LF401-20\User (5) FS-LAB303-EDLT002\USUARIO (5) FCE-LF402-07\DTICD (5)	Adult/Sexually Explicit
www-slideshare-net.translate.goog	135	PROONE440\User (25) CTE-LAB403-PC07\User (5) CTE-LAB403-PC14\User (5) CTE-LAB403-PC16\User (4) CTE-LAB305-PC05\User (4)	Proxies & Translators
www-sciencedirect-com.translate.goog	133	HP\User (18) EDIF-DIR-NA00X\user (8) Dell\User (5) EA-DEACI-CM310\CMancheno (4) CTE-LAB402-PC16\User (4)	Proxies & Translators
pmc-ncbi-nlm-nih-gov.translate.goog	125	EA-DEACI-CM310\CMancheno (27) HP\User (16) CTE-LAB304-PC17\User (5) CTE-LAB304-PC18\User (4) Dell\Usuario (4)	Proxies & Translators
microsofttranslator.com	111	FCE-LF301-05\DTIC (17) FCE-LF402-04\DTICD (11) PROONE440\User (10) FCE-LABB101-25\User (7) FCE-LF402-06\DTICD (5)	Proxies & Translators
urban-vpn.com	107	CTE-LAB404-PC13\User (68) HP\User (29) FCE-LF301-09\DTIC (7) FCE-LF301-17\DTIC (2) LAB401-PC11\User (1)	Proxies & Translators
my-clevelandclinic-org.translate.goog	101	EA-DEACI-CM310\CMancheno (26) HP\User (6)	Proxies & Translators

Sitios bloqueados

Sophos Cloud

Sitio	Visitas	Principales 5 usuarios (visitas)	Categorías
www-ncbi-nlm-nih-gov.translate.goog	86	EA-DEACI-CM310\CMancheno (11) HP\User (10) Dell\Usuario (5) Dell\G 302 (3) CTE-LAB304-PC14\User (2)	Proxies & Translators
www-quora-com.translate.goog	84	EDIF-DIR-NA00X\user (8) PROONE440\User (6) CTE-LAB404-PC22\User (4) HP\User (3) EA-TH-PB-AC-01\User (2)	Proxies & Translators
mytranslator.app	83	EA-DEACI-XL301\XLopez (83)	Proxies & Translators
www-investopedia-com.translate.goog	80	PROONE440\User (39) HP\User (5) Dell\User (3) LAB401-PC16\User (2) LAB401-PC6\User (2)	Proxies & Translators
www-shakespeare-org-uk.translate.goog	48	FCE-LABB101-22\User (3) FCE-LABB101-05\User (2) FCE-LABB101-08\User (2) FCE-LABB101-03\User (2) FCE-LABB101-21\User (2)	Proxies & Translators
www-researchgate-net.translate.goog	39	PROONE440\User (14) EDIF-DIR-NA00X\CTE (2) CTE-LAB305-PC12\User (2) CTE-LAB304-PC06\User (1) CTE-LAB402-PC16\User (1)	Proxies & Translators
study-com.translate.goog	38	EDIF-DIR-NA00X\user (5) HP\User (2) PROONE440\User (2) FCE-LF401-02\User (2) CTE-LAB304-PC21\User (2)	Proxies & Translators
editor-codecogs-com.translate.goog	38	CTE-LAB402-PC17\User (5) CTE-LAB402-PC13\User (4) CTE-LAB402-PC06\User (4) CTE-LAB402-PC08\User (3) CTE-LAB402-PC07\User (3)	Proxies & Translators
www-merriam--webster-	37	PROONE440\User (5)	Proxies & Translators

Anexo 3. Carta de Compromiso de la institución

Riobamba, 4 de diciembre 2024

ACTA DE COMPROMISO DE LA INSTITUCIÓN

Yo, **José Javier Haro Mendoza**, en mi calidad de **Director del Departamento de Tecnologías de la Información y Comunicación**, me comprometo a brindar asesoría y apoyo al estudiante **Daniel Marcelo Machado Espinoza** en el desarrollo de su tesis titulada **Desarrollo de Estrategias de Ciberseguridad para la Protección de la Infraestructura Tecnológica de la Universidad Nacional de Chimborazo utilizando la Detección y Respuesta de Endpoints**. Proyecto se está llevando a cabo bajo la dirección de la **Mgs. Alejandra del Pilar Pozo Jara**, quien actúa como mi **Tutor De Tesis.**

Como **director del Departamento de Tecnologías de la Información y Comunicación**, asumo los siguientes compromisos:

- Orientar y guiar al estudiante durante todas las etapas del proceso de investigación y desarrollo de la tesis.
- Revisar y retroalimentar de manera oportuna y constructiva los avances del trabajo de investigación presentados por el estudiante.
- Supervisar y monitorear el cumplimiento de los objetivos y el cronograma establecido para la tesis.
- Fomentar el desarrollo de habilidades investigativas y de redacción en el estudiante.
- Velar por el cumplimiento de los estándares éticos y metodológicos en la investigación.
- Facilitar, en la medida de lo posible, los recursos y herramientas necesarias para el desarrollo efectivo de la tesis.
- Mantener una comunicación efectiva y constante con el estudiante, brindando asesoría y resolviendo dudas de manera oportuna.
- Promover el pensamiento crítico y la capacidad de análisis en el estudiante.
- Brindar retroalimentación constructiva y sugerencias para mejorar el trabajo de investigación.
- Apoyar al estudiante en la preparación y presentación de la tesis.

Estoy comprometido a trabajar de manera conjunta con el estudiante, con respeto y profesionalismo, para lograr el éxito en el desarrollo de la tesis y contribuir al avance del conocimiento en el área de investigación correspondiente.

Firmado electrónicamente por:
JOSE JAVIER HARO MENDOZA

Ing.Javier Haro. Mag.
Director del Departamento de
Tecnologías de la Información y Comunicación