Universidad Nacional Autónoma de México

Facultad de Ciencias

Análisis de un modelo matemático que permite estudiar la propagación de amenazas tipo secuestro de datos (ransomware).

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

Licenciado en Matemáticas Aplicadas

PRESENTA:

Alan Uriel Monroy Pérez Negrón

TUTORES

Dra. Bibiana Obregón Quintana
Mtro. en TI. Edgar Alberto Chillón Escárcega

Ciudad Universitaria, 2024

Quizá la mariposa sea el mejor ejemplo para demostrar, que después de momentos de oscuridad algo hermoso sucede.

Anónimo

Dicen que, en el Derby de Kentucky, el caballo ganador se queda sin oxígeno después de la primera media milla, y el resto de la distancia la corre con el corazón.

John C. Maxwell, Las 21 leyes irrefutables del liderazgo

Agradecimientos

Es un honor y un privilegio para mí haber llegado a este punto en mi vida y carrera universitaria. A medida que me acerco a la finalización de mi tesis y culmino mis estudios, quiero tomarme un momento para expresar mi sincero agradecimiento a todas las personas que han sido una parte fundamental en este viaje lleno de aprendizaje y crecimiento.

En primer lugar, quiero agradecer a mi familia por su inquebrantable apoyo, amor y aliento a lo largo de los años. Su constante respaldo emocional me ha permitido concentrarme en mis estudios y perseguir mis metas académicas con determinación y pasión. Cada sacrificio que han hecho ha sido una fuente constante de inspiración para mí, y les estoy eternamente agradecido.

De manera especial quiero agradecer a la Dra. Bibiana Obregón Quintana y al Mtro. en TI. Edgar Alberto Chillón Escárcega, quiero expresar mi gratitud por su dedicación y paciencia al guiarme en el desarrollo de este trabajo y por todas las enseñanzas que me han dejado tanto académica como personalmente. Gracias por ser no solo mis tutores, sino mentores y guías en este camino hacia la culminación de mi formación académica.

Estimados Dr. Edwin Montes Orozco, Dr. José Antonio Marmolejo Saucedo y Dr. Pedro Eduardo Miramontes Vidal, quiero expresar mi sincero agradecimiento por su tiempo y dedicación durante mi proceso de titulación. La oportunidad de recibir sus comentarios y orientación ha sido fundamental para mi crecimiento académico. Aprecio sinceramente la manera en que cada uno de ustedes ha contribuido a enriquecer mi trabajo y aportar perspectivas valiosas. Este logro no habría sido posible sin su apoyo. Gracias por su profesionalismo y por ser parte esencial de este importante hito en mi carrera académica.

A mis amigos y compañeros de clase, gracias por su apoyo, sus risas, conversaciones y colaboración. Me han ayudado a superar los momentos difíciles y a disfrutar plenamente de esta experiencia universitaria.

Finalmente, a ustedes, mamá y papá, quiero decir que todo lo que he logrado en mi carrera y vida hasta ahora es gracias a su amor, guía y paciencia. Su apoyo constante ha sido el faro que me ha iluminado en los momentos de incertidumbre y desafío. Su confianza en mí y su ejemplo de perseverancia me han impulsado a esforzarme y superar obstáculos.

A medida que llego al final de este capítulo y miro hacia el futuro, quiero que sepan cuán orgulloso estoy de convertirme en las personas que son. Gracias por ser unos modelo a seguir y por creer en mí incondicionalmente.

Índice general

Índice de figuras

Índice de tablas

Introducción

Desde hace unos años la información se ha convertido en uno de los activos de mayor importancia para las organizaciones a nivel mundial. Dado al gran número de tecnologías emergentes y los elevados índices de ataques informáticos día tras día, es necesario que las empresas cuenten con robustos niveles de seguridad y políticas organizacionales que permitan detener el detrimento a sus activos por parte de las ***amenazas*** externas e internas. Principalmente, las áreas de ciberseguridad son las encargadas de la aplicación de tecnologías, procesos y controles para proteger los sistemas, las redes, los dispositivos y los datos que puedan verse afectados ante amenazas internas o externas. En la actualidad, los expertos en este campo detienen y previenen miles de ataques, lo cual ha permitido descubrir que el número de amenazas cada vez es mayor y, por ende, la ciberseguridad está empezando a desempeñar un rol fundamental en el mundo.

El ***Hacking ético*** es la rama de la ciberseguridad encargada de medir los niveles de seguridad informática dentro de una organización, según los estándares, metodologías y ***frameworks*** modernos con la finalidad de presentar un cuadro de mando de madurez que destaque el ***riesgo*** general, las ***vulnerabilidades*** presentes y sugerencias para mejorar el estado de seguridad en las organizaciones. Al hacer uso de ***hackers éticos***, las organizaciones obtienen una idea de sus propias vulnerabilidades, lo cual permite crear medidas de protección en contra de futuros ataques informáticos. El beneficio principal del hacking ético es evitar que los atacantes maliciosos roben y utilicen indebidamente los datos, al igual que:

- Descubrir vulnerabilidades desde el punto de vista de un atacante para que se puedan atender según el modelo de riesgos planteado por la organización.
- Implementar una red segura que evite brechas de seguridad.
- Defender la seguridad organizacional mediante la protección de datos ante todo tipo de amenazas.
- Ayudar a proteger las redes con evaluaciones actualizadas y apegadas a las mejores prácticas.
- Ganar la confianza de clientes e inversores al garantizar la seguridad de sus productos y datos.

Para alcanzar los mejores resultados en el Hacking ético se hace uso de las ***pruebas de intrusión*** (también conocidas como pruebas de penetración), en donde a través de un ejercicio de seguridad se identifican los puntos débiles en sistemas informáticos que puedan ser aprovechados, así entonces, un ***pentester*** intenta explotar dichas deficiencias y/o vulnerabilidades con el fin de demostrar los

estados de inseguridad de la organización por un lado, así como la capacidad de defensa y respuesta de la empresa por otro. Una de las formas de categorizar las pruebas de intrusión es a través de una clasificación según el nivel de conocimiento y acceso otorgado al pentester [16]:

- Ciego (Blind).- En este escenario el pentester se enfrenta al objetivo sin conocimiento previo de sus defensas, activos o canales. Por su parte, el objetivo se prepara para las pruebas, conociendo de antemano todos los detalles. La amplitud y profundidad de este ejercicio puede ser tan grande como lo permita el conocimiento aplicable y la eficiencia del pentester. A menudo se le describe como **War Gaming** o **Role Playing**.

- Doble Ciego (Double Blind).- En este escenario el pentester se enfrenta al objetivo sin conocimiento previo de sus defensas, activos o canales. No se notifica al objetivo con anticipación el alcance de la auditoría, los canales probados ni los vectores de prueba. Este escenario pone a prueba las habilidades del pentester y la preparación del objetivo ante posibles ataques. También se conoce como prueba de caja negra.

- Caja Gris (Gray box).- El pentester se enfrenta al objetivo con un conocimiento limitado de sus defensas y activos y un conocimiento completo de los canales. Por su parte, el objetivo se prepara para la auditoría, conociendo de antemano todos los detalles. La naturaleza de la prueba es la eficiencia, mientras que la amplitud y la profundidad dependen de la calidad de la información proporcionada al pentester antes de la prueba, así como del conocimiento aplicable. Este tipo de prueba también es conocida como Prueba de vulnerabilidad y, con mayor frecuencia, el objetivo la inicia como una autoevaluación.

- Doble Caja Gris (Double Gray Box).- El pentester se enfrenta al objetivo con un conocimiento limitado de sus defensas y activos y un conocimiento completo de los canales. El objetivo es notificado por adelantado del alcance y el marco de tiempo de las pruebas, pero no los canales probados o los vectores de prueba. Este ejercicio pone a prueba las habilidades del analista y la preparación del objetivo ante posibles ataques. La amplitud y la profundidad dependen de la calidad de la información proporcionada al pentester antes de la prueba, así como del conocimiento aplicable del mismo. También se conoce como prueba de caja blanca.

- Tandem.- en este caso tanto el pentester como el objetivo están preparados para la auditoría, conociendo ambos de antemano todos los detalles. Aquí se busca probar la protección y los controles del objetivo. Sin embargo, no puede probar la preparación del objetivo a variables desconocidas como posibles ataques. La verdadera naturaleza de la prueba es minuciosidad, ya que el analista tiene una visión completa de todas las pruebas y sus respuestas. A menudo se le conoce como una auditoría interna o una prueba **Crystal Box** y el analista suele ser parte del proceso de seguridad.

- Reversible (Reversal).- El pentester interactúa con el objetivo con pleno conocimiento de sus procesos y seguridad operativa, pero el objetivo no sabe nada de qué, cómo o cuándo se realizarán las pruebas. La verdadera naturaleza de esta prueba es auditar la preparación del objetivo ante posibles ataques. También se conoce como **Red Team**.

Al finalizar las pruebas de intrusión, en particular desde un enfoque interno, las empresas generalmente preguntan qué vulnerabilidades deben mitigar primero, qué acciones deben tomar para fortalecer los niveles de seguridad o cuánto tiempo aproximadamente deben tardar para mitigar los

hallazgos encontrados. En realidad, las respuestas a todas estas preguntas no son sencillas, pues solamente las mismas empresas conocen la importancia de los equipos de su red, del aplicativo analizado y los controles de seguridad establecidos. Sin embargo, la experiencia y el trabajo del pentester permite brindar al cliente una posible manera de mitigar sus problemas y, aunque depende fuertemente de los hallazgos encontrados, en general es posible utilizar los siguientes recursos para hacer esto posible:

- Mapa de compromiso que permita ver qué vulnerabilidades tienen un mayor impacto sobre la organización y cuáles permitieron una etapa de post-explotación proactiva.
- Ponderación mediante el sistema de puntuación de vulnerabilidades (CVSS, por sus siglas en inglés), el cual es un estándar para evaluar la gravedad de las vulnerabilidades, que permite obtener una evaluación objetiva y consistente. También ayuda a priorizar qué vulnerabilidades deben ser corregidas primero, en función de su impacto potencial: crítico, alto, medio o bajo.

Problemática

A pesar de que las pruebas de intrusión dan visibilidad sobre la falta de controles de seguridad de las organizaciones, es necesario dar nuevos enfoques que fortalezcan la seguridad en las redes organizacionales y se convierta en una prioridad estratégica robustecer la ciberseguridad frente a la constante evolución de las *tácticas* y *técnicas* desarrolladas por los ciberdelincuentes y salvaguardar la integridad, disponibilidad y confidencialidad en los activos tecnológicos.

Justificación

La rápida evolución de los ataques utilizados por los ciberdelincuentes subraya la necesidad de mejorar la seguridad presente y la resiliencia de las organizaciones. Por tanto, es necesario comprender y contrarrestar la evolución de estos ataques para desarrollar nuevas estrategias defensivas eficaces.

Objetivo General

Este trabajo tiene como **objetivo** medir el nivel de propagación de amenazas tipo ransomware en diferentes escenarios tecnológicos, al simular diversas redes organizacionales con diferentes controles de defensa establecidos mediante el análisis de la red.

Objetivos Particulares

I Desarrollar un código en python que simule el comportamiento del ransomware WannaCry [3] sobre diversas ***redes lógicas*** y ***redes físicas*** cuyos equipos conectados no superen los 150 nodos, esto con la finalidad de enfocar el trabajo a las pequeñas y medianas empresas (pymes), en donde los equipos vulnerables únicamente tienen sistema operativo Windows.

II Desarrollar un código en python que modele la infraestructura de la red interna de una organización en una red conexa cuyos nodos tengan asignadas ciertas características.

III Desarrollar un código en python que permita buscar los nodos de mayor relevancia y localizaciones estratégicas al tomar en cuenta la centralidad de vector propio y el algoritmo PageRank para establecer controles de seguridad basados en los cinco principios establecidos en el framework del Instituto Nacional de Estándares y Tecnología, (NIST, por sus siglas en inglés) para la gestión de riesgos asociados a la seguridad de la información.

Para concluir esta sección, el presente trabajo esta estructurado de la siguiente manera: El capítulo 1, ofrece un panorama general sobre ciberseguridad, los múltiples frameworks existentes y el ransomware. El capítulo 2 aborda los acontecimientos históricos de mayor relevancia para el desarrollo de la teoría de redes, así como los conceptos y definiciones utilizadas a lo largo del trabajo. El capítulo 3 muestra los pasos seguidos para la modelación de la red, los límites considerados para su desarrollo y se especifican las fuentes donde se obtuvieron los datos. En el capítulo 4 se generan los escenarios para simular el ransomware y con el código desarrollado se mide e interpreta el esparcimiento. En seguida, se discuten los resultados relevantes de cada escenario y cómo ayudan los controles de seguridad. Por último, se presentan las conclusiones generales del análisis realizado, así como estudios futuros para darle continuidad a este proyecto y obtener nuevos resultados.

Como complemento del trabajo existe un glosario con las definiciones relevantes de los conceptos utilizados y, a través de un apéndice, se comparte el código desarrollado y los nodos que conforman las redes al igual que sus características.

Capítulo 1

Antecedentes

Este capítulo muestra un breve resumen sobre la historia y los hechos importantes que han ocurrido en el área de la ciberseguridad desde sus albores, Además, se mencionan diversos marcos de ciberseguridad existentes como el *NIST*, *Cyber Kill Chain* y *Mitre ATT&CK* (ver apartados 1.1.1, 1.4 y 1.3 respectivamente) y cómo ayudan a gestionar los riesgos y amenazas a los cuales se enfrenta una organización. Por último, se va a explicar el *ransomware*, la forma en que actúa y por qué afecta tanto a las organizaciones.

1.1. Ciberseguridad

En 1943 fue creada la primera computadora digital, el Internet aún no existía y sólo había algunas computadoras ubicadas alrededor del mundo. No había conexión entre los equipos para mover datos o archivos y esto creó, lo que podría considerarse, un ambiente seguro, las amenazas eran casi inexistentes. Sin embargo, a finales de esta década ya se empezaban a desarrollar teorías sobre los ***virus***. John von Neumann [41] creía que podría ocurrir algún tipo de "organismo mecánico" que dañaría a las máquinas, podría replicarse a sí mismo como un virus natural y también infectar nuevos equipos.

Durante la década de 1950 y principios de 1960, las computadoras eran sistemas muy grandes y costosos que se instalaban en grandes habitaciones lejos del público en general y pocas personas podían tener acceso. Curiosamente a finales de 1950, se desarrolló el término ***hacker*** cuando un grupo de personas comprometió el club de modelos ferroviarios tecnológicos del Instituto Tecnológico de Massachusetts (MIT, por sus siglas en inglés) para ajustar la funcionalidad de los trenes de alta tecnología [21].

También en la década de 1950 empezó el ***hacking***, aunque originalmente no se había desarrollado como una forma de realizar acciones con computadoras, sino que se vinculaba con el uso del teléfono cuando comenzó una tendencia llamada ***phreaking***. En este caso los usuarios malintencionados — denominados como ***phreakers*** — eran personas que tenían un interés significativo en el funcionamiento de los teléfonos e intentaban secuestrar los protocolos vigentes que permitían a los ingenieros trabajar en la red telefónica. Esto permitió a las personas realizar llamadas gratuitas y reducir los peajes para las llamadas de larga distancia, esta práctica continuó durante algunos

años y dejó a muchas compañías telefónicas expuestas sin una forma de evitar que ocurriera, siendo John Thomas Draper, también conocido como "Capitán Crunch", el padre de esta técnica [14].

Es hasta la década de 1970, cuando la ciberseguridad nace de manera oficial con un proyecto denominado Red de Agencias de Proyectos de Investigación Avanzada (ARPANET, por sus siglas en inglés), desarrollado por parte del Departamento de Defensa de los Estados Unidos para utilizarla como medio de comunicación entre las diferentes instituciones académicas y estatales [22], esta fue la red de conectividad desarrollada antes de la propia Internet. En 1971, un hombre llamado Bob Thomas determinó que era posible que un programa se moviera a través de una red y para probarlo desarrolló un programa que pudiera moverse entre las ***terminales Tenex*** en ARPANET. Este programa recibió el nombre de *Creeeper*, el cual no era un programa malicioso, y simplemente viajaba por la red replicándose a sí mismo y mostrando el mensaje: "I'M THE CREEPER: CATCH ME IF YOU CAN" por donde pasaba. El alcance que tuvo Creeper despertó el interés y cierta preocupación de los investigadores y fue Ray Tomlinson el encargado de desarrollar un nuevo programa para detener a Creeper, ese programa fue llamado Reaper y ha sido considerado como el primer antivirus de la historia [15].

La década de 1980 trajo consigo numerosos problemas para la ciberseguridad, se llevaron a cabo un gran número de ataques relevantes y fue en 1983, cuando se desarrollaron nuevos términos para describir esos ataques: virus informáticos y ***T*roya*n*os**. También, debido a la guerra fría, el gobierno de Estados Unidos estableció nuevas pautas y recursos para manejar el ***c*iberespionaje** y las nuevas amenazas. Para lograr esto, el Departamento de Defensa de Estados Unidos (DOD, por sus siglas en inglés) desarrolló lo que se conoce como *Trusted Computer System Evaluation Criteria* [1], más tarde conocido como *El Libro Naranja*.

Toda la década de 1990 y del 2000 tuvieron un cambio en el paradigma de la seguridad informática debido a los nuevos ataques desarrollados por los ciberdelincuentes, las consecuencias que trajo consigo la Guerra Fría y otros sucesos mundiales importantes, más personas estaban investigando cómo crear virus mortíferos y efectivos. Cuantas más personas desarrollaban ***m*alware**, más evolucionaba y se volvía más invasivo, pero esto también permitió que la industria de la ciberseguridad creciera y con eso algunos desarrollos clave que ayudaron a sentar las bases para los virus y amenazas modernas [25], entre los que destacan:

- **Virus polimórficos**.- En 1990, se desarrolló el primer código que mutaba a medida que infectaba nuevos equipos, aunque siempre mantenía el algoritmo original. Los virus polimórficos se diseñaron para evitar la detección, lo cual hizo más difícil para los usuarios saber que estaban infectados.
- ***Virus en macros*** **y técnicas de sigilo**.- En 1996, se desarrolló la capacidad de sigilo por parte de los virus y también se lanzaron los virus escritos en macro. Ambos crearon más desafíos y requirieron nuevos desarrollos de software antivirus con el objetivo de aumentar las formas de protegerse contra los riesgos. A medida que se desarrollaban nuevos grupos de ciberdelincuentes, las empresas enfrentaban muchos nuevos desafíos para mejorar la seguridad y minimizar las fugas de datos.
- **Sitios web maliciosos**.- A principios de la década del 2000, se produjo un nuevo tipo de

infección en la que ya no era necesario descargar archivos, ahora sólo bastaba con ir a un sitio web que contuviera el virus para ser infectado.

- **Hackeos a instituciones financieras**.- Los hackeos de tarjetas de crédito también empezaron en la década de los años 2000. Destacó el grupo de Albert Gonzales [40], ya que lograron sustraer información confidencial de 45.7 millones de tarjetas de crédito a través de bases de datos de minoristas. Esto creó una necesidad más amplia de centrarse en la seguridad de la información en varios sectores.

Si bien las amenazas se intensificaron, también se desarrollaron nuevas soluciones y métodos de detección para contrarrestar rápidamente las problemáticas. Algunas de las soluciones creadas siguen siendo utilizadas hoy en día con sus respectivas mejoras y actualizaciones, entre las que destacan:

- Cortafuegos.- Un *firewall* o cortafuegos es un dispositivo de seguridad que ayuda a proteger una red al filtrar el tráfico y evitar que personas externas o no autorizadas obtengan acceso a los datos privados de un dispositivo. Un firewall no sólo bloquea el tráfico no deseado, sino que también puede ayudar a evitar que ***software*** malintencionado infecte a las computadoras.

- ***Protocolo*** *Secure Socket Layer* (SSL).- El protocolo SSL fue desarrollado para garantizar la privacidad, la autenticación y la integridad de los datos en las comunicaciones. Hoy en día este protocolo se encuentra obsoleto, pero es el predecesor del cifrado *Transport Layer Security* (TLS, por sus siglas en inglés) moderno que se utiliza hoy en día y también fungió como base para el desarrollo del protocolo *HyperText Transfer Protocol Secure* (HTTPS, por sus siglas en inglés).

- Factor de doble autenticación.- Este proceso agrega una capa adicional de seguridad al proceso de autenticación, ya que dificulta que los atacantes obtengan acceso a los dispositivos o cuentas de una persona. Si la contraseña de un usuario se ve afectada por alguna ***fuga de datos*** o problemas de seguridad similares, se requiere que el usuario se identifique de dos maneras diferentes. La teoría detrás de la verificación en dos pasos es que, para poder autenticarte en una cuenta, la verificación de la identidad está vinculada a "saber algo" y "tener algo".

- Informática forense.- Esta rama de la informática se enfoca en la investigación y el análisis de los dispositivos tecnológicos, con el objetivo de recopilar la información necesaria a través de una investigación adecuada y bien estructurada para descubrir qué sucedió en un dispositivo.

- Centros de Operaciones de Seguridad (SOC, por sus siglas en inglés).- La función de un centro de operaciones de seguridad es monitorear, detectar, investigar y responder a las amenazas las 24 horas del día mediante una jerarquía que permite actuar como el centro o puesto de mando central, y recibir la información de toda la infraestructura del área de la Tecnología de la información (TI) de una organización, incluidas sus redes, dispositivos, almacenes de información, dondequiera que se sitúen los equipos.

- ***Threat Hunting***.- Esta es una rama de la ciberseguridad especializada en generar una búsqueda de seguridad proactiva a través de redes, puntos finales y conjuntos de datos para buscar actividades maliciosas, sospechosas o riesgosas que han eludido la detección del SOC y demás mecanismos de seguridad.

- Hackeo ético.- Esta práctica genera un proceso para la detección de vulnerabilidades, al analizar una organización y buscar puntos débiles en la infraestructura o funcionalidades de una aplicación o sistema sobre el cual un ciberdelincuente o usuario malintencionado pudiera afectar o causar daños. Con esto, es posible medir los niveles de seguridad internos y externos de las organizaciones.

1.1.1. Marco de Ciberseguridad del NIST

El marco de seguridad del NIST consta de estándares, pautas y mejores prácticas para administrar el riesgo relacionado con la seguridad informática, mediante un enfoque priorizado y flexible que promueve la protección y la resiliencia de la infraestructura crítica y los demás sectores importantes para la seguridad de las empresas e instituciones. Este marco puede ser comprendido mediante cinco funciones [5], las cuales representan los pilares principales para un programa de seguridad exitoso y holístico que permite que las organizaciones expresen su gestión del riesgo y faciliten la toma de decisiones en la gestión, estas funciones son:

- Identificar.- Consiste en desarrollar una comprensión organizacional para administrar el riesgo de seguridad informática para sistemas, personas, activos, datos y capacidades. Además, permite a una organización enfocar y priorizar los esfuerzos de acuerdo con una estrategia de gestión de riesgos y las necesidades comerciales.
- Proteger.- Describe las medidas de seguridad adecuadas para garantizar la prestación de servicios de infraestructura crítica. La función de protección admite la capacidad de limitar o contener el impacto de un posible evento de ciberseguridad.
- Detectar.- Define las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad y permite el descubrimiento oportuno de estos eventos.
- Responder.- Esta función incluye actividades apropiadas para tomar medidas con respecto a un incidente de ciberseguridad detectado. La función de respuesta admite la capacidad de contener el impacto de un posible incidente.
- Recuperar.- Permite identificar las actividades apropiadas para mantener los planes de resiliencia y restaurar cualquier capacidad o servicio que se vio afectado debido a un incidente de ciberseguridad. Admite la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente.

Para poder implementar estas cinco funciones las empresas deben hacer uso de diversos controles de seguridad (contramedidas que se utilizan para reducir las posibilidades de que una amenaza tome ventaja de una vulnerabilidad) y así evitar poner en riesgo la confidencialidad, integridad y disponibilidad de la información.

La implementación efectiva de un control de seguridad se basa la clasificación con relación al incidente, las clasificaciones más utilizadas están establecidas en la certificación "Profesional certificado en seguridad de sistemas de información" (CISSP, por sus siglas en inglés) [18], del Consorcio Internacional de Certificación de Seguridad de Sistemas de Información (ISC)^2, por sus siglas en inglés] que divide los múltiples controles de seguridad existentes en distintas categorías de acuerdo a sus funcionalidades, cada categoría al igual que la tecnología característica se expresa a continuación:

- Controles preventivos.- son la primera línea de defensa y están diseñados para intentar evitar que ocurra un incidente.
  - ***Hardening***.- Es el proceso de reducir la exposición a la seguridad y reforzar los controles de seguridad.
  - Capacitaciones sobre seguridad.- Brindar educación sobre ciberseguridad a los trabajadores respecto a la gran variedad de amenazas que afectan la seguridad de la información y las políticas y procedimientos de la empresa para abordarlas.
  - Política de desactivación de cuentas.- Una política que define qué hacer con las cuentas de acceso para empleados que ya no forman parte de la organización.
  - ***IPS***.- El Sistema de Prevención de Intrusión (IPS, por sus siglas en inglés) es una tecnología de seguridad de red que supervisa el tráfico en la red para detectar anomalías en el flujo de tráfico. Los sistemas de seguridad IPS interceptan el tráfico de la red y pueden prevenir rápidamente la actividad maliciosa descartando paquetes o restableciendo las conexiones.
  - Antivirus.- Es un programa diseñado para detectar y eliminar virus y otro tipo de malware de las computadoras.
- Controles detectivos.- estos no funcionan en tiempo real, sino que están diseñados para detectar incidentes después de que hayan ocurrido
  - ***SIEM***.- El gestor de eventos e información de seguridad (SIEM, por sus siglas en inglés) es un conjunto de herramientas y servicios que ofrece una visión de la seguridad de la información de una organización mediante registros operativos de varios sistemas.
  - Supervisión de registros.- El monitoreo de registros es un método de diagnóstico utilizado para analizar eventos en tiempo real o datos almacenados para garantizar la disponibilidad y monitorear el estado de la aplicación.
  - ***IDS***.- Un sistema de detección de intrusos (IDS, por sus siglas en inglés) es una aplicación que monitorea el tráfico de la red y busca amenazas conocidas y actividad sospechosa o maliciosa.
- Controles correctivos.- Están diseñados para restaurar los sistemas a su forma original después de que haya ocurrido un incidente.
  - Copias de seguridad y recuperación del sistema.- Es necesario contar con copias de los datos y archivos para usar en caso de que los originales se pierdan, se destruyan o se corrompan.
- Controles disuasivos.- Están diseñados para intentar desalentar a los actores maliciosos de causar un incidente, usualmente se conforman de objetos tangibles o personas.
  - Guardias de seguridad.
  - Equipo de videovigilancia.
  - Alarmas
- Controles de recuperación.- Están enfocados en reparar recursos, capacidades y funciones después de que ocurre un incidente. Muchas veces no sólo reparan el daño causado, sino que también evitan que vuelva a ocurrir.

    - Copias de seguridad.
    - Sistemas de accionamiento tolerantes a fallos.
    - Agrupación de servidores.

- Controles compensatorios.- Son controles alternativos que se utilizan cuando un control primario no es factible.
    - Cifrado.- La información dentro de las bases de datos, los correos electrónico y otras herramientas deben estar cifrados para mejorar su seguridad.

Cabe mencionar que un control puede formar parte de uno o más tipos de clasificaciones.

1.1.2. Tecnología Tradicional vs Siguiente Generación

Los diversos controles de seguridad existentes han estado en una constante evolución, tratando de adaptarse para poder hacer frente ante las constantes amenazas que surgen día a día. Actualmente existe la tecnología denominada *Siguiente Generación* (Next Generation, en inglés) que brinda una nueva forma de defensa ante las organizaciones. Las principales diferencias entre las defensas tradicionales, en particular antivirus y firewalls, y las nuevas en el mercado de acuerdo con Gartner [12], se enlistan a continuación:

- Los firewalls de siguiente generación ofrecen inspección profunda de paquetes, control de aplicaciones, detección de intrusos, prevención de malware y visibilidad completa de los usuarios y dispositivos conectados a la red. Los firewall tradicionales se enfocan en inspeccionar y controlar el tráfico de red a nivel de puertos y protocolos mediante una serie de reglas. No pueden inspeccionar el tráfico en profundidad para detectar y prevenir amenazas avanzadas.
- Los firewalls de próxima generación ofrecen una configuración centralizada y automatizada que reduce los errores humanos y facilita la implementación de políticas de seguridad coherentes y efectivas. Los firewalls tradicionales no tienen la capacidad de detectar y prevenir intrusiones y malware. Además, no correlacionan eventos de seguridad en tiempo real.
- Los antivirus de siguiente generación utilizan técnicas avanzadas de análisis de amenazas, como el aprendizaje automático y la inteligencia artificial, para detectar amenazas conocidas y desconocidas, mientras que los antivirus tradicionales se basan principalmente en firmas de virus.
- Los antivirus de siguiente generación tienen un impacto mínimo en el rendimiento del sistema, gracias a la utilización de técnicas de análisis más eficientes y al uso de hardware especializado, mientras que los antivirus tradicionales pueden ralentizar el rendimiento del sistema debido al escaneo constante de archivos.

1.2. Ransomware

El ransomware es un tipo de ataque que cifra los datos de una víctima hasta que se realiza un pago al atacante. Si no se realiza el pago del rescate, el actor malintencionado puede publicar los datos en sitios de filtración de datos (DLS, por sus siglas en inglés) o bloquear el acceso a los archivos a perpetuidad. Es una de las tácticas más rentables para los ciberdelincuentes, con pago de rescate promedio de $570,000 mil dólares para el año 2021 y un costo total anual total de $20 billones de dólares en el año 2020 [33].

1.2.1. Tipos de Ransomware y Métodos de Infección

En la actualidad los ataques de ransomware cuentan con diversos mecanismos de propagación y con ello la manera en que consiguen afectar y comprometer a los equipos vulnerables es distinta a pesar de que los objetivos (casi siempre económicos) son similares. A continuación, se describe los tipos de ransomware y los métodos de infección más comunes.

- Ransomware de cifrado (***Encrypting ransomware***).- En este caso, el ransomware cifra sistemáticamente los archivos del disco duro del sistema, que se vuelve difícil de descifrar sin pagar el rescate por la clave de descifrado. Generalmente el pago se solicita mediante Bitcoin, MoneyPak, PaySafeCard, Ukash o una tarjeta de prepago (débito).
- Bloqueadores de pantalla (***Screen lockers***).- Este tipo de ransomware bloquea completamente la computadora o sistema, por lo que los archivos y aplicaciones son inaccesibles. Por lo general, exhiben una pantalla de bloqueo donde muestra la demanda de rescate, posiblemente con un reloj de cuenta regresiva para aumentar la urgencia y hacer que las víctimas actúen.
- ***Ransomware as a Service (RaaS)***.- Se refiere al malware alojado de forma anónima por grupos de ciberdelincuentes que se encargan de todos los aspectos del ataque, desde la distribución de ransomware hasta la recogida de pagos y la restauración del acceso, a cambio de una parte del pago final.
- ***Scareware***.- El scareware es una táctica que utiliza ventanas emergentes para convencer a las víctimas de que tienen un virus y les indica que descarguen software falso para solucionar el problema, en general este software es ransomware u otro tipo de malware.

Figura 1.1: Mensaje mostrado al usuario afectado por el Ransomware WannaCry. Fuente:[11]

El ransomware se distribuye a través de correos electrónicos de ***phishing***, ataques de ingeniería social o redes de publicidad maliciosa. En la mayoría de los casos, la víctima termina haciendo clic en un enlace malicioso y descarga —muchas veces sin saberlo— la variante del ransomware en su dispositivo. Después de que un dispositivo o sistema ha sido infectado, el ransomware se pone a trabajar inmediatamente para identificar y cifrar los archivos de la víctima —esto depende del tipo de malware—. Una vez que han sido cifrados los datos, se requiere una clave de descifrado para desbloquear los archivos y, para obtener esta clave, la víctima debe seguir las instrucciones dejadas en una nota de rescate que describen cómo pagar al atacante. Los usuarios malintencionados cuentan con que los usuarios se desesperen por recuperar el acceso oportuno a los datos, por lo que estarán dispuestos a desembolsar un considerable rescate por la clave de descifrado necesaria para acceder a los datos.

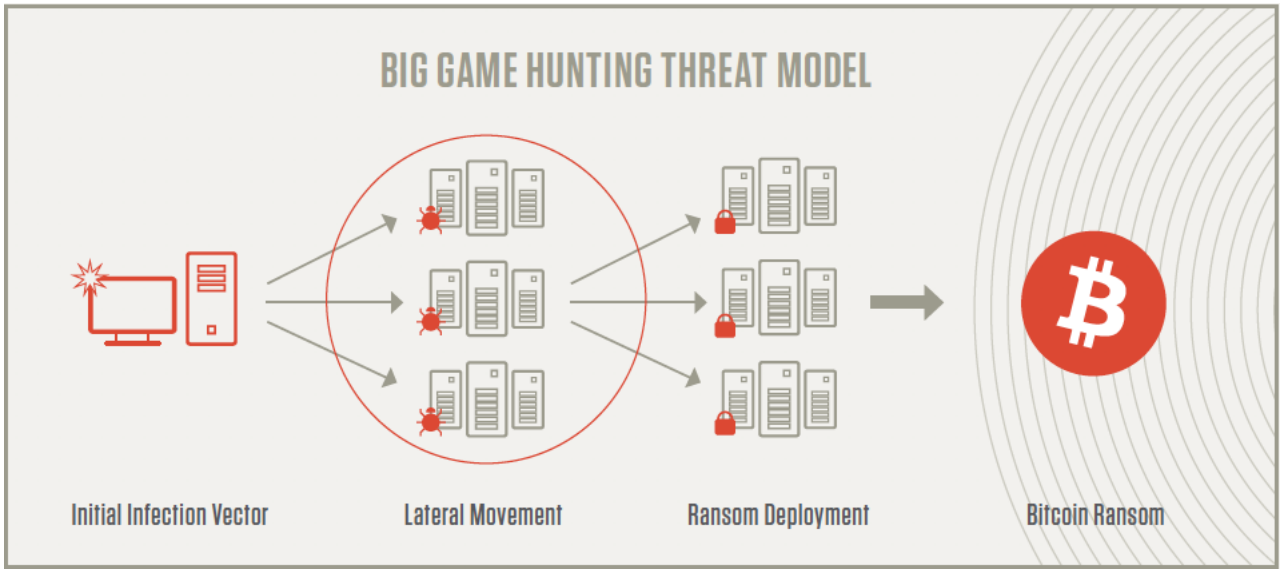


Figura 1.2: Flujo del ataque con Ransomware.
Fuente:[10]

1.2.2. A Quién Afecta el Ransomware.

Todo tipo de organizaciones puede ser blanco de ransomware, aunque suele estar dirigido a los gobiernos estatales y locales, que a menudo son más vulnerables debido a malas prácticas de seguridad, deficientes controles de seguridad y falta de concientización de los empleados. También las pequeñas y medianas empresas (pymes) son el objetivo por varias razones, desde el dinero y la propiedad intelectual, hasta los datos y el acceso de los clientes —de hecho, el acceso puede ser un factor principal porque las pymes se pueden utilizar como vector para atacar una organización o la cadena de suministro de un objetivo más grande—.

Dentro de las organizaciones atacadas mundialmente fuera del ámbito gubernamental, destacan las universidades, ya que a menudo tienen equipos de seguridad más pequeños y una gran base de usuarios comparten muchos archivos, por lo que las defensas se podrían evadir más fácilmente. También están las instituciones médicas porque a menudo necesitan acceso inmediato a datos y las vidas de los pacientes pueden estar en juego, lo que las llevaría a pagar de inmediato. De hecho, ataques que utilizan el ransomware sobre hospitales ya han cobrado vidas humanas alrededor del mundo [8][34]. Por último, es más probable que las instituciones financieras y los bufetes de abogados paguen el rescate debido a la sensibilidad de sus datos, y que lo hagan de manera discreta para evitar situaciones negativas como multas o afectaciones reputacionales.

1.2.3. Defensa Contra el Ransomware

Una vez que el ransomware ha tomado acciones sobre el equipo infectado, es común que resulte demasiado tarde para recuperar los datos o tomar acciones reversivas instantáneas, es por eso que la mejor defensa contra ransomware se basa en la prevención proactiva. Sin embargo, la evolución constante del ransomware ha hecho que la protección sea un desafío para muchas organizaciones, aunque los expertos recomiendan fuertemente seguir las siguientes acciones:

- Capacitar a todos los empleados sobre prácticas de ciberseguridad.- Los empleados son la primera línea de seguridad en las empresas, por ello deben seguir buenas prácticas de seguridad como: el uso de contraseñas robustas, conectarse sólo a redes WiFi seguras y nunca dar clic en enlaces de correos electrónicos no solicitados o maliciosos.

- Mantener los sistemas operativos y demás software actualizado.- Los ciberdelincuentes buscan constantemente vulnerabilidades para explotar, por eso, al tener actualizado correctamente los sistemas, se minimiza la exposición a vulnerabilidades conocidas.

- Implementar y mejorar la seguridad del correo electrónico.- El correo electrónico es una de las fuentes que permiten la esparsión de ransomware con mayor velocidad y sencillez, por eso se deben implementar soluciones de seguridad sobre el correo electrónico que realice el filtrado de ***URL*** y también el ***sandboxing*** de archivos adjuntos. Para optimizar estos esfuerzos, se puede utilizar una capacidad de respuesta automatizada que permita la cuarentena retroactiva de los correos electrónicos entregados antes de que el usuario interactúe con ellos.

- Supervisar continuamente el entorno y la red para detectar actividades maliciosas e indicadores de ataques (IOA, por sus siglas en inglés).- Dentro del alcance organizacional se deben vigilar todos los activos y capturar los eventos para la detección automática de actividades maliciosas no identificadas por métodos de prevención y brindando visibilidad para la búsqueda de amenazas proactiva.

- Integrar la inteligencia sobre amenazas en la estrategia de seguridad.- Es necesario supervisar los sistemas en tiempo real y mantenerse al día con la inteligencia de amenazas más reciente para detectar ataques rápidamente, comprender la mejor manera de responder y evitar que se propague.

- Implementar un programa de protección de identidad sólido.- Las organizaciones pueden mejorar su postura de seguridad, mediante la implementación de un programa de protección de identidades sólido para comprender la higiene del almacenamiento local y en la nube. Deben poder determinar las brechas y analizar el comportamiento y las desviaciones de cada cuenta de los trabajadores (usuarios humanos, cuentas privilegiadas, cuentas de servicio) y aún más deben ser capaces de detectar movimientos laterales e implementar accesos condicionales basados en riesgos para detectar y detener amenazas de ransomware.

La seguridad es un asunto de vital importancia para las organizaciones y es necesario que exista un compromiso de seguridad en las tecnologías informáticas. Esto implica la implementación de diversas normas, políticas y tecnologías de tal manera que, apoyado de las tres líneas de defensa: gestión operativa, cumplimiento y auditoría interna, permitan poner en favor las condiciones atmosféricas a favor de la seguridad informática [28]. Estas condiciones pueden estar presentes de diversas maneras desde la instalación de parches y actualización de antivirus, hasta la conectividad permanente y el monitoreo activo en tiempo real de la infraestructura de la red. Evitar favorecer las condiciones atmosféricas a favor de los ciberdelincuentes es fundamental, ya que sólo estas amenazas logran tener control en ese ambiente y lo aprovechan en su favor.

1.3. MITRE ATT&CK

El MITRE ATT&CK es una base de conocimiento de *tácticas* y *técnicas* basado en observaciones del mundo real sobre los distintos *adversarios* existentes. ATT&CK proporciona una taxonomía tanto para el ataque como para la defensa, y se ha convertido en una herramienta conceptual útil en la ciberseguridad al lograr transmitir inteligencia sobre amenazas y mejorar las defensas de las redes y los sistemas en contra de las intrusiones.

1.3.1. Modelo de ATT&CK

La base de ATT&CK es el conjunto de técnicas y subtécnicas que representan acciones que los adversarios pueden realizar para lograr sus objetivos. Esos objetivos están representados por las categorías tácticas a las que pertenecen las técnicas y sus respectivas subtécnicas [39].

1.3.2. Matriz de ATT&CK

La matriz ATT&CK contiene un conjunto de técnicas utilizadas por los adversarios para lograr un objetivo específico. Esos objetivos se clasifican como tácticas y se presentan linealmente, desde el punto de reconocimiento, hasta el objetivo final de exfiltración o impacto. La matriz está clasificada en las siguientes tácticas:

- Reconocimiento.- Trata sobre la recopilación de información para planificar futuras operaciones del adversario, es decir, información sobre la organización objetivo.
- Desarrollo de recursos.- Permite establecer recursos para apoyar las operaciones, es decir, establecer una infraestructura de comando y control.
- Acceso inicial.- Tiene como meta ingresar a la red de la organización mediante diversas formas.
- Ejecución.- Busca intentar ejecutar código malicioso en los sistemas.
- Persistencia.- Trata de mantener el punto de acceso a un sistema previamente comprometido.
- Escalada de privilegios.- Trata de obtener permisos de un usuario superior.
- Evasión de defensa.- Busca evitar ser detectado una vez dentro de la red.
- Acceso con credenciales.- Autenticación con nombres y contraseñas de usuarios válidos.
- Descubrimiento.- Trata de descubrir el entorno e identificar lo que se puede controlar.
- Movimiento lateral.- Busca moverse a través del entorno para pivotar a través de múltiples sistemas.
- Recopilación.- Busca recopilar los datos de interés para el objetivo del adversario.
- Comando y control.- Intenta establecer comunicación con los sistemas comprometidos para controlarlos.

- Exfiltración: Intenta robar datos de la organización comprometida, generalmente mediante la transferencia de datos a una cuenta en la nube.
- Impacto.- Trata de manipular, interrumpir o destruir los sistemas y datos.

Al hacer referencia a la matriz, los ataques de ransomware por lo general se mueven de izquierda a derecha a lo largo de las tácticas. Es posible que un ataque no aproveche necesariamente todas las tácticas, y no siga un orden estructurado. Por ejemplo, si un equipo se ve comprometido, es probable que ese equipo se utilice para repetir algunas de las mismas tácticas y técnicas una vez que se obtenga acceso a otros adicionales.

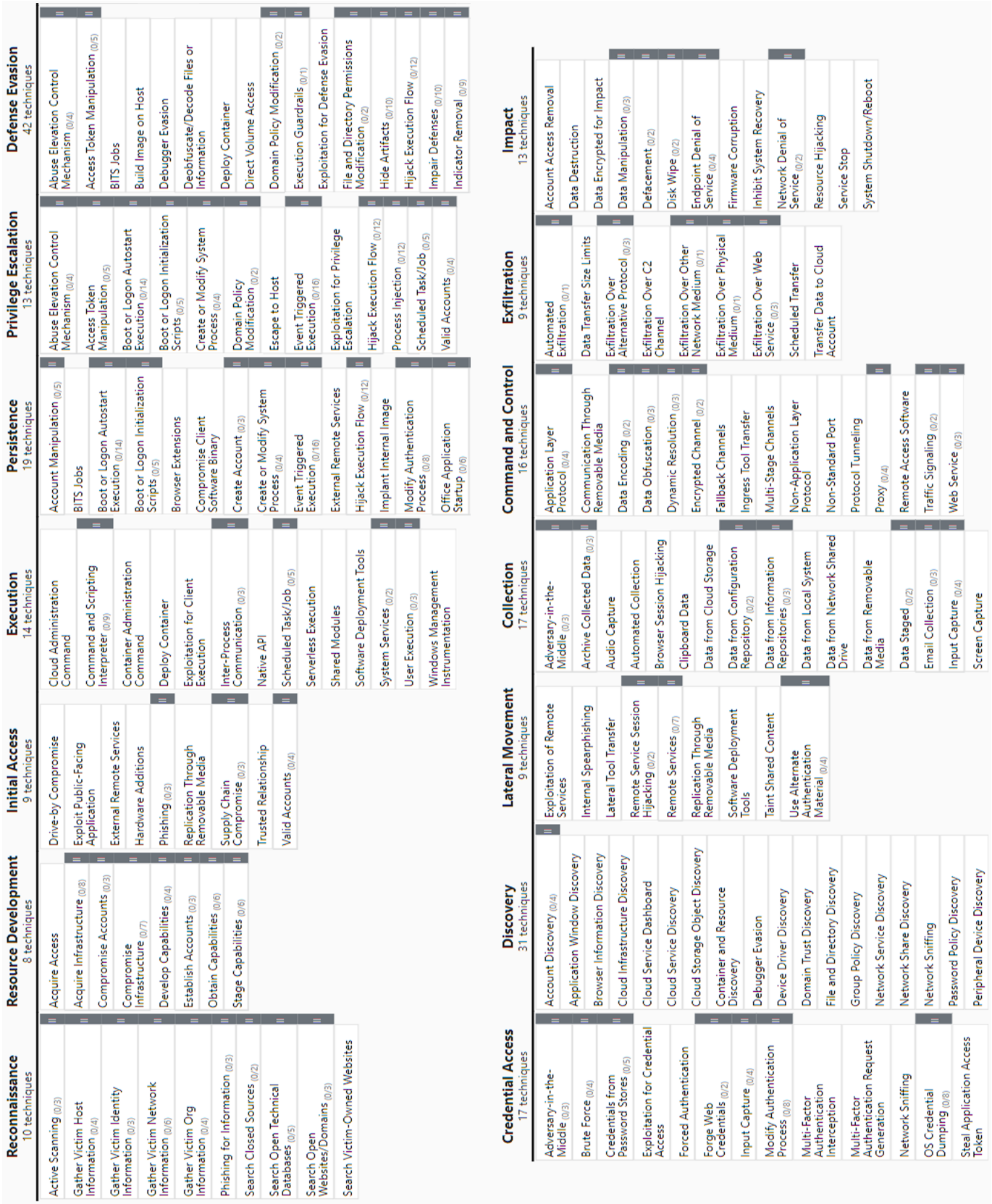


Figura 1.3: Algunas de las técnicas y tácticas presentes en la matriz de Mitre ATT&CK [27].

1.4. Cyber Kill Chain

El marco de seguridad Cyber Kill Chain permite identificar y prevenir las intrusiones informáticas dentro de una organización o sistema. El modelo describe las diversas etapas que los adversarios deben completar para lograr su objetivo y, por tanto, los puntos en los que el equipo de seguridad de las organizaciones pueda prevenir, detectar o interceptar a los adversarios [24].

1.4.1. Fases del Cyber Kill Chain

El marco de seguridad está constituido de siete pasos que mejoran la visibilidad de un ataque y enriquecen la comprensión de una organización ante las tácticas, técnicas y procedimientos de un adversario. Estos siete pasos se describen a continuación:

Fase 1: Reconocimiento.- En esta primera fase los adversarios tratan de identificar un objetivo y explorar vulnerabilidades y debilidades que pueden explotarse dentro de la red. Cuanta más información pueda ser recopilada, más sofisticado y convincente será el ataque y, por lo tanto, mayor será la probabilidad de éxito.

Fase 2: Armamento.- El atacante crea un vector de ataque utilizando diversos tipos de malware. También puede configurar ***backdoors*** para poder continuar accediendo al sistema si los administradores de red identifican y bloquean su punto de entrada original.

Fase 3: Distribución.- El intruso lanza el ataque en contra de la organización. Esta actividad puede combinarse con técnicas de ingeniería social para aumentar la efectividad.

Fase 4: Explotación.- El código malicioso se ejecuta dentro del sistema de la víctima.

Fase 5: Instalación.- Inmediatamente después de la fase de Explotación, el malware u otro vector de ataque se instalará en el sistema de la víctima. Este es un punto de inflexión en el ciclo de vida del ataque, ya que el atacante ha ingresado al sistema y puede asumir el control.

Fase 6: Comando y Control.- El atacante puede utilizar el malware para asumir el control remoto de un dispositivo dentro de la red. En esta etapa, el atacante también puede trabajar para moverse lateralmente por la red, ampliando su acceso y estableciendo más puntos de entrada para el futuro.

Fase 7: Acciones sobre el objetivo.- En esta última etapa, el atacante toma medidas para llevar a cabo sus objetivos previstos, que pueden incluir el robo, la destrucción, el cifrado o la exfiltración de datos.

Figura 1.4: Representación gráfica de la metodología.
Fuente:[23]

Capítulo 2

Marco Teórico

En este capítulo se tratarán los conceptos importantes para el estudio de las redes, primero se iniciará con una breve recapitulación de antecedentes históricos, para así presentar los conceptos básicos y las métricas que se usarán en el análisis del comportamiento del ransomware ante los diversos controles de seguridad.

2.1. Antecedentes Históricos

En el siglo XVlll, Königsberg (hoy llamada Kaliningrado) fue una famosa y rica ciudad de la Prusia Oriental (actualmente Rusia) que se encontraba atravesada por siete puentes. Los ciudadanos se sentían muy orgullosos de los puentes de la ciudad y entre ellos surgió un pequeño juego para entretenerse en los momentos de aburrimiento, los habitantes se preguntaban si era posible hacer un paseo en el que se terminase en el lugar donde se comenzó habiendo pasado sólo una vez por cada puente (ver Figura 2.1).

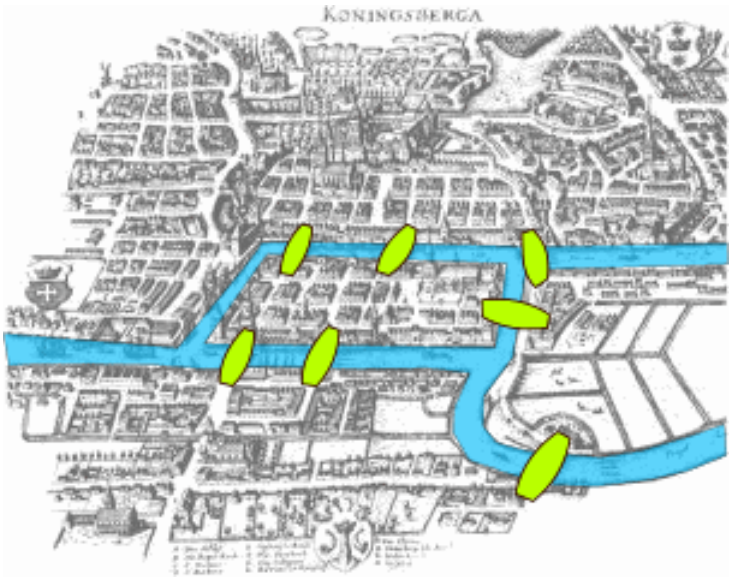


Figura 2.1: Representación de los puentes de Königsberg.

Algunos de los habitantes de Königsberg opinaban que sí era posible, mientras que otros estaban seguros que no, lo cual siguió siendo una incógnita hasta que Leonard Euler publicó la respuesta a esta pregunta [4]. Para resolver el problema, Euler creó una representación abstracta de las islas que componían la ciudad y los puentes al sustituir cada uno de los trozos de tierra firme por un punto y cada puente por una línea. Así, las islas quedaron representadas por cuatro puntos los cuales estaban conectados por siete líneas en total. La figura resultante era una gráfica en donde los distintos territorios de la ciudad se convirtieron en nodos y los puentes en aristas. Esta manera abstracta de visualizar el problema lo llevó a demostrar que tal paseo era imposible de realizar y, de este modo, se inició el estudio de la teoría de gráficas.

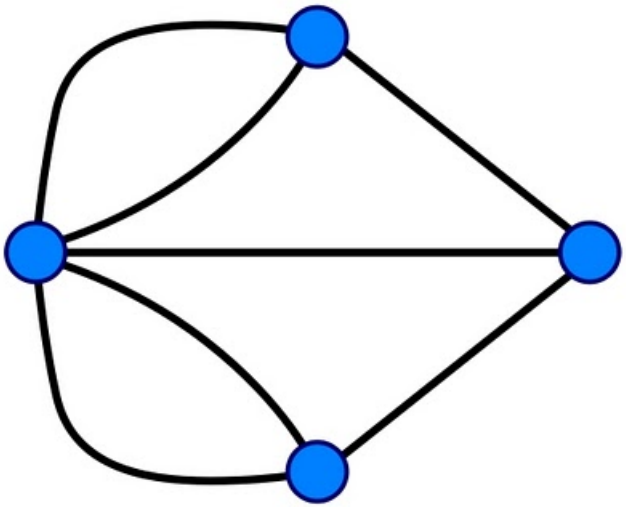


Figura 2.2: Gráfica resultante de modelar los puentes de Königsberg.

Después del trabajo realizado por Euler, diversos estudios ayudaron al desarrollo de la teoría de gráficas. Algunas investigaciones relevantes fueron realizadas por Gustav Kirchhoff (1845) [30], con los circuitos de cálculo de voltaje, y Francis Guthrie (1852) [32], con la coloración de gráficas que buscaba una solución, donde con sólo cuatro colores fuera posible colorear un mapa geográfico de forma que países vecinos no compartieran nunca un mismo color.

Posteriormente, gracias a los estudios de Paul Erdös y Alfréd Rényi en 1959, surgió lo que se denominan las redes aleatorias o también conocidas como *modelo Erdös-Rényi* que ofrecen un modelo simple y poderoso con muchas aplicaciones. En este modelo, un nuevo nodo se enlaza con igual probabilidad con el resto de la red, es decir que un nodo esté conectado a otro depende única y exclusivamente del mismo nodo [13].

Años después, el psicólogo estadounidense Stanley Milgram en 1967, introdujo el concepto del mundo pequeño [26] y la teoría de los seis grados de separación. Milgram, realizó un experimento en el cual varias personas elegidas al azar hicieron llegar cartas a destinatarios desconocidos recurriendo al intermediario más verosímil, que a su vez tendría que recurrir a otro y así sucesivamente hasta que el paquete llegara a su destino, es decir, si la persona conocía al destinatario se la mandaría directamente, caso contrario buscaría entregársela a un intermediario que considerara con la mayor probabilidad de conocerlo, eligiendo únicamente a sus amigos y conocidos. La entrega de cada carta sólo implicó, la colaboración de entre cinco y siete intermediarios.

Duncan Watts y Steven Strogatz en 1998 propusieron un modelo para describir las redes de mundo pequeño en honor al trabajo de Milgram. Estas redes resultaron ser altamente efectivas para la transmisión de información debido a que combinaban un coeficiente de agrupamiento alto y distancias cortas entre cualquier par de nodos. Con esto, mostraron que en las redes de mundo pequeño existen conexiones entre los nodos vecinos y entre cualesquiera dos nodos existe un camino corto [42].

Conforme fue avanzando el estudio de la teoría de redes y el nacimiento de la web, Albert-László Barabási y Réka Albert en 1999, construyeron un mapa de la red en donde para su sorpresa, la web no presentaba una distribución del grado de conectividad usual. En lugar de esto, identificaron que algunos pocos nodos, a los que llamaron *hubs*, estaban mucho más conectados que el resto, lo que significaba que este tipo de redes tenía la peculiaridad de reforzar la centralización en pocos elementos de la red.

En la actualidad la teoría de gráficas es usada en casi todas las áreas de estudio y en la vida diaria de las personas [7]. El gran crecimiento de la web, que excede 1.10 billones de páginas activas e inactivas [17], obliga a que los motores de búsqueda modernos como Google, Yahoo, entre otros vean más allá de solamente el contenido de las páginas para proveer buenos resultados, esto se logra al modelar la web como una red compleja y utilizar múltiples algoritmos. Por ejemplo, los algoritmos PageRank y GoogleBot [20] permiten que sea posible ordenar los resultados de búsqueda para los usuarios al determinar la importancia de una página según el valor de sus páginas padre y así brindar una mejor experiencia, con lo que los sitios con mayores referencias de valor son considerados más relevantes y podrían ser de los primeros en aparecer.

2.2. Conceptos Básicos de Redes

Una *red* G consiste de un conjunto finito no vacío $V = V(G)$ de objetos llamados *nodos* o *vértices* y un conjunto $E = E(G)$ de conexiones entre pares de nodos que reciben el nombre de *aristas*, *arcos* o *enlaces*. Para todo elemento $x \in E$, existen $i, j \in V$ tales que se puede representar al elemento x como $x = (i, j)$ o x_{ij} en donde i es conocido como extremo inicial de x y j es conocido como extremo final de x. Así, una red es un par ordenado de los conjuntos V y E y puede denotarse como $G = (V,E)$.

Las redes pueden ser *dirigidas* o *no dirigidas*, las redes no dirigidas cumplen que para toda $x \in E$ existen $i, j \in V$ tal que $x_{ij} = x_{ji}$, i.e., existe una arista que va del nodo i al nodo j que también permite que el nodo j se comunique con el nodo i. En cambio, las redes dirigidas cumplen que para todo $x \in E$ existen $i, j \in V$ tal que $x_{ij} \neq x_{ji}$, esto implica que existe una arista que permite moverse del nodo i al nodo j, pero no necesariamente existe la arista que permita ir del nodo j al nodo i.

En muchas aplicaciones, cada arista de la red puede tener un número asociado llamado *peso* o también denominado *costo*. El peso puede ser una medida de la longitud de una ruta, la

capacidad de una línea, la energía requerida para moverse entre ubicaciones a lo largo de una ruta, etc. En caso de no tener un valor asociado se considera que la arista tiene peso con valor de uno.

Una red se puede representar geométricamente mediante un dibujo, en el cual los nodos son puntos y las aristas son líneas que conectan a los puntos. Una visualización de redes no dirigidas y dirigidas está presente en la Figura 2.3.

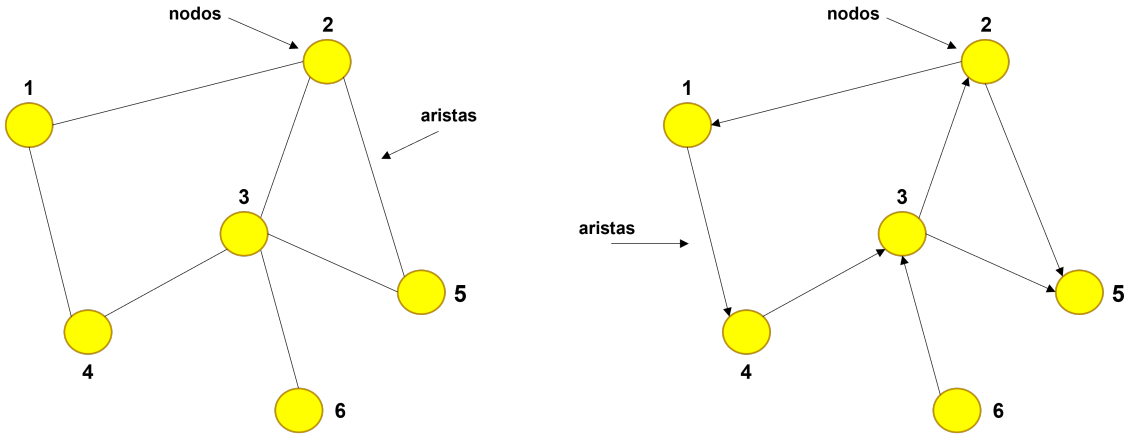


Figura 2.3: Red no dirigida (izquierda) y red dirigida (derecha)

El número de nodos de una red es conocido como *orden* y el número de aristas es el *tamaño*, si una arista x_{ij} relaciona los nodos i y j, estos son *adyacentes* o *vecinos*, caso contrario son independientes. En una red no dirigida, la *vecindad* $N_G(i)$ de un nodo $i \in V$ es el conjunto de todos los vecinos de i, i.e., $\{N_G(i) = j \mid x_{ij} \in E\}$, para una red dirigida $N_G^+(i)$ denota la vecindad de los nodos salientes y $N_G^-(i)$ la vecindad de los nodos entrantes.

La *matriz de adyacencia* A es la forma de representar matemáticamente una red, está constituida por elementos a_{ij} tal que:

$$a_{ij} = \begin{cases} 1, & \text{si existe una arista entre el nodo } i \text{ y el nodo } j \\ 0, & \text{en otro caso.} \end{cases} \tag{2.1}$$

Para reafirmar mejor este concepto, la matriz de adyacencia de la red no dirigida mostrada en la Figura 2.3 es:

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \tag{2.2}$$

Dos puntos a notar sobre la matriz de adyacencia son, que para una red sin nodos con aristas apuntando a ellos mismos como la red del ejemplo, los elementos de la matriz diagonal son todos

cero y, segundo, en una red no dirigida la matriz es simétrica, ya que, si hay una arista entre i y j, también hay una arista entre j e i. Además, si se suman las entradas de un renglón se obtiene el grado de salida, pero si se suman las entradas de una columna resulta el grado de entrada que se definirán a continuación.

El *grado* k_i de un nodo en una red es el número de aristas conectadas a él. Para una red no dirigida de n vértices, el grado se puede escribir en términos de la matriz de adyacencia, $A = a_{ij}$ como se muestra en (2.3). Así, un nodo i tiene mayor grado que un nodo j si $k_i > k_j$,

$$k_i = \sum_{j=1}^{n} a_{ij}. \tag{2.3}$$

En este tipo de redes, el número total de aristas m puede ser expresada como la suma del grado de los nodos, pero como el número de extremos de las aristas también es igual a la suma de los grados de todos los nodos se tiene:

$$m = \sum_{i=1}^{n} \frac{1}{2} k_i = \sum_{j=1}^{n} \frac{1}{2} a_{ij}. \tag{2.4}$$

En donde el factor $\frac{1}{2}$ corrige el hecho de que cada arista es contada dos veces en una red no dirigida. En el caso de las redes dirigidas los nodos poseen grado de entrada y de salida, el grado de entrada (2.5) es el número de aristas entrantes conectadas a un nodo, en cambio el grado de salida (2.6) es el número de aristas salientes:

$$\sum_{i=1}^{n} k_i^{in}. \tag{2.5}$$

$$\sum_{i=1}^{n} k_i^{out}. \tag{2.6}$$

En las redes dirigidas, el número total de aristas m está representado por la fórmula (2.7). El factor $\frac{1}{2}$ visto en (2.4) ahora está ausente, ya que las redes dirigidas cuentan por separado los grados entrantes y salientes.

$$m = \sum_{i=1}^{n} k_i^{in} = \sum_{i=1}^{n} k_i^{out}. \tag{2.7}$$

La *distribución de grado* $P(k)$ describe la probabilidad de que al seleccionar aleatoriamente un nodo de la red, este tenga grado k. Juega un papel fundamental en las redes, ya que permite observar tendencias generales y en función de dichas tendencias, dar una clasificación. Por ejemplo, las redes aleatorias y los modelos de mundo pequeño tienen una distribución de grados homogénea, con un pico en el valor promedio y con un decaimiento exponencial, por lo que siguen una distribución Poisson [6]. Sin embargo, las redes complejas de gran tamaño son libres de escala y sus distribuciones de grado siguen una ley de potencias [6], la cual indica que coexisten componentes de tamaños

bastante diferentes, i.e., existen nodos con muy pocas conexiones y hay unos pocos nodos que tienen muchas, de forma que los nodos no se agrupan alrededor de un valor medio característico.

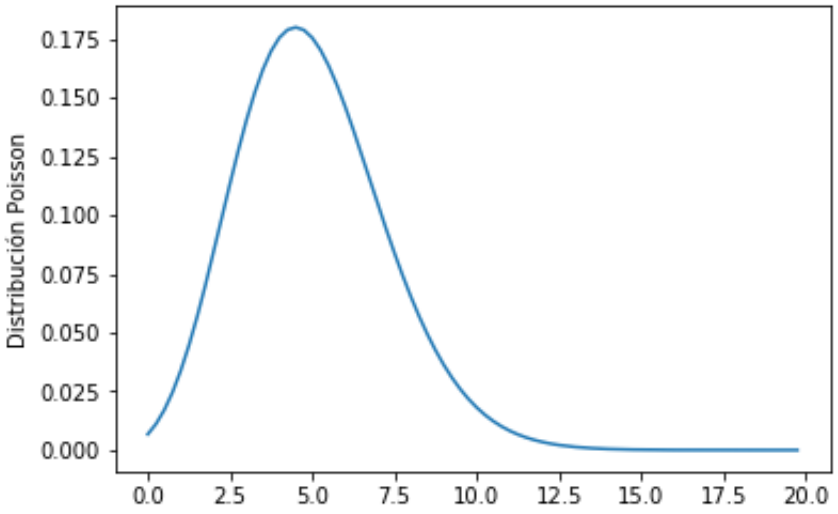


Figura 2.4: Distribución de grado Poisson.

La *ruta más corta*, o *ruta geodésica*, entre dos nodos en una red es una ruta con el número mínimo de aristas, a pesar de que no son necesariamente únicas, la distancia geodésica está bien definida, ya que todas las rutas geodésicas tienen la misma longitud.

2.3. Medidas de Centralidad

Las medidas de centralidad son un concepto fundamental en el análisis de las redes y, dependiendo del contexto, permiten medir la importancia de un nodo dentro de una red. El estudio de estas métricas abre las puertas al análisis, de tal manera que permiten modelar y encontrar respuestas o fenómenos de interés en diversas áreas científicas y sociales.

2.3.1. Centralidad de Grado

La *centralidad de grado* k_i es la métrica más sencilla de estudiar y está formada únicamente del grado de los nodos. En una red no dirigida, la centralidad de grado puede calcularse a partir de la matriz de adyacencia $A = a_{ij}$ de tal manera que:

$$k_i = \sum_{j=1}^{n} a_{ij}. \tag{2.8}$$

2.3.2. Centralidad Intermedia

Que un nodo tenga mayor grado sobre los otros no siempre implica que sea más influyente o tenga mayor relevancia en la comunicación, para medir este aspecto existe la *centralidad intermedia* $BC(i)$, que pondera la importancia de un nodo en la comunicación entre cualquier par de nodos. Asume que la información entre ellos viaja de manera equiprobable y siempre lo hace por el camino más corto. La centralidad intermedia de un nodo i está dada por:

$$BC(i) = \sum_j \sum_k \frac{\rho(j,i,k)}{\rho(j,k)}, i \neq j \neq k, \tag{2.9}$$

donde $\rho(j,k)$ representa el número de rutas geodésicas que conectan al nodo j con el nodo k, mientras $\rho(j,i,k)$ es la cantidad de esas rutas que pasan por i.

2.3.3. Centralidad de Vector Propio

Una extensión natural de la centralidad de grado es la *centralidad de vector propio* x_i, en la cual un nodo recibe una mayor importancia dependiendo de qué tan importante son los nodos con los que está conectado [29]. Así, los nodos con una mayor centralidad de vector propio implican que tienen muchos vecinos o vecinos importantes, para un nodo i la centralidad de vector propio esta dada por:

$$x_i = \kappa_1^{-1} \sum_j a_{ij} x_j, \tag{2.10}$$

donde κ_1 es el mayor de los valores propios de la matriz de adyacencia, para comprender mejor esta centralidad, considere la Figura 2.5 extraída de una de las redes utilizadas en este trabajo:

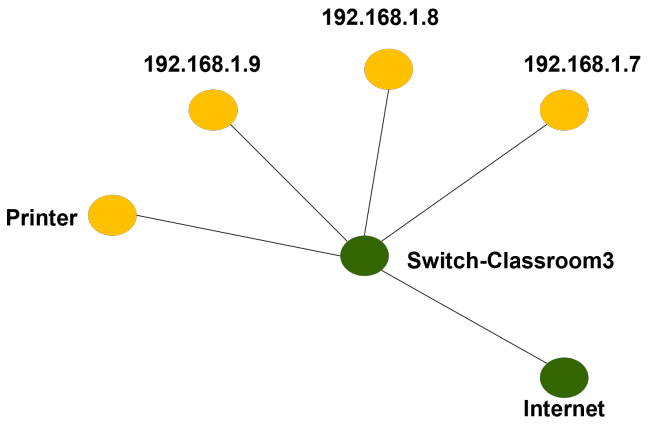


Figura 2.5: Ejemplo para mostrar la métrica de vector propio.

Primero, es necesario construir la matriz de adyacencia A asociada a la red y obtener los valores propios al calcular el determinante.

$$A = \begin{array}{c} \\ P \\ 9 \\ 8 \\ 7 \\ I \\ SW \end{array} \begin{array}{c} \begin{array}{cccccc} P & 9 & 8 & 7 & I & SW \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \end{array} \tag{2.11}$$

Para obtener los valores propios, se plantea el sistema de ecuaciones 2.12 en forma matricial: $(A - \lambda I)C_e = 0$ donde $C_E = [u_1, u_2, u_3, u_4, u_5, u_6]^T$ e I es la matriz identidad.

$$\begin{bmatrix} 0-\lambda & 0 & 0 & 0 & 0 & 1 \\ 0 & 0-\lambda & 0 & 0 & 0 & 1 \\ 0 & 0 & 0-\lambda & 0 & 0 & 1 \\ 0 & 0 & 0 & 0-\lambda & 0 & 1 \\ 0 & 0 & 0 & 0 & 0-\lambda & 1 \\ 1 & 1 & 1 & 1 & 1 & 0-\lambda \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{2.12}$$

Así, el determinante de A está dado por.

$$det(A - \lambda I) = \begin{bmatrix} 0-\lambda & 0 & 0 & 0 & 0 & 1 \\ 0 & 0-\lambda & 0 & 0 & 0 & 1 \\ 0 & 0 & 0-\lambda & 0 & 0 & 1 \\ 0 & 0 & 0 & 0-\lambda & 0 & 1 \\ 0 & 0 & 0 & 0 & 0-\lambda & 1 \\ 1 & 1 & 1 & 1 & 1 & 0-\lambda \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{2.13}$$

Al resolver el sistema de ecuaciones resulta el polinomio $\lambda^6 - 5\lambda^4$, cuyas raíces y valores propios son: $\lambda_1 = -2.2361, \lambda_2 = 2.2361, \lambda_3 = 0, \lambda_4 = 0, \lambda_5 = 0, \lambda_6 = 0$, considerando el valor propio mas grande y sustiyuyendo en las incógnitas de la ecuación 2.12 se obtiene la centralidad de vector propio asociada a los nodos.

$$C_e = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \end{bmatrix} = \begin{bmatrix} 0.4472 \\ 0.4472 \\ 0.4472 \\ 0.4472 \\ 0.4472 \\ 1 \end{bmatrix} \tag{2.14}$$

En donde el nodo “Switch-Classroom3” tiene una centralidad de 1 y los restantes 0.4472, por lo que el primero resulta de mayor relevancia.

2.3.4. PageRank

Gracias a la creación de la web surgen nuevas formas de poder analizar redes, entre las que destaca el algoritmo PageRank $PR(i)$, que resulta ser una extensión de la centralidad de vector propio. Este algoritmo permite medir la importancia de un nodo con base en la importancia de los nodos que apuntan a él. A diferencia de la centralidad de vector propio, PageRank considera el número y la calidad de los enlaces para determinar una estimación aproximada de la importancia del nodo, está enfocado en trabajar con redes dirigidas y puede ser obtenido con la fórmula:

$$PR(i) = 1 - \alpha + \alpha \sum_{i=1}^{n} \frac{PR(i)}{C(i)}, \tag{2.15}$$

donde α es una constante positiva conocido como factor de amortiguamiento, k_j es el grado del j-ésimo nodo e $C(i)$ es el número de enlaces salientes del nodo i.

Para comprender mejor esta métrica considere el extracto de red mostrado en la Figura 2.5, como PageRank esta enfocada en trabajar con redes dirigidas, primero se le asigna dirección a la red, al intercambiar la arista sin dirección por dos aristas dirigidas que van en direcciones opuestas, de tal manera que van a existir las aristas $x_{i,j}$ y $x_{j,i}$ para todo par de nodos $i, j \in E$.

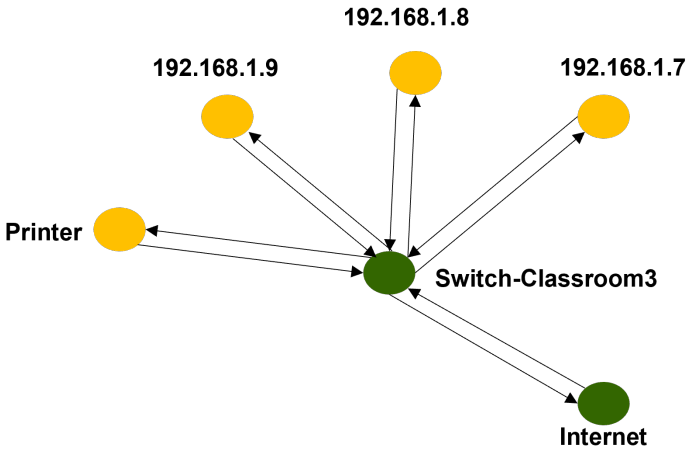


Figura 2.6: Red dirigida

Inicialmente, el PageRank de todos los nodos se considera como 1 y el peso de la arista es la probabilidad de ir del nodo i al nodo j de manera equiprobable. Por ejemplo, el nodo Switch-Classroom3 tiene cinco enlaces de salida, por lo tanto, la probabilidad de visitar cada nodo es $\frac{1}{5}$. Después de expresar en términos de probabilidades el peso de las aristas y asignar dirección, la nueva red es visible en la Figura 2.7:

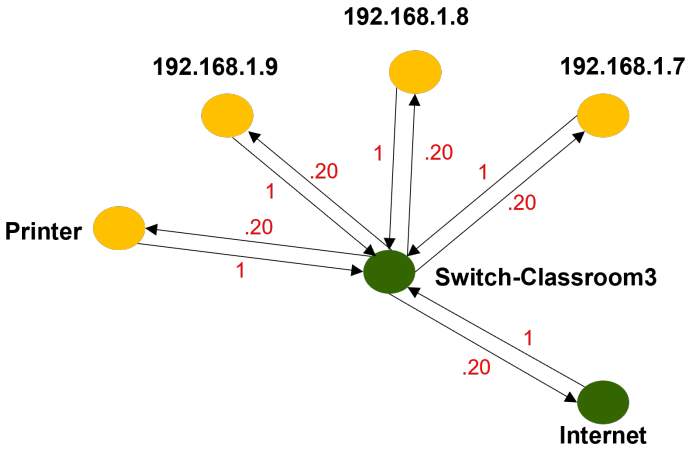


Figura 2.7: Red con probabilidades en las aristas

El PageRank de cada nodo se determina aplicando la ecuación 2.15. Este proceso se repite hasta que el algoritmo converge, es decir, los valores del ranking del nodo no cambian más allá de un valor pequeño (conocido como épsilon, por lo general fijo como $1e^{-4}$). El factor de amortiguamiento α se introduce para agregar algo de aleatoriedad sobre la red, es decir, α es la probabilidad de que un paquete se mueva al nodo vinculado y $1-\alpha$ es la probabilidad de elegir un nodo aleatorio, generalmente se considera como 0.85. Para la primer iteración quedaría:

$$
\begin{aligned}
PR_1(192.168.1.7) &= 0.15 + 0.85 * (1 * \frac{1}{5}) \\
PR_1(192.168.1.8) &= 0.15 + 0.85 * (1 * \frac{1}{5}) \\
PR_1(192.168.1.9) &= 0.15 + 0.85 * (1 * \frac{1}{5}) \\
PR_!(Printer) &= 0.15 + 0.85 * (1 * \frac{1}{5}) \\
PR_1(Switch - Classroom3) &= 0.15 + 0.85 * (1 * \frac{1}{1} + 1 * \frac{1}{1} + 1 * \frac{1}{1} + 1 * \frac{1}{1} + 1 * \frac{1}{1}) \\
PR_1(Internet) &= 0.15 + 0.85 * (1 * \frac{1}{5})
\end{aligned}
$$

De tal manera que el nuevo PageRank para todos los nodos, a excepción del Switch- Classroom3, es de 0.32, mientras que para este último es de 4.40. Con estos nuevos valores se realiza la segunda iteración (PR_2)y se continua sucesivamente hasta 9que se cumple la condición $PR_{n+1} - PR_n < 1e^{-4}$. De esta manera el PageRank obtenido para cada nodo en la red es:

$$
\begin{aligned}
PR_1(Switch - Classroom3) &= 0.474 \\
PR_1(192.168.1.7) &= 0.105 \\
PR_1(192.168.1.8) &= 0.105 \\
PR_1(192.168.1.9) &= 0.105 \\
PR_1(Internet) &= 0.105 \\
PR_1(Printer) &= 0.105
\end{aligned}
\tag{2.16}
$$

Por lo que el nodo Switch-Classroom3 es el de mayor relevancia. Aún más, al comparar los resultados obtenidos en 2.14 y 2.16, se obtienen resultados similares, aunque la interpretación es distinta.

2.4. Conceptos Básicos de Algoritmos

En general, no existe una definición formal de algoritmo, aunque muchos autores lo definen como una lista de instrucciones para resolver un problema. Una definición más formal está descrita por Sedgewick y Wayne [36], en donde señalan que un algoritmo se utiliza para describir un método finito, determinista y eficaz para resolver un problema en lenguaje natural, o mediante un programa de computadora que implemente el procedimiento.

Al programar y desarrollar un algoritmo, surge el concepto de costo computacional, el cual mide la cantidad de recursos necesarios para ejecutar un algoritmo y se basa en el tiempo de ejecución y la cantidad de memoria. El tiempo de ejecución, es la suma del número de operaciones elementales que se ejecuta por cada instrucción dada en el algoritmo, mientras que la cantidad de memoria depende de la longitud del código y las estructuras de datos, que son formas de organizar y almacenar datos en la memoria de una computadora [31]. Las principales estructuras de datos son:

- Arreglos (Arrays).- Almacena elementos del mismo tipo en una secuencia contigua de memoria. Se accede a los elementos mediante un índice, y el costo computacional para acceder a un elemento específico es constante $O(1)$. La inserción y eliminación de elementos en el medio del arreglo tienen un costo lineal $O(n)$, ya que requiere reorganizar los elementos.
- Listas enlazadas (Linked Lists).- Los elementos están enlazados mediante punteros. Cada elemento, llamado nodo, contiene un valor y un puntero al siguiente nodo. El acceso a un elemento en una lista enlazada tiene un costo lineal $O(n)$, ya que se debe recorrer la lista desde el principio. La inserción y eliminación de elementos en cualquier posición tiene un costo constante $O(1)$ si se mantiene un puntero al nodo anterior.
- Pilas (Stacks).- Una pila sigue el principio ***LIFO*** (Last In, First Out). Los elementos se agregan y se eliminan sólo en la parte superior de la pila. Las operaciones de inserción y eliminación tienen un costo constante $O(1)$, ya que sólo se manipulan los elementos en la parte superior.
- Colas (Queues).- Una cola sigue el principio ***FIFO*** (First In, First Out). Los elementos se agregan al final de la cola y se eliminan desde el frente. Las operaciones de inserción y eliminación tienen un costo constante $O(1)$, ya que sólo se manipulan los elementos en los extremos.
- Árboles (Trees).- Los árboles son estructuras de datos no lineales y tienen una estructura jerárquica. El costo computacional de las operaciones en árboles depende del tipo específico de árbol y la operación en cuestión.

La complejidad O de un algoritmo, esta determinada por la cantidad de recursos computacionales que requiere para resolver un problema, a medida que el tamaño de los datos de entrada

aumenta. Los órdenes de complejidad más comunes en la solución de un problema están en la Tabla 2.1.

Tabla 2.1: Clases de complejidad.

Notación O	Categoría
$O(1)$	Constante
$O(log(n))$	Logarítmica
$O(n)$	Lineal
$O(n^2)$	Cuadrática
$O(2^n)$	Exponencial

El primer paso para representar una red en una computadora es etiquetando los nodos para que cada uno pueda ser identificado de manera única. La forma más sencilla de realizar esta actividad es asignando a cada uno de los nodos en la red una etiqueta numérica de enteros consecutivos, aunque depende del enfoque que se busque dar, por ejemplo, los nodos en una red social pueden tener nombres, en caso de modelar el Internet podrían ser ***direcciones IP*** o ***números AS***. Todas estas notaciones y valores son almacenados directamente en la memoria de la computadora.

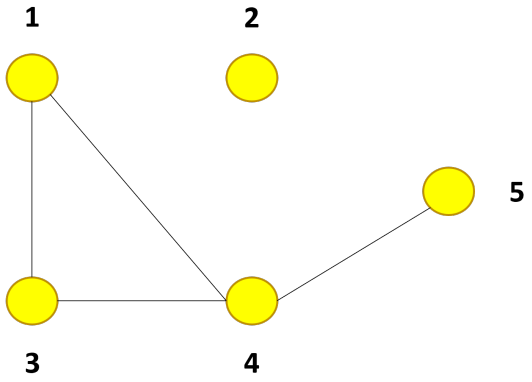
Como se mencionó previamente, la matriz de adyacencia es la forma de representar una red, aunque computacionalmente no es lo óptimo, pues el costo computacional O se eleva demasiado y no es viable para trabajar con redes con un número alto de nodos. Para poder trabajar este tipo de redes se hace uso de las listas de adyacencia, las cuales constan de un conjunto de listas, una para cada nodo, y cada una contiene las etiquetas de los otros nodos a los que está conectado por una arista.

La Tabla 2.2 ilustra el costo computacional de cuatro operaciones para varias representaciones de una red de n nodos y m aristas. Las operaciones están compuestas por agregar un nodo a la red (insertar), eliminar un nodo de la red (eliminar), probar si un par dado de nodos están conectados por una arista (encontrar), y enumerar los vecinos de un nodo dado (enumerar).

Tabla 2.2: Comparativa del costo computacional entre la matriz y lista de adyacencias.

Operación	Matriz de adyacencia	Lista de adyacencias
Insertar	$O(1)$	$O(1)$
Eliminar	$O(1)$	$O(m/n)$
Encontrar	$O(1)$	$O(m/n)$
Enumerar	$O(n)$	$O(m/n)$

Para entender mejor este concepto, considere la red y su respectiva lista de adyacencia en la Figura 2.8 .



(a) red de ejemplo

Nodo	Vecino(s)
1	3,4
2	
3	1,4
4	1,3,5
5	4

(b) lista de adyacencia

Figura 2.8: Lista de adyacencia (lado derecho) asociada a la red de ejemplo (lado izquierdo).

El ejemplo de la Figura 2.8 muestra cómo la lista de adyacencias brinda una mayor flexibilidad al trabajar con redes. Al modelar una red no dirigida, cada nodo aparece dos veces en las listas, por ejemplo, la existencia de la arista entre los nodos 1 y 3, significa que el nodo 3 está en la lista nodo 1 como vecino y el nodo 1 también aparece como vecino del nodo 3, entonces para representar m vértices es necesario únicamente almacenar $2m$ enteros que es mucho mejor que los n^2 enteros utilizados para almacenar la matriz de adyacencia.

Otra representación bastante simple de una red, aunque es menos utilizada, es la lista de aristas, que es una lista de las etiquetas de pares de nodos que están conectados por aristas. Por ejemplo, en la red de la Figura 2.8 la representación de la lista sería (1,3), (4,1), (4,3), (4,5), cabe destacar que, por ser una red no dirigida, el orden de las aristas no suele importar, ni el orden de los nodos en cada par de nodos. El principal problema de esta representación surge al no permitir determinar rápidamente si un determinado nodo existe, ya que sería necesario revisar toda la lista para responder esa pregunta.

2.4.1. Algoritmos Graph Trasversal

La idea detrás de los algoritmos *Graph Trasversal*, es marcar cada nodo cuando se visita por primera vez y hacer un seguimiento de lo que aún no se explora. Estos dictaminan cómo recorrer los nodos en una red y ayudan a determinar el orden de visita [37]. La ventaja de este tipo de algoritmos es que encuentran todas las aristas que se emplean en el proceso de búsqueda sin generar ciclos, i.e., evitan que el primer y último nodo sean el mismo al utilizar una estructura de datos y gestionar los nodos visitados, así los nodos se clasifican en dos categorías: visitado y no visitado.

El algoritmo más utilizado, es el denominado algoritmo de búsqueda en amplitud (BFS, por sus siglas en inglés), el cual comienza en un nodo de origen y, capa por capa a través de la red, analiza los nodos directamente relacionados con el nodo de origen [31]. De acuerdo con el BFS, se debe atravesar la red en una dirección transversal con movimientos horizontales hasta visitar todos los nodos de la capa actual y continuar con la siguiente hasta finalizar.

El algoritmo BFS se resume en los siguientes pasos (Algoritmo 1):

Algoritmo 1 Recorrido de red utilizando BFS

Require: $G = (V, E)$, red con nodos V y aristas E
Ensure: Matriz de visitas M

```
Inicializar matriz de visitas M de tamaño |V| × |V| con todos los elementos a falso
Inicializar cola Q
Seleccionar un nodo inicial i_1
Agregar i_1 a la cola Q
mientras la cola Q no está vacía hacer
    n ← eliminar el primer elemento de la cola Q
    Marcar n como visitado en la matriz M
    para cada nodo adyacente m de n hacer
        si m no ha sido visitado entonces
            Agregar m a la cola Q
        end si
    end para
end mientras
```

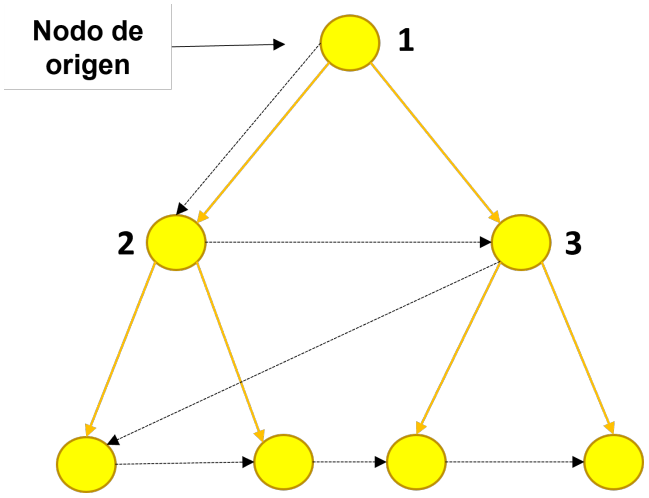


Figura 2.9: Ejemplo del algoritmo BFS, las flechas en color negro indican el recorrido por capas y en color amarillo, los nodos que puede alcanzar el nodo inicial.

De tal manera, el algoritmo BFS visita todos los nodos y aristas de la red y tiene un costo computacional de $O(V + E)$, donde V es el número de nodos y E es el número de aristas.

Capítulo 3

Metodología y Representación de Datos

En este capítulo se describe la metodología empleada en la investigación, los retos, pasos y suposiciones hechas para modelar las redes y el origen de las arquitecturas modeladas. De igual manera se menciona el lenguaje de programación y librerías utilizadas para desarrollar el proyecto.

3.1. Obtención de Datos

Para lograr una modelación realista, las redes modeladas tendrían distintas características y diversas prácticas de seguridad implementadas. La primera red se obtuvo del módulo 4.4.1.2 del curso CCNA Routing and Switching de Cisco, en el cual explicaban las características de una red lógica y física, esta red no contaría con ningún control de seguridad activo [2]. La segunda red se obtuvo de un diagrama de mejores prácticas, especialmente diseñado para proteger las redes de pequeñas empresas y agencias gubernamentales [19], por lo que ya contaba con un gran número de controles de seguridad establecidos. Por último, la tercera red se modeló a partir de la arquitectura de red de una empresa y para evitar difundir información se modificaron nombres de equipos y segmentos de red. El número de nodos y aristas utilizados para modelar cada red, están reflejados en la Tabla 3.1:

Tabla 3.1: Tamaño de las redes utilizadas.

Red	Nodos	Aristas
Red 1	100	99
Red 2	28	27
Red 3	35	34

La implementación de las nuevas tecnologías en la red se basó en las tres clasificaciones de los controles de seguridad de acuerdo al CISSP, agrupándolas con base en sus funciones: disuasivos y preventivos, detectivos y compensatorios, así como correctivos y de recuperación. Bajo estas agrupaciones, únicamente se consideraron en cuenta las tecnologías características de cada una:

- Firewall
- Firewall-NG*

- SIEM
- Antivirus
- Antivirus-NG*
- NIDS
- SOC

*Las tecnologías Next Generation cuentan con funcionalidades de sistemas IDS e IPS, por lo que no fueron tomadas en cuenta estas últimas.

Con las agrupaciones generadas previamente, se obtuvo un promedio ponderado que fungiría como indicador para determinar si un nodo se infectaría o no. En la Tabla 3.2 se encuentran los valores asignados.

Tabla 3.2: Valores asignados sobre las categorías de los controles de seguridad para calcular el promedio ponderado.

Controles de seguridad	Valor
Disuasivos y preventivos	1.4
Detectivos y compensatorios	1.1
Correctivos y de recuperación	0.50

3.2. Modelación de la Red

Al modelar las redes de estudio se asignaron características a los nodos para que cada uno de estos representara un equipo tecnológico (computadoras, servidores, hub, switch, entre otros) y las aristas fueran la conexión existente entre los equipos. La Tabla 3.3 resume las características en cuestión.

Tabla 3.3: Características asignadas a los nodos

Característica	**Descripción**
Nombre	Es la etiqueta asignada al nodo para identificar qué componente de la red es.
Grupo General	Representa las distintas áreas de una empresa sobre las cuales puede tener segmentada su red.
Grupos particulares	Representa al grupo de ***hardware*** al que pertenece el equipo.
Hardware	Especifica el tipo de sistema informático
Estado	Da a conocer si el equipo está infectado o no.
Susceptible	Permite saber si un nodo puede ser infectado o no.
Defensa	Establece el tipo de control de seguridad con el que puede contar un equipo.

Debido a que es posible encontrar distintos tipo de redes en la vida real, se utilizaron los siguientes criterios para modelar las redes de estudio:

- Las redes modeladas fueron planas.- Esto implicaba que existiría una libre comunicación para cada par de nodos en la red. Cabe mencionar que la adaptación del trabajo a la vida real

se ve beneficiada con esta condición, pues muchas pymes, al no contar con un presupuesto alto, tampoco pueden optar por las mejores arquitecturas de seguridad y mejores prácticas dentro de la organización.

- Existirían grupos que simulaban las áreas operativas de una organización.- Cada grupo contaría con un control de seguridad para los equipos que formaban parte de este y, además, cada equipo en lo individual tendría su propio control.
- Limitantes en los equipos afectados.- Se estableció que sólo una parte de los equipos serían vulnerables, pues el ransomware WannaCry únicamente aprovecharía una vulnerabilidad en particular para infectar un sistema.
- Consideraciones de las aristas.- En una red computacional la comunicación es bilateral, lo que permite una libre comunicación en ambas direcciones. Por tanto, las aristas en la red no tendrían peso ni dirección.
- Implementación de controles en la red.- Para estudiar cómo los controles de seguridad bien implementados ayudarían a reducir el impacto del ransomware, se crearon diversas redes a partir de la original, con la diferencia de que las nuevas versiones contarían con distintas soluciones de seguridad.
- Colores en la red.- Para distinguir el estado del nodo en la red se asignaron tres colores distintos: el color verde indicaba que el equipo no era vulnerable, el amarillo que era susceptible y el rojo que estaba infectado.

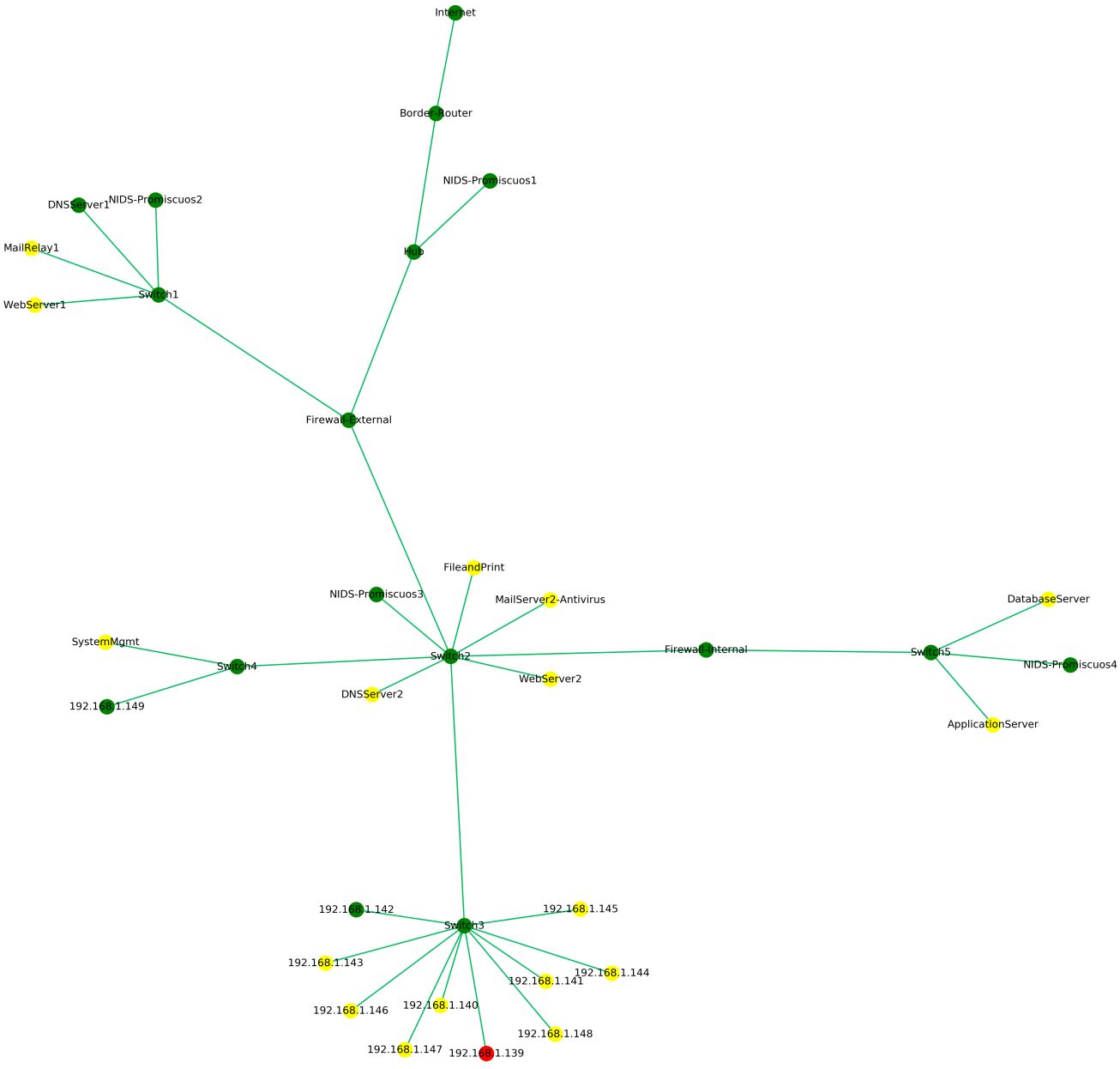


Figura 3.1: Modelación de la Red 2 en donde los nodos verdes corresponden a equipos que no son vulnerables y por ende están seguros; los nodos amarillos son equipos susceptibles y el nodo rojo es el nodo infectado inicial.

3.2.1. Modelado del Ransomware

La modelación del método de dispersión del malware en la red estuvo basada en el comportamiento del ransomware WannaCry, que tuvo un gran impacto en los sistemas operativos Windows. Para iniciar el modelado fue necesario tener una red con las características descritas en la sección anterior. Desde el nodo infectado inicial, se hizo uso del algoritmo BFS para enlistar aquellos nodos

con los que podría comunicarse. Sobre estos se verificaba si eran susceptibles, en caso de ser así se tomaba en cuenta un promedio ponderado considerando tres aspectos:

1. El equipo analizado contaba con algún control preventivo, por ejemplo, antivirus.
2. El grupo o segmento donde se encontraba el equipo tenía algún control de seguridad.
3. El número y tipo de controles de seguridad por los que pasaría un nodo infectado, para intentar infectar a otro en la red.

La finalidad del promedio ponderado sería trabajar con las funciones de seguridad establecidas por el NIST, de tal manera que los controles detectivos y compensatorios junto con los controles disuasivos y preventivos tuvieran un mayor peso en la prevención del esparcimiento del ransomware.

Con el promedio ponderado se definiría si un nodo susceptible se infectaría o no, en caso de ser así, ese nodo se agregaría a una lista de nodos con el mismo estado, los cuales posteriormente servirían como nuevos focos de infección. En este proceso existía una variable que simulaba ser el tiempo de detección en el que una organización lograría detener el ransomware. La idea detrás del algoritmo modelado y el diagrama de flujo se encuentran a continuación (Algoritmo 2 y Figura 3.2):

Algoritmo 2 Simulación de propagación de infección en una red

Require: Red G con nodos clasificados como no vulnerables, susceptibles e infectados
Ensure: Lista I de nodos infectados, tiempo de infección T

```
Inicializar lista I con el nodo infectado inicial x_i0 y variable de tiempo T a 0
mientras T < t y existan nodos susceptibles en G hacer
    Obtener lista V de nodos alcanzables desde el nodo infectado x_i utilizando BFS
    para cada nodo v_i en V hacer
        si v_i es susceptible entonces
            Calcular probabilidad p de que v_i sea infectado
            si p > valor dado entonces
                Agregar v_i a la lista I y cambiar su estado a infectado
            end si
        end si
    end para
    Incrementar T en una unidad
end mientras
Mostrar al usuario los nodos infectados en la lista I y el tiempo de infección T
```

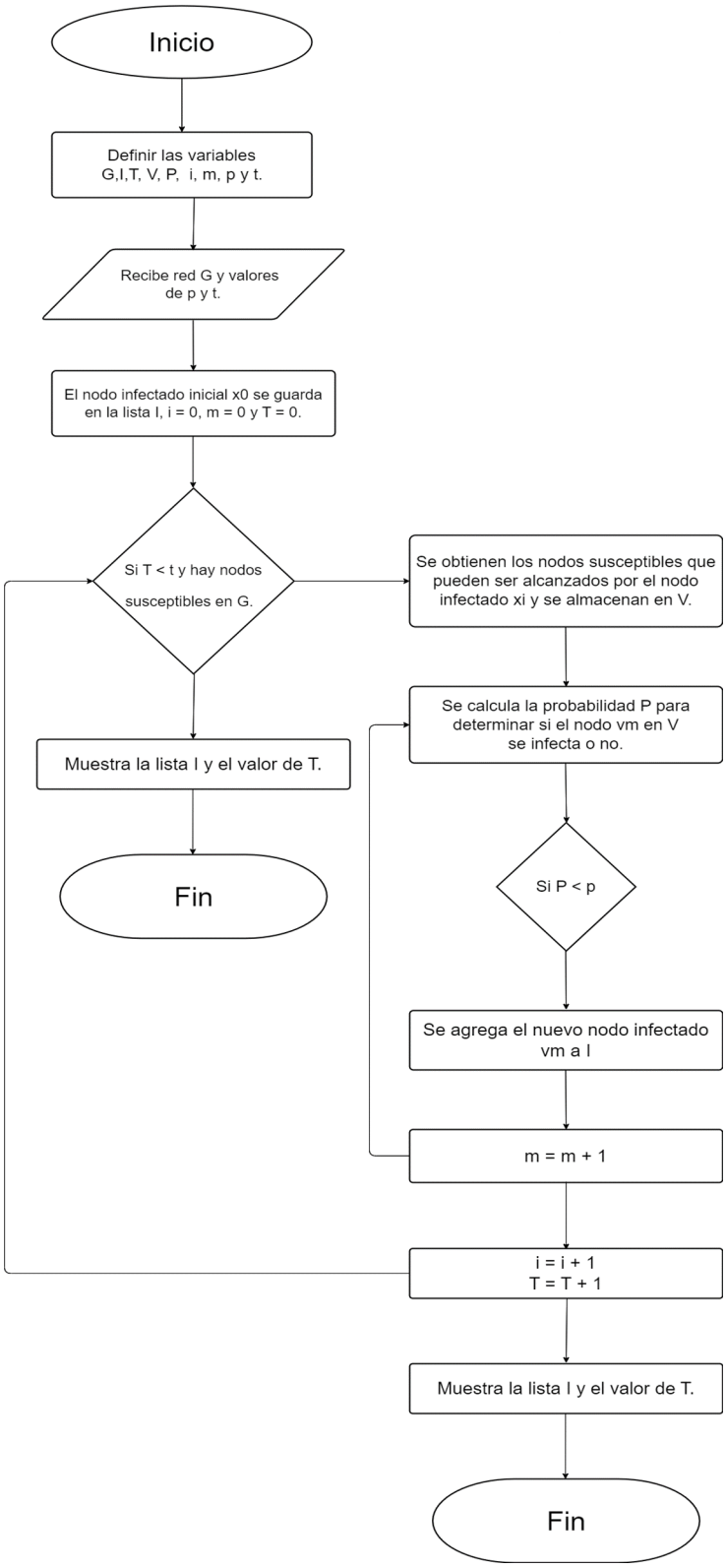


Figura 3.2: Diagrama de flujo del código desarrollado.

El modelo creado simulaba las mismas tácticas, técnicas y procedimientos que el ransomware WannaCry, de tal manera la matriz del Mitre asociada al modelo puede ser vista en la Figura 3.3:

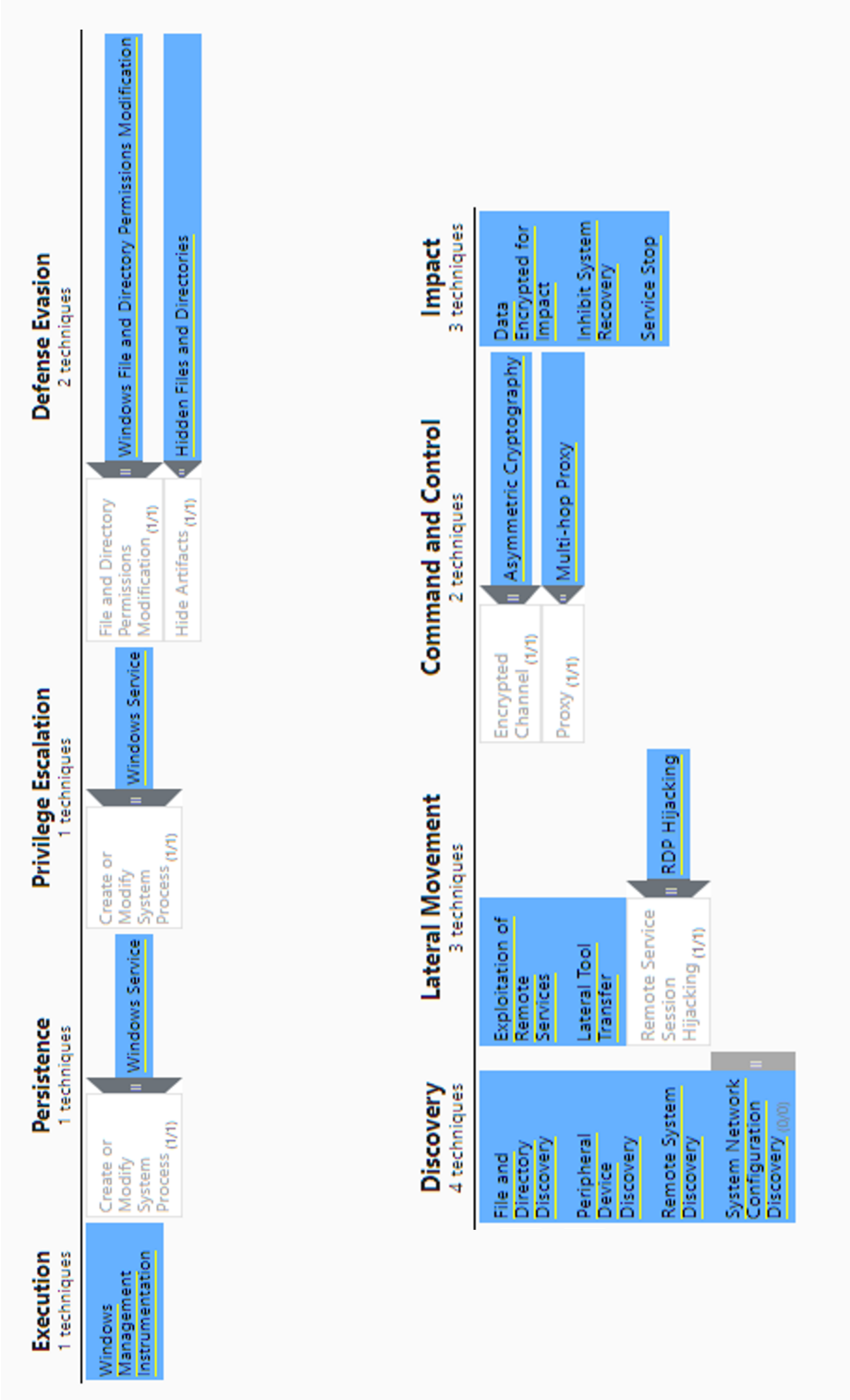


Figura 3.3: Matriz Mitre ATT&CK asociada a WannaCry para Windows.

Por su parte, al considerar los pasos establecidos en la metodología Cyber Kill Chain, el ransomware únicamente tendría un enfoque sobre cuestiones tecnológicas i.e., partiría de la etapa de explotación (ver Figura 3.4).

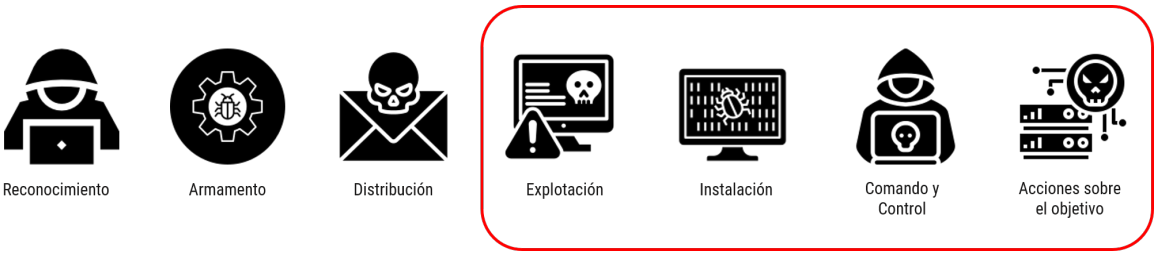


Figura 3.4: Fases del Cyber Kill Chain utilizadas para la modelación del ransomware.

3.3. Software Utilizado

La creación de las gráficas y el cómputo de las centralidades fueron hechas con el lenguaje de programación *Python* versión 3.7.3 mediante la paquetería especializada en el trabajo con redes *networkx*. Esta paquetería permitió realizar el análisis de la red con el fin de obtener los mejores resultados. Adicionalmente, para complementar el cómputo de las centralidades y la cuestión de visualización de las gráficas se hizo uso de las paqueterías *numpy* y *matplotlib*, respectivamente.

Capítulo 4

Análisis de Resultados

En este capítulo, se realiza un análisis exhaustivo del comportamiento del ransomware en una red, mediante la aplicación de métricas de centralidad de vector propio y el algoritmo PageRank para la implementación estratégica de controles de seguridad. Asimismo, se efectúa una comparativa detallada entre los resultados obtenidos y su potencial aplicación en la mejora de la seguridad en redes de las organizaciones.

4.1. Visualización

En las redes informáticas destaca la presencia constante de flujos de información que circulan entre los diversos sistemas conectados. En particular, las redes planas, que son utilizadas en este trabajo, permiten una comunicación fluida entre todos los sistemas, esta característica, sumada a la representación topológica intrínseca de las redes, permite emplear modelos de redes conexas y no dirigidas para ilustrar la propagación del ransomware. Cuando un nodo en una red se ve comprometido por el ransomware, el diseño topológico desempeña un papel crítico en la propagación del malware [38]. Este aspecto cobra importancia al permitir que los controles de seguridad establecidos operen y supervisen eficazmente las diversas anomalías.

Para el proyecto se generan nuevos modelos de redes a partir de las configuraciones originales. Estos nuevos modelos presentan características distintivas que permiten observar de manera precisa el impacto del ransomware al implementar medidas de seguridad en la red. Una característica esencial de estas redes es la adopción de una estructura jerárquica que incluye subredes interconectadas mediante múltiples ***routers***, que se identifican con el nombre *Ethernet*. Otras características clave de estos nuevos modelos junto a su identificador son:

- UAV.- Se parte de la red original con la diferencia de que los sistemas cuentan con soluciones antivirus implementadas en equipos de usuarios y servidores. Además, se consideran los controles de seguridad ya existentes en la red.
- FWEV y FWPR.- Se elimina la presencia del antivirus, a menos que esté presente en los sistemas originalmente. En esta situación, se implementan controles de seguridad disuasivos y detectivos. La colocación estratégica de estos controles se basa en la centralidad de vector propio y el algoritmo PageRank, respectivamente.

- AVFWEV y AVFWPR.- Se introduce el antivirus en todos los sistemas y se implementan controles de seguridad disuasivos y preventivos. La ubicación de estos controles se basa en la centralidad de vector propio y el algoritmo PageRank, respectivamente.
- AVSOCYFWEV y AVSOCYFWPR.- En estas últimas redes se consideran todos los tipos de controles de seguridad, así como la presencia de un SOC y antivirus en todos los equipos. La ubicación de los controles se rige por la centralidad de vector propio y el algoritmo PageRank, respectivamente.

Es relevante enfatizar que los controles de seguridad implementados en las redes se dividen en dos categorías distintas: Next Generation y Tradicionales. Para fines de las simulaciones, se aborda una única categoría en cada caso. Una observación importante es que sólo se incorpora el Centro de Operaciones de Seguridad (SOC) en un escenario, ya que las empresas que cuentan con esta infraestructura suelen disponer de un mayor presupuesto para la ciberseguridad. Además, la presencia del SOC puede indicar un nivel más avanzado en el desarrollo de la cultura de ciberseguridad.

Cada una de las redes modeladas contempla dos escenarios distintos. El primero aborda condiciones atmosféricas favorables a los ciberdelincuentes, donde la probabilidad de infección de sistemas vulnerables por parte del ransomware es mayor. En contraste, el segundo escenario considera condiciones atmosféricas que favorecen la seguridad informática, reduciendo la probabilidad de que el ransomware afecte a un sistema.

Para establecer los nuevos nodos en la red que representen los controles de seguridad, es necesario definir condiciones que dictaminen si es necesario un nuevo nodo o que ayuden a encontrar la mejor ubicación posible, enseguida se enumeran estas:

(I) Si todos los nodos adyacentes al nodo en cuestión ya son controles de seguridad, no es necesario introducir un nuevo nodo de seguridad. Esto garantiza una distribución equilibrada de los controles y evita redundancias innecesarias.

(II) Cuando sólo un nodo adyacente al nodo analizado es un control de seguridad, se procede a implementar un nuevo nodo entre los vecinos restantes, con la excepción de que los nodos sean equipos de usuarios y el nodo en cuestión sea un switch. Esta medida optimiza la cobertura y asegura que no se descuiden áreas vulnerables.

(III) En situaciones en las que los nodos adyacentes permitan la colocación de nuevos controles de seguridad, se da prioridad a los nodos que funcionan como componentes tecnológicos para la retransmisión de paquetes en la red. Es crucial destacar que esta preferencia favorece a nodos como routers o switches en comparación con dispositivos individuales como PCs, debido a su mayor capacidad y función en la infraestructura de red.

(IV) No puede haber nodos adyacentes en los que ambos sean controles de seguridad. Esta restricción evita la redundancia en el despliegue de controles y garantiza una distribución más eficiente de la seguridad en la red.

4.2. Análisis y Resultados

Con una comprensión más sólida de las redes modeladas, la metodología subyacente y los conceptos involucrados, es momento de abordar un análisis más riguroso de los resultados obtenidos.

El análisis se llevará a cabo a través de diversas fases, cada una de las cuales detalla las redes bajo consideración y las circunstancias específicas. Cada uno de estos escenarios será sometido a cinco simulaciones, con el propósito de recopilar datos estadísticos que permitan evaluar con precisión el impacto de los controles de seguridad. Además, permitirá identificar posibles implicaciones adicionales derivadas de la fortificación de la seguridad en la red.

4.2.1. Primer Escenario

El primer escenario se enfoca en analizar el comportamiento del ransomware en relación con la red inicial propuesta, junto con sus diversos modelos que representan la evolución de la red al implementar controles de seguridad. En su estado original, esta red está equipada únicamente con un firewall, y ningún equipo en la red posee antivirus, la configuración inicial se puede apreciar en la Figura 4.1. Aunque esta situación puede parecer poco probable, es relevante considerar que podría ser representativa en el contexto de organizaciones pequeñas [9].

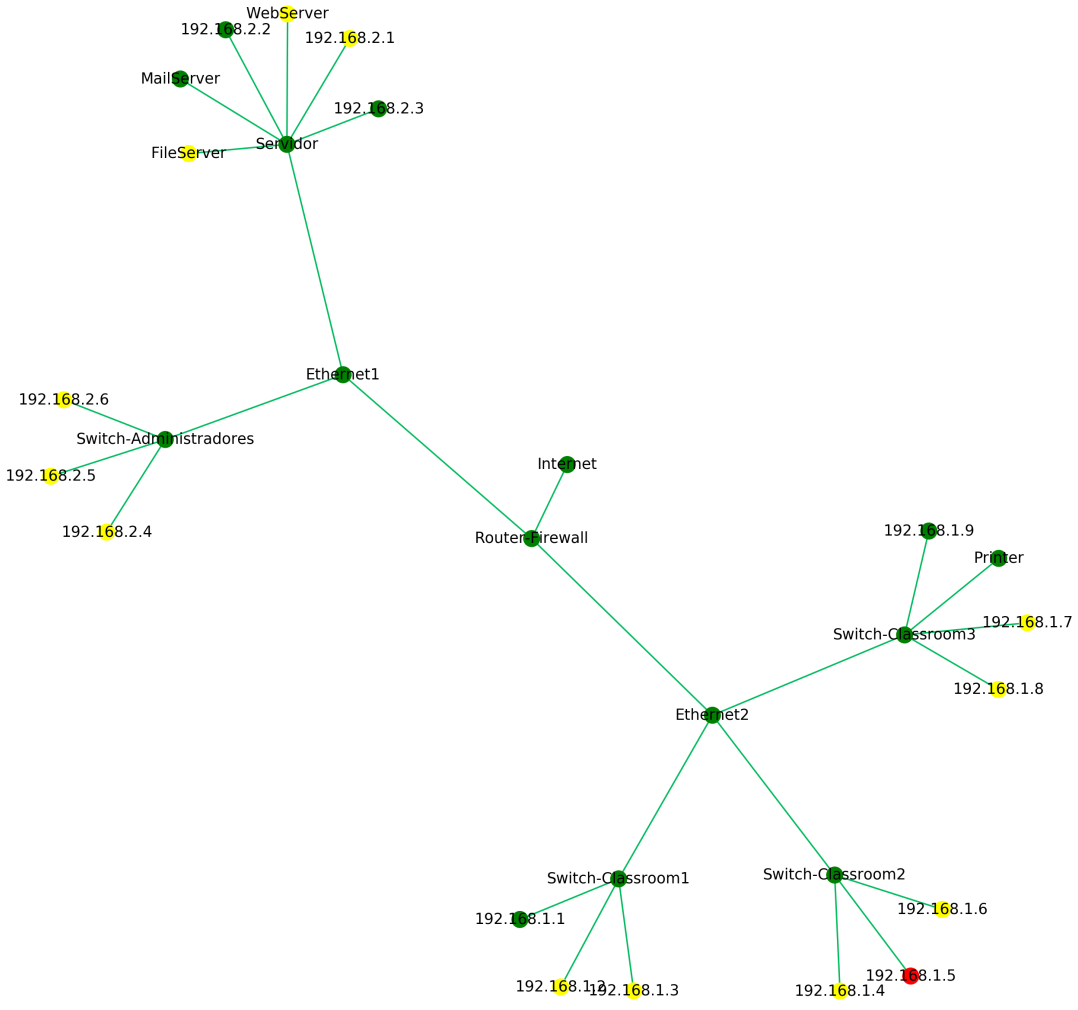


Figura 4.1: Estado original de la primera red.

Con el propósito de determinar la ubicación estratégica óptima para los nuevos controles de seguridad, se aplicaron los conceptos de centralidad de vector propio y el algoritmo PageRank a la red. Para la selección de los sitios de implementación de los controles, se eligieron los primeros cinco nodos con las centralidades o valores calculados más elevados. Posteriormente, se consideraron las condiciones establecidas en (I), (II), (III) y (IV) para refinar la ubicación de estos controles. Los resultados de este proceso se presentan en la Tabla 4.1.

Tabla 4.1: Valores de la centralidad de vector propio y PageRank asociados a cada nodo de la red original.

Nodo	Vector propio
Servidor	0.5408
Ethernet1	0.3605
Ethernet2	0.2832
Router-Firewall	0.2628
Switch-Administradores	0.2077
Switch-Classroom3	0.2053
WebServer	0.1928
MailServer	0.1928
192.168.2.1	0.1928
192.168.2.2	0.1928
192.168.2.3	0.1928
FileServer	0.1928
Switch-Classroom2	0.1631
Switch-Classroom1	0.1631
Internet	0.0937
192.168.2.6	0.074
192.168.2.5	0.074
192.168.2.4	0.074
192.168.1.9	0.0732
Printer	0.0732
192.168.1.8	0.0732
192.168.1.7	0.0732
192.168.1.2	0.0581
192.168.1.6	0.0581
192.168.1.5	0.0581
192.168.1.4	0.0581
192.168.1.3	0.0581
192.168.1.1	0.0581

Nodo	PageRank
Servidor	0.1229
Switch-Classroom3	0.0886
Switch-Administradores	0.0723
Switch-Classroom2	0.0717
Switch-Classroom1	0.0717
Ethernet2	0.065
Router-Firewall	0.0498
Ethernet1	0.0498
192.168.2.6	0.0207
192.168.2.4	0.0207
192.168.2.5	0.0207
192.168.1.2	0.0206
192.168.1.1	0.0206
192.168.1.6	0.0206
192.168.1.5	0.0206
192.168.1.4	0.0206
192.168.1.3	0.0206
192.168.1.9	0.0204
Printer	0.0204
192.168.1.8	0.0204
192.168.1.7	0.0204
192.168.2.3	0.0203
192.168.2.2	0.0203
192.168.2.1	0.0203
FileServer	0.0203
MailServer	0.0203
WebServer	0.0203
Internet	0.0195

Al examinar la tabla previa sobre la centralidad de vector propio, los cinco nodos con la centralidad más alta son: Servidor, Ethernet1, Ethernet2, Router-Firewall y Switch Administradores. Estos nodos son considerados para la implementación de los controles de seguridad. En el contexto de la red original (ver Figura 4.1), el nodo Servidor es adyacente al nodo Ethernet1, y a su vez, Ethernet1 está conectado a Switch Administradores y Router-Firewall. Dado que se satisface la condición (II) para el nodo Ethernet1, se establece un nuevo control que enlace los nodos Servidor

y Switch Administradores. Asimismo, el nodo Ethernet2 también cumple con la condición (II), por lo que se implementará un control adicional para conectarlo con sus nodos adyacentes restantes. Al seguir esta estrategia, la representación actualizada de la red se puede visualizar en la Figura 4.2.

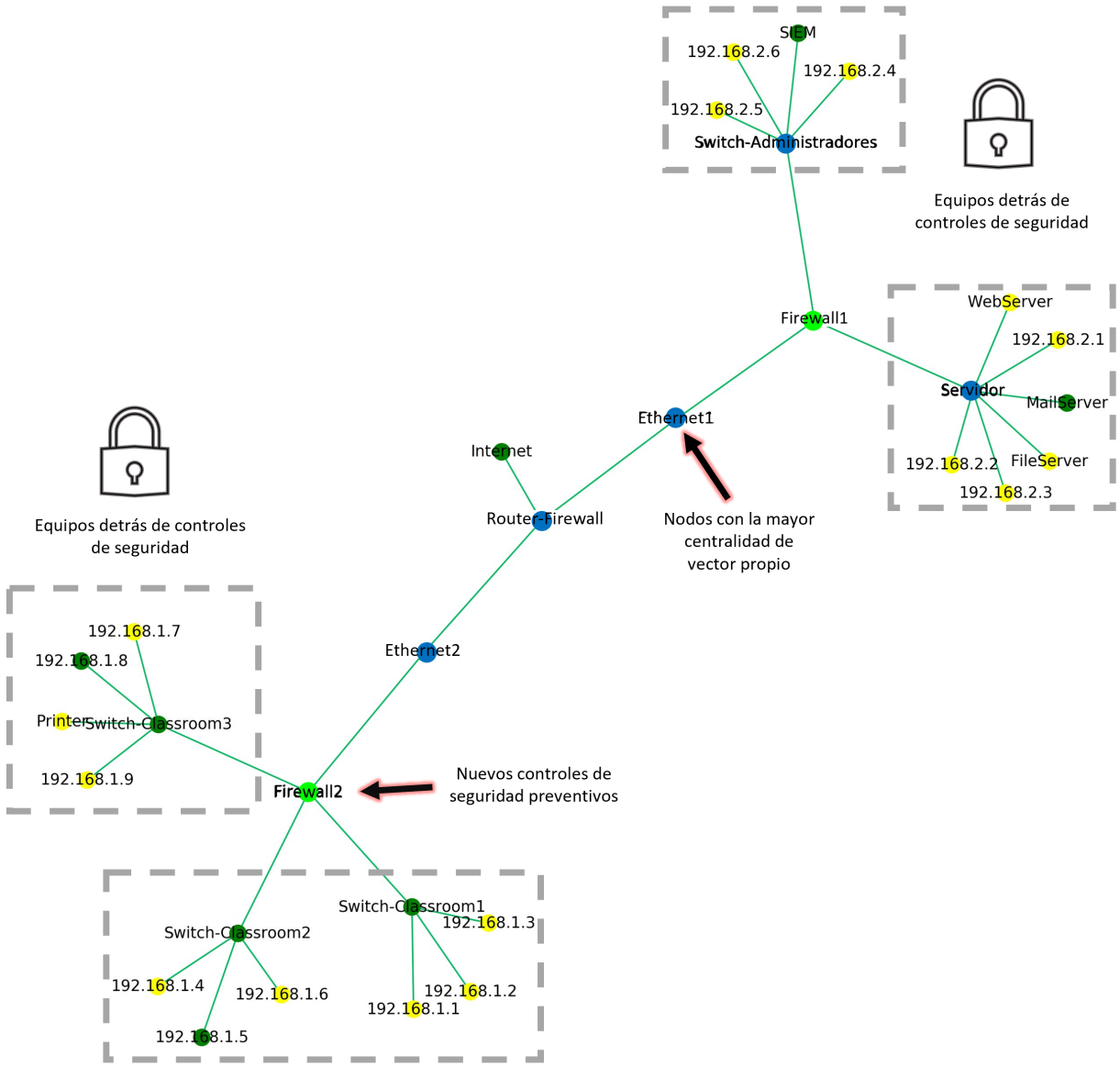


Figura 4.2: Controles de seguridad implementados al contemplar la centralidad de vector propio sobre la red original.

Por otro lado, al analizar los resultados obtenidos mediante el algoritmo PageRank, destacan los nodos más relevantes, que son: Servidor, Switch- Classroom3, Switch-Administradores, Switch-Classroom2 y Switch-Classroom1, en este caso, es evidente la importancia que desempeñan los switches en la red. Conforme a la condición (III), se establece la necesidad de implementar un control de seguridad para cada switch y su nodo Ethernet adyacente correspondiente. La regla uno requiere la existencia de un control entre los nodos Ethernet1, Servidor y Switch-Administradores.

Sin embargo, considerando la importancia destacada de estos dos últimos según la métrica calculada, se opta por instaurar controles de seguridad independientes para maximizar su protección. El resultado final se refleja en la nueva representación de la red, visible en la Figura 4.3.

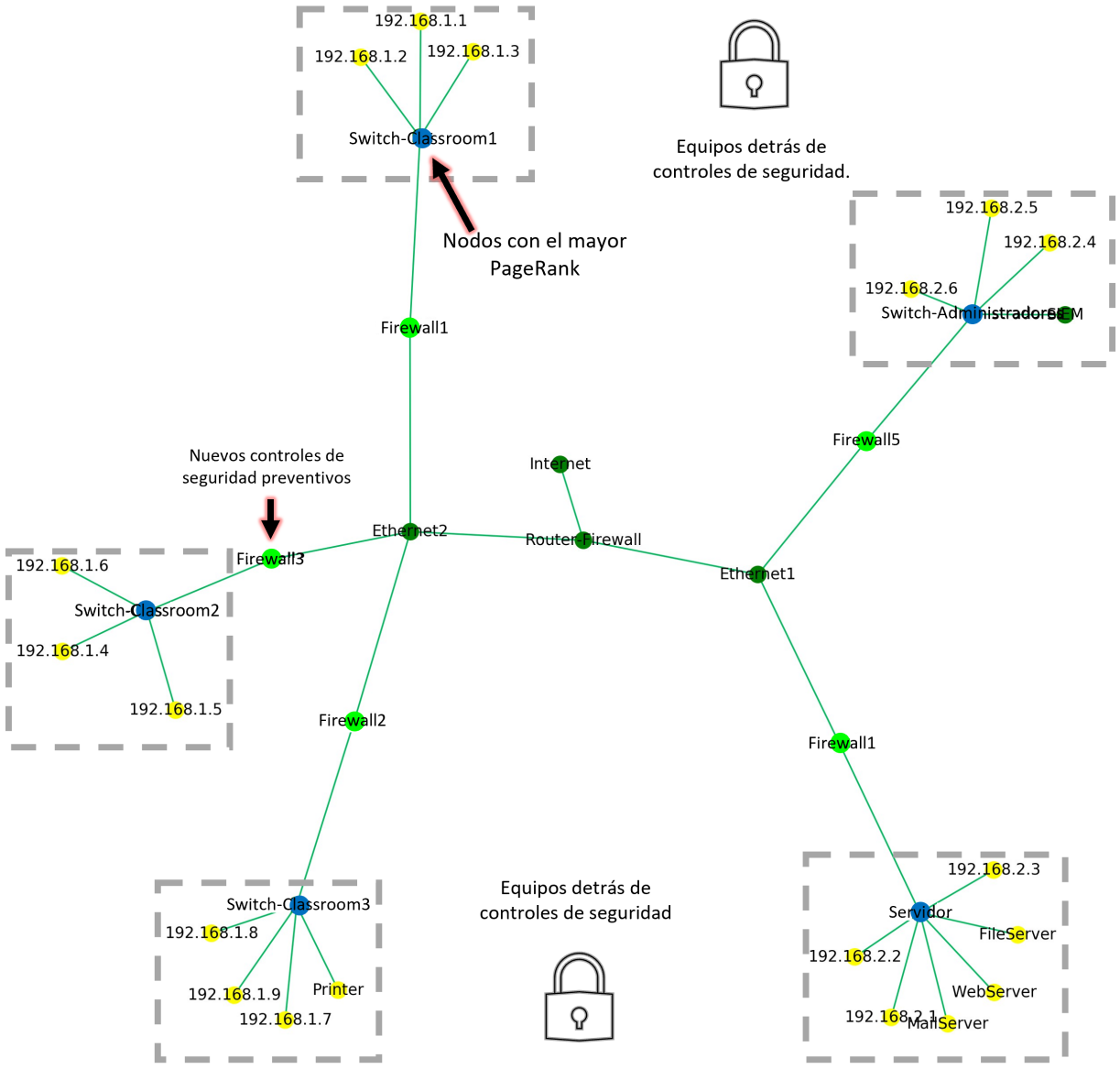


Figura 4.3: Controles de seguridad implementados utilizando la métrica PageRank sobre la red original.

Las redes previamente obtenidas desempeñan un papel fundamental en el análisis del patrón de propagación del ransomware. Se inicia considerando las condiciones atmosféricas que favorecen a los ciberdelincuentes y bajo este contexto, se exploran los diversos controles que pueden ser implementados en cada escenario. Los resultados obtenidos de calcular el promedio tras ejecutar el algoritmo cinco veces se encuentran en la Tabla 4.2:

Tabla 4.2: Efecto de los controles de seguridad ante el ransomware bajo condiciones atmosféricas a favor de los ciberdelincuentes.

Algoritmo	Antivirus	Firewall	SOC	Nodos Vulnerables	Nodos Infectados	Tiempo	Probabilidad	Escenario
Ninguno	No	Tradicional	No	16	16	1.0	0.6	Original
Ninguno	No	Next Generation	No	14.6	14.6	1.0	0.6	Original
Ninguno	Tradicional	Tradicional	No	14.8	14.8	1.4	0.6	UAV
Ninguno	Next Generation	Next Generation	No	16.0	16.0	3.0	0.6	UAV
Vector propio	No	Tradicional	No	16.2	16.2	1.0	0.6	FWEV
Vector propio	No	Next Generation	No	15.2	15.2	1.0	0.6	FWEV
PageRank	No	Tradicional	No	15.2	15.2	1.0	0.6	FWPR
PageRank	No	Next Generation	No	15.6	15.6	1.0	0.6	FWPR
Vector propio	Tradiconal	Tradicional	No	15.0	15.0	1.4	0.6	AVYFWEV
Vector propio	Next Generation	Next Generation	No	15.4	15.4	5.0	0.6	AVYFWEV
PageRank	Tradicional	Tradicional	No	16.0	16.0	1.4	0.6	AVYFWPR
PageRank	Next Generation	Next Generation	No	16.2	16.2	6.2	0.6	AVYFWPR
Vector propio	Tradicional	Tradicional	Sí	15.4	15.4	2.2	0.6	AVSOCYFWEV
Vector propio	Next Generation	Next Generation	Sí	15.6	15.3	7.9	0.6	AVSOCYFWEV
PageRank	Tradicional	Tradicional	Sí	14.6	14.6	2.4	0.6	AVSOCYFWPR
PageRank	Next Generation	Next Generation	Sí	15.0	14.4	9.0	0.6	AVSOCYFWPR

La Tabla 4.2 muestra un incremento progresivo en el tiempo promedio necesario para que el ransomware infecte los nodos. Esta tendencia refleja que la implementación de controles de seguridad ejerce una influencia significativa en la dificultad que enfrenta el ransomware para propagarse. Cabe destacar que, en el último escenario, ya con la presencia del SOC, se logra evitar la infección en algunos nodos. En este contexto, la presencia de tecnologías de tipo Next-Generation juega un papel esencial al ralentizar y, en ciertos casos, incluso detener el avance del ransomware, a pesar de las condiciones atmosféricas.

En contraste, al examinar la influencia de condiciones atmosféricas que favorezcan la ciberseguridad y considerar los subescenarios previamente mencionados, los resultados resultantes de las simulaciones se detallan en la Tabla 4.3:

Tabla 4.3: Efecto de los controles de seguridad ante el ransomware bajo condiciones atmosféricas a favor de la ciberseguridad.

Algoritmo	Antivirus	Firewall	SOC	Nodos Vulnerables	Nodos Infectados	Tiempo	Probabilidad	Escenario
Ninguno	No	Tradicional	No	16.2	16.2	1.0	0.5	Original
Ninguno	No	Next Generation	No	15.8	15.8	1.0	0.5	Original
Ninguno	Tradicional	Tradicional	No	16.6	16.6	2.0	0.5	UAV
Ninguno	Next Generation	Next Generation	No	14.2	14.2	5.4	0.5	UAV
Vector propio	No	Tradicional	No	15.0	15.0	1.2	0.5	FWEV
Vector propio	No	Next Generation	No	16.8	16.8	1.6	0.5	FWEV
PageRank	No	Tradicional	No	16.4	16.4	1.8	0.5	FWPR
PageRank	No	Next Generation	No	16.8	16.8	2.2	0.5	FWPR
Vector propio	Tradiconal	Tradicional	No	16.4	16.4	2.4	0.5	AVYFWEV
Vector propio	Next Generation	Next Generation	No	17.4	16.8	9.4	0.5	AVYFWEV
PageRank	Tradicional	Tradicional	No	16.4	16.4	2.4	0.5	AVYFWPR
PageRank	Next Generation	Next Generation	No	15.2	13.2	9.2	0.5	AVYFWPR
Vector propio	Tradicional	Tradicional	Sí	17.6	17.6	3.4	0.5	AVSOCYFWEV
Vector propio	Next Generation	Next Generation	Sí	15.2	12.8	10.0	0.5	AVSOCYFWEV
PageRank	Tradicional	Tradicional	Sí	17.0	17.0	3.8	0.5	AVSOCYFWPR
PageRank	Next Generation	Next Generation	Sí	15.7	9.2	10.0	0.5	AVSOCYFWPR

En la Tabla 4.3 se observa una tendencia similar a los hallazgos previos, con la particularidad de que se registra un aumento más pronunciado en el tiempo promedio requerido para que el ransomware infecte los nodos desde el inicio. Esta observación refleja la destacada influencia de la implementación de controles de seguridad en la dificultad de propagación del ransomware. Es esencial resaltar que en el último escenario, en el cual el SOC está presente, se logra prevenir la

infección de manera más eficiente en algunos nodos. En este contexto, la adopción de tecnologías de próxima generación desempeña un papel esencial al ralentizar e incluso detener, en algunos casos, el avance del ransomware, respaldada por las condiciones atmosféricas favorables.

4.2.2. Segundo Escenario

El segundo escenario se caracteriza por la presencia inicial de varios firewalls distribuidos en la red y sólo un servidor cuenta con antivirus, como se muestra en la Figura 4.4. Este escenario proporciona una visión más amplia de los equipos expuestos en la web y de aquellos que conforman la red interna. En particular, se destaca la existencia de un firewall externo, denotado como "Firewall-External", que actúa como una demarcación en la frontera, otorgando seguridad contra los ataques provenientes del exterior y que buscan ingresar a la red interna.

Mediante el cálculo de la centralidad de vector propio y el PageRank en esta red, se identifican las ubicaciones estratégicas para la incorporación de nuevos controles de seguridad. La implementación se basa en los mismos requisitos presentados en el primer escenario, se seleccionan los cinco nodos con los valores calculados más altos, y se aplican las condiciones (I), (II), (III) y (IV). Los resultados obtenidos de estas métricas se encuentran presentes en la Tabla 4.4.

Tabla 4.4: Valores de la centralidad de vector propio y PageRank asociados a cada nodo de la segunda red, en su estado original.

Nodo	Vector propio
Switch3	0.5804
Switch2	0.4751
Firewall-External	0.1659
192.168.1.140	0.1613
192.168.1.141	0.1613
192.168.1.148	0.1613
192.168.1.147	0.1613
192.168.1.146	0.1613
192.168.1.145	0.1613
192.168.1.144	0.1613
192.168.1.143	0.1613
192.168.1.142	0.1613
192.168.1.139	0.1613
Switch4	0.1562
Firewall-Internal	0.1468
NIDS-Promiscuos3	0.1321
WebServer2	0.1321
FileandPrint	0.1321
MailServer2-Antivirus	0.1321
DNSServer2	0.1321
Switch1	0.0667
Hub	0.0549
Switch5	0.0531
192.168.1.149	0.0434
SystemMgmt	0.0434
WebServer1	0.0185
MailRelay1	0.0185
DNSServer1	0.0185
NIDS-Promiscuos2	0.0185
Border-Router	0.0166
NIDS-Promiscuos1	0.0153
DatabaseServer	0.0148
NIDS-Promiscuos4	0.0148
ApplicationServer	0.0148
Internet	0.0046

Nodo	PageRank
Switch3	0.1506
Switch2	0.116
Switch1	0.0712
Switch5	0.059
Switch4	0.0435
Hub	0.0427
Firewall-External	0.0394
Border-Router	0.0314
Firewall-Internal	0.0278
Internet	0.0176
DatabaseServer	0.0168
ApplicationServer	0.0168
NIDS-Promiscuos4	0.0168
192.168.1.149	0.0166
SystemMgmt	0.0166
NIDS-Promiscuos1	0.0164
NIDS-Promiscuos2	0.0164
DNSServer1	0.0164
WebServer1	0.0164
MailRelay1	0.0164
192.168.1.146	0.0159
192.168.1.148	0.0159
192.168.1.147	0.0159
192.168.1.145	0.0159
192.168.1.144	0.0159
192.168.1.143	0.0159
192.168.1.142	0.0159
192.168.1.141	0.0159
192.168.1.139	0.0159
192.168.1.140	0.0159
DNSServer2	0.0152
MailServer2-Antivirus	0.0152
FileandPrint	0.0152
WebServer2	0.0152
NIDS-Promiscuos3	0.0152

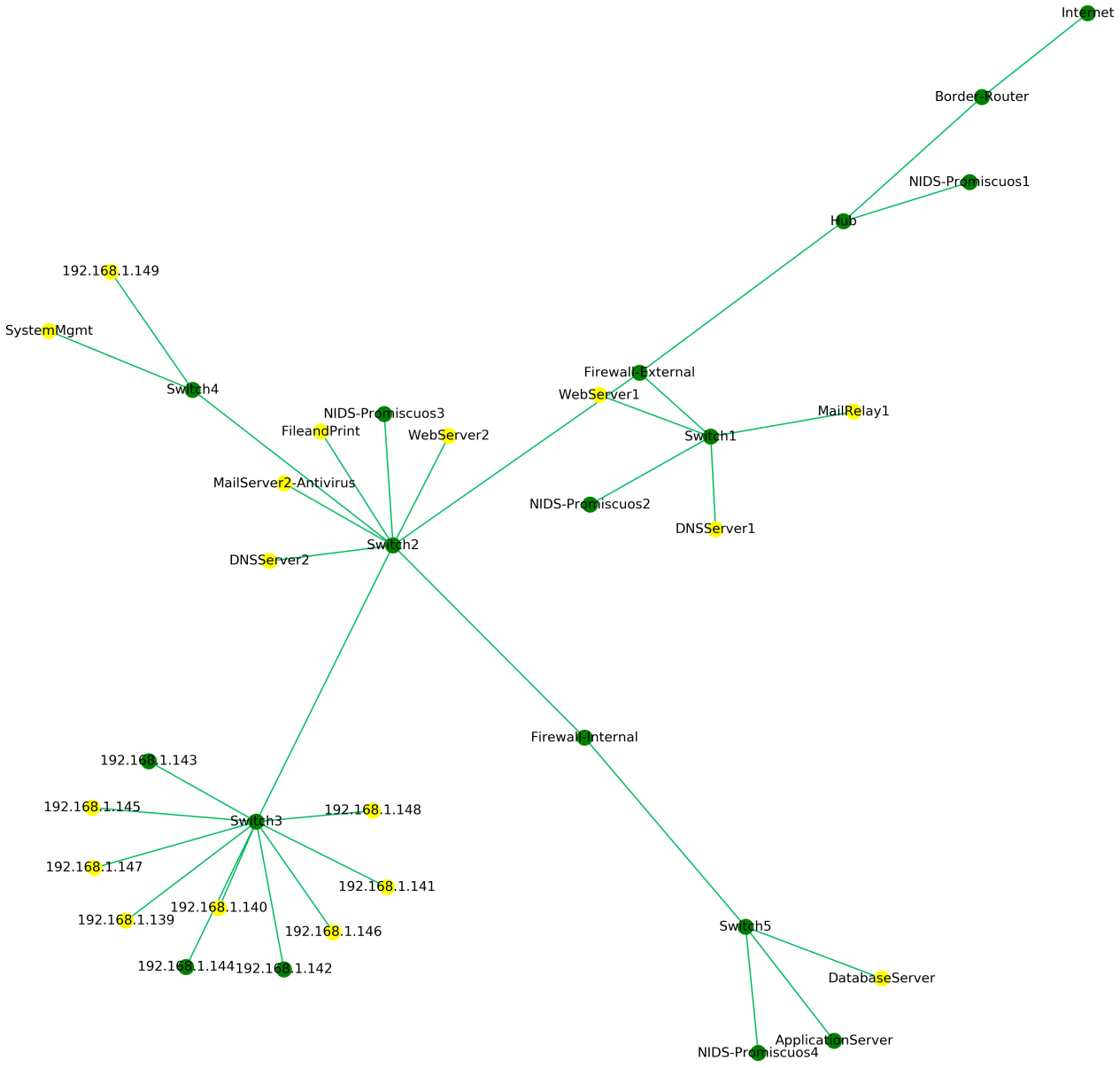


Figura 4.4: Estado original de la segunda red.

Al analizar los resultados presentados en la Tabla 4.4, se puede llevar a cabo la modelación de las nuevas redes. Con la centralidad de vector propio, destacan cinco nodos con los valores más altos: Switch3, Switch2, Firewall-External y una serie de nodos que representan equipos de usuarios, todos con igual valor. Estos nodos se considerarán para la implementación de los controles.

En particular, el nodo Switch3 es adyacente a los equipos de usuarios, lo que lleva a colocar un nuevo firewall entre estos dos elementos según la condición (III). Además, la condición (II) posibilita la incorporación de más equipos detrás del firewall, ya que el nodo Switch2 es adyacente a nodos que representan controles de seguridad. Por lo tanto, el firewall inducido por Switch3 también debe proteger los nodos cercanos a Switch2.

Por la condición (IV), el Firewall-External no experimenta cambios, lo que representa que sólo es necesario introducir un nuevo nodo. La nueva red mejorada se puede observar en la Figura 4.5.

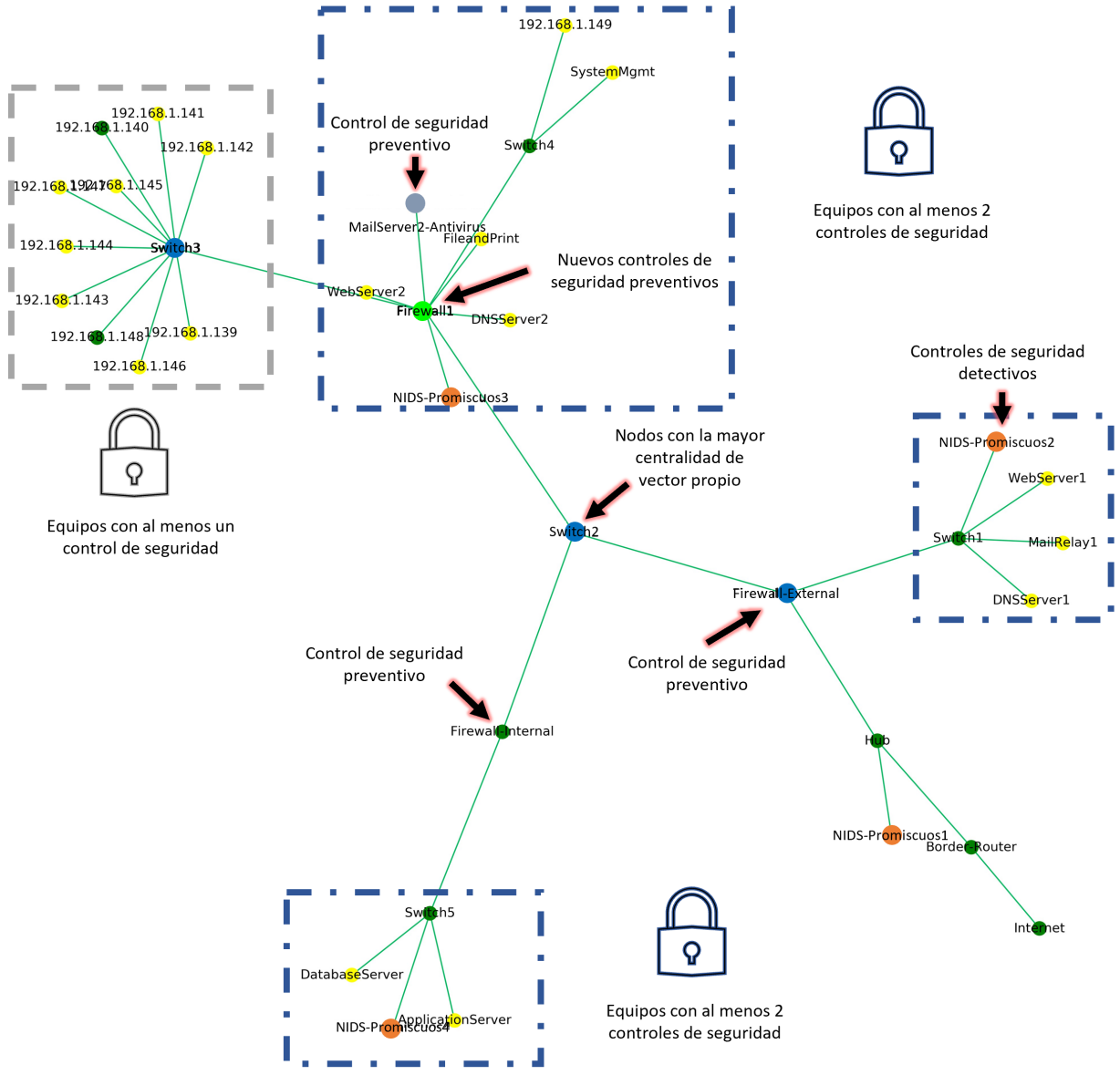


Figura 4.5: Controles de seguridad implementados utilizando la centralidad de vector propio sobre la red original.

Por otro lado, al considerar los resultados obtenidos mediante el algoritmo PageRank, los nodos más influyentes son Switch3, Switch2, Switch1, Switch5 y Switch4. Switch3 está conectado a diversos equipos de usuarios y al Switch2, que a su vez está enlazado con múltiples otros nodos. Se sigue la condición (II) aplicada al nodo Switch2, por lo que todos los nodos adyacentes a este, excepto Firewall-External y Firewall-Internal, deben estar protegidos detrás de un firewall. Si bien un único firewall podría garantizar la seguridad de los sistemas, se decide asignar un firewall exclusivo para cada uno de los nodos relevantes, como Switch3 y Switch4, según lo indicado por su alta relevancia de acuerdo al PageRank, esto implica que cada uno de estos switches contará

con su propio firewall, conectándolos al nodo Switch2.

En cuanto a los demás nodos vecinos de Switch2 que no pueden tener firewalls exclusivos, pero deben estar tras uno, pueden ser colocados de manera indistinta en relación con los nuevos firewalls implementados. La nueva red resultante puede visualizarse en la Figura 4.6.

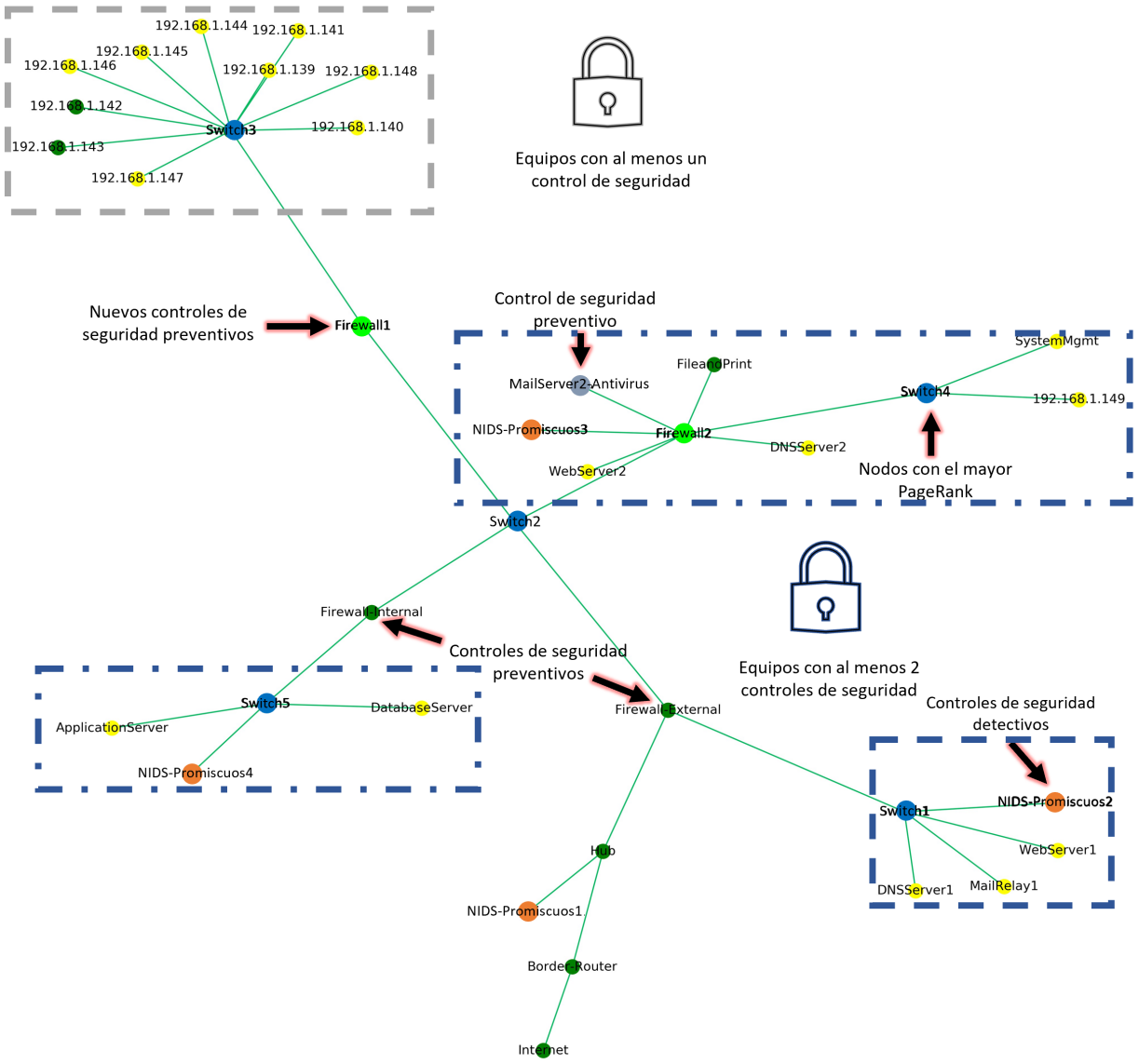


Figura 4.6: Controles de seguridad implementados utilizando el algoritmo PageRank sobre la red original.

Con los escenarios derivados de los análisis previos y al considerar las condiciones atmosféricas a favor de los ciberdelincuentes, los resultados generados tras realizar la simulación del algoritmo en cinco iteraciones se encuentran detallados en la Tabla 4.5.

Tabla 4.5: Efecto de los controles de seguridad ante el ransomware en la segunda red, bajo condiciones atmosféricas a favor de los ciberdelincuentes.

Algoritmo	Antivirus	Firewall	SOC	Nodos Vulnerables	Nodos Infectados	Tiempo	Probabilidad	Escenario
Ninguno	Tradicional*	Tradicional	No	18.2	18.2	1.0	0.6	Original
Ninguno	Next Generation*	Next Generation	No	17.4	17.4	1.6	0.6	Original
Ninguno	Tradicional	Tradicional	No	17.6	17.6	1.2	0.6	UAV
Ninguno	Next Generation	Next Generation	No	16.6	16.6	4.2	0.6	UAV
Vector propio	No	Tradicional	No	17.8	17.8	1.0	0.6	FWEV
Vector propio	No	Next Generation	No	16.8	16.8	2.4	0.6	FWEV
PageRank	No	Tradicional	No	16.8	16.8	1.2	0.6	FWPR
PageRank	No	Next Generation	No	18.8	18.8	1.6	0.6	FWPR
Vector propio	Tradicional	Tradicional	No	17.6	17.6	1.6	0.6	AVYFWEV
Vector propio	Next Generation	Next Generation	No	17.2	17.2	4.0	0.6	AVYFWEV
PageRank	Tradicional	Tradicional	No	16.2	16.2	1.6	0.6	AVYFWPR
PageRank	Next Generation	Next Generation	No	17.6	17.6	3.8	0.6	AVYFWPR
Vector propio	Tradicional	Tradicional	Sí	17.0	17.0	2.0	0.6	AVSOCYFWEV
Vector propio	Next Generation	Next Generation	Sí	17.0	17.0	5.2	0.6	AVSOCYFWEV
PageRank	Tradicional	Tradicional	Sí	18.4	18.4	1.8	0.6	AVSOCYFWPR
PageRank	Next Generation	Next Generation	Sí	16.8	16.8	5.8	0.6	AVSOCYFWPR

Tradicional* y Next Generation* hacen referencia a que sólo los equipos que originalmente contaban con antivirus sean considerados con este tipo de seguridad.

La Tabla 4.5 exhibe cómo el nivel de infección en la red decrece a medida que se incorporan nuevos controles de seguridad. No obstante, es crucial reconocer que en ningún escenario se logra detener por completo el ataque. Esta observación podría estar relacionada con las condiciones atmosféricas, sin embargo, el aspecto destacable es la concentración mayoritaria de nodos en una sección específica de la red. A pesar de que la red es plana y no impone limitaciones en la comunicación entre nodos, esta concentración favorece la identificación de dispositivos vulnerables. Esto, a su vez, intensifica la etapa de explotación de vulnerabilidades aprovechadas por el ransomware y sus etapas posteriores. En este contexto, basta con que un dispositivo dentro de esta concentración sea infectado, independientemente de si es el nodo inicial o no, para aumentar significativamente el riesgo potencial en los demás.

Al considerar la presencia de condiciones atmosféricas a favor de la ciberseguridad y los mismos subescenarios, los resultados están presentes en la Tabla 4.6:

Tabla 4.6: Efecto de los controles de seguridad ante el ransomware en la segunda red, bajo condiciones atmosféricas a favor de la ciberseguridad.

Algoritmo	Antivirus	Firewall	SOC	Nodos Vulnerables	Nodos Infectados	Tiempo	Probabilidad	Escenario
Ninguno	Tradicional*	Tradicional	No	18.2	18.2	1.8	0.5	Original
Ninguno	Next Generation*	Next Generation	No	18.0	18.0	3.2	0.5	Original
Ninguno	Tradicional	Tradicional	No	16.8	16.8	2.6	0.5	UAV
Ninguno	Next Generation	Next Generation	No	18.0	17.8	7.6	0.5	UAV
Vector propio	No	Tradicional	No	16.6	16.6	1.6	0.5	FWEV
Vector propio	No	Next Generation	No	16.2	16.2	4.0	0.5	FWEV
PageRank	No	Tradicional	No	16.6	16.6	1.2	0.5	FWPR
PageRank	No	Next Generation	No	17.2	17.2	5.6	0.5	FWPR
Vector propio	Tradiconal	Tradicional	No	15.2	15.2	2.6	0.5	AVYFWEV
Vector propio	Next Generation	Next Generation	No	18.6	18.2	8.6	0.5	AVYFWEV
PageRank	Tradicional	Tradicional	No	17.6	17.6	3.2	0.5	AVYFWPR
PageRank	Next Generation	Next Generation	No	17.4	17.0	8.8	0.5	AVYFWPR
Vector propio	Tradicional	Tradicional	Sí	16.2	16.2	3.4	0.5	AVSOCYFWEV
Vector propio	Next Generation	Next Generation	Sí	14.6	12.6	9.6	0.5	AVSOCYFWEV
PageRank	Tradicional	Tradicional	Sí	16.2	16.2	3.6	0.5	AVSOCYFWPR
PageRank	Next Generation	Next Generation	Sí	16.4	14.8	10.0	0.5	AVSOCYFWPR

Tradicional* y Next Generation* hacen referencia a que sólo los equipos que originalmente contaban con antivirus sean tomados en cuenta.

Al evaluar el algoritmo PageRank, se constata un incremento en el tiempo que requiere el ransomware para propagarse en la red desde el inicio. A pesar de este resultado positivo, la concentración de nodos en un segmento específico de la red favorece la expansión del malware. Esta dinámica incrementa su alcance y el riesgo inherente a la organización, al facilitar la identificación de nodos vulnerables. En consecuencia, basta con que un nodo dentro de esta concentración se vea afectado para que aumente considerablemente el peligro para los demás, independientemente de si es el nodo de inicio o no.

4.2.3. Tercer Escenario

El tercer escenario presenta una configuración con múltiples controles de seguridad distribuidos a lo largo de toda la red, como se ilustra en la Figura 4.7. Este caso representa a una organización que posee un nivel de madurez en ciberseguridad más avanzado en comparación con los anteriores. La empresa, de la cual se extrajo el modelo, dispone de un área de ciberseguridad y sigue rigurosamente las mejores prácticas establecidas por estándares y marcos normativos internacionales. En esta configuración, todos los controles de seguridad son de tipo Next Generation, incluyendo firewalls, antivirus (implementados en todos los equipos) y un sistema SIEM. Para efectos prácticos, al analizar la eficacia de los controles de seguridad en la mitigación del ransomware, sólo se toman en cuenta los escenarios que son aplicables con los controles establecidos desde el principio. Aunque, también se realizarán simulaciones considerando tanto controles tradicionales como Next Generation.

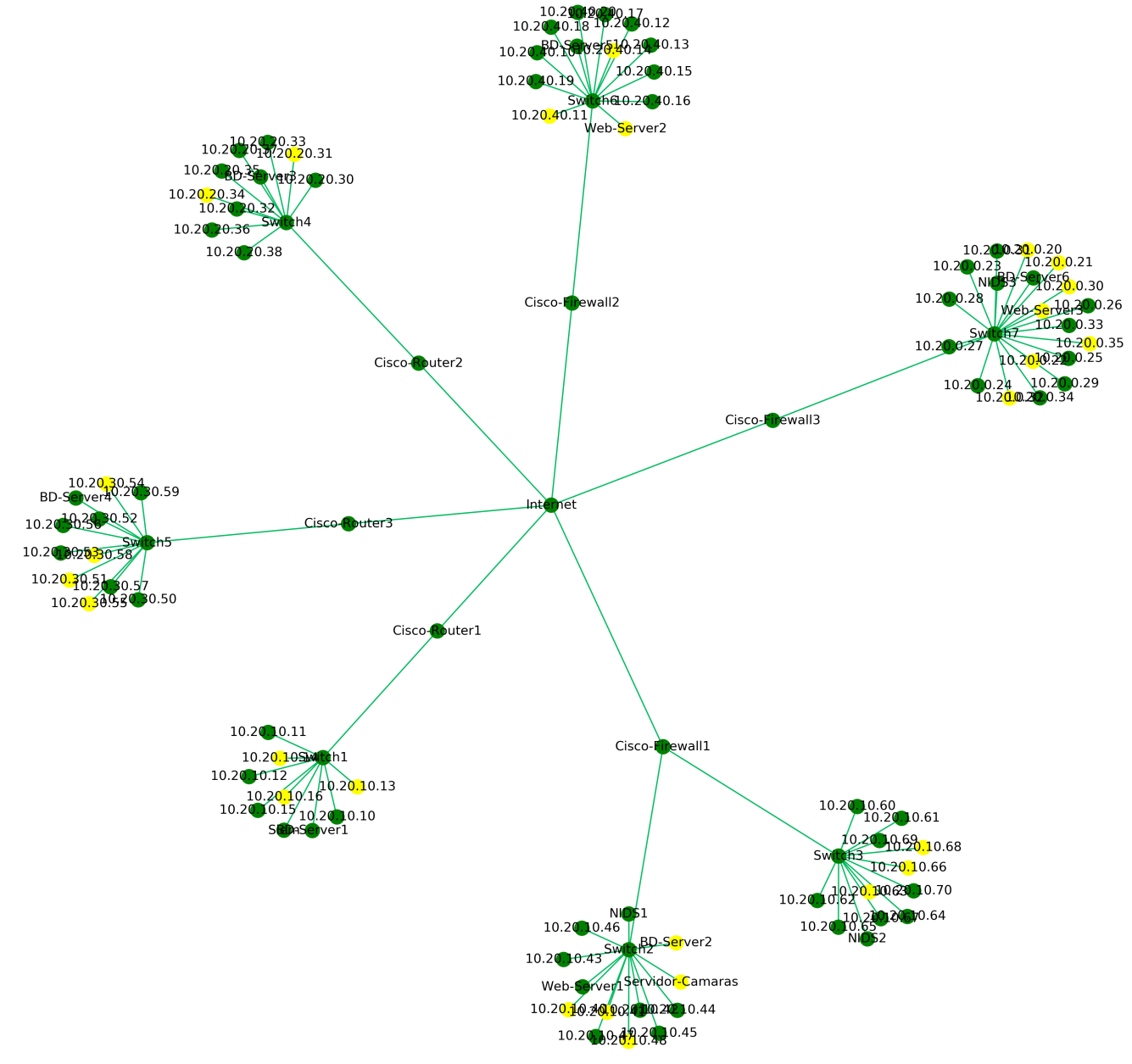


Figura 4.7: Estado original de la tercera red.

A la red de la Figura 4.7 se le calculó la centralidad de vector propio y el PageRank con el fin de identificar las ubicaciones estratégicas para la implementación de nuevos controles de seguridad. Para llevar a cabo esta implementación, se mantuvo la base de requisitos presentados en el primer escenario. y se aplican las condiciones establecidas por los requisitos (I), (II), (III) y (IV).

Los resultados obtenidos a partir de estas métricas y el proceso de implementación de controles se encuentran detallados en la Tabla 4.7. Este análisis permite comprender cómo las estrategias de seguridad influyen en la propagación del ransomware en esta configuración específica de la red.

Tabla 4.7: Valores de la centralidad de vector propio asociados a cada nodo de la tercera red, en su estado original.

Nodo	Vector propio
Switch7	0.7048
Cisco-Firewall3	0.1692
10.20.0.25	0.1573
BD-Server6	0.1573
NIDS3	0.1573
Web-Server3	0.1573
10.20.0.20	0.1573
10.20.0.21	0.1573
10.20.0.22	0.1573
10.20.0.23	0.1573
10.20.0.24	0.1573
10.20.0.35	0.1573
10.20.0.27	0.1573
10.20.0.28	0.1573
10.20.0.29	0.1573
10.20.0.30	0.1573
10.20.0.31	0.1573
10.20.0.32	0.1573
10.20.0.33	0.1573
10.20.0.34	0.1573
10.20.0.26	0.1573
Internet	0.0533
Cisco-Firewall1	0.0162
Cisco-Firewall2	0.0139
Cisco-Router3	0.0134
Cisco-Router2	0.0132
Cisco-Router1	0.0131
Switch2	0.0103
Switch3	0.009
Switch6	0.0088
Switch5	0.0066
Switch4	0.0059
Switch1	0.0053
10.20.10.40	0.0023
NIDS1	0.0023
10.20.10.41	0.0023
BD-Server2	0.0023

Nodo	Vector propio
Servidor-Cámaras	0.0023
10.20.10.43	0.0023
Web-Server1	0.0023
10.20.10.42	0.0023
10.20.10.46	0.0023
10.20.10.45	0.0023
10.20.10.44	0.0023
10.20.10.47	0.0023
10.20.10.48	0.0023
10.20.10.70	0.0020
10.20.10.62	0.0020
10.20.10.69	0.0020
10.20.10.60	0.0020
10.20.10.61	0.0020
10.20.10.63	0.0020
NIDS2	0.0020
10.20.10.64	0.0020
10.20.10.65	0.0020
10.20.10.66	0.0020
10.20.10.67	0.0020
10.20.10.68	0.0020
10.20.40.14	0.0020
10.20.40.10	0.0020
BD-Server5	0.0020
Web-Server2	0.0020
10.20.40.13	0.0020
10.20.40.20	0.0020
10.20.40.15	0.0020
10.20.40.16	0.0020
10.20.40.17	0.0020
10.20.40.18	0.0020
10.20.40.19	0.0020
10.20.40.12	0.0020
10.20.40.11	0.0020
10.20.30.56	0.0015
10.20.30.59	0.0015
10.20.30.52	0.0015

Nodo	Vector propio
10.20.30.58	0.0015
10.20.30.50	0.0015
10.20.30.51	0.0015
BD-Server4	0.0015
10.20.30.53	0.0015
10.20.30.54	0.0015
10.20.30.55	0.0015
10.20.30.57	0.0015
10.20.20.36	0.0013
BD-Server3	0.0013
10.20.20.30	0.0013
10.20.20.31	0.0013
10.20.20.32	0.0013
10.20.20.33	0.0013

Nodo	Vector propio
10.20.20.34	0.0013
10.20.20.35	0.0013
10.20.20.37	0.0013
10.20.20.38	0.0013
10.20.10.10	0.0012
10.20.10.11	0.0012
10.20.10.13	0.0012
10.20.10.14	0.0012
BD-Server1	0.0012
10.20.10.15	0.0012
10.20.10.16	0.0012
Siem	0.0012
10.20.10.12	0.0012

Tabla 4.8: Valores del algoritmo PageRank asociados a cada nodo de la tercera red, en su estado original.

Nodo	PageRank
Switch7	0.0932
Switch6	0.0659
Switch2	0.0654
Switch3	0.0609
Switch5	0.0567
Switch4	0.0522
Switch1	0.0476
Internet	0.024
Cisco-Firewall1	0.0128
Cisco-Router1	0.0089
Cisco-Router2	0.0089
Cisco-Router3	0.0089
Cisco-Firewall2	0.0089
Cisco-Firewall3	0.0089
10.20.10.13	0.0055
10.20.10.16	0.0055
10.20.10.15	0.0055
10.20.10.14	0.0055
10.20.10.10	0.0055
10.20.10.12	0.0055
10.20.10.11	0.0055
BD-Server1	0.0055
Siem	0.0055
BD-Server3	0.0055
10.20.20.38	0.0055
10.20.20.36	0.0055
10.20.20.35	0.0055
10.20.20.34	0.0055
10.20.20.33	0.0055
10.20.20.32	0.0055
10.20.20.31	0.0055
10.20.20.30	0.0055
10.20.20.37	0.0055
10.20.30.56	0.0055
10.20.30.57	0.0055
10.20.30.54	0.0055
10.20.30.53	0.0055

Nodo	PageRank
10.20.30.52	0.0055
10.20.30.51	0.0055
10.20.30.50	0.0055
10.20.30.58	0.0055
10.20.30.59	0.0055
10.20.30.55	0.0055
BD-Server4	0.0055
10.20.40.16	0.0055
10.20.40.15	0.0055
10.20.40.17	0.0055
10.20.40.13	0.0055
10.20.40.12	0.0055
10.20.40.11	0.0055
10.20.40.10	0.0055
10.20.40.18	0.0055
10.20.40.19	0.0055
10.20.40.20	0.0055
BD-Server5	0.0055
Web-Server2	0.0055
10.20.40.14	0.0055
NIDS2	0.0055
10.20.10.61	0.0055
10.20.10.62	0.0055
10.20.10.70	0.0055
10.20.10.63	0.0055
10.20.10.64	0.0055
10.20.10.65	0.0055
10.20.10.66	0.0055
10.20.10.67	0.0055
10.20.10.60	0.0055
10.20.10.68	0.0055
10.20.10.69	0.0055
10.20.10.48	0.0055
10.20.10.47	0.0055
10.20.10.46	0.0055
10.20.10.40	0.0055
10.20.10.45	0.0055

NIDS1	0.0055
BD-Server2	0.0055
10.20.10.44	0.0055
10.20.10.43	0.0055
10.20.10.42	0.0055
Servidor-Cámaras	0.0055
Web-Server1	0.0055
10.20.10.41	0.0055
NIDS3	0.0054
10.20.0.20	0.0054
BD-Server6	0.0054
10.20.0.28	0.0054
10.20.0.22	0.0054
10.20.0.23	0.0054
10.20.0.24	0.0054
10.20.0.25	0.0054
10.20.0.26	0.0054
10.20.0.27	0.0054
10.20.0.29	0.0054
10.20.0.21	0.0054
10.20.0.30	0.0054
10.20.0.31	0.0054
10.20.0.32	0.0054
10.20.0.33	0.0054
10.20.0.34	0.0054
10.20.0.35	0.0054
Web-Server3	0.0054

Al iniciar el análisis con la centralidad de vector propio, disponible en la Tabla 4.7, destaca que los cinco nodos con mayor centralidad son Switch7, Cisco-Firewall3 y varios nodos con valores iguales que comparten el nodo Switch7. Al aplicar las condiciones (I), (II), (III) y (IV), se determina que no se requiere la introducción de nuevos nodos, ya que la presencia del nodo Cisco-Firewall3 cumple con la protección requerida para estos equipos.

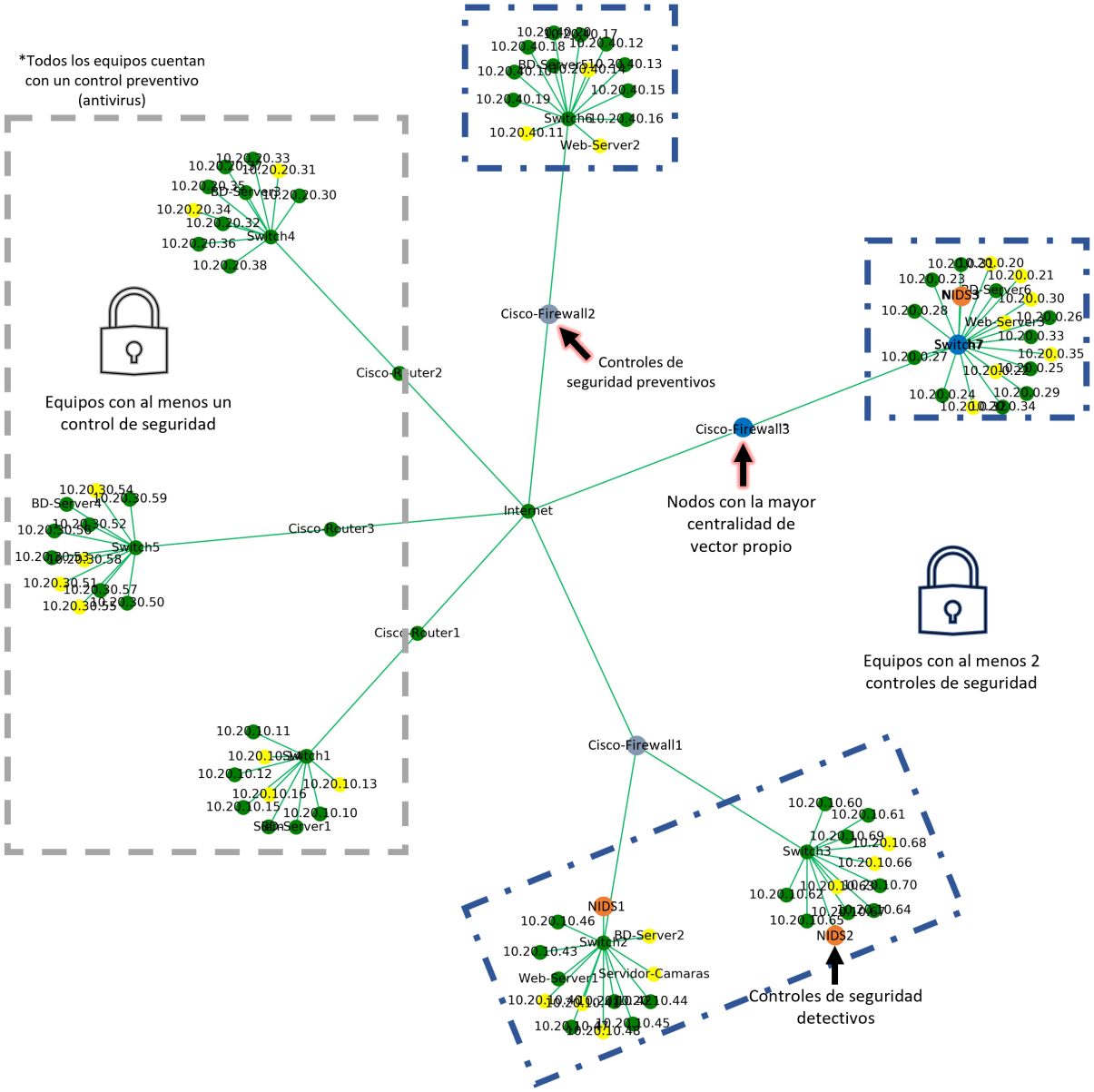


Figura 4.8: Controles de seguridad implementados utilizando la centralidad de vector propio sobre la red original.

En cambio, al considerar el algoritmo PageRank resaltan los nodos Switch7, Switch6, Switch2, Switch3 y Switch5. Entre estos, los primeros cuatro ya cuentan con firewalls asignados. En consecuencia, sólo es necesario implementar un nuevo nodo de control para el nodo Switch5. Aunque el nodo Cisco-Router3 podría ser reemplazado por un Cisco-Firewall por razones de claridad, se ha optado por añadir un nodo adicional para distinguir el nuevo control. Si bien este nuevo nodo también podría ofrecer protección a Switch1 y Switch4, no se les considera debido a su posición menos relevante. La configuración resultante se ilustra en la Figura 4.9.

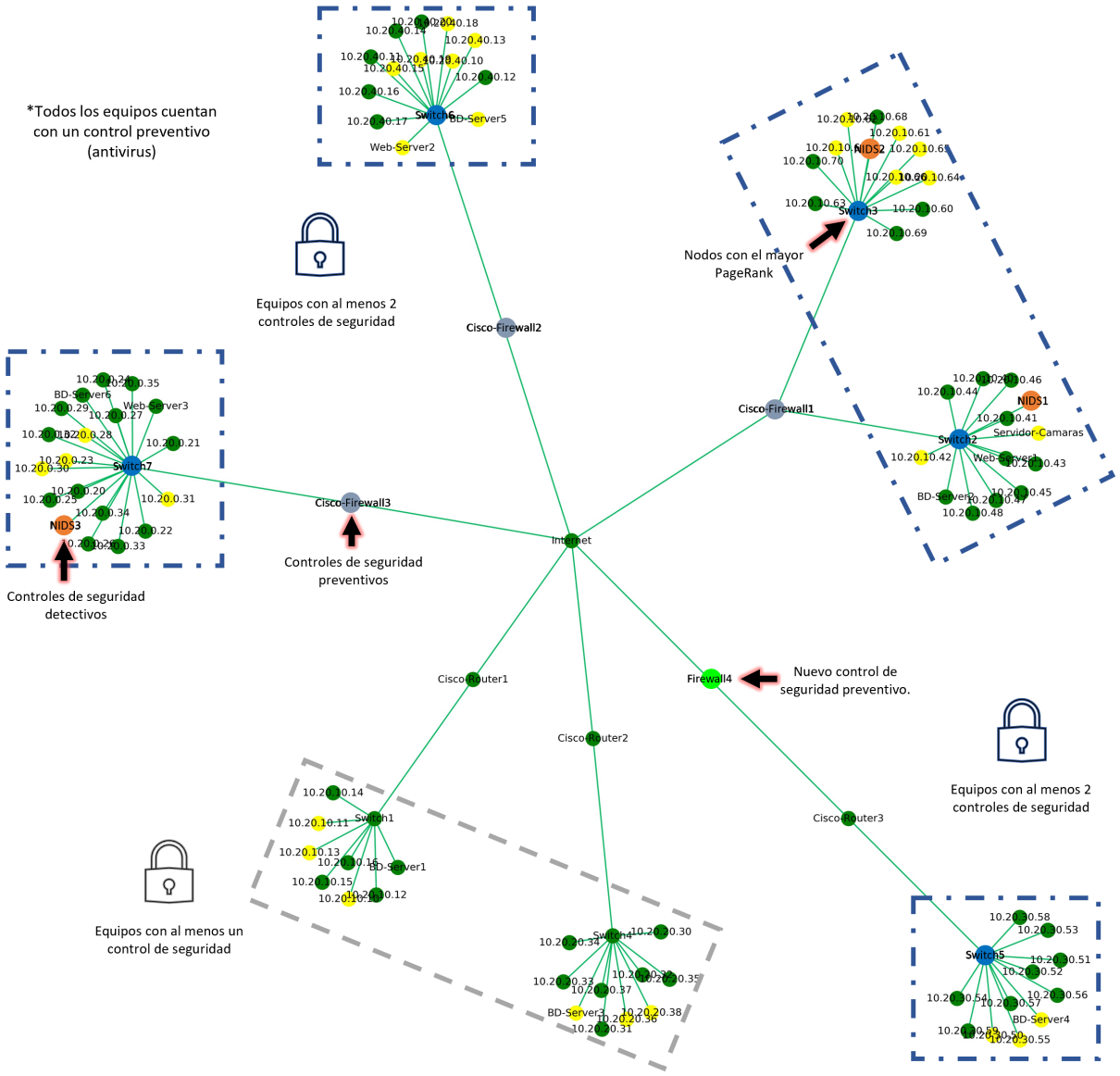


Figura 4.9: Controles de seguridad implementados utilizando el algoritmo PageRank sobre la red original.

Al considerar las redes previamente obtenidas y las condiciones atmosféricas a favor de los ciberdelincuentes, los resultados derivados de cinco simulaciones del algoritmo están detallados en la Tabla 4.9. Es importante destacar que, debido a la ausencia de nuevos nodos, se dispondrá de un número de escenarios menor en comparación con el algoritmo PageRank.

Tabla 4.9: Efecto de los controles de seguridad ante el ransomware en la tercera red, bajo condiciones atmosféricas a favor de los ciberdelincuentes.

Algoritmo	Antivirus	Firewall	SOC	Nodos Vulnerables	Nodos Infectados	Tiempo	Probabilidad	Escenario
Ninguno	Tradicional	Tradicional	No	28.7	28.7	1.7	0.6	Original
Ninguno	Next Generation	Next Generation	No	27.2	27.2	4.8	0.6	Original
PageRank	Tradicional	Tradicional	No	25.3	25.3	1.8	0.6	AVYFWPR
PageRank	Next Generation	Next Generation	No	30.2	30.2	5.8	0.6	AVYFWPR
Vector propio	Tradicional	Tradicional	Sí	32.0	32.0	2.3	0.6	AVSOCYFWEV
Vector propio	Next Generation	Next Generation	Sí	35.5	35.5	6.8	0.6	AVSOCYFWEV
PageRank	Tradicional	Tradicional	Sí	31.2	31.2	2.2	0.6	AVSOCYFWPR
PageRank	Next Generation	Next Generation	Sí	29.2	29.1	8.4	0.6	AVSOCYFWPR

La Tabla 4.9 confirma la constante tendencia hacia la reducción de la propagación del ransomware a medida que se implementan nuevos controles de seguridad en la red. A pesar de la segmentación de la red para los usuarios y la incorporación de múltiples medidas de protección, estos no logran contener la amenaza del ransomware de manera absoluta. Este hallazgo plantea una reflexión sobre la suficiencia de la tecnología por sí sola para enfrentar de manera eficiente las diversas amenazas que prevalecen.

Al explorar el impacto de condiciones atmosféricas favorables a la ciberseguridad en los mismos subescenarios, los resultados se encuentran en la Tabla 4.10:

Tabla 4.10: Efecto de los controles de seguridad ante el ransomware en la tercera red, bajo condiciones atmosféricas a favor de la ciberseguridad.

Algoritmo	Antivirus	Firewall	SOC	Nodos Vulnerables	Nodos Infectados	Tiempo	Probabilidad	Escenario
Ninguno	Tradicional*	Tradicional	No	31.3	31.3	4.7	0.5	Original
Ninguno	Next Generation*	Next Generation	No	30.3	29.8	7.5	0.5	Original
PageRank	Tradicional	Tradicional	No	32.2	32.2	3.0	0.5	AVYFWPR
PageRank	Next Generation	Next Generation	No	32.5	31.8	8.8	0.5	AVYFWPR
Vector propio	Tradicional	Tradicional	Sí	32.3	32.3	3.8	0.5	AVSOCYFWEV
Vector propio	Next Generation	Next Generation	Sí	39.2	36.4	10.0	0.5	AVSOCYFWEV
PageRank	Tradicional	Tradicional	Sí	30.5	30.5	4.3	0.5	AVSOCYFWPR
PageRank	Next Generation	Next Generation	Sí	34.6	30.7	10.0	0.5	AVSOCYFWPR

La Tabla 4.10 muestra una notoria eficacia en la contención del ransomware desde el inicio, lo cual se refleja en el tiempo con el que se logra infectar los nodos. Es relevante destacar que los escenarios que incorporan un SOC, además de las controles como antivirus y firewalls, demuestran una capacidad de defensa proactiva para la organización. Esta defensa se manifiesta en la detección y detención oportuna del ransomware, lo cual también puede estar influenciado por las condiciones atmosféricas presentes y la concientización en materia de seguridad que subyace.

4.3. Discusión

A continuación, se presenta la discusión generada con los puntos y observaciones relevantes de los resultados previos.

4.3.1. Resultados Generales

Los resultados obtenidos resaltan la importancia crítica de la consideración del factor humano en el contexto de la ciberseguridad. A pesar de que las tecnologías modernas de última generación desempeñan un rol fundamental en la defensa contra el ransomware, no se debe subestimar la necesidad de educar y sensibilizar a los usuarios. Si se sigue la estructura de las cinco funciones establecidas por el NIST (Identificar, Proteger, Detectar, Responder y Recuperar), se establece un enfoque sólido para abordar tanto los aspectos tecnológicos como los factores humanos y de gestión en la ciberdefensa.

En este contexto, se establece una estructura sólida para abordar no sólo los aspectos tecnológicos, sino también los factores humanos y de gestión en la ciberdefensa. Se requiere una estrategia diversificada que abarque tanto las soluciones tecnológicas como firewalls, sistemas de detección avanzada y control de acceso, como también la educación y la conciencia de los usuarios. Este enfoque integral puede contrarrestar de manera más efectiva las amenazas en constante evolución y el panorama del ransomware. Además, se hace hincapié en la importancia de seguir marcos de referencia y modelos como el MITRE ATT&CK, así como considerar las fases de la Cyber Kill Chain para establecer una defensa holística y estratégica.

La madurez en términos de ciberseguridad, como se refleja en los diversos escenarios generados a partir de las redes originales, es esencial para comprender cómo la implementación efectiva de controles de seguridad puede influir en la propagación del ransomware. Esto resalta la importancia de analizar en detalle la ubicación y la topología de los dispositivos en la red, y cómo estos aspectos interactúan con las estrategias de seguridad. Dicho fenómeno se ilustra claramente en el tiempo requerido (mayor número de iteraciones) y la disminución de equipos infectados a medida que se implementan controles de seguridad. La combinación de medidas de seguridad físicas, lógicas y administrativas, junto con el uso de técnicas de seguridad avanzadas contribuye a una defensa proactiva contra el ransomware.

Esta defensa es igualmente aplicable a organizaciones de todos los tamaños, no importa si la organización es grande o pequeña, todas presentan desafíos únicos. La topología de la red y la ubicación estratégica de los nodos son elementos cruciales en la propagación de amenazas como el ransomware. Un aspecto fundamental para abordar estos riesgos de manera efectiva es la implementación de la microsegmentación en la red. La microsegmentación es una estrategia clave que busca dividir la red en segmentos más pequeños y controlables. Cada segmento tiene políticas de seguridad específicas, lo que reduce drásticamente la superficie de ataque y limita la propagación del ransomware en caso de un compromiso. Además, la aplicación del modelo de seguridad Zero Trust, que implica la verificación continua y la autenticación rigurosa de cada dispositivo y usuario en la red, complementa de manera efectiva la microsegmentación al establecer el enfoque de "nunca confiar, siempre verificar" [35].

La consideración de los aspectos económicos en la implementación de medidas de seguridad emerge como una conclusión fundamental derivada en esta discusión y de los escenarios analizados

en las Tablas 4.9 y 4.10. Aunque la introducción de nuevos controles de seguridad conlleva una disminución en la tasa de infección en la red, se plantea una cuestión esencial: ¿en qué medida resulta efectiva la inversión realizada? La evaluación de soluciones de seguridad no debe basarse únicamente en las capacidades técnicas, sino también en la relación costo-beneficio, la facilidad de gestión y en la capacidad para enfrentar de manera eficaz tanto las amenazas actuales como las emergentes. Con esta perspectiva el Cuadrante de Gartner surge como una herramienta invaluable para la adquisición de tecnologías de ciberseguridad. Este cuadro posiciona a los proveedores de soluciones en función de su capacidad de ejecución y su visión completa, lo que permite a las organizaciones seleccionar las mejores soluciones de ciberseguridad que se alineen mejor con sus necesidades específicas, considerando tanto aspectos técnicos como económicos.

Este análisis junto con los enfoques del MITRE ATT&CK y la aplicación de la Cyber Kill Chain que aporta una visión detallada del ciclo de vida del ciberataque, permiten entender las tácticas, técnicas y procedimientos utilizados por las diversas amenazas en su camino hacia la explotación exitosa y cómo lograr reducir el impacto que representan. Así, la ciberseguridad se transforma en un equilibrio entre inversiones en defensa y los posibles daños causados por amenazas. Por tanto, se hace necesario considerar tanto las pérdidas financieras como las implicaciones en la reputación y la continuidad de la organización ante la toma de decisiones estratégicas en el impacto global de la seguridad.

Conclusiones

El análisis matemático obtenido de analizar el algoritmo PageRank y la centralidad de vector propio proporciona una perspectiva cuantitativa valiosa para identificar los nodos estratégicos en la red, que conforme se fue observando en las redes originales y los controles de seguridad establecidos, las posiciones obtenidas están apegadas a la realidad. Además, la consideración del Cyber Kill Chain permite comprender cómo los ciberatacantes avanzan en sus tácticas, y el uso de herramientas y técnicas específicas para comprometer sistemas. En última instancia, la intersección de estos enfoques en ciberseguridad y teoría de redes proporciona una base sólida para una defensa informada y adaptativa contra las crecientes amenazas de ransomware y otros ataques. De tal manera, se logra un panorama integral para identificar nodos cruciales en la red al utilizar las métricas PageRank y vector propio, lo cual agrega una dimensión matemática y cuantitativa a esta estrategia de ciberseguridad, brindando una visión más completa y fundamentada de la postura de seguridad de una organización. Así, el objetivo del trabajo se cumple, pues se logra medir la propagación del ransomware en la red y el comportamiento que este tiene ante los controles de seguridad implementados, aún más, las posiciones estratégicas obtenidas con la centralidad de vector propio y PageRank resultan tener una similitud apegada a la realidad.

Los resultados muestran medidas que deben ser adoptadas para prevenir y disminuir el impacto del ransomware. Las empresas deben implementar soluciones antivirus actualizadas tipo Next Generation, contar con planes de respuesta a incidentes, implementar la microsegmentación y adoptar el modelo de seguridad Zero Trust. Además, la concientización constante de los empleados sobre las amenazas y la adopción de buenas prácticas de seguridad son cruciales para evitar ataques de ransomware. Asimismo, realizar respaldos regulares puede ser la diferencia entre una rápida recuperación y una larga interrupción operativa en caso de un ataque exitoso.

Para las personas se recomienda mantener un alto nivel de conciencia sobre las amenazas cibernéticas, lo que incluye evitar hacer clic en enlaces sospechosos o descargar archivos de fuentes no confiables. La realización periódica de copias de seguridad de los datos personales y el uso de software antivirus o antimalware son prácticas que pueden reducir significativamente el impacto de un ataque de ransomware.

Respecto al trabajo futuro existen grandes áreas de mejora en este estudio que abren las puertas a seguir profundizando. En primer lugar, agregar restricciones adicionales a las redes, particularmente la implementación de la segmentación que es una barrera fundamental contra el ransomware. En segundo lugar, explorar algoritmos adicionales, como la centralidad de Katz, y la asignación de pesos en la red basados en la criticidad de los equipos. Estos enfoques alternativos podrían enriquecer la identificación de posiciones estratégicas para la implementación de los controles de seguridad. En tercer lugar, a medida que la tecnología en la nube es utilizada por un mayor número de organizaciones, es fundamental centrarse en cómo el ransomware afecta a estos entornos

y adaptar las estrategias de seguridad a estas nuevas tecnologías.

Glosario

En este apartado se muestran las diversas definiciones de las palabras técnicas que serán utilizadas a lo largo del trabajo.

Pruebas de intrusión.- Práctica utilizada para obtener garantías en la seguridad de un sistema informático al intentar comprometer parte o la totalidad de la seguridad de ese sistema, mediante las mismas herramientas y técnicas que podría usar un ciberdelincuente.

Pentester.- Persona encargada de realizar las pruebas de intrusión a los sistemas, aplicaciones y redes informáticas de una empresa.

Vulnerabilidad.- Se refiere a una debilidad en el hardware, software o procedimientos, lo cual permite crear una brecha a través de la cual una amenaza puede obtener acceso a un sistema.

Amenaza.- Se refiere al evento hipotético en el que un atacante utiliza una vulnerabilidad para dañar o destruir un sistema o activo.

Riesgo.- Es la intersección de activos, amenazas y vulnerabilidades, lo que representa el potencial de pérdida, daño o destrucción de un activo cuando una amenaza se aprovecha de una vulnerabilidad.

Hacker ético o pentester.- Es un experto en seguridad que actúa como un intruso malicioso para comprometer un sistema informático y revelar vulnerabilidades a los propietarios. Siempre cuentan con el permiso de la organización que los contrata y, por ende, no cometen ninguna actividad ilegal.

Ciberdelincuente.- Es aquel usuario que busca cometer acciones ilícitas para sacar provecho de los fallos de seguridad de los sistemas informáticos.

Malware.- Es el nombre que se le da a una serie de variantes de software malicioso, incluidos virus, ransomware y spyware. El malware generalmente consiste en un código desarrollado por ciberdelincuentes, diseñado para causar daños extensos a los datos y sistemas o para obtener acceso no autorizado a una red.

Ransomware.- Definición disponible en la sección 1.2.

Fuga de datos.- Es la pérdida de confidencialidad de la información, mediante la obtención de la misma o el conocimiento del contenido de esta por parte de personas no autorizadas para ello.

Red física.- Se refiere a las conexiones físicas e identifica cómo se interconectan los dispositivos finales y de infraestructura, como los routers, los switches y los puntos de acceso inalámbrico.

Red lógica.- Se refiere a la forma en que una red transfiere tramas de un nodo al siguiente.

Virus.- Es un programa en las computadoras que puede copiarse a sí mismo e infectar una computadora sin permiso o conocimiento del usuario. Un virus puede corromper o eliminar datos

en una computadora, usar programas de correo electrónico para propagarse a otras computadoras e inclusive borrar todo en un disco duro.

Backdoor.- Se refiere a cualquier método mediante el cual los usuarios autorizados y no autorizados pueden eludir las medidas de seguridad normales como flujos de autenticación y obtener acceso de usuario de alto nivel en un sistema, red o aplicación.

Hacking.- Se refiere al uso indebido de dispositivos como computadoras, teléfonos inteligentes, tabletas y redes para dañar o corromper sistemas, recopilar información sobre los usuarios, robar datos y documentos o interrumpir la actividad relacionada con los datos.

Terminales Tenex.- También conocida como tcsh, es un terminal de UNIX basado y compatible con la terminal C (csh) sobre la cual ofrece muchas mejoras para el usuario.

Troyanos.- Es un programa que contiene código malicioso oculto que logra evadir los mecanismos de seguridad al aprovechar la autorización legítima de un usuario o entidad del sistema que invoca el programa.

Ciberespionaje.- Es un ataque malicioso donde un usuario no autorizado intenta acceder a datos confidenciales o de propiedad intelectual con el fin de poder utilizarlos para crear una ventaja competitiva o vender para obtener ganancias financieras.

Virus en macros.- Es un tipo de virus que está escrito en macro, un lenguaje de programación enfocado para aplicaciones de software como Microsoft Office. Este lenguaje de programación es útil porque permite a los usuarios automatizar tareas con unas pocas pulsaciones de teclas y mejorar el flujo de trabajo.

Software.- Es un programa informático generalmente en memoria de sólo lectura (ROM) o memoria de sólo lectura programable (PROM), de modo que los programas y datos no se pueden escribir o modificar dinámicamente durante la ejecución de los programas.

Hardware.- Son aquellos componentes físicos o materiales que forman una computadora o un sistema informático.

Phishing.- Es un tipo de ataque durante el cual un usuario malintencionados envía mensajes haciéndose pasar por una persona o entidad de confianza. Los mensajes de phishing manipulan a un usuario, lo que hace que realice acciones como instalar un archivo malicioso, hacer clic en un enlace malicioso o divulgar información confidencial, como contraseñas. El phishing es el tipo más común de ingeniería social, que es un término general que describe los intentos de manipular o engañar a los usuarios de computadoras.

URL.- Es el significado de localizador uniforme de recursos el cual es una dirección que hace referencia a un objeto en Internet.

Dirección IP.- Es un número que se asigna a cada dispositivo conectado a una red que utiliza el protocolo de Internet. La dirección IP se utiliza para identificar y comunicarse con dispositivos en la red.

Número AS.- Es un número único que se asigna a un sistema autónomo en una red de computadoras. Un sistema autónomo es un conjunto de dispositivos y redes que están bajo el control de una misma entidad administrativa y que utilizan un protocolo de enrutamiento común para intercambiar información y tráfico de red.

Sandboxing.- Una sandbox es un sistema que permite que una aplicación que no es de confianza, se ejecute en un entorno altamente controlado donde los permisos de la aplicación están

restringidos. En particular, una aplicación en un sandbox generalmente tiene restringido el acceso al sistema de archivos o la red.

Directorio Activo.- Es un servicio de directorio de Microsoft utilizado para la gestión de recursos en una red de computadoras. El Directorio Activo se utiliza como una herramienta importante para la gestión de la identidad y los accesos en una organización.

Táctica.- Describe los objetivos técnicos inmediatos (el "qué") que los atacantes intentan lograr, como obtener acceso inicial, o mantener la persistencia. Invariablemente, los atacantes deben usar múltiples tácticas para completar con éxito un ataque.

Técnica.- Describe el "cómo" son los métodos que utilizan los atacantes para lograr una táctica. Todas las tácticas en cada matriz tienen múltiples técnicas. Un ejemplo de esto es la técnica de phishing que utilizan los atacantes para obtener acceso inicial (una táctica). Las tres subtécnicas asociadas al phishing son el archivo adjunto de spearphishing, el enlace de spearphishing y el spearphishing a través de un servicio.

Procedimientos.- Describe las implementaciones específicas de las técnicas y subtécnicas que han utilizado las APT, o puede referirse a malware específico u otras herramientas que han utilizado los atacantes.

Adversario.- Es una entidad que intenta atacar o comprometer un sistema o red de computadoras.

Apéndice A

Código

Este apéndice muestra el código desarrollado para simular el ransomware WannaCry, esta compuesto por tres archivos distintos donde cada uno de estos se encarga de realizar una macrotarea. El primer archivo calcula la probabilidad de que un nodo se infecte o no, por su parte el segundo grafica la red y da una representación visual al usuario y, por último, el tercer archivo simula el comportamiento del ransomware e invoca a las funciones de los otros dos archivos. Para tener una mayor comprensión de las funciones se dividirá cada archivo en las microtareas que los componen y, para conjuntar el archivo original, basta unirlas en el orden que aparecen.

A.1. Código Para Calcular Probabilidades

Este código tiene como meta calcular la probabilidad de que un nodo se infecte o no, para tal motivo se consideran tres tipos distintos de probabilidades:

- probabilidad de que el antivirus o un control instalado en el equipo de un usuario bloquee el ransomware.
- probabilidad de que un control implementado en el segmento o grupo al que pertenece el usuario bloquee el ataque.
- probabilidad de que el ransomware sea detenido, mientras se propaga en la red por los controles preventivos y detectivos, de preferencia tipo firewall.

A.1.1. Probabilidad Grupo

```
1 import numpy
2 import sys
3 import networkx as nx
4 from generador_graficas import create_graph
5 sys.path.append("ruta absoluta al directorio donde se encuentren
6 los otros códigos")
7
8 #Variables globales
9 Soc="Yes"
```

```
AV="NG"
FW="NG"

#La siguiente función identifica cuántos grupos existen en la red
def grupos_red(G):
        grupos = []
        for node,attr in G.nodes(data=True):
            if attr["Grupo"] not in grupos:
                grupos.append(attr["Grupo"])
        return grupos

#proba_grupo() permite conocer la probabilidad de infectar un equipo dentro de un grupo
def proba_grupo(G,grupos):
    diccionario = {}
    for i in grupos:
        counter = 1
        lista = [node for node,attr in G.nodes(data=True) if
        attr['Grupo'] == i]
        for j in lista:
            if G.nodes[j]["Categorizacion"] in ['NIDS','SIEM']:
                counter += 1
        n = numpy.random.uniform(0,0.9)
        diccionario[i] = n**(1/counter)
    #print(diccionario)
    return diccionario
```

A.1.2. Probabilidad General

```
#La función proba_general es clave, ya que determina si un nodo vulnerable se infecta del ransomware o no. Esta compuesta por  funciones anidadas donde cada una esta asociada a las tres probabilidades que serán tomadas en cuenta y fueron enunciadas en un principio.

def proba_general(nodo_analizar, nodo_atacante):
    print('nodo atacante es: ',nodo_atacante)
    print('nodo analizado: ' , nodo_analizar)

    #Los siguientes valores son las ponderaciones que se les da a las clasificaciones de los controles para calcular cuánta protección brindan ante el ransomware; a mayor valor, mayor relevancia.
    w_infecteduser = 1.4
    w_infectedpath = 1.1
    w_probagrupo = 0.50
    G = create_graph()

    #Esta función permite obtener una probabilidad ante la presencia  de controles de seguridad instalados en el equipo o sistema.
    def infected_user(nodo_vulnerable):
        proba_equipo = numpy.random.uniform(0,0.10)
        if G.nodes[nodo_vulnerable]['Defensa'] in ['IDS','Antimalware']:
            proba_equipo = numpy.random.uniform(0,0.50)
        elif G.nodes[nodo_vulnerable]['Defensa'] in ['Antivirus']
        and AV=="NG":
```

```
20              proba_equipo = numpy.random.uniform(0.25,0.80)
21          elif G.nodes[nodo_vulnerable]['Defensa'] in ['Antivirus']
22          and AV=="Tr":
23              proba_equipo = numpy.random.uniform(0,0.40)
24          return proba_equipo
25
26      #Esta función determina si es posible infectar un nodo vulnerable  desde un
            nodo infectado, tomando en cuenta el total de controles de seguridad
        que debe evadir hasta llegar a su destino.
27      def path_infected(nodo_infectado, nodo_vulnerable):
28          path = nx.shortest_path(G, nodo_infectado, nodo_vulnerable)
29          m = 0
30          n = 0
31          #print(path)
32          for i in path:
33              if G.nodes[i]['Categorizacion'] in ["IPS"] and m < 9:
34                  m += 1
35              elif G.nodes[i]['Categorizacion'] in ["Firewall"]
36              and n <= 9 and FW=="NG":
37                  n += 2
38              elif G.nodes[i]['Categorizacion'] in ["Firewall"]
39              and n <= 9 and FW=="Tr":
40                  n += 1
41              else:
42                  proba_total = numpy.random.uniform(0,0.25)
43
44          min_proteccion = float("."+str(n)+str(m))
45          proba_total = numpy.random.uniform(min_proteccion,0.99)
46          return proba_total
47
48      #Esta función conjunta las 3 probabilidades anteriormente calculadas y con
            un promedio ponderado calcula la     probabilidad final de que el nodo
            se infecte, en caso  de que el SOC este presente la probabilidad final
            también aumenta.
49      def probabilidad_total(proba_user, proba_ruta,proba_grupos,
50      nodo_analizar):
51          pg = proba_grupos[G.nodes[nodo_analizar]['Grupo']]
52          proba_final = ((w_infecteduser*proba_user) +
53          (w_infectedpath*proba_ruta) + (w_probagrupo*pg))
54          /(w_infectedpath + w_infecteduser + w_probagrupo)
55          if Soc == "Yes":
56              proba_final = proba_final * 1.10
57          return proba_final
58
59      #Para cada nodo vulnerable que pueda ser alcanzado por el nodo  infectado,
            se calcula la probabilidad de que se infecte.
60      proba_usuario = infected_user(nodo_analizar)
61      proba_ruta = path_infected(nodo_analizar,nodo_atacante)
62      grupos_totales = grupos_red(G)
63      probabilidades_grupos = proba_grupo(G,grupos_totales)
64      p = probabilidad_total(proba_usuario,proba_ruta,
65      probabilidades_grupos,nodo_analizar)
66      print("Proba Total: ", p, "\n")
67      return p
```

A.2. Código Para Generar las Redes

Este código tiene como meta leer dos archivos txt con la información de los nodos y las aristas para generar las redes. De acuerdo al estado del nodo (infectado, vulnerable y no vulnerable) asigna un color y hace la distinción visual para el usuario.

A.2.1. Creación de la Red

```
from itertools import combinations, groupby
import matplotlib.pyplot as plt
import networkx as nx
from numpy import  random
import time
from random import sample

#La siguiente función lee los archivos txt e itera sobre las líneas para ir construyendo la red
def create_graph(path="ruta absoluta al directorio donde se encuentren los archivos txt con la información de los nodos y las aristas"):
    G=nx.Graph()
        #Esta primer parte lee el archivo con las características e información de los nodos.
        with open(path+"archivo-nodos.txt",encoding = 'utf-8') as ff:
        next(ff)
        for nodes in ff:
            nodo=nodes.rstrip("\n").split(";")
            #Se crea un nodo y se le asignan sus características
            G.add_node(nodo[0], Grupo=nodo[1].strip(),
                Categorizacion=nodo[2].strip(),
                Hardware=nodo[3].strip(), Estado=nodo[4].strip(),
                Seguridad=nodo[5].strip(), Defensa=nodo[6].strip())
    #Esta parte agrega las aristas a la red
    with open(path+"archivo-aristas.txt",encoding = 'utf-8') as f:
        for edge in f:
            ruta = edge.rstrip("\n").split(" ")
            G.add_edge(ruta[0],ruta[1])
```

A.2.2. Coloración de los Nodos

```
#Una vez generada la gráfica, aleatoriamente se selecciona un grupo de nodos para ser vulnerables
    elementosafectados_poisson = random.poisson(20)
    while elementosafectados_poisson > 0:
        node = sample(list(G.nodes()),1)
        n = random.uniform(0,1)
        #Como solo ciertos equipos en una red pueden infectados, se
        excluyen aquellos que no podrían ser vulnerables
        if G.node[node[0]]["Hardware"] not in
        ["Internet", "Firewall", "Hub", "Router", "Switch", "NID", "IPS",
        "SIEM"] and n > 0.6
        and elementosafectados_poisson > 0:
```

```
            G.node[node[0]]["Seguridad"] = "Vulnerable"
            elementosafectados_poisson -= 1
    return G
```

A.2.3. Impresión de la Red

```
#La siguiente función genera de manera visual la red.
def plotting(G):
    fig = plt.figure(1, figsize=(31,31), dpi=130)
    color_map = ['red' if attr['Estado'] == "Infectado" else 'yellow'
                 if attr["Seguridad"] == "Vulnerable" else "green"
                 for node,attr in G.nodes(data=True)]
    nx.draw(G, node_color=color_map, node_size=850,
            edge_color='#00bb5e',width=2.5, edge_cmap=plt.cm.Blues,
            with_labels=True,font_size=20)
    plt.show()
```

A.3. Simulación del Ransomware

Este código representa la simulación del ransomware WannaCry, parte de la etapa inicial de reconocimiento de equipos en la red, hasta la explotación para comprometer un sistema. Empieza seleccionando aleatoriamente un nodo infectado inicial y tiene dos formas de detenerse, la primera al infectar todos los nodos vulnerables y la segunda al ser detectado después de un cierto tiempo definido por el usuario.

A.3.1. Condiciones Atmosféricas

```
import sys
import pandas as pd
from generador_graficas import create_graph,plotting
from probabilidades import proba_general, aux_valores
from collections import deque
from random import sample
import networkx as nx
sys.path.append("ruta absoluta al directorio donde se encuentren  los otros có
    digos")

#La siguiente función conjunta aquellos nodos con los que el nodo i se comunica
     y los guarda en un diccionario.
def add_edge(G):
        adj = [[] for i in range(len(G.edges())+1)]
    dict_mapeo = { list(G.nodes)[i]:i for i in range(0, len(G.nodes))}
    for v,w in G.edges():
        adj[dict_mapeo.get(v)].append(w)
        adj[dict_mapeo.get(w)].append(v)
    return adj, dict_mapeo

#La siguiente función auxiliar agrega múltiples valores en un
```

```
diccionario de la llave dada.
def add_values_in_dict(sample_dict, key, list_of_values):
        if key not in sample_dict:
        sample_dict[key] = list()
        sample_dict[key].extend(list_of_values)
    return sample_dict

#La siguiente función se complementa con el algoritmo BFS y es clave para
   simular el esparcimiento del ransomware, empieza generando la red G,
   enseguida obtiene los nodos que pueden comunicarse con otros y marca
   aquellos que ya han sido visitados al igual que verifica cuáles son los
   vulnerables y empieza la infección en un nodo aleatoriamente.
def worm_ransomware(probabilidad=0.60):
    #El valor de la variable probabiliad controla la simulación de las
    condiciones atmosféricas; 0.6 a favor de los ciberdelicuentes y 0.5
    a favor de la ciberseguridad.
    G = create_graph()
    adj, mapeo = add_edge(G)
    visited_node = [0 for i in range(len(G.edges())+1)]
    vulnerable_nodes = [node for node,attr in G.nodes(data=True)
                        if attr["Hardware"] not in ["Internet",
                        "Router", "Switch", "Firewall", "NIDS"]
                        and attr["Seguridad"] in ["Vulnerable"]]
    infected_nodes = sample(vulnerable_nodes,1)
    G.nodes[infected_nodes[0]]['Estado'] = "Infectado"
    plotting(G)
```

A.3.2. Algoritmo BFS

```
#La siguiente función forma parte del algoritmo BFS utilizado para obtener los
   nodos alcanzables dado un nodo
    def BFS_operation(component_num, src):
        queue = deque()
        queue.append(src)
        visited_node[src] = 1
        reachableNodes = []
        while (len(queue) > 0):
            u = queue.popleft()
            reachableNodes.append(u)
            for itrs in adj[u]:
                itr = mapeo.get(itrs)
                if (visited_node[itr] == 0):
                    visited_node[itr] = 1
                    queue.append(itr)
        return reachableNodes

    #La siguiente función muestra al usuario los nodos alcanzables
    partiendo de un nodo.
    def displayReachableNodes(m):
        for i in m:
            print(i, end = " ")
        print()

    #La siguiente función verifica si un nodo puede alcanzar a otro
```

```
    def findReachableNodes(my_list, n):
        a = []
        reachable_dict = {}
        component_num = 0
        for i in range(n):
            u = my_list[mapeo.get([k for k in mapeo.keys()
            if mapeo[k] == i][0])]
            v = mapeo.get(u)
            if (visited_node[v] == 0):
                component_num += 1
                a = BFS_operation(component_num, v)
            add_values_in_dict(reachable_dict,u,a)
        return a, reachable_dict
```

A.3.3. Núcleo de la Simulación

```
#Esta función conjunta las funciones auxiliares definidas previamente  e invoca
    las funciones creadas en los otros documentos. Es el núcleo     de la
   simulación para el ransomware.
    def infection(reachable_dict,infected_nodes):
        #La variable T representa el tiempo que toma en ser detectado el
           ransomware, en caso de que T sea igual a un valor dado por el
           usuario la variable booleana "bandera" cambia su valor a false   y
           el algoritmo termina.
        T = 0
        bandera = True
        while bandera == True:
            #En el siguiente ciclo, para cada nodo infectado se verifica si aún
                hay nodos vulnerables y si aún hay tiempo para infectar equipos
                .
            for i in infected_nodes:
                if len(infected_nodes) < len(vulnerable_nodes) and T < 10:
                    rea_nodos = reachable_dict.get(i)
                    #Sobre cada nodo que pueda ser alcanzado por el nodo
                       infectado, se verifica si se puede infectar, para esto
                       se calcula una probabilidad y en caso de ser menor al
                       valor definido por el usuario el nodo se infecta y se
                       agrega a la lista de nodos infectados
                    for j in rea_nodos:
                        nodo_analizado = [k for k in mapeo.keys()
                        if mapeo[k] == j][0]
                        if G.node[nodo_analizado]["Seguridad"] ==
                        "Vulnerable" and G.node[nodo_analizado]["Hardware"]
                        not in ["Internet", "Firewall", "Hub", "Router",
                        "Switch", "NID", "IPS", "SIEM"] and
                        nodo_analizado not in infected_nodes:
                            p = proba_general(nodo_analizado,i)
                            if p <= probabilidad and nodo_analizado in
                            vulnerable_nodes:
                                  G.nodes[nodo_analizado]['Estado'] =
                                  "Infectado"
                                  if nodo_analizado not in infected_nodes:
                                      infected_nodes.append(nodo_analizado)
                    T += 1
```

```
28                  else:
29                      bandera = False
30                      break
31
32          if len(infected_nodes) == len(vulnerable_nodes):
33              print("Se infectaron todos los nodos vulnerables")
34          elif T>=10:
35              print("Detectaron el ataque")
36          else:
37              print("Ya no se pueden infectar mas nodos")
38
39          print('\n')
40          return T
41
42      arr_len = len(vulnerable_nodes)
43      a, reachable_dict = findReachableNodes(vulnerable_nodes, arr_len)
44      tiempos_infeccion = infection(reachable_dict,infected_nodes)
45      plotting(G)
46      return len(infected_nodes), len(vulnerable_nodes),
47      tiempos_infeccion, probabilidad
```

Apéndice B

Nodos

Los nodos utilizados a lo largo de la simulación cuentan con varias características útiles para la lógica del programa. Las características y categorías definidas para cada nodo se encuentran a continuación.

- Nombre. - designa y distingue los nodos en la red.
- Grupo. - representa el área o departamento de la empresa en la que se encuentra el nodo.
- Hardware. - representa el tipo de componente físico al cual corresponde el nodo.
- Categorización. - conjunta los nodos con aquellos en los que comparta el mismo hardware y/o que están asignados a la misma tarea.
- Estado. - define si un nodo está infectado o es seguro.
- Seguridad. - especifica si el nodo es vulnerable o no vulnerable.
- Defensa. - establece el control de seguridad con el que cuenta un equipo.

Enseguida se muestran los nodos definidos para cada una de las redes utilizadas en su forma original.

Tabla B.1: Nodos de la primera red.

Nombre	Grupo	Categorización	Hardware	Estado	Seguridad	Defensa
Internet	Internet	Internet	Internet	Seguro	No vulnerable	No
Router-Firewall	General	Router-Firewall	Router	Seguro	No vulnerable	No
Ethernet1	General	Routers	Router	Seguro	No vulnerable	No
Ethernet2	General	Routers	Router	Seguro	No vulnerable	No
Servidor	General	Servidores	Servidor	Seguro	No vulnerable	No
Switch-Administradores	Generall	Switches	Switch	Seguro	No vulnerable	No
Switch-Classroom1	General	Switches	Switch	Seguro	No vulnerable	No
Switch-Classroom2	General	Switches	Switch	Seguro	No vulnerable	No
Switch-Classroom3	General	Switches	Switch	Seguro	No vulnerable	No
MailServer	General	Servidores	Servidor	Seguro	No vulnerable	No
192.168.2.1	General	Usuarios	PC	Seguro	No vulnerable	No
WebServer	General	Servidores	Servidor	Seguro	No vulnerable	No
FileServer	General	Servidores	Servidor	Seguro	No vulnerable	No
192.168.2.2	General	Usuarios	PC	Seguro	No vulnerable	No
192.168.2.3	General	Usuarios	PC	Seguro	No vulnerable	No
192.168.2.4	General	Usuarios	PC	Seguro	No vulnerable	No
192.168.2.5	General	Usuarios	PC	Seguro	No vulnerable	No
192.168.2.6	General	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.1	General	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.2	General	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.3	General	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.4	General	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.5	General	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.6	General	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.7	General	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.8	General	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.9	General	Usuarios	PC	Seguro	No vulnerable	No
Printer	General	Impresoras	Impresoras	Seguro	No vulnerable	No
Firewall1	General	Firewall	Firewall	Seguro	No vulnerable	No
Firewall2	General	Firewall	Firewall	Seguro	No vulnerable	No
SIEM	General	SIEM	SIEM	Seguro	No vulnerable	No

Tabla B.2: Nodos de la segunda red.

Nombre	Grupo	Categorización	Hardware	Estado	Seguridad	Defensa
Internet	Internet	Internet	Internet	Seguro	No vulnerable	No
Border-Router	NA	Routers	Router	Seguro	No vulnerable	No
Hub	DMZ	Hubs	Hub	Seguro	No vulnerable	No
NIDS-Promiscuos1	DMZ	NIDS	NID	Seguro	No vulnerable	No
Firewall-External	NA	Firewall	Firewall	Seguro	No vulnerable	No
Switch1	NA	Switches	Switch	Seguro	No vulnerable	No
Switch2	NA	Switches	Switch	Seguro	No vulnerable	No
Switch3	Client Subnet	Switches	Switch	Seguro	No vulnerable	No
Switch4	Management Subnet	Switches	Switch	Seguro	No vulnerable	No
Switch5	Application Subnet	Switches	Switch	Seguro	No vulnerable	No
WebServer1	Screened-Subnet	Servidores	Servidor	Seguro	No vulnerable	No
MailRelay1	Screened-Subnet	Servidores	Servidor	Seguro	No vulnerable	No
DNSServer1	Screened-Subnet	Servidores	Servidor	Seguro	No vulnerable	No
NIDS-Promiscuos2	Screened-Subnet	NIDS	NID	Seguro	No vulnerable	No
SystemMgmt	Management Subnet	Servidores	Servidor	Seguro	No vulnerable	No
192.168.1.149	Management Subnet	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.139	Client Subnet	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.140	Client Subnet	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.141	Client Subnet	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.142	Client Subnet	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.143	Client Subnet	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.144	Client Subnet	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.145	Client Subnet	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.146	Client Subnet	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.147	Client Subnet	Usuarios	PC	Seguro	No vulnerable	No
192.168.1.148	Client Subnet	Usuarios	PC	Seguro	No vulnerable	No
DNSServer2	Shared Services Subnet	Servidores	Servidor	Seguro	No vulnerable	No
MailServer2-Antivirus	Shared Services Subnet	Servidores	Servidor	Seguro	No vulnerable	Antivirus
FileandPrint	Shared Services Subnet	Servidores	Servidor	Seguro	No vulnerable	No
WebServer2	Shared Services Subnet	Servidores	Servidor	Seguro	No vulnerable	No
NIDS-Promiscuos3	Shared Services Subnet	NIDS	NID	Seguro	No vulnerable	No
Firewall-Internal	Application Subnet	Firewall	Firewall	Seguro	No vulnerable	No
ApplicationServer	Application Subnet	Servidores	Servidor	Seguro	No vulnerable	IDS
DatabaseServer	Application Subnet	Servidores	Servidor	Seguro	No vulnerable	IDS
NIDS-Promiscuos4	Application Subnet	NIDS	NID	Seguro	No vulnerable	No

Tabla B.3: Nodos de la tercera red.

Nombre	Grupo	Categorización	Hardware	Estado	Seguridad	Defensa
Internet	Internet	Internet	Internet	Seguro	No vulnerable	NA
Cisco-Router1	Corporativo	Routers	Router	Seguro	No vulnerable	NA
Siem	Corporativo	Siem	Siem	Seguro	No vulnerable	Antivirus
Cisco-Firewall1	Corporativo	Firewall	Firewall	Seguro	No vulnerable	NA
Servidor-Camaras	Corporativo	Servidores	Servidor	Seguro	No vulnerable	Antivirus
BD-Server1	Corporativo	Servidores	Servidor	Seguro	No vulnerable	Antivirus
BD-Server2	Corporativo	Servidores	Servidor	Seguro	No vulnerable	Antivirus
Switch1	Corporativo	Switches	Switch	Seguro	No vulnerable	NA
Switch2	Corporativo	Switches	Switch	Seguro	No vulnerable	NA
Switch3	Corporativo	Switches	Switch	Seguro	No vulnerable	NA
NIDS1	Corporativo	NIDS	NID	Seguro	No vulnerable	Antivirus
NIDS2	Corporativo	NIDS	NID	Seguro	No vulnerable	Antivirus
Web-Server1	Corporativo	Servidores	Servidor	Seguro	No vulnerable	Antivirus
10.20.10.10	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.11	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.12	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.13	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.14	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.15	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.16	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.40	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.41	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.42	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.43	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.44	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.45	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.46	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.47	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.48	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.60	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.61	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.62	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.63	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.64	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.65	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.66	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.67	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.68	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.69	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.10.70	Corporativo	Usuarios	PC	Seguro	No vulnerable	Antivirus
Cisco-Router2	CDs	Routers	Router	Seguro	No vulnerable	NA
Switch4	CDs	Switches	Switch	Seguro	No vulnerable	NA
BD-Server3	CDs	Servidores	Servidor	Seguro	No vulnerable	Antivirus
10.20.20.30	CDs	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.20.31	CDs	Usuarios	PC	Seguro	No vulnerable	Antivirus

Tabla B.4: Nodos de la tercera red.

Nombre	Grupo	Categorización	Hardware	Estado	Seguridad	Defensa
10.20.20.32	CDs	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.20.33	CDs	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.20.34	CDs	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.20.35	CDs	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.20.36	CDs	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.20.37	CDs	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.20.38	CDs	Usuarios	PC	Seguro	No vulnerable	Antivirus
Cisco-Router3	SSI	Routers	Router	Seguro	No vulnerable	NA
Switch5	SSI	Switches	Switch	Seguro	No vulnerable	NA
BD-Server4	SSI	Servidores	Servidor	Seguro	No vulnerable	Antivirus
10.20.30.50	SSI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.30.51	SSI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.30.52	SSI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.30.53	SSI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.30.54	SSI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.30.55	SSI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.30.56	SSI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.30.57	SSI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.30.58	SSI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.30.59	SSI	Usuarios	PC	Seguro	No vulnerable	Antivirus
Cisco-Firewall2	SCI	Firewall	Firewall	Seguro	No vulnerable	NA
Switch6	SCI	Switches	Switch	Seguro	No vulnerable	NA
Web-Server2	SCI	Servidores	Servidor	Seguro	No vulnerable	Antivirus
BD-Server5	SCI	Servidores	Servidor	Seguro	No vulnerable	Antivirus
10.20.40.10	SCI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.40.11	SCI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.40.12	SCI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.40.13	SCI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.40.14	SCI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.40.15	SCI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.40.16	SCI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.40.17	SCI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.40.18	SCI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.40.19	SCI	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.40.20	SCI	Usuarios	PC	Seguro	No vulnerable	Antivirus
Cisco-Firewall3	Call-Center	Firewall	Firewall	Seguro	No vulnerable	NA
Switch7	Call-Center	Switches	Switch	Seguro	No vulnerable	NA
BD-Server6	Call-Center	Servidores	Servidor	Seguro	No vulnerable	Antivirus
NIDS3	Call-Center	NIDS	NID	Seguro	No vulnerable	Antivirus
Web-Server3	Call-Center	Servidores	Servidor	Seguro	No vulnerable	Antivirus
10.20.0.20	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.0.21	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.0.22	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.0.23	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus

Tabla B.5: Nodos de la tercera red.

Nombre	Grupo	Categorización	Hardware	Estado	Seguridad	Defensa
10.20.0.24	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.0.25	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.0.26	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.0.27	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.0.28	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.0.29	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.0.30	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.0.31	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.0.32	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.0.33	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.0.34	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus
10.20.0.35	Call-Center	Usuarios	PC	Seguro	No vulnerable	Antivirus

Apéndice C

Lista de Acrónimos

Acrónimo	Significado
ARPANET	Advanced Research Projects Agency Network (Red de la Agencia de Proyectos de Investigación Avanzada)
ATTA&CK	Adversarial Tactics, Techniques, and Common Knowledge (Tácticas, Técnicas y Conocimiento Común Adversario)
BFS	Breadth-First Search (Búsqueda en Amplitud)
CISPP	Certified Information Systems Security Professional (Profesional Certificado en Seguridad de Sistemas de Información)
CVSS	Common Vulnerability Scoring System (Sistema Común de Puntuación de Vulnerabilidades)
DLS	Dynamic Link Library Services (Servicios de Biblioteca de Enlaces Dinámicos)
DOD	Department of Defense (Departamento de Defensa)
FIFO	First In, First Out (Primero en Entrar, Primero en Salir)
HTTPS	Hypertext Transfer Protocol Secure (Protocolo de Transferencia de Hipertexto Seguro)
IDS	Intrusion Detection System (Sistema de Detección de Intrusiones)
IOA	Indicator of Attack (Indicador de Ataque)
IPS	Intrusion Prevention System (Sistema de Prevención de Intrusiones)
ISC	Information Security Controls (Controles de Seguridad de la Información)
LIFO	Last In, First Out (Último en Entrar, Primero en Salir)

MIT	Massachusetts Institute of Technology (Instituto Tecnológico de Massachusetts)
NIST	National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología)
PROM	Programmable Read-Only Memory (Memoria de Solo Lectura Programable)
PYMES	Pequeñas y Medianas Empresas (Small and Medium-sized Enterprises)
RAAS	Ransomware as a Service (Ransomware como Servicio)
ROM	Read-Only Memory (Memoria de Solo Lectura)
SIEM	Security Information and Event Management (Gestión de Información y Eventos de Seguridad)
SOC	Security Operations Center (Centro de Operaciones de Seguridad)
SSL	Secure Sockets Layer (Capa de Conexiones Seguras)
TLS	Transport Layer Security (Seguridad en la Capa de Transporte)
TI	Information Technology (Tecnologías de la Información)

Bibliografía

[1] DoD 5200.28-STD. *Trusted Computer System Evaluation Criteria*. Dod Computer Security Center, 26 de Diciembre de 1985. `https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf`.

[2] Cisco Networking Academy. Introduction to networks. http://cisco.num.edu.mn/CCNA_R&S1, Enero del 2020. Consultado el 10 de enero del 2022.

[3] Maxat Akbanov and Vassilios Vassilakis. Wannacry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. *Journal of Telecommunications and Information Technology*, 1:113–124, 04 2019. doi: 10.26636/jtit.2019.130218.

[4] Gerald Alexanderson. About the cover: Euler and the königsberg bridges: A historical view. *Bulletin (New Series) of the American Mathematical Society*, 43:567–573, 10 2006. doi: 10.1090/S0273-0979-06-01130-X.

[5] William C. Barker, William Fisher., Karen Scarfone, and Murugiah Souppaya. *Ransomware Risk Management: A Cybersecurity Framework Profile*. NIST, Febrero del 2022. `https://doi.org/10.6028/NIST.IR.8374`.

[6] Albert-László Barábasi. Network science by albert-laszlo barabási. https://networksciencebook.com/, 2014. Consultado el 24 de marzo del 2023.

[7] John A. Bondy and Murty U. S. R. *Graph Theory with Applications*. Elsevier, New York, 1976.

[8] Kevin Collier. Baby died because of ransomware attack on hospital. https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465, 30 de sSeptiembre del 2021. Consultado el 29 de Diciembre del 2021.

[9] Linda Comerford. Why small businesses are vulnerable to cyberattacks. https://www.securitymagazine.com/blogs/14-security-blog/post/97694-why-small-businesses-are-vulnerable-to-cyberattacks, 25 de Mayo del 2022. Consultado el 02 de enero del 2023.

[10] Crowdstrike. History of ransomware. https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware, 08 de Enero del 2021. Consultado el 07 de Enero del 2022.

[11] Crowdstrike. 5 most common types of ransomware. https://www.crowdstrike.com/cybersecurity-101/ransomware/types-of-ransomware/, 24 de Mayo del 2021. Consultado el 07 de Enero del 2022.

[12] Jeremy D'Hoinne, Adams Hils, and Rajpreet Kaur. Magic quadrant for network firewalls. https://www.gartner.com/en/documents/3992870/, Noviembre del 2020. Consultada el 03 de mayo del 2023.

[13] Paul Erdös and Alfréd Rényi. On random graphs i. *Publicationes Mathematicae Debrecen*, 6: 290–297, 1959.

[14] David Gilmour. Meet john draper, the hacker who inspired apple's founders. https://www.dailydot.com/layer8/john-draper-captain-crunch/, 22 de Mayo del 2022. Consultado el 02 de septiembre del 2022.

[15] GReAT. 1970s. https://encyclopedia.kaspersky.com/knowledge/years-1970s/, 6 de diciembre del 2013. Consultado el 01 de septiembre del 2022.

[16] Pete Herzog. *The Open Source Security Testing Methodology Manual v3*. ISECOM, 14 de Diciembre del 2010.

[17] Nick Huss. How many websites are there around the world? https://siteefy.com/how-many-websites-are-there/, 16 de Febrero del 2023. Consultado el 20 de marzo del 2023.

[18] Infosec. Understanding control frameworks and the cissp. https://resources.infosecinstitute.com/certification/understanding-cissp-control-frameworks/, 12 de Mayo del 2017. Consultado el 01 de marzo del 2023.

[19] Stan Jenkins. Secure network architecture: Best practices for small business and government entities. In *SANS Institute*, pages 3–4, 2003.

[20] Amy N. Langville and Carl D. Meyer. *Google's PageRank and beyond, the science of search engine rankings*. Princeton Univ. Press, 2006.

[21] Steven Levy. *Hackers: Heroes of the Computer Revolution*. Anchor Press/Doubleday, 1984. ISBN 9780385191951. URL `https://books.google.com.mx/books?id=o3YfAQAAIAAJ`.

[22] John Leyden. Arpanet anniversary: The internet's first transmission was sent 50 years ago today. https://portswigger.net/daily-swig/arpanet- anniversary-the-internets-first-transmission-was-sent-50-years-ago- today, 29 de Octubre del 2019. Consultado el 12 de enero del 2023.

[23] Martin Lockheed. The cyber kill chain®. *Lockheed Martin Corporation*, 2011. URL `https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html`. Consultado el 20 de Septiembre del 2023.

[24] Martin Lockheed. Seven ways to apply the cyber kill chain® with a threat intelligence platform [pdf]. *Lockheed Martin Corporation*, 2015. URL `https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf/`. Consultado el 20 de Diciembre del 2022.

[25] David McCandless. World's biggest data breaches & hacks. https://www.informationisbeautiful.net /visualizations/worlds-biggest-data-breaches-hacks/, Jun 2022. Consultado el 20 de Julio del 2022.

[26] Stanley Milgram. The Small-World Problem. *Psychology Today*, 1(1):61–67, 1967.

[27] Mitre. Matrix - enterprise. https://attack.mitre.org/matrices/enterprise/, Abril del 2022. Consultada el 03 de mayo del 2023.

[28] Eduardo Ugalde Nava. *El Arte de la Guerra SUN TZU Seguridad en las Tecnologías Informáticas*. Qm Editorial, 22 septiembre 2022.

[29] Mark Newman. *Networks: an introduction*. Oxford University Press, Oxford; New York, 2010.

[30] John J. O' Connor and Edmund F. Robertson. Gustav kirchhoff - biography. https://mathshistory.st-andrews.ac.uk/Biographies/Kirchhoff/, Agosto del 2022. Consultado el 17 de julio del 2022.

[31] Daniel Page. *Advanced data structures: An introduction to data structures and algorithms*. PageWizard Games, Learning & Entertainment., 2020.

[32] Maritz Pieter and Mouton Sonja. *Francis Guthrie: A Colourful Life*. Math Intelligencer 34, 2012. URL `https://doi.org/10.1007/s00283-012-9307-y`.

[33] Purplesec. Cyber security statistics the ultimate list of stats data, & trends for 2023, Julio del 2022. `https://purplesec.us/resources/cyber-security-statistics/`,Consultada el 01 de septiembre del 2022.

[34] William Ralston. The untold story of a cyberattack, a hospital and a dying woman. https://www.wired.co.uk/article/ransomware-hospital-death-germany, 11 de Noviembre del 2020. Consultado el 29 de Diciembre del 2021.

[35] Scott Rose, Oliver Borchet, Stru Mitchell, and Sean Connelly. Zero trust architecture. *Special Publication (NIST SP)*, 2020. doi: 10.6028/NIST.SP.800-207. URL `https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420`. Consultado el 19 de Septiembre del 2023.

[36] Robert Sedgewick and Kevin Wayne. *Algorithms, 4th Edition*. Addison-Wesley, 2011. ISBN 978-0-321-57351-3.

[37] Steven S. Skiena. *The Algorithm Design Manual*. Springer, London, 2008.

[38] Kayla M. Straub, Avik Sengupta, Joseph M. Ernst, Robert W. McGwier, Merrick Watchorn, Richard Tilley, and Randolph Marchany. Malware propagation in fully connected networks: A netflow-based analysis. In *MILCOM 2016 - 2016 IEEE Military Communications Conference*, pages 497–502, 2016. doi: 10.1109/MILCOM.2016.7795376.

[39] Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, and Cody B. Thomas. *MITRE ATT&CK: Design and Philosophy*. The MITRE Corporation, Julio del 2018.

[40] Pierre Thomas and Lee Ferran. Hacker behind massive credit data theft gets 20 years. https://abcnews.go.com/GMA/TheLaw/hacker-sentenced-largest-theft-credit-debit-cardnumbers/story?id=10208613, 23 de marzo del 2010. Consultado el 23 de diciembre del 2021.

[41] John von Neumann. *Theory of Self-Reproducing Automata*. University of Illionois Press, Champain, IL, 1966. https://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf.

[42] Duncan J. Watts and Steven H. Strogatz. Collective dynamics of 'small-world' networks. *Nature*, 393(6684):440–442, 1998. doi: 10.1038/30918.