Recomendaciones para la detección y mitigación de malware en equipos de cómputo utilizando herramientas de seguridad cibernética

Robinson Harry Henao Ortiz

Asesor

Christian Hernán Obando Ibarra

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

Dedico este trabajo de grado inicialmente a Dios por darme la salud, la fortaleza, el conocimiento, la actitud y los demás factores que implican la disciplina en cuanto a la educación se refiere, igualmente a mis padres por el apoyo incondicional en este proceso todo ello con el objetivo de ver avanzar y evolucionar a uno de sus hijos.

A mis directores de curso y tutores por la paciencia y direccionamiento que han tenido durante todo este proceso lo cual ha hecho parte fundamental no solamente en el conocimiento si no en el desarrollo intelectual en un especialista en Seguridad Informática.

Agradecimientos

A toda la comunidad educativa de la Universidad Nacional Abierta y a Distancia dentro de los que se destacan los directores de curso y los tutores quienes día a día en cada uno de los campos del conocimiento quisieron transmitir hoy cada proceso para el desarrollo de sus estudiantes no solamente como profesionales en la ingeniería sino en la especialización de la seguridad informática.

A mi familia por el apoyo incondicional durante todo el proceso educativo quienes han desarrollado un rol muy importante en el acompañamiento de este proceso.

Resumen

El crecimiento acelerado de las tecnologías digitales ha transformado el manejo de la información, pero también ha incrementado los riesgos asociados a programas maliciosos como el malware. Estos pueden comprometer la integridad de los sistemas informáticos, causar daños en componentes físicos y lógicos, y facilitar el robo de información sensible. Este trabajo analiza los mecanismos utilizados por los atacantes para crear e introducir malware en los sistemas, así como las estrategias para detectarlo, enfrentarlo y prevenirlo.

Se enfatiza la necesidad de implementar herramientas de seguridad efectivas, incluso en infraestructuras tecnológicas pequeñas, y se propone un enfoque preventivo basado en la detección temprana, la capacitación de usuarios y el uso de soluciones tecnológicas especializadas.

Palabras clave: adware, ciberdelincuente, ciberseguridad, malware, spyware.

Abstract

The rapid expansion of digital technologies has significantly transformed information management while increasing exposure to malicious software such as malware. These threats can compromise the integrity of information systems, damage hardware and software components, and lead to the theft of sensitive data. This study explores the techniques used by cyber attackers to develop and deploy malware, as well as the methods for its detection, mitigation, and prevention. The research highlights the importance of adopting effective cybersecurity tools even in small-scale systems and promotes a proactive approach through early detection, user awareness, and specialized technological solutions.

Keywords: adware, cybercriminal, cybersecurity, malware, spyware.

Tabla de contenido

Lista de Figuras

Introducción

Los ataques a los sistemas informáticos son cada vez más constantes, por ello, se deben tener en cuenta los parámetros para el análisis y utilización de la Ciberseguridad, es importante tener la conceptualización y el conocimiento de la seguridad de la información, sobre todo en cómo se está manejando, como se ha reglamentado y como está siendo utilizada a nivel local, nacional y mundial, sus avances y actualizaciones que hacen parte del crecimiento tecnológico.

Igualmente se debe analizar en un proceso de implementación de la Ciberseguridad, como las diferentes organizaciones están reglamentándola, cuáles han sido las propuestas de actualización de dichas leyes y decretos y que la academia influya desde temprano en estos procesos de conocimiento y utilización.

Todo esto debe ir a la vanguardia de la evolución tecnológica ya que esto hace parte de la seguridad de la información, componente que afecta a todos.

Planteamiento del Problema

"¿Qué recomendaciones de seguridad pueden implementarse para mejorar la detección y aplicar medidas efectivas contra el malware en equipos de cómputo mediante el uso de herramientas informáticas?"

"El malware representa una amenaza creciente para la integridad de los sistemas informáticos, provocando pérdidas de información y daños a nivel de hardware y software. Entre las amenazas más comunes se encuentran virus, troyanos, ransomware, spyware y adware, los cuales pueden comprometer datos críticos, por lo tanto la detección a tiempo se hace indispensable en los equipos de cómputo evitando daños e intrusiones en los mismos, para ello se hace necesario realizar una correcta detección y una adecuada prevención por medio de un software de seguridad óptimo, unas actualizaciones periódicas regulares al sistema en general y una educación continua a los usuarios del sistema. Todo esto teniendo en cuenta que en la actualidad es de fácil acceso a este tipo de elementos malignos, desde ingresar a visualizar un video en YouTube hasta la apertura de un archivo desconocido".

Justificación

Esta monografía es fundamental debido al creciente número de amenazas informáticas que comprometen la seguridad, privacidad e integridad de los equipos de cómputo. El malware, en sus diversas formas, afecta tanto a usuarios individuales como a organizaciones, generando pérdidas de información, interrupciones operativas y vulnerabilidades críticas en los sistemas.

En este contexto, el uso adecuado de herramientas informáticas de seguridad, combinado con recomendaciones prácticas y actualizadas, permite fortalecer la protección de los dispositivos y reducir significativamente los riesgos. Además, muchos usuarios desconocen las medidas básicas de prevención o no las aplican correctamente, lo cual aumenta la exposición frente a ataques.

Por tanto, esta monografía busca aportar conocimiento útil y aplicable sobre estrategias de detección y contramedidas contra el malware, fomentando una cultura de seguridad informática basada en el uso responsable de tecnologías, actualizaciones periódicas y capacitación continua.

El trabajo servirá como una guía práctica tanto para usuarios como para instituciones que deseen fortalecer sus defensas digitales.

Uno de estos posibles ataques y muy básicos está en los correos electrónicos con documentos adjuntos o links de acceso que me lleve a sitios donde se pueda establecer posibles ataques, igualmente en las USB infectadas, aplicaciones o programas infectados y mensajes con phishing.

Para nombrar algunos de ellos podemos identificar el virus básico que suele venir en correos electrónicos como archivos adjuntos, el ransomware que es uno de los malware más utilizados para el robo de información rentable para los ciberdelincuentes, los scareware que son

utilizados para comprar aplicaciones falsas, los populares gusanos que se reproducen de máquina en máquina según donde sea instalada, los spyware los cuales se instalan en alguna computadora que obtiene información personal sobre el usuario y por último los troyanos que son malware disfrazados de aplicaciones básicas y sencillas para extraer información personal y espiar actividades del usuario dentro del sistema de información.

Es por ello por lo que se deben establecer reglamentos internos para que cada uno de los usuarios tenga el conocimiento básico de identificación de cualquier virus o malware que se pueda encontrar en un sistema de información.

La mayoría de las infecciones que se puedan encontrar en un sistema de información puede que no se logren detectar de manera inmediata pero estos ataques básicamente se activan cuando se descarga algún tipo de información o se ingresa a alguna página maliciosa, ingresando códigos informáticos obviamente dañinos y maliciosos por medio del cual pueda extender un ataque de manera global dentro de un sistema de información e incluso en los mismos dispositivos móviles.

Objetivos

Objetivo General

Analizar los elementos de seguridad para la detección de los malware a través de la ingeniería social para disminuir la ciberdelincuencia.

Objetivos Específicos

Identificar las configuraciones de seguridad que deben existir en una red para mitigar posibles ataques.

Reconocer estrategias de detección de malware por medio de un software libre para contratacarlos.

Establecer reglas de seguridad por medio de manuales para mitigar posibles ataques.

Marco Referencial

Antecedentes

Teniendo en cuenta los primeros hallazgos de malware, podemos identificar al "Creeper" y el "Elk Cloner", igualmente los primeros virus y gusanos, como el "ILOVEYOU" y el "Melissa", los cuales marcaron un cambio en la manera en que el malware se propagaba y afectaba a los sistemas.

Hablando de la ciberseguridad, la transición a Ransomware y Spyware: Explica cómo y por qué los tipos de malware evolucionaron para incluir ransomware y spyware. Los Cambios en la Propagación y Evasión analizan cómo las técnicas de propagación y evasión del malware se han vuelto más sofisticadas con el tiempo.

(Alegsa, (2023))

Marco Conceptual

El concepto de malware se refiere a cualquier tipo de software creado con intenciones maliciosas que comprometen la seguridad de sistemas informáticos. Estos programas pueden robar información, dañar componentes o permitir el acceso remoto no autorizado, afectando tanto a usuarios individuales como a organizaciones.

Entre los conceptos fundamentales para comprender el funcionamiento y mitigación del malware, destacan los siguientes:

Virus Informático. Son programas capaces de replicarse y propagarse de un archivo o sistema a otro, con el objetivo de alterar el funcionamiento normal del equipo, dañar información o entorpecer procesos.

Antivirus. Software diseñado para identificar, bloquear y eliminar programas maliciosos. Su eficacia depende de una correcta configuración y actualización constante para reconocer nuevas amenazas.

Vector de Ataque. Medio o técnica utilizada por los ciberdelincuentes para introducir malware en un sistema. Puede tratarse de un archivo adjunto en un correo electrónico, una memoria USB infectada, una página web comprometida, entre otros.

El malware adopta múltiples formas según su funcionalidad, y es utilizado con diversos fines ilícitos, entre ellos:

- Obtener acceso a datos personales o financieros de los usuarios.
- Interferir en el funcionamiento de redes o sistemas críticos.
- Realizar fraudes informáticos o extorsiones.
- Explotar recursos de los dispositivos para actividades como la minería de criptomonedas.

- Un vector de ataque se define como el medio a través del cual un ciberdelincuente puede hacer llegar un malware a un objetivo específico, es decir, no es solo instalar un software que contrataque sino visualizar y analizar los componentes de dichos ataques para así mismo tener las herramientas para mitigarlos.

(¿Que es un Malware?, 2024)

Marco Legal

La legislación colombiana ha avanzado significativamente en la regulación de la seguridad digital, reconociendo la creciente amenaza que representa el malware para la protección de los datos y la infraestructura tecnológica del país. En este contexto, se han

establecido normativas que buscan garantizar la integridad, confidencialidad y disponibilidad de la información, tanto en el ámbito público como privado.

Entre los principales referentes normativos se encuentran:

- Ley 1273 de 2009, que introduce la protección de los datos y sistemas informáticos como un bien jurídico, y tipifica delitos relacionados con el acceso no autorizado, la interceptación ilegal de datos y el sabotaje informático.
- Ley 1581 de 2012, orientada a la protección de datos personales, establece los principios y procedimientos para el tratamiento seguro de la información, enfatizando el consentimiento y la responsabilidad en el manejo de bases de datos.
- Decreto 1008 de 2018, que define los lineamientos de la política de Gobierno Digital, promoviendo el uso responsable de tecnologías y la gestión adecuada de los riesgos cibernéticos en las entidades públicas.
- Ley 1712 de 2014, sobre acceso a la información pública, refuerza la necesidad de transparencia en la gestión de datos, lo cual también implica proteger los sistemas contra amenazas digitales como el malware.
- CONPES 3701 de 2011, que establece una estrategia nacional de ciberseguridad y ciberdefensa, incluyendo acciones para prevenir y responder a incidentes relacionados con ataques informáticos.

(Planeacion, 2016)

Todos los aspectos en términos legales para la actual investigación han surgido a medida de los tiempos teniendo en cuenta los diferentes tipos de ataques a nivel mundial en cuanto a sistemas informáticos se refiere, se han establecido parámetros legales por los cuales se han encontrado muy buenos resultados hoy en cuanto a las maneras de castigar a quienes atentan

contra los sistemas informáticos privados y públicos, la protección de los datos es clave fundamental siempre y cuando se establezcan los parámetros de seguridad óptimos y correctamente configurados hoy que limiten la privacidad de la información de la forma más adecuada e igualmente establecer las propiedades intelectuales de la información que se tenga en cualquier sistema informático.

En Colombia se establecieron normas y leyes como el Decreto 338 de 2022 por medio del cual se establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital.

Los Principios Éticos se basan en la revisión de los principios éticos aplicables a la investigación de malware, como la integridad y la transparencia en el manejo de datos e igualmente el consentimiento y Autorización que concierne a la necesidad de obtener consentimiento y autorización para la investigación.

Diseño Metodológico

Los Avances en Tecnología de la Información hacen parte de los avances en hardware y software quienes influyen directamente en la evolución del malware. Incluye el desarrollo de redes, sistemas operativos, y plataformas que pueden ser vulnerables a nuevas formas de ataque.

Las tecnologías emergentes, como la inteligencia artificial, el Internet de las Cosas (IoT) y la computación en la nube, están creando nuevas oportunidades para el malware.

Igualmente es importante establecer como parámetro de seguridad de manera global, incluyendo las redes y sistemas que hacen parte de la infraestructura tecnológica común y que en la actualidad proporciona una visión general de las tecnologías y prácticas en la seguridad informática que se utilizan para prevenir y mitigar ataques de malware.

Enfoque de Investigación - Documental

Tipo de Investigación Exploratoria y Analítica donde se busca la mayor parte de información oportuna que despliegue análisis de nuevos elementos de seguridad y prevención, igualmente, en ciberseguridad, el enfoque exploratorio se centra en la observación y análisis de posibles amenazas en un entorno controlado antes de ser introducidas en la red o infraestructura operativa real, esto busca explorar patrones, comportamientos y técnicas de los atacantes sin comprometer la seguridad real de los sistemas en producción. Como objetivo de observación y análisis, las siguientes herramientas son enfocadas al objetivo de esta investigación no solo para la detección y alerta, sino para mitigar posibles ataques.

Una de las herramientas exploratorias son los **Sandboxes**, estos son entornos aislados donde se puede ejecutar código o analizar archivos sospechosos sin riesgo de afectar sistemas operativos o redes. En un entorno exploratorio, las sandboxes permiten simular el

comportamiento de malware o actividades maliciosas para estudiar su funcionamiento y detectar vulnerabilidades sin comprometer el sistema real.

Escenario de prueba:

- Se ejecuta un archivo sospechoso o un programa en un entorno aislado (sandbox) para observar su comportamiento, se deben validar los datos detectados con el objetivo de verificar por medio del sandbox el tipo de información y así mismo detectar y controlar las actividades maliciosas (como la ejecución de código no autorizado, acceso a archivos críticos, y comunicación con servidores externos).

Otra de las herramientas para este tipo de investigación son los **sistemas de detección de intrusos** (IDS), siendo estas herramientas diseñadas para monitorear el tráfico de red y las actividades en un sistema con el fin de identificar comportamientos anómalos o maliciosos, se deben configurar de manera estratégica teniendo en cuenta la ubicación y los objetivos principales, direccionando las respuestas o análisis de manera adecuada identificando las intrusiones y respondiendo según lo identificado.

Escenario de prueba:

- En un entorno de nube, se simulan ataques dirigidos a servicios como bases de datos, máquinas virtuales, o aplicaciones alojadas, los ataques pueden incluir exploits, fugas de datos, o infecciones por malware. El sandbox actúa como un entorno de análisis para los archivos maliciosos y el IDS detecta patrones de tráfico o actividades sospechosas en la red.

Las herramientas utilizadas en los anteriores escenarios de prueba se aplicaron en esta investigación enfocados en las exploraciones y análisis de las estructuras tecnológicas básicas, estas herramientas buscan recolectar, preservar y analizar los datos relacionados con dispositivos electrónicos como computadoras, teléfonos móviles, servidores, redes, etc.

Enfoque Metodológico Cualitativo que impacte en las características de prevención a diferentes ataques informáticos por medio del malware que impacten a la sociedad no solo en la prevención sino en medidas correctivas en los diferentes casos que se puedan presentar.

Formular las preguntas clave en la investigación que puedan establecer los parámetros de prevención ante los diferentes tipos de malware.

Establecer la metodología de Recolección de Datos por medio de las diferentes fuentes que establezcan datos no solo primarios sino secundarios dentro de la investigación a través de análisis demuestras de malware y la revisión documental existente.

Igualmente, tener en cuenta los siguientes métodos para establecer de manera óptima una investigación con metodología cualitativa:

- ✓ Estudio de Casos
- ✓ Observación
- ✓ Entrevistas y Encuestas con Expertos en Ciberseguridad
- ✓ Análisis de Contenido
- ✓ Análisis de Redes Sociales y Foros de Ciberseguridad
- ✓ Análisis Comparativo de Malware

Ventajas del Enfoque Cualitativo:

Profundización en el comportamiento del malware: Permite una comprensión más detallada y contextualizada de cómo el malware se propaga y se comporta dentro de un sistema.

Identificación de patrones emergentes: Ayuda a identificar amenazas desconocidas o emergentes que podrían no ser detectadas fácilmente mediante métodos cuantitativos o automatizados.

Análisis en tiempo real: Puede complementar la detección automática al ofrecer una perspectiva basada en la experiencia humana, lo que es particularmente útil en entornos dinámicos y de constante cambio.

Identificar las Configuraciones de Seguridad que Deben Existir en una Red para Mitigar Posibles Ataques

La seguridad en las redes informáticas es un pilar fundamental para prevenir la propagación de malware y otros tipos de amenazas. Este capítulo analiza las configuraciones esenciales que deben implementarse en una red para garantizar su integridad y proteger los activos digitales de una organización.

Evaluación Inicial de Seguridad

El primer paso en una estrategia de protección es el análisis de la arquitectura de red. Es fundamental revisar la topología, identificar los dispositivos críticos (como routers, switches y firewalls), y comprobar la segmentación en zonas (red interna, DMZ, red de invitados). Además, las políticas de seguridad deben estar actualizadas y contemplar protocolos de respuesta a incidentes.

Configuración de Dispositivos de Red

Los dispositivos de red deben ser gestionados adecuadamente para restringir el acceso no autorizado. Los firewalls deben establecer reglas específicas para el tráfico entrante y saliente, mientras que routers y switches deben configurarse con autenticación robusta y protocolos seguros. La implementación de IDS/IPS permite detectar actividades anómalas en tiempo real.

Seguridad en el Acceso y Autenticación

El control de acceso basado en roles (RBAC) y el uso de autenticación multifactorial (MFA) fortalecen la defensa contra accesos indebidos. Las contraseñas deben cumplir con requisitos de complejidad y cambiarse periódicamente. Es crucial auditar regularmente los privilegios otorgados a usuarios.

Protección de Datos y Comunicaciones

El cifrado es clave para preservar la confidencialidad de la información, tanto en tránsito como en reposo. Se recomienda el uso de VPNs y protocolos como TLS para comunicaciones seguras. Asimismo, se deben aplicar filtros en el correo electrónico y herramientas de navegación segura para prevenir ataques de phishing y acceso a sitios maliciosos.

Monitoreo y Auditoría

La recolección y análisis de registros de eventos (logs) permite detectar incidentes de forma proactiva. Las auditorías periódicas y las pruebas de penetración ayudan a identificar vulnerabilidades y fortalecer la postura de seguridad.

Mantenimiento y Actualización

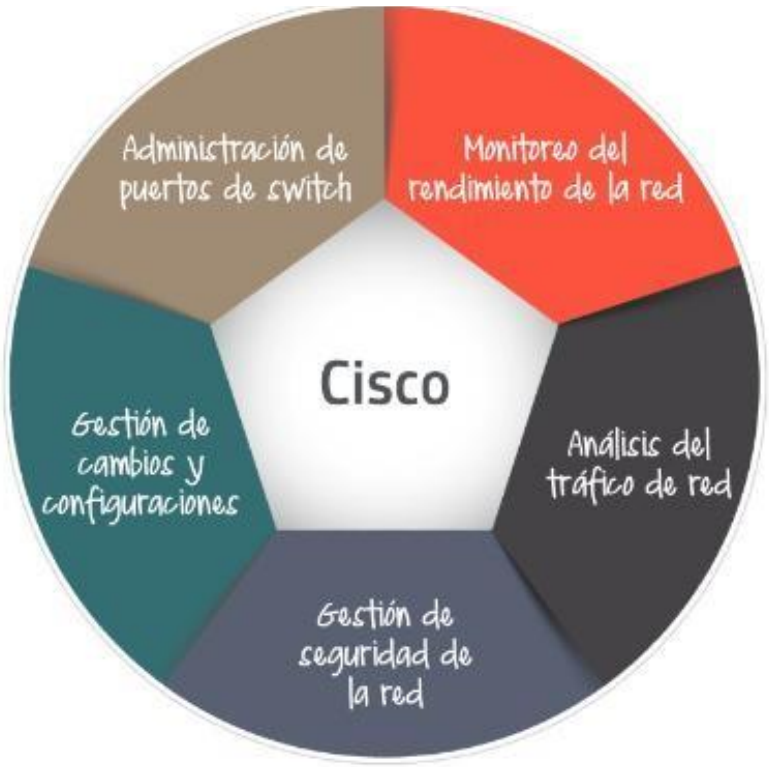
Los sistemas deben mantenerse actualizados con parches de seguridad y configuraciones revisadas frecuentemente. Las actualizaciones automáticas y la revisión de dispositivos obsoletos reducen significativamente el riesgo de ataques.

Documentación y Reporte

Toda la configuración de red debe estar documentada de forma clara y actualizada. Esto incluye políticas, procedimientos, configuraciones de dispositivos y reportes de incidentes, lo cual facilita la gestión y respuesta ante eventos de seguridad.

Figura 1

Rendimiento de Redes



Nota. Monitoreo y administración de redes con OpManage, Tomado de. Monitoreo y administración de redes Cisco con OpManager. (2024). *https://www.manageengine.com/latam/network-monitoring/software-monitoreo-redes-cisco.html*

Reconocer Estrategias de Detección de Malware por Medio de un Software Libre para Contratacarlos

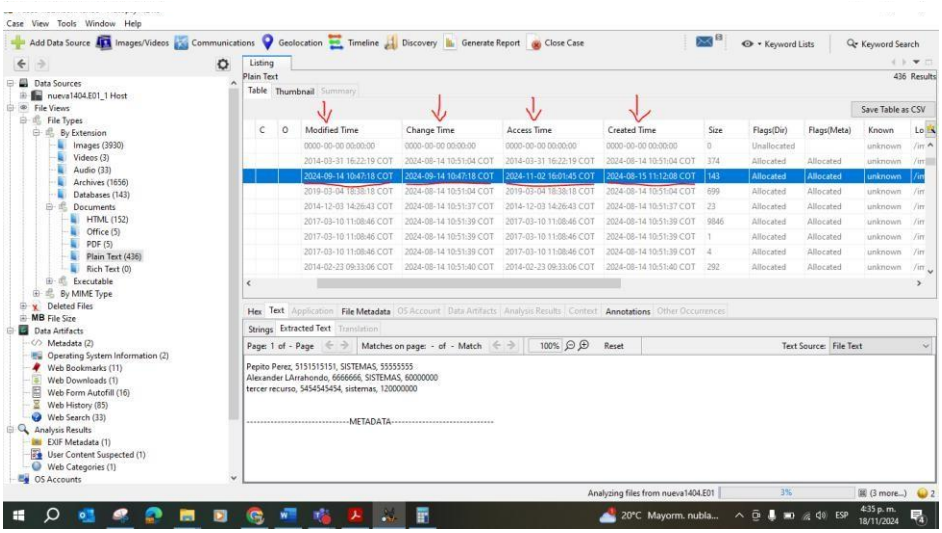
La detección efectiva del malware es una de las principales líneas de defensa frente a ataques informáticos. Este capítulo aborda los distintos tipos de software y metodologías empleadas para identificar amenazas, analizando sus características, beneficios y limitaciones, así como su integración en una estrategia de defensa integral.

- Antivirus y antimalware: Utilizan firmas conocidas, análisis heurístico y monitoreo de comportamiento para identificar amenazas. Algunas soluciones comerciales reconocidas son Bitdefender, Malwarebytes y McAfee.
- Sistemas de detección y prevención de intrusiones (IDS/IPS): Permiten monitorear el tráfico de red en busca de patrones anómalos. Herramientas como Snort o Suricata ofrecen reglas personalizables y actualizaciones frecuentes para detectar ataques conocidos y emergentes.
- Entornos de análisis (Sandboxes): Simulan entornos controlados donde se ejecutan archivos sospechosos para estudiar su comportamiento sin comprometer el sistema real. Esto facilita la detección de malware sofisticado que evita métodos tradicionales.
- Herramientas de análisis forense digital: Se utilizan para examinar evidencia tras un incidente de seguridad. Aplicaciones como FTK Imager y Autopsy permiten identificar alteraciones en archivos y rastros de ejecución maliciosa.

Bajo la herramienta Autopsy:

Figura 2

Análisis Archivo Nominat.Txt (Autopsy)

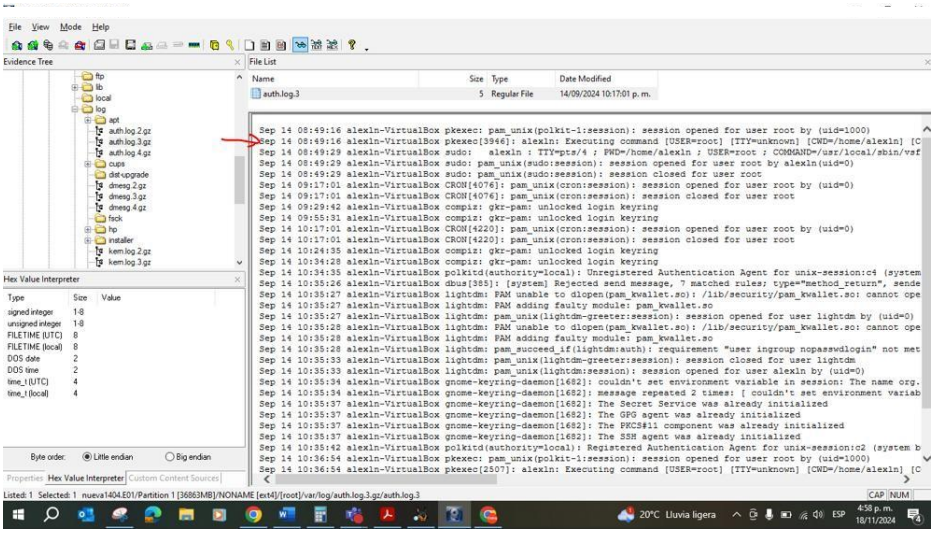


Nota. Elaboración Propia en escaneo archivo nomina.txt con Autopsy

Bajo la herramienta FTK Imager:

Figura 3

Análisis Archivo Nomina.txt (FTK Imager)



Nota. Elaboración Propia en escaneo archivo nomina.txt con FTK Imager.

A continuación, se presenta la hipótesis de lo sucedido con las evidencias respectivas que identifican las actividades de modificación realizados por el atacante sobre la maquina presuntamente comprometida:

Podemos evidenciar que antes de realizar el respectivo ataque y modificación de archivos y documentos, se realizaron ejecuciones, tareas, ingresos y modificaciones con el objetivo de identificar inicialmente las posibles vulnerabilidades y posteriormente realizar el ataque en diferentes frentes, pero principalmente al archivo NOMINA.txt cómo lo podemos evidenciar en el siguiente análisis:

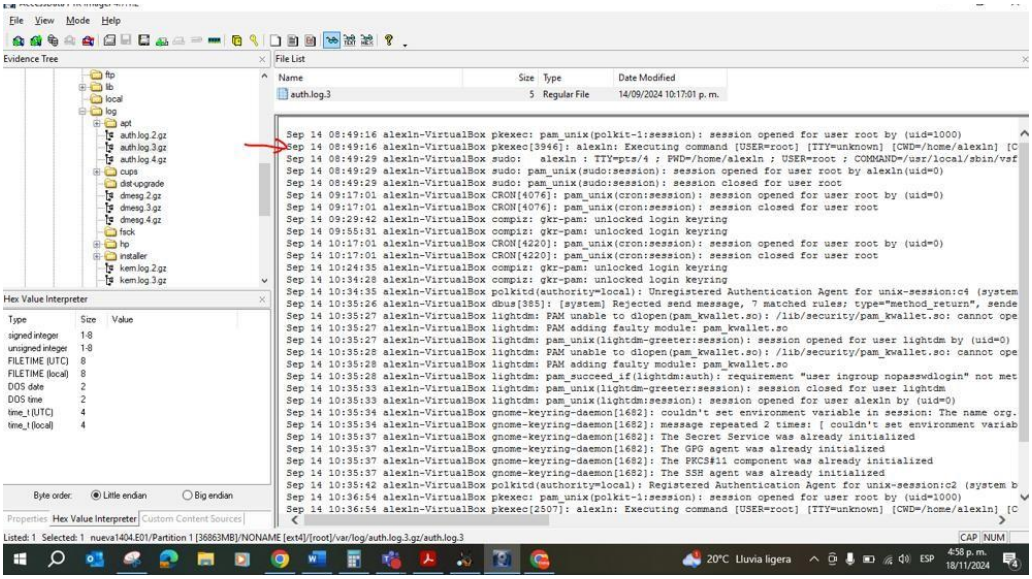
En múltiples sectores del registro, el usuario “alexln” está ejecutando comandos que tienen privilegios altos por medio de la utilización de pkexec y sudo. Estos logs muestran que se ejecutaron comandos como root, en la linea /usr/lib/update-notifier/package-system-locked y /usr/local/sbin/vsftpd (probablemente relacionado con la configuración de un servidor FTP).

- Podemos visualizarlo en la siguiente línea:

Sep 14 08:49:16 pkexec: alexln: Executing command [USER=root] [COMMAND=/usr/lib/update-notifier/package-system-locked]

Figura 4

Hipótesis



Nota. Elaboración Propia en Hipótesis.

CRON está utilizando o ejecutando tareas como root, estas tareas se registran en el sistema, y se indica cuándo se abren y cierran las sesiones.

Sep 14 09:17:01 CRON[4076]: pam_unix(cron:session): session opened for user root by (uid=0)

Técnicas De Detección

Las estrategias empleadas por estas herramientas se basan en enfoques complementarios:

Basadas en Firmas. Comparan archivos con una base de datos de amenazas conocidas. Son rápidas y precisas, pero no detectan nuevas variantes.

Heurísticas: Analizan patrones sospechosos sin depender de firmas específicas.

Son útiles para amenazas desconocidas, aunque pueden generar falsos positivos.

Análisis de Comportamiento. Observan en tiempo real las acciones de programas activos, detectando comportamientos anómalos, como cambios en el sistema o conexiones no autorizadas.

Análisis de Integridad. Comparan versiones actuales de archivos o configuraciones del sistema con versiones anteriores, alertando sobre modificaciones sospechosas.

Monitoreo del Tráfico de Red. Permite identificar conexiones con servidores maliciosos o comportamientos típicos de troyanos y botnets.

Implementación y Respuesta

El uso de herramientas de detección debe complementarse con una estrategia bien estructurada:

Configuración Adecuada. Asegurar que todas las soluciones estén actualizadas y ajustadas a las necesidades de la organización.

Monitoreo Constante. Realizar supervisión en tiempo real para actuar ante cualquier alerta de forma inmediata.

Respuesta a Incidentes: Incluir mecanismos de contención, eliminación del malware y análisis forense para determinar el origen del ataque y prevenir recurrencias.

Revisión y Mejora Continua. Evaluar periódicamente la efectividad de las herramientas utilizadas, actualizando estrategias conforme a las nuevas amenazas del entorno digital.

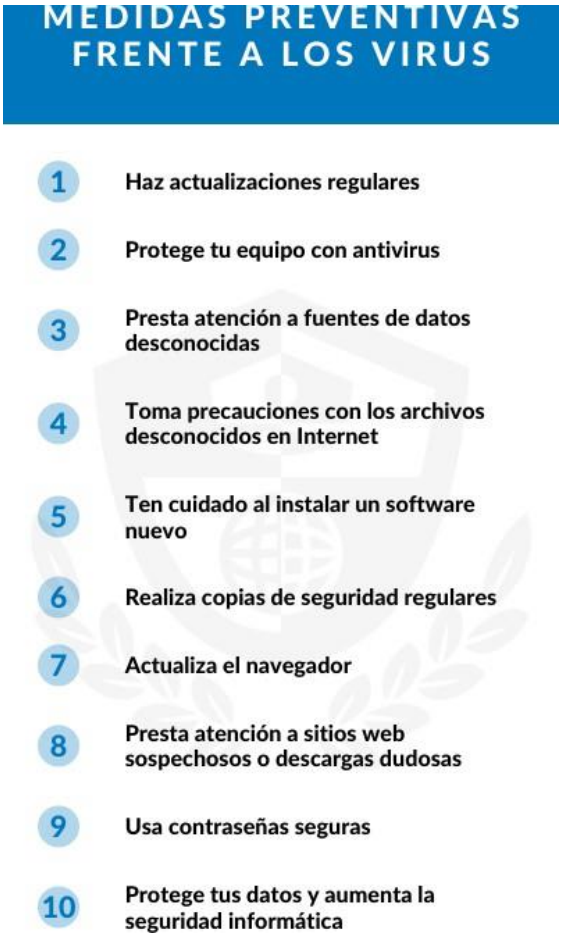
Integración con la Seguridad Organizacional

Una estrategia de detección efectiva debe ir acompañada de otras medidas preventivas como el uso de firewalls, políticas de control de acceso, capacitación continua y simulacros de respuesta ante incidentes. Además, la documentación de cada incidente permite crear una base de conocimiento que fortalece el aprendizaje organizacional frente a ciberataques.

(Malwarebytes, 2024) (Nordsterntech, 2020)

Figura 5

Medidas Preventivas Frente a los Virus



Nota. Qué son los virus: tipos, modus operandi, medidas preventivas y consejos. Tomado de. (2024). https://www.lisainstitute.com/blogs/blog/que-son-los-virus-tipos-modus-operandi-medidas-preventivas-y-consejos?srsltid=AfmBOorFZOZkszkJAXNHF-jWpHB6zabUlarbtyVkl4FG6RIHkq_Ab6hG

Ejemplos de herramientas que ha detectado Malwarebytes con éxito:

- Ataque de Ransomware WannaCry (2017):

Contexto: El ransomware WannaCry fue uno de los ataques más devastadores que afectó a miles de organizaciones en todo el mundo, utilizando una vulnerabilidad en el protocolo SMB (Server Message Block) en sistemas Windows.

Cómo Snort ayudó: Snort, como un sistema de detección de intrusiones basado en firmas, fue capaz **de** identificar patrones de tráfico asociados con el exploit **EternalBlue** que WannaCry utilizaba para propagarse. Al tener reglas actualizadas que cubrían este ataque, Snort detectó y alertó sobre el tráfico sospechoso que intentaba explotar esta vulnerabilidad, permitiendo a los administradores bloquearlo a tiempo.

(CLOUDFLARE, 2024)

- Malware Emotet (2018-2021):

Contexto: Emotet es un troyano que se propaga principalmente a través de correos electrónicos de phishing con documentos maliciosos adjuntos. Este malware está diseñado para robar información financiera y entregar otros tipos de malware, incluidos troyanos de acceso remoto y ransomware.

Cómo Malwarebytes ayudó: Malwarebytes detectó y bloqueó activamente las variantes de Emotet a medida que se distribuían. Gracias a su motor de análisis heurístico y de firmas, **malwarebytes** identificó el comportamiento sospechoso de los archivos adjuntos y los enlaces en los correos electrónicos. Esto permitió que los usuarios bloqueasen el malware antes de que pudiera ejecutarse y propagarse en sus sistemas.

(EUROPOL, 2021)

Estadísticas y Resultados de Estrategias de Detección de Malware: Snort

Eficacia en la detección de malware y ataques de red (2017-2020):

- Estudio de caso realizado por la Universidad de Maryland y otras instituciones académicas en colaboración con empresas de seguridad, demostró que Snort podía detectar más del 98% de las amenazas conocidas, incluidas exploits de SMB (como EternalBlue) y ataques de tipo DDoS cuando se utilizaba en combinación con otras herramientas de defensa en profundidad. Esto fue especialmente efectivo para exploits de día cero cuando se actualizaron las reglas con rapidez.

- En un entorno simulado, utilizando Snort para detectar ataques basados en WannaCry y otros ransomware propagados por vulnerabilidades de SMB, Snort identificó con éxito más del 90% del tráfico malicioso antes de que pudiera afectar los sistemas objetivo. Los resultados mostraron una reducción del 87% en los incidentes de ransomware dentro de redes protegidas por Snort, comparado con redes que no usaban un sistema de detección de intrusos (IDS).

Malwarebytes: Reducción de infecciones por Ransomware (2019-2021):

- Un informe de malwarebytes publicado en 2021 destacó que las organizaciones que implementaron malwarebytes Endpoint Protection experimentaron una reducción del 80% en incidentes de ransomware, en comparación con las empresas que no usaron soluciones de protección proactiva.

- En un estudio de laboratorio realizado con simulaciones de ransomware Ryuk, malwarebytes detectó y eliminó 96% de los intentos de infección antes de que el malware pudiera cifrar archivos en entornos de prueba. Además, mostró una capacidad de detección temprana en el 91% de las infecciones de ransomware basadas en phishing.

Detección de Malware y PUPs (Programas Potencialmente No Deseados):

- Un análisis realizado por AV-TEST (una empresa de pruebas de software antivirus) mostró que malwarebytes logró una tasa de detección del 99.4% en su capacidad para bloquear adware y PUPs (Programas Potencialmente No Deseados).

- En un entorno simulado de navegación web, donde se descargaron archivos sospechosos con software de adware y PUPs, malwarebytes identificó y bloqueó con éxito el 98% de los archivos maliciosos antes de que pudieran ejecutar sus cargas útiles, lo que resultó en una mejora significativa en la seguridad de los sistemas frente a infecciones que afectan a la productividad.

Reglas de Seguridad

Establecer reglas de seguridad por medio de manuales tiene como objetivo principal proteger los sistemas informáticos y la información crítica ante posibles ataques de malware, estandarizando buenas prácticas que todos los usuarios deben seguir. Estos manuales permiten reducir la exposición a amenazas, mejorar la respuesta ante incidentes y fortalecer la cultura de ciberseguridad dentro de una organización o entorno académico.

La implementación de reglas de seguridad:

- Previenen errores humanos, una principal causa de infección por malware.
- Proveen instrucción clara y actualizada para actuar ante amenazas informáticas.
- Fomentan el uso responsable de los recursos tecnológicos, promoviendo la protección de datos personales y corporativos.
- Facilitan la formación continua de los usuarios, ayudándolos a reconocer comportamientos de riesgo y actuar con mayor precaución.
- Unifican criterios de seguridad, permitiendo que todos los miembros de una organización trabajen bajo las mismas reglas.

Seguridad para Endpoints

Los equipos de cómputo deben contar con software antimalware actualizado, configurado para realizar análisis automáticos de forma periódica. Además, se debe restringir la ejecución de software no autorizado mediante herramientas de control de aplicaciones. Estas medidas reducen el riesgo de infección por archivos descargados, dispositivos USB o redes no seguras.

1. Implementar y Actualizar el Antivirus/Antimalware

Acción: Instala una solución de antivirus y antimalware en todos los dispositivos finales. Frecuencia: Actualiza las definiciones de virus diariamente.

Monitoreo: Realiza análisis completos una vez por semana.

2. Políticas de Escaneo Automático

- Acción: Configura análisis automáticos para detectar amenazas en descargas, archivos adjuntos y dispositivos USB.

- Frecuencia: Escaneo programado al menos una vez al día.

3. Restringir Ejecución de Software No Autorizado

- Acción: Usa herramientas como AppLocker (Windows) o SELinux (Linux) para permitir solo aplicaciones aprobadas.

Seguridad para Red

Las redes deben protegerse mediante firewalls correctamente configurados, que permitan solo el tráfico necesario y bloqueen servicios no utilizados. La segmentación de la red y el uso de sistemas de detección de intrusos (IDS) refuerzan la capacidad de respuesta ante actividades sospechosas.

1. Implementar un firewall de Red

- Acción: Configura un firewall perimetral para bloquear tráfico entrante y saliente sospechoso.

2. Reglas específicas:

- Bloquear puertos no utilizados.

- Permitir solo protocolos necesarios (por ejemplo, HTTP/HTTPS).

Seguridad para Correo Electrónico y Navegación

El correo electrónico es uno de los vectores más utilizados para distribuir malware. Por tanto, deben implementarse filtros que identifiquen archivos adjuntos maliciosos, enlaces

sospechosos y remitentes no verificados. En cuanto a la navegación web, se recomienda el uso de herramientas de filtrado para prevenir el acceso a sitios potencialmente peligrosos.

1. Filtro de Correos Phishing y Malware

- Acción: Implementa filtros que bloqueen correos con enlaces o archivos adjuntos sospechosos.

- Política: Rechazar correos de dominios no verificados.

2. Análisis Automático de Archivos Adjuntos

- Acción: Escanea automáticamente los adjuntos con una solución antimalware antes de entregar los correos a los usuarios.

Seguridad para Sistemas Operativos

Los sistemas operativos y aplicaciones deben mantenerse actualizados con parches de seguridad oficiales. Las configuraciones deben revisarse periódicamente para adaptarse a nuevas amenazas, y los privilegios de los usuarios deben limitarse al mínimo necesario.

1. Aplicar Actualizaciones de Seguridad

- Acción: Configura actualizaciones automáticas para sistemas operativos y aplicaciones.

- Frecuencia: Al menos semanalmente.

2. Políticas de Control de Cuentas de Usuario (UAC)

- Acción: Limitar privilegios de usuario y requerir permisos administrativos para cambios críticos.

Formación y Conciencia de los Usuarios

La capacitación continua es esencial para reforzar el conocimiento sobre riesgos digitales y el uso seguro de los sistemas. Las sesiones de formación deben abordar prácticas seguras, reconocimiento de intentos de phishing y respuesta ante incidentes.

1. Entrenamientos Periódicos

- Acción: Capacita a empleados sobre buenas prácticas de seguridad.
- Frecuencia: Cada trimestre.

Métricas para medir la efectividad

Para medir la efectividad de las políticas de seguridad, se deben establecer indicadores como la tasa de detección de malware, el número de intentos de intrusión bloqueados, y la frecuencia de actualización del software. Estos datos permiten evaluar el impacto de las medidas implementadas y realizar mejoras continuas.

Métricas para Endpoints

1. **Tasa de Detección de Malware**

- **Definición**: Porcentaje de amenazas detectadas y bloqueadas por el antivirus/antimalware.
- **Fórmula**: Tasa de Detección= (Amenazas Detectadas / Total de Amenazas Identificadas)×100
- **Objetivo**: ≥ 95%.

Métricas para Seguridad de Red

2. Tasa de Bloqueo de Tráfico Sospechoso

- Definición: Porcentaje de intentos de intrusión o tráfico malicioso bloqueado por el firewall o IDS/IPS.

- Fórmula: Tasa de Bloqueo= (Intentos Bloqueados / Total de Intentos Detectados)×100
- Objetivo: ≥ 98%.

Conclusiones

En un entorno digital cada vez más expuesto a amenazas cibernéticas, la mitigación del malware en equipos informáticos se ha convertido en una prioridad para garantizar la integridad, disponibilidad y confidencialidad de la información. A lo largo de esta monografía se han analizado diversas estrategias, herramientas y buenas prácticas orientadas a prevenir, detectar y contrarrestar la acción de programas maliciosos que comprometen tanto el funcionamiento de los sistemas como los datos almacenados en ellos.

A partir de la identificación de las configuraciones de seguridad necesarias en una red, no solamente reduce las vulnerabilidades del sistema, sino que también permite una respuesta más rápida y eficiente ante amenazas. Asimismo, la correcta aplicación de estas medidas contribuye significativamente a mantener la integridad, disponibilidad y confidencialidad de los datos.

El reconocimiento de estrategias de detección de malware mediante el uso de software libre y al estar disponibles de forma gratuita, representan una alternativa viable especialmente para entornos con recursos limitados. Además, el software libre fomenta la transparencia, la colaboración y la constante mejora por parte de comunidades especializadas, lo que incrementa su capacidad de respuesta ante amenazas emergentes.

La elaboración y aplicación de manuales con reglas de seguridad permiten estandarizar procedimientos, fortalecer la conciencia sobre riesgos digitales y promover comportamientos preventivos entre los usuarios. Al establecer lineamientos claros sobre el uso seguro de los sistemas y recursos tecnológicos, se reduce significativamente la probabilidad de incidentes causados por descuidos, desconocimiento o malas prácticas.

Referencias Bibliográficas

¿Que es un Malware? (2024).¿Que es un Malware?: https://www.mcafee.com/es-co/antivirus/malware.html

Alegsa, L. ((2023)). *Definición de Virus*. https://www.alegsa.com.ar/Dic/virus.php Aleman, h., & Rodríguez, C. (29 de 01 de 2019). *Metodologías Para el Análisis de Riesgos en los SGSi*. http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

Arenas, A. (2021). Métodos mixtos de investigación. *Magisterio*.

Bruzza, M. (2020). *Diseño de un modelo para la implementación de gobierno electrónico en instituciones estatales*. https://dialnet.unirioja.es/servlet/dctes?codigo=356713

CLOUDFLARE. (2024).¿Qué fue el ataque del ransomware WannaCry?: https://www.cloudflare.com/es-es/learning/security/ransomware/wannacry-ransomware/

De León Camelo, J. (2019). *Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001 para entidades del estado*. https://repository.unad.edu.co/bitstream/handle/10596/27821/%20%09jcdeleonc.pdf?sequence=3&isAllowed=y

Departamento Nacional de Planeación. (2015). *Documento Conpes.* https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

EUROPOL. (27 de Enero de 2021). World's most dangerous malware EMOTET disrupted through global action: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

Funcion Publica. (2020). *Políticas de Operación Proceso de Tecnologías de la Información.* Seguridad de la Información Documento Técnico Marzo de 2020: https://www1.funcionpublica.gov.co/documents/418537/36701283/politica-de-seguridad-de-la-informacion.pdf.pdf/325019e5-a92f-0b44-3676-2356bd71240c?t=1586355315672

Función Publica. (2021). *Ley 1581 de 2012 - Gestor Normativo.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Función Pública. (2022). *Ley 1712 de 2014 - Gestor Normativo.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

Guacanés Castro , M., & Vilatuña Morales, J. (2022). *Propuesta de diseño de un SGSI basado en la norma ISO/IEC 27001. Caso de estudio la empresa Ultralink.* https://bibdigital.epn.edu.ec/handle/15000/22812

Hernandez Sampieri, R., & Mendoza Torres, C. (2018). *Metodologia de la investigacion. Las rutas cuantitativa, cualitativa y mixta.* Mexico.

IISO. (2018). *ISO/IEC 27000 family*. https://www.iso.org/standard/iso-iec-27000- family

ISACA. (2019). *COBIT 2019: Framework for Governance and Management of Enterprise IT.* https://www.isaca.org/resources/cobit

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability (Switzerland).*

López Aguado, M., & Gutiérrez Provecho, L. (2019). Cómo realizar e interpretar un análisis factorial exploratorio utilizando SPSS. *REIRE* , 1-14.

Malwarebytes. (2024). *Software Antivirus*. https://www.malwarebytes.com/es/cybersecurity/basics/antivirus

Martelo, R., Maderay, J., & Betín , A. (2016). Software para gestión documental, un componente modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Informacion Tecnologica*, 129-134.

McAfee, *¿Qué es malware?* (2024).¿Por qué los delincuentes cibernéticos usan malware?: https://www.mcafee.com/es-co/antivirus/malware.html

Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid.

MinTIC. (2018). *Guía para la Gestión y Clasificación de Activos de Información.* https://gobiernodigital.mintic.gov.co/692/articles-150528_G5_Gestion_Clasificacion.pdf

MinTIC. (2018). *Implementación de la Política de Gobierno Digital* . https://gobiernodigital.mintic.gov.co/692/channels-594_manual_gd.pdf

MinTIC. (2021). *Política General de Seguridad y Privacidad de la Información.* https://gobiernodigital.mintic.gov.co/692/articles-176922_recurso_1.docx

Morales, M. (2019). "Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte.". *Revista peruana de computación y sistemas 2.2* , págs. 43-60.

Nordsterntech. (23 de 11 de 2020). Básicos de Ciberseguridad personal: los 5 mejores programas contra malware: https://www.nordsterntech.com/post/b%C3%A1sicos-de-ciberseguridad-personal-los-5- mejores-programas-contra-malware

Personeria Municipal de Armenia. (2023). *Portafolio de Servicios.* https://personeria-municipal-de-armenia.micolombiadigital.gov.co/sites/personeria-municipal-de-armenia/content/files/000021/1020_portafolio-servicios.pdf

Personería Municipal de Armenia en Quindío. (2024). *Personería Municipal de Armenia en Quindío*. https://www.personeria-armenia.gov.co/entidad/mision-y-vision

Planeacion, D. N. (2016). *Política Nacional de Seguridad Digital en Colombia*. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Quezada Sarmiento, P., Chango Canaveral , P., Benavides Cordova , V., Jumbo Flores, L., Barba Guaman, L., & Calderon-Cordova , C. (2017). Marco de referencia para gobernanza de TI utilizando estándares: COBIT 5 y ISO 38500.

Robles Chaparro, E., Riatiga Ibañez, J., & Delgado Romero, A. (2023). *Guia de Derecho de Autor*. DNA Direccion Nacional del Derecho de Autor: https://www.derechodeautor.gov.co/sites/default/files/2024-03/Gu%C3%ADa-de-Derecho-de-Autor-para-creadores-y-usuarios.pdf

Ruiz Peña, J. (2018). *Diseño de un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO/IEC 27001: 2013, en la Cooperativa Multiactiva del personal del Sena, en Bogotá.* https://repository.unad.edu.co/bitstream/handle/10596/17300/80267708.pdf?sequence=1&isAllowed=y

Soluciones de Software OTRS. (2025). *SGSI – Sistema de Gestión de Seguridad de la Información*. https://otrs.com/es/casos-de-uso/sgsi/#:~:text=%C2%BFQu%C3%A9%20es%20un%20SGSI%3F,que%20deben%20llevarse%20a%20cabo.

Tonysé de la Rosa, M. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001. *Universidad y Sociedad,* 495-506.

Valencia Duque , F., & Orozco Alzate , M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao,* 73-88.

Viegas , V., & Kuyucu , O. (2021). *IT Security Controls: A Guide to Corporate Standards and Frameworks.* Doha, Qatar.