Universidad Internacional de La Rioja
Escuela Superior de Ingeniería y Tecnología

Máster Universitario en Ciberseguridad

Metodología para la evaluación de controles ISO 27001:2022 usando BAS y MITRE ATT&CK

Trabajo fin de estudio presentado por:	Diego Ulises Uchofen Zapana
Tipo de trabajo:	Desarrollo de metodología
Director/a:	Daniel Martinez Ortiz
Fecha:	Febrero 2025

Resumen

El presente Trabajo Fin de Master desarrolla una metodología para la evaluación continua de los controles de la norma ISO 27001:2022 en una organización, mediante la implementación de una herramienta BAS y el uso del marco MITRE ATT&CK. La metodología consta de seis fases que forman un ciclo continuo de mejora en el cumplimiento de los controles de la norma en los activos organizacionales, permitiendo su evaluación rápida y continua. La propuesta se ha validado mediante una prueba de concepto en una empresa, demostrando su capacidad de brindar una medición más eficiente del cumplimiento de los controles y mejorar el estado de protección de las herramientas de seguridad. Los resultados evidencian la viabilidad de aplicar esta metodología para realizar evaluaciones de los controles ISO 27001:2022 a demanda, concluyéndose que no solo permite mejorar el cumplimiento normativo, sino que también mejora la capacidad de respuesta ante amenazas.

Palabras clave: BAS, cumplimiento normativo, MITRE ATT&CK, emulación de ataques, ISO 27001.

Abstract

This Master's Thesis develops a methodology for the continuous evaluation of ISO 27001:2022 controls within an organization through the implementation of a BAS tool and the MITRE ATT&CK framework. The methodology consists of six phases forming a continuous improvement cycle in compliance with the standard's controls across organizational assets, enabling rapid and ongoing assessment. The proposed approach has been validated through a proof of concept in a company, demonstrating its ability to provide a more efficient measurement of compliance and enhance the protection of security tools. The results show the feasibility of applying this methodology to perform on-demand evaluations of ISO 27001:2022 controls, concluding that it not only improves regulatory compliance, but also enhances the ability to respond to threats.

Keywords: BAS, regulatory compliance, MITRE ATT&CK, attack emulation, ISO 27001.

Índice de contenidos

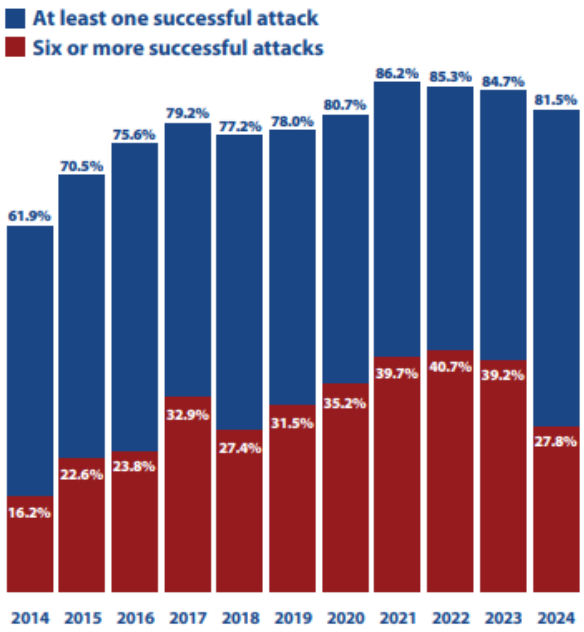
Índice de Figuras

Índice de tablas

1. Introducción

La cantidad de ciberamenazas a las que están expuestas las organizaciones es tan elevada que la gran mayoría se ve comprometida por un ciberataque, incluso a pesar de la implementación de herramientas de seguridad que deberían proporcionar una protección adecuada. Esta situación revela una brecha significativa entre las medidas de defensa adoptadas y la efectividad real de estas soluciones. Según la Figura 1, tomada de ISC2 (2024), más del 80% de las organizaciones han enfrentado al menos un ataque exitoso cada año y más del 25% han experimentado seis o más ataques exitosos, una tendencia que se ha mantenido constante durante los últimos cuatro años.

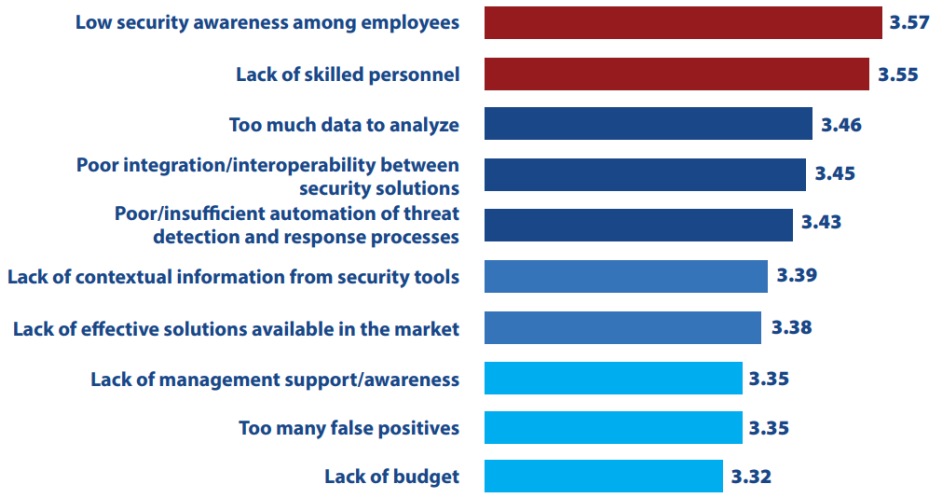
Figura 1. *Porcentaje de organizaciones que experimentan al menos 1 o más de 6 ataques exitosos cada año.*



Fuente: ISC2 Cyberthreat Defense Report, 2024.

Asimismo, ISC2 (2024) destaca en la Figura 2 que, entre las cinco principales barreras que enfrentan las organizaciones para implementar defensas efectivas contra los ciberataques, se encuentran la falta de concientización de los colaboradores en materia de ciberseguridad, la escasez de personal cualificado, el exceso de datos para su análisis, la baja integración entre las herramientas de seguridad y la limitada automatización de los procesos de detección y respuesta ante amenazas.

Figura 2. *Barreras para establecer defensas efectivas ante ciberataques.*



Fuente: ISC2 Cyberthreat Defense Report, 2024.

Si bien el factor humano ocupa un lugar destacado entre las cinco principales barreras y desempeña un papel fundamental en la protección de infraestructuras, es esencial que los aspectos tecnológicos sean robustos y eficaces para prevenir ciberataques en las organizaciones, ya que en principio son más fáciles de controlar.

Los controles sobre las herramientas de seguridad se realizan en base a normativas, estándares y/o directrices. Sin embargo, muchas veces la falta de conocimiento en el proceso de configuración, la gran cantidad de información generada (logs), la diversidad de herramientas en uso junto con la falta de integración y automatización entre las mismas, hace dificultoso el llevar a cabo evaluaciones y/o auditorías constantes que permitan detectar cualquier incumplimiento o mala práctica que pueda dar lugar a posibles brechas de seguridad.

Según A-LIGN (2024), como se muestra en la Figura 3, el 66% de las empresas necesita más de tres meses de preparación para las auditorías cada año, lo que destaca la complejidad del proceso y su relevancia en el contexto organizacional. Este tiempo de preparación está impulsado por tres fuerzas clave: los requerimientos regulatorios, que representan el 24% de las motivaciones; la generación de confianza con clientes y socios, que aporta un 19%; y la validación de la eficacia de los controles dentro de TI, con un 17%.

Figura 3. *Tiempo empleado por las organizaciones para preparar auditorias de seguridad.*

Fuente: A-LIGN Compliance Benchmark Report, 2024.

Una de las normas de seguridad de la información más utilizadas y aceptadas en todo el mundo es la norma ISO/IEC 27001, el 25 de octubre de 2022 se publicó la tercera edición de la norma como ISO/IEC 27001:2022 para hacer frente a los retos mundiales de ciberseguridad y mejorar la confianza digital. (Malatji, 2023)

El anexo A de la norma ISO 27001 en su versión 2022 cuenta con 93 controles, los cuales se dividen en 4 categorías:

- Controles organizacionales: Con un total de 37 controles.
- Controles de Personas: Con un total de 8 controles.
- Controles Físicos: Con un total de 14 controles.
- Controles tecnológicos: Con un total de 34 controles.

Aunque los controles establecidos por la ISO 27001:2022 se auditan, como se ha evidenciado, el proceso tradicional de auditoría puede extenderse por varios meses, lo que hace necesario un enfoque más rápido y continuo que ayude a garantizar el cumplimiento constante.

1.1. Motivación

La norma ISO 27001:2022 proporciona un enfoque estructurado para gestionar la seguridad de la información, pero su implementación efectiva requiere herramientas que permitan validar y medir la eficacia de los controles establecidos. Existen controles de la norma que son implementados en herramientas de seguridad de la organización como firewalls, antivirus, IDS, IPS, EDR, XDR, DLP, WAF, DBF, etc. con el fin de proteger los activos. Teniendo en cuenta ello, cualquier cambio, modificación o mala práctica implementada debe ser auditada constantemente.

Aunque las organizaciones realizan la auditoría de estas herramientas a través de escaneos de vulnerabilidades y pruebas de penetración (pentesting), este tipo de evaluaciones no se realizan de forma continua debido a los costos (si es que es llevado a cabo por una entidad externa) y al tiempo necesario para su planificación y ejecución. Como resultado, las configuraciones y ajustes realizados tras la ejecución de las pruebas no son validados hasta la siguiente, lo que puede generar períodos en los que nuevas vulnerabilidades o configuraciones incorrectas pasen desapercibidas, exponiendo a la organización a riesgos de seguridad no detectados.

En este sentido, resulta crucial que las organizaciones dispongan de una metodología que les permita evaluar de manera continua los controles establecidos por la norma ISO 27001:2022 en sus herramientas de seguridad. Esta capacidad de medición en tiempo real proporcionaría a las organizaciones la posibilidad de conocer y medir su postura de seguridad en cualquier momento, asegurando el cumplimiento de la norma y una gestión más ágil y efectiva de los riesgos y amenazas a los que están expuestas.

1.2. Planteamiento del problema

El problema radica en la deficiencia de las organizaciones para evaluar continuamente los controles de la norma ISO 27001:2022 en las herramientas de seguridad implementadas.

Dentro de las causas se encuentran: El desinterés de la Alta Dirección por la evaluación continua, lo que crea una cultura organizativa que prioriza auditorías anuales sobre un enfoque proactivo; la falta de una herramienta que permita medir continuamente el estado de cumplimiento de los controles, la tercerización de la administración de las herramientas de seguridad que favorece la falta de visibilidad en el cumplimiento normativo, la inexistencia de

un proceso que guíe a las organizaciones como realizar mediciones continuas de los controles de la norma ISO 27001:2022, el costo alto que implica realizar evaluaciones o auditorias continuas a la organización y la falta de una metodología clara para realizar evaluaciones continuas de los controles de la ISO 27001:2022.

En este contexto, se propone y desarrolla una nueva metodología que permite auditar los controles de la norma 27001:2022 que son implementados en las herramientas de seguridad de la organización, mediante el uso de herramientas BAS (Breach and Attack Simulation) y las técnicas del marco MITRE ATT&CK, superando las limitaciones de los métodos tradicionales de auditoría y proporcionando una evaluación más rápida que simula ataques reales bajo demanda sobre las herramientas de seguridad de la organización, lo que permite medir su eficacia de manera constante.

El uso de esta metodología no solo incrementará la visibilidad de la postura de seguridad de la organización, sino que también permitiría obtener una medición continua del estado de cumplimiento de los controles de la norma ISO 27001:2022, garantizando que estos no solo estén debidamente documentados, sino que también sean efectivamente resilientes ante las amenazas actuales.

Abordar este problema beneficiará a la comunidad educativa al ampliar el alcance de las herramientas BAS, que generalmente se utilizan para simular ataques, integrándolas en la evaluación de los controles de la norma ISO 27001:2022. Además, contribuirá a la comunidad científica al proporcionar un mapeo detallado de las técnicas del marco MITRE ATT&CK con los controles establecidos en la norma ISO 27001:2022. Esta conexión entre la parte ofensiva y defensiva permite que ambos enfoques cooperen entre sí y puedan entrelazar funciones, integrando ambas partes para una misma finalidad y objetivo.

Siendo este problema relevante porque responde a la necesidad del cumplimiento normativo continuo que no existe en las organizaciones. Al implementarlo, contribuye al ahorro de costos al reducir la necesidad de pruebas de penetración externas, fomenta la concientización sobre la seguridad de la información en el personal de seguridad ofensiva interna y facilita la mejora en el cumplimiento de los controles establecidos por la norma ISO 27001, fortaleciendo así la postura de seguridad de la organización en su conjunto.

1.3. Estructura del trabajo

La estructura del presente trabajo se distribuye de la siguiente manera:

Capítulo 1 - Introducción: En este apartado se define a modo general la necesidad de la investigación, motivación y planteamiento del problema.

Capítulo 2 - Estado del arte: En este apartado se desarrollan conceptos necesarios para entender la metodología y se presentan investigaciones previas existentes del problema.

Capítulo 3 - Objetivos concretos y metodología de trabajo: En este apartado se describen los objetivos del trabajo y la metodología que se aplicará para ejecutarlo.

Capítulo 4 - Desarrollo especifico de la contribución: Se desarrollan los pasos de la metodología propuesta para abordar el problema.

Capítulo 5 - Conclusiones y trabajo futuro: Se brindan las conclusiones en base a la evaluación realizada, asimismo se brindan trabajos y enfoques futuros.

2. Estado del arte

2.1. Enfoques para la seguridad informática

Las organizaciones dependiendo de su nivel de madurez y experiencia para proteger sus equipos de seguridad pueden optar por diferentes medidas para mejorar su seguridad informática, entre las cuales, se encuentran:

- Hardening o bastionado: Esta sería el primer nivel, según CTX (2024) tiene como objetivo la implantación de medidas y políticas de seguridad que nos permitan reducir la vulnerabilidad de los equipos y herramientas informáticas frente a ataques.
  Algunos ejemplos:
  - Eliminar todo software que la empresa ya no use o que esté obsoleto.
  - Actualizar el firmware de los equipos a su última versión para que incluyan las nuevas opciones de protección.
  - Implementar antivirus o antimalware para evitar, prevenir o actuar rápidamente ante ataques eternos.
  - Desarrollar una política de contraseñas segura.
- Tecnologías de detección y respuesta: Este sería el segundo nivel y se enfoca en amenazas que no fueron bloqueadas por las medidas implementadas en el hardening. Estas abarcan soluciones como NDR y EDR.
  - Según Vectra (2024), un NDR es una herramienta que supervisa continuamente la red de una organización para detectar ciberamenazas y comportamientos anómalos mediante herramientas o técnicas no basadas en firmas y responde automáticamente a estas amenazas.
  - De acuerdo a IBM (2024), un EDR es una herramienta que emplea análisis en tiempo real y automatización impulsada por IA para proteger a los dispositivos finales que usan los usuarios de una organización contra las amenazas que superan el software antivirus y otras herramientas tradicionales de seguridad endpoint instaladas.
- Escaneo y gestión de vulnerabilidad: Este sería un tercer nivel en donde se busca identificar debilidades explotables en los hosts de la organización, para ello se programan escaneos semanales y/o mensuales a fin de evaluar nuevas

vulnerabilidades existentes y realizar la mitigación de las mismas. Ejemplo de herramientas tenemos a Nessus, Tenable, NMAP, OpenVAS, etc.

- Pentesting: Este sería el cuarto nivel, en el cual se busca explotar vulnerabilidades, errores de configuración y otras debilidades a fin de dar a conocer los hallazgos y elaborar un informe sobre el rendimiento defensivo de la organización. Sin embargo, estos no son llevados a cabo de manera continua debido al tiempo y costo de planificación y ejecución.
- Ejercicios de Red Team: Este sería el quinto nivel, este tipo de ejercicio tiene un enfoque totalmente ofensivo en el cual además de explotar las vulnerabilidades, incluyen técnicas de post explotación como movimiento lateral, persistencia y elevación de privilegios. Sin embargo, aún carece de una continua validación del rendimiento defensivo de la organización debido a que tienen un alcance limitado por el riesgo de dañar los sistemas, siendo además acotado el contenido de ataques en base al conocimiento y experiencia de los miembros del Red Team.
- Simulación de ataques: En este último nivel estarían las herramientas BAS, las cuales permiten realizar simulación de ataques en los entornos de producción, permitiendo realizar pruebas a una medida continua y a demanda en los dispositivos de la organización.

2.2. Evolución del pentesting

Un pentesting se realiza en un único punto en el tiempo, proporcionando una instantánea de la seguridad en el momento específico de las pruebas. Según Pilleux (2021), existen diversos tipos de pentesting, entre los cuales se incluyen: pentesting de infraestructura (enfocado en firewalls, servidores, routers, switches, computadoras e impresoras), pentesting de aplicaciones web y móviles (para evaluar la seguridad de aplicaciones, bases de datos y servidores web), client-side pentesting (dirigido a la seguridad de servicios utilizados por los empleados, como correo electrónico y suites de oficina), pentesting de redes inalámbricas (para examinar las conexiones y dispositivos conectados a la red Wi-Fi), pentesting de ingeniería social (evaluación de las personas, en especial los empleados, para detectar vulnerabilidades humanas) y pentesting físico (que simula amenazas físicas con el objetivo de comprometer entradas a las instalaciones).

Asimismo, el pentesting debe llevarse a cabo procurando no dañar la infraestructura a evaluar, para ello se definen las acciones que los profesionales asignados al ejercicio de pentesting pueden o no realizar, los cuales quedan establecidas en el alcance de las pruebas. Por ejemplo, en Li et al. (2015), se realiza una investigación de pentesting en entornos en nube, con el objetivo de minimizar el daño colateral en producción al ejecutar estas pruebas. Para ello, se plantea que en este tipo de ambientes resulta más factible evitar este daño mediante el clonado en paralelo de máquinas virtuales. En base a esto, se propone realizar el clonado en vez de una migración en tiempo real de las máquinas virtuales desplegadas, desarrollando "Potasium", una herramienta que facilita el clonado usando Openstack, permitiendo así evaluar las maquinas clonadas sin causar daño colateral a las maquinas en producción.

Adicionalmente, el enfoque actual de pentesting está experimentando un cambio hacia la automatización, con el objetivo de ejecutar automáticamente las etapas de reconocimiento, descubrimiento y explotación. Así como también, un cambio hacia la integración modular, esto se evidencia en las investigaciones realizadas que buscan consolidar diferentes herramientas de pentesting en una única plataforma.

De hecho, en la misma investigación de Pilleux (2021) se desarrolla una plataforma que automatiza la ejecución de múltiples herramientas de pentesting. Para ello, hace uso de contenedores para cada una de las herramientas que la componen: ZAP, Wapiti y W3AF. La aplicación se desarrolla con una arquitectura modular, que permite su extensión mediante la implementación de módulos adicionales específicos que se integran con la plataforma.

La investigación de Cano (2019) identifica el problema de un proceso manual de pentesting con herramientas disgregadas. Para solucionarlo, desarrolla una herramienta que ejecuta de forma automática las etapas de reconocimiento, descubrimiento y explotación, además de generar un informe de auditoría y evidencias de las explotaciones. Para ello, propone un modelo incremental de funcionalidades (se escogen pocas herramientas para cada etapa). Este modelo es incremental tanto verticalmente (porque el módulo de reconocimiento se integra con el de descubrimiento y luego con el de explotación) como horizontalmente (en cada etapa se pueden añadir nuevas herramientas).

2.3. Herramientas BAS

BAS (Breach and Attack Simulation) es una herramienta que permite a las organizaciones simular ataques cibernéticos. Al igual que el pentesting tradicional, BAS se enfoca en explotar vulnerabilidades, errores o debilidades en los sistemas, pero en base a una lista de ataques definidos que se ejecutan de forma automatizada, lo que lo convierte en una solución mucho más eficiente y flexible.

Una de las principales ventajas de BAS es su capacidad para realizar pruebas de seguridad de manera diaria. A diferencia del pentesting convencional, que se realiza en intervalos de tiempo específicos y requiere esfuerzos manuales considerables (por parte del profesional externo o interno contratado), BAS facilita la automatización de los escenarios de ataque, lo que posibilita su ejecución continua en los sistemas productivos de la organización.

Por ello, en la actualidad se propone el uso de BAS como el reemplazo de un pentesting, ya que esta actividad requiere al menos 30 días para su realización. En cambio, con una herramienta BAS se puede realizar en 1 día y a demanda, lo que convierte al BAS en una herramienta de pentesting automatizado. (Ben-Yossef, 2024)

En cuanto a las técnicas empleadas en las simulaciones BAS, estas incluyen simulaciones de tráfico de red o comandos basados en host. Aunque suelen utilizarse para realizar pruebas de seguridad operativa contra tácticas de amenazas persistentes avanzadas (APT) o ciberataques emergentes, también podrían servir para validar la eficacia y el estado de implementación de los controles de seguridad. A diferencia de otros enfoques, no se centra en facilitar la explotación, sino en ejecutar todo un escenario de intrusión, el cual podría configurarse para replicar un control de seguridad específico, permitiendo comprobar cómo reaccionan las defensas del entorno y contribuyendo a reducir el tiempo necesario para auditar los controles de seguridad.

Según Ramiro (2019), las plataformas BAS permiten a las organizaciones ejecutar simulaciones continuas de ciberseguridad bajo demanda en cualquier momento sin afectar a los sistemas de producción. Simula ataques múltiples, internos o externos, centrados en las vulnerabilidades más recientes. A través de estas simulaciones, se exponen posibles brechas de seguridad, lo que proporciona a las organizaciones la oportunidad de evaluar si la

arquitectura de seguridad brinda la protección adecuada y si las configuraciones se implementaron correctamente.

En resumen, una herramienta BAS se centra en 5 principales capacidades:

- Ejecutar ciberataques de forma controlada y segura en entornos reales.
- Determinar si los ataques han sido bloqueados o mitigados.
- Identificar si se generaron eventos o alertas producto de los ataques generados.
- Permitir ejecutar las simulaciones repetidamente para evaluar las defensas.
- Alojar una biblioteca extensible de ataques, incluidos ataques personalizados por los usuarios.

De acuerdo a Engström y Lagerström (2022) quienes realizaron la revisión de investigaciones asociadas a simulaciones de ataques publicadas entre 1999 y 2019, esta materia aún no se ha abordado como un tema de investigación diferenciado. La mayoría de investigaciones proponen herramientas de simulación básicas, concluyendo que las cuestiones y observaciones realizadas hasta ahora podrían indicar un estado pobre e inmaduro del tema. Adicionalmente, menciona que un punto débil constante en los trabajos revisados era la validez externa, ya que muchos se basaban en ejemplos y escenarios hipotéticos.

Asimismo, en Kruck (2023), indica que el concepto BAS es nuevo en ciberseguridad y construido desde ideas como “pentesting automático”. Este se enfoca en como las defensas y defensores responden a una multitud de ciberataques, incluyendo que ataques son bloqueados, detectados y alertados.

En cuanto al funcionamiento práctico de un BAS, en AttackIQ (2022) se detalla:

1. El operador escoge el comportamiento del atacante a simular.
2. BAS ejecuta la operación en el entorno a evaluar.
3. Los operadores observan la respuesta de las herramientas al ataque: Si detecta, bloquea o alerta.

Adicionalmente, en el estudio de Ferraz (2022), se propone una plataforma que facilita la ejecución de escenarios de ataque en un conjunto de máquinas de prueba, mientras recopila registros y alertas generadas por herramientas de seguridad para evaluar si la infraestructura de seguridad es capaz de detectar o bloquear partes del ataque. Además, permite identificar qué técnicas de ataque pueden ser gestionadas por la infraestructura y cuáles no. La

plataforma también etiqueta automáticamente las técnicas que son detectadas y aquellas que no lo son. Para ello, se emplea una arquitectura compuesta por:

- Un agente remoto que recibe y ejecuta comandos desde un servidor central.
- Una plataforma central que coordina los agentes.
- Un motor de recolección de registros y procesamiento, que evalúa el comportamiento frente a las técnicas utilizadas.
- Un modelo de evaluación para clasificar el rendimiento de toda la infraestructura de seguridad

Finalmente, en la tesis doctoral de Kruck (2023) se presenta la primera investigación que propone el uso de BAS aplicado a los controles de seguridad de la información. Para ello, toma como referencia el estándar NIST 800-53, con el objetivo de determinar si la herramienta BAS puede emplearse para supervisar continuamente los controles y detectar cambios que provoquen no conformidades. Utiliza herramientas de Kali Linux como plataforma BAS para generar ataques, y en conjunto con un SIEM, evalúa si los ataques fueron mitigados o detectados por las defensas. Prueba su arquitectura en un entorno virtualizado configurado para cumplir con los controles de la NIST 800-53. Al final, valida la hipótesis de la auditoria continua de los controles, pudiéndose realizar pruebas a intervalos de 10 minutos por control. El estudio concluye que la brecha de conocimiento entre las capacidades de las técnicas BAS y la validación de los controles de aseguramiento de la información constituye un área prometedora para investigación y experimentación.

2.4.MITRE ATT&CK

El marco MITRE ATT&CK fue desarrollado en 2013 como un catálogo de tácticas, técnicas y procedimientos (TTPs) basados en observaciones de ciberataques en el mundo real. Para ello cataloga un determinado número de tácticas, donde cada táctica contiene grupos de técnicas y cada técnica contiene un conjunto de procedimientos. (MITRE, 2024a)

En IBM (2024) se brinda las siguientes definiciones:

- Tácticas: Cada táctica representa un objetivo específico del atacante. Siendo estas las que se corresponden con las etapas de un ciberataque. En la Tabla 1 se muestra la lista completa de las tácticas.

Tabla 1. *Tácticas MITRE ATT&CK.*

Táctica	Descripción
Reconocimiento	Es la recopilación de toda información relacionada con la víctima.
Desarrollo de recursos	Creación, compra o robo de recursos de la víctima que se usarán para el ataque.
Acceso inicial	Uso de varios vectores de ataque para lograr acceso a la red.
Ejecución	Ejecución de código malicioso en uno o varios sistemas de la víctima.
Persistencia	Lograr mantener acceso a los sistemas de la víctima a pesar de reinicios, cambio de credenciales o interrupciones.
Elevación de privilegios	Obtener acceso o permisos de nivel superior. Ejemplos: Administrador, SYSTEM o root.
Evasión de defensa	Evitar ser detectado dentro del sistema.
Acceso con credenciales	Robo de cuentas de usuario y contraseñas.
Descubrimiento	Investigar el entorno de la víctima: sistema y red interna.
Movimiento lateral	Obtener acceso a recursos adicionales de la red de la víctima.
Recopilación	Recopilar datos de interés de la víctima.
Comando y control	Establecer comunicaciones con sistemas bajo el control del atacante dentro de la red de la víctima.
Exfiltración	Robar datos de la víctima.
Impacto	Manipular, interrumpir o destruir datos y sistemas de la víctima.

Fuente: Elaboración propia.

- Técnicas: Representan la forma en la cual se llevarán a cabo las tácticas. Por lo que cada táctica puede tener 1 o más técnicas, asimismo cada técnica proporciona la siguiente información:
    - Descripción de la técnica.
    - Subtécnica asociada.
    - Ejemplos de procedimientos relacionados.
    - Mitigaciones: Prácticas de seguridad que bloquean la técnica.
    - Métodos de detección.

El estudio de Rahman & Williams (2022) relacionado con el mapeo entre las técnicas del marco MITRE ATT&CK y los controles de la NIST 800-53, propone que las organizaciones decidan los controles a implantar en base a las técnicas ATT&CK usadas por los atacantes, indicando que los controles NIST deberían ser adoptados en primer lugar para cubrir la mayor cantidad de técnicas ATT&CK. Para ello, investiga si dado un determinado control de la NIST puede mitigar una o más técnicas, encontrando que solo 101 controles de 298 pueden mitigarlas, mientras que 53 técnicas no pueden ser mitigadas por ningún control. Como resultado de su análisis, presentan una lista de 20 controles clave que cubren la mayor cantidad de técnicas, recomendando su adopción prioritaria por las organizaciones.

A partir del análisis del estado del arte actual, se concluye lo siguiente:

- Existen investigaciones en las cuales se han utilizado herramientas BAS para validar controles de seguridad, lo que evidencia que estas herramientas podrían contribuir a mejorar el ciclo de mejora continua en ciberseguridad.
- Las investigaciones relacionadas con herramientas BAS no cuentan mucho con validez externa, generalmente las pruebas se realizan en entornos de laboratorio.
- Si bien las investigaciones han demostrado la viabilidad de aplicar las herramientas BAS a auditorías de ciberseguridad, aun se requiere el desarrollo de una metodología que guíe la implementación.
- No se han encontrado estudios que relacionen los controles de la ISO 27001 con el marco ATT&CK, por lo que es un área de investigación aún no documentada.

3. Objetivos concretos y metodología de trabajo

3.1. Objetivo general

Documentar los pasos y uso de tecnologías que permitan evaluar los controles de seguridad establecidos en la norma ISO 27001:2022 mediante la implementación de herramientas BAS y el marco MITRE ATT&CK.

3.2. Objetivos específicos

- Desarrollar un mapeo que permita alinear las técnicas del marco MITRE ATT&CK con los controles establecidos en la norma ISO 27001:2022.
- Realizar un análisis comparativo de diversas herramientas BAS existentes, identificando la herramienta más adecuada para llevar a cabo la evaluación de los controles de la norma ISO 27001:2022.
- Elaborar un procedimiento metodológico para la evaluación de los controles de la norma ISO 27001:2022 utilizando la herramienta BAS seleccionada.
- Evaluar el uso de la metodología desarrollada en la auditoría continua de los controles de la norma ISO 27001:2022.

3.3. Metodología del trabajo

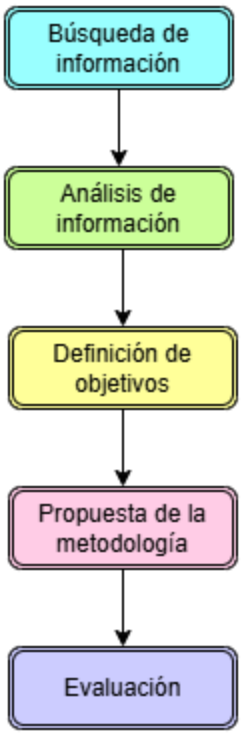
Para el desarrollo del presente trabajo, se decide abordar el problema de investigación realizando los siguientes pasos:

- **Fase 1 – Búsqueda de información:** Se realizó una indagación académica abarcando los siguientes puntos:
    - Revisión minuciosa de artículos científicos, tesis de maestría, tesis doctorales, etc.; asimismo se revisó el estado del arte hasta la fecha.
    - Revisión de la normativa ISO 27001:2022, los controles de la 27002:2022 y lista de las tácticas, técnicas y mitigaciones del marco MITRE ATT&CK.
- **Fase 2 – Análisis de información:** Con la información recopilada, se procedió a analizar las relaciones existentes entre las herramientas BAS, los controles de la ISO 27001:2022 y el marco MITRE ATT&CK, identificándose el área de estudio con falta de investigación.

- **Fase 3 – Definición de objetivos:** Una vez identificado el problema, se deciden y detallan el objetivo general y los objetivos específicos del trabajo.
- **Fase 4 – Propuesta de la metodología:** Se diseñaron los pasos metodológicos a seguir, que incluyen el mapeo de los controles ISO 27001 a las técnicas del marco MITRE ATT&CK, la elaboración de la matriz en Mitre Navigator, el despliegue y administración de la herramienta BAS, etc.
- **Fase 5 – Evaluación:** Con el fin de validar la metodología propuesta, se implementan los pasos en un entorno empresarial, demostrando que esta puede ser adaptada al contexto de la organización que desea hacer uso de ella.

En la Figura 4 se muestra el flujo de la metodología seguida para la elaboración del presente trabajo.

Figura 4. *Proceso de la metodología de trabajo.*



Fuente: Elaboración propia.

4. Desarrollo específico de la contribución

4.1. Identificación de requisitos

En el presente apartado se indican los requisitos necesarios para aplicar la metodología adecuadamente, a continuación, se detallan:

4.1.1. Contexto de uso

Se propone la metodología para ser utilizada por toda organización, empresa o institución que hace uso de la norma ISO 27001 y desea realizar una evaluación continua de los controles ISO 27001 aplicables.

Si bien, como se detallará más adelante, el proceso de mapeo entre los controles de la ISO 27001 con las tácticas y técnicas usadas del MITRE ATT&CK se realizó utilizando la versión 2022 de la norma, el procedimiento descrito también puede aplicarse en versiones futuras de la normativa.

4.1.2. Identificación de roles

En la Tabla 2 se muestran los roles implicados durante la aplicación de la metodología:

Tabla 2. *Roles involucrados en la metodología.*

Rol	Descripción
Alta Dirección	Responsable de proporcionar el liderazgo estratégico, apoyo y aprobación para la implementación de la metodología. Brindan los recursos necesarios y se aseguran de tomar decisiones en base a los hallazgos encontrados posterior a la implementación.
Auditor interno de cumplimiento	Responsable de definir el inventario de activos y los controles ISO 27001 que son aplicables a la organización. Asimismo, coordina con el evaluador de seguridad ofensiva para definir la lista de controles ISO 27001 a evaluar en la metodología. Encargado de validar los resultados de la ejecución de los ataques simulados en la herramienta BAS.
Evaluador de seguridad ofensiva	Responsable de definir las tácticas, técnicas del MITRE ATT&CK y su orden de aplicación para la evaluación de la metodología.

	Encargado de administrar la plataforma BAS y ejecutar los ataques simulados. Apoya a validar los resultados de las pruebas, brindando su conocimiento de las técnicas ATT&CK.
Administrador de infraestructura TI	Responsable de brindar los accesos a los recursos tecnológicos (redes, servidores, etc.). Define la lista de herramientas de seguridad involucradas en base a la topología de pruebas definida por el Líder Técnico. Ayudará a identificar el resultado de la ejecución de ataques en las herramientas de seguridad. Ejecutará los cambios o medidas correctivas derivadas de los hallazgos de la aplicación de la metodología.
Lider técnico	El profesional encargado de coordinar las actividades de los equipos técnicos, supervisando la aplicación de la metodología y la correcta implementación de las pruebas de evaluación de los controles. Define la topología de pruebas. Responsable de traducir los resultados de las evaluaciones en acciones técnicas concretas para mejorar la seguridad de la infraestructura. Comunica a la Alta Dirección los resultados.
Asistente técnico	Encargado de apoyar a la implementación de la metodología. Tiene un rol transversal durante el desarrollo de las actividades. Coordina con el líder técnico, auditor interno de cumplimiento y evaluador de seguridad ofensiva para la asignación de tareas.

Fuente: Elaboración propia.

Es importante destacar que los roles mencionados no están asociados a una persona específica ni a un único miembro del personal. Cada rol puede ser asignado a una o varias personas, y, de igual manera, una persona puede desempeñar múltiples roles en el ámbito de la metodología.

4.1.3. Tecnologías implicadas

Para la implementación de la metodología, es necesario que el personal asignado disponga de conocimientos en las siguientes tecnologías:

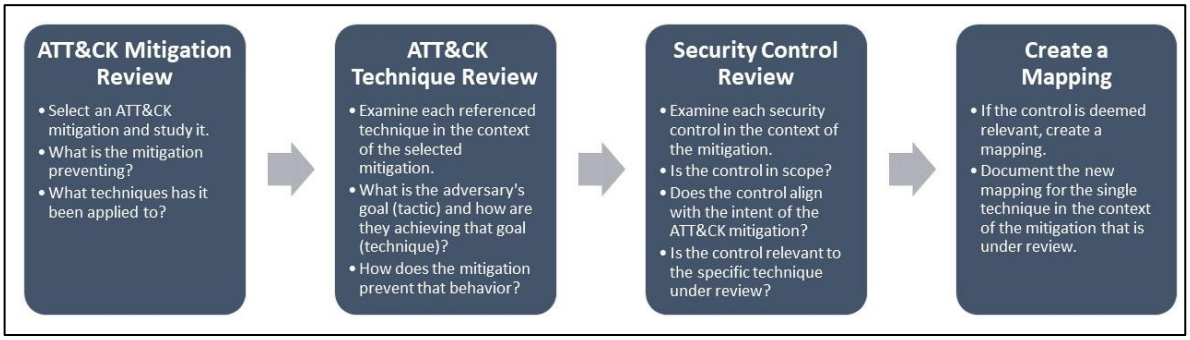
- Microsoft Excel: Herramienta que permite la visualización y ordenamiento de los datos recolectados, además de brindar una representación básica durante el uso de archivos en formato CSV, JSON y TXT.
- Python: Lenguaje de programación utilizado para desarrollar los scripts necesarios para el tratamiento, mapeo y exportación de los archivos que se emplearán durante la implementación de la metodología.
- Marco MITRE ATT&CK: Catálogo que incluye tácticas, técnicas y procedimientos empleados por los atacantes, también cuenta con una lista de mitigaciones que agrupan las técnicas y subtécnicas según acciones similares destinadas a reducir el riesgo de explotación.
- MITRE ATT&CK Navigator: Herramienta web que permite representar gráficamente el mapeo de los controles de la ISO 27001:2022 a las técnicas del marco ATT&CK. De esta forma, el personal asignado puede tener una representación gráfica de los resultados obtenidos.
- BAS Caldera: Plataforma BAS necesaria para realizar la simulación de las tácticas y técnicas del MITRE ATT&CK en base a los controles de la ISO 27001:2022.
- Normativa ISO 27001:2022: Estándar internacional que en su versión de 2022 incluye 93 controles de seguridad de la información, organizados en cuatro categorías: 8 controles para personas, 14 controles físicos, 34 controles tecnológicos y 37 controles organizacionales.
- Lista de controles ISO 27002:2022: Estándar internacional que desarrolla los controles de la ISO 27001, de esta forma permite obtener una descripción más detallada de cada control.
- Docker: Software que permite realizar la creación del contenedor para el BAS Caldera, permitiendo su portabilidad y ejecución en cualquier tipo de sistema operativo.

4.1.4. Metodología de mapeo MITRE ATT&CK a controles ISO 27001

En Hardey (2021) se nos muestra una serie de pasos para realizar el mapeo de controles NIST 800-53 a técnicas del marco MITRE ATT&CK. Su metodología propuesta, representada en la Figura 5, se basa en 4 pasos:

- Revisión de la lista de mitigaciones MITRE ATT&CK.
- Revisión de las técnicas MITRE ATT&CK: Entender los objetivos del adversario en la técnica y subtécnica.
- Revisión de los controles de seguridad NIST en contexto de la mitigación ATT&CK.
- Creación del mapeo por cada control a la técnica o subtécnicas asociadas.

Figura 5. *Pasos para mapeo técnicas ATT&CK a NIST 800-53.*



Fuente: Hardey Steven, 2021.

Como se muestra en la Tabla 3, en el presente trabajo se propone la siguiente metodología, basada en la investigación mencionada, que consta de seis pasos para realizar el mapeo de las tácticas MITRE ATT&CK a controles ISO 27001:

Tabla 3. *Pasos para mapeo técnicas ATT&CK a controles ISO 27001.*

Fase	Descripción	Roles Involucrados
1. Obtención de las Mitigaciones MITRE ATT&CK	Descargar las mitigaciones desde la página oficial de MITRE ATT&CK y en formato Excel.	Evaluador de seguridad ofensiva, Líder técnico

2. Revisión de las Mitigaciones ATT&CK	Revisión y análisis de las mitigaciones ATT&CK con participación de los roles mencionados.	Evaluador de seguridad ofensiva, Auditor interno de cumplimiento, Líder técnico
3. Obtención de la normativa ISO 27001 e ISO 27002	Adquirir las normativas ISO 27001 e ISO 27002 en su versión 2022.	Alta Dirección
4. Revisión de las Normativas ISO 27001 e ISO 27002	Análisis detallado de las normativas para entender los controles y su aplicación.	Auditor interno de cumplimiento, Líder técnico
5. Mapeo de Controles ISO 27001 a Mitigaciones ATT&CK	Relacionar los controles ISO 27001 con las mitigaciones de MITRE ATT&CK, considerando ciertas restricciones.	Auditor Interno de cumplimiento, Evaluador de seguridad ofensiva, Líder técnico
6. Mapeo de Controles ISO 27001 a Técnicas MITRE ATT&CK	Trasladar las mitigaciones a las técnicas específicas de MITRE ATT&CK, creando un archivo Excel final y un mapa en ATT&CK Navigator.	Auditor Interno de cumplimiento, Evaluador de seguridad ofensiva, Líder técnico

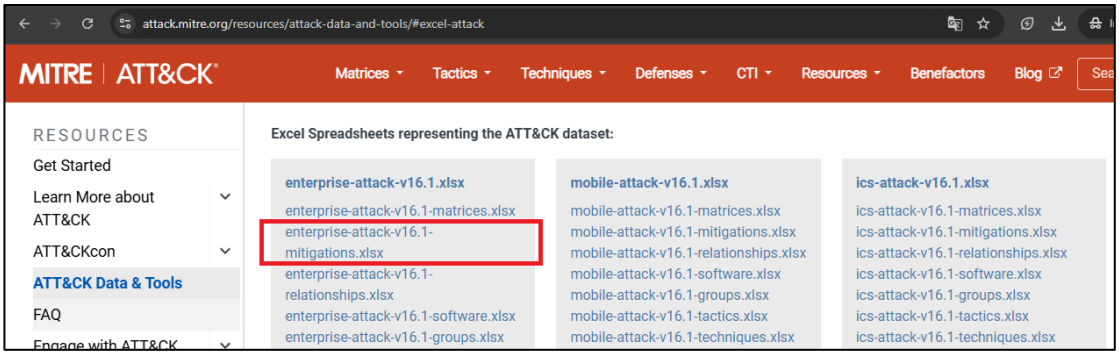
Fuente: Elaboración propia.

A continuación, se describe a detalle los pasos a realizar:

1. **Obtención de las mitigaciones MITRE ATT&CK:** Desde la página oficial MITRE (2024b) se pueden visualizar la lista completa de las mitigaciones ATT&CK, tal como se visualiza en la Figura 6. Asimismo, desde MITRE (2024c) se descarga en formato Excel la lista de mitigaciones actuales, en la Figura 6 se muestra la opción de descarga.

Los roles involucrados para la actividad, serían los de “Evaluador de seguridad ofensiva” y “Líder técnico”.

Figura 6. *Opción para descargar la lista de mitigaciones MITRE ATT&CK.*



Fuente: Elaboración propia.

2. **Revisión de las mitigaciones ATT&CK:** Proceder con la revisión y análisis de cada una de las mitigaciones existentes, este paso debe ser realizado por los roles de “Evaluador de seguridad ofensiva”, “Auditor interno de cumplimiento” y “Líder técnico”, quienes deben reunirse para revisar de la lista actualizada.
3. **Obtención de la normativa ISO 27001 e ISO 27002 en sus versiones 2022:** Ambas normativas son de pago y se asume que la organización que usará la metodología propuesta en este trabajo dispone de ambos documentos proveídos por la “Alta Dirección”. En caso no contar con ellos, pueden adquirirse a través de las siguientes páginas oficiales: ISO 27001:2022 (https://www.iso.org/standard/27001) e ISO 27002:2022 (https://www.iso.org/standard/75652.html). La metodología ISO 27001 desarrolla los pasos para realizar la implantación del SGSI, mientras que la ISO 27002 nos muestra a detalle los controles de la norma 27001.
4. **Revisión de las normativas ISO 27001 e ISO 27002:** Proceder con una revisión exhaustiva de ambas normas para poder identificar el porqué de cada control y entender la finalidad y alcance de su aplicación. Este paso debería ser realizado por los roles de “Auditor interno de cumplimiento” y “Líder técnico” en conjunto para poder identificar adecuadamente los controles a evaluar en el siguiente paso.
5. **Mapeo de controles ISO 27001 a mitigaciones ATT&CK:** En este paso, los roles involucrados son “Auditor Interno de cumplimiento”, “Evaluador de seguridad

ofensiva" y el "Líder Técnico". Para realizar el mapeo tener en cuenta las siguientes consideraciones:

a. De la lista de controles ISO 27001 seleccionados, validar cuales mitigaciones MITRE ATT&CK pueden cumplir con dicho control.
b. No mapear las siguientes mitigaciones:
    i. M1055 (Do Not Mitigate): Debido a que engloba técnicas cuya mitigación aumenta el riesgo de compromiso al ser aplicada.
    ii. M1056 (Pre-compromise): Debido a que engloba técnicas que no pueden ser mitigadas con controles preventivos, agrupando técnicas ATT&CK que se encuentran en las etapas de Reconocimiento y Desarrollo de recursos.
c. No todos los controles de la ISO 27001 tienen una mitigación asociada:
    i. Iniciar con el mapeo de los controles tecnológicos de la norma ISO 27001 a mitigaciones ATT&CK.
    ii. Con respecto a los demás tipos de controles, su asignación depende de los acuerdos entre los roles involucrados. Sin embargo, durante el mapeo realizado en el estudio actual solo se encontró coincidencias en los siguientes controles no tecnológicos: 5.7, 5.15, 5.17 y 6.3 (Revisar Anexo A).
d. Elaborar un archivo Excel que contenga el resultado del mapeo realizado, teniendo mínimamente las columnas "Código Control" y "Mitigación asociada". Siendo esta última columna en la cual se debe ir colocando la mitigación o mitigaciones que corresponden con el control respectivo. En la Figura 7 se muestra parte de la hoja Excel elaborada (Revisar Anexo A para visualizar la tabla completa).

Figura 7. *Hoja Excel de controles ISO 27001.*

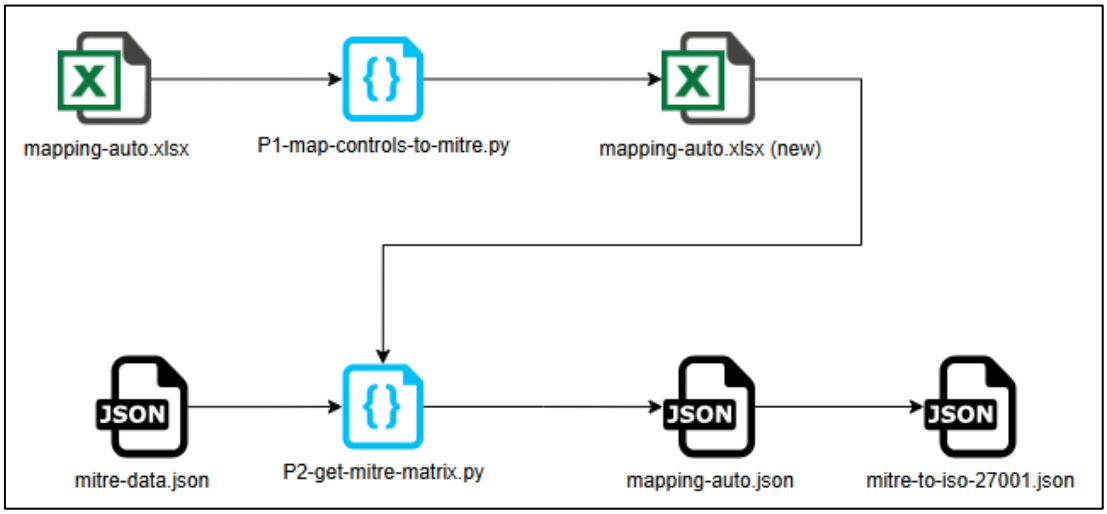
Codigo Control	Control tecnologico	Mitigación asociada
5.7	Inteligencia de amenazas	M1019
5.15	Control de acceso	M1035, M1030, M1022, M1024, M1039, M1043
5.17	Información de autenticación	M1027
6.3	Concienciación, educación y formación en seguridad de la información	M1017
8.1	Dispositivos de punto final de usuario	M1033, M1034, M1037, M1040, M1041, M1049, M1053, M1021
8.2	Derechos de acceso privilegiado	M1026, M1052, M1018
8.3	Restricción del acceso a la información	M1035, M1022, M1024, M1039, M1041, M1048
8.4	Acceso al código fuente	M1038, M1044
8.5	Autenticación segura	M1032, M1036, M1027, M1015
8.6	Gestión de la capacidad	M1042, M1028

Fuente: Elaboración propia.

6. **Mapeo de controles ISO 27001 a técnicas MITRE ATT&CK:** En este paso se obtiene el archivo final, en el que se deben presentar todas las técnicas del marco MITRE ATT&CK junto con los controles ISO 27001 asociados. En el paso 5, ya se estableció la relación entre los controles ISO 27001 y las mitigaciones de ATT&CK correspondientes. Ahora, en esta fase, se transfiere la aplicación de la mitigación a las técnicas asociadas, lo que permite generar el mapeo entre los controles de ISO 27001 y las técnicas específicas de ATT&CK. Los roles involucrados serían "Auditor Interno de cumplimiento", "Evaluador de seguridad ofensiva" y el "Líder Técnico".

   Se recomienda el uso de scripts debido a la gran cantidad de técnicas MITRE ATT&CK. Los scripts usados en el presente apartado se encuentran en el Anexo B, asimismo en la Figura 8 se muestra el diagrama de flujo del proceso.

Figura 8. *Diagrama de flujo para mapeo ISO 27001 a técnicas MITRE ATT&CK.*



Fuente: Elaboración propia.

A continuación, se detallan los pasos para obtener el mapeo final:

   a. Se agrupa el archivo Excel obtenido en el paso 5d con la lista de mitigaciones obtenida en el paso 1 para formar el archivo "mapping-auto.xlsx", sus tablas correspondientes se muestran en la Figura 9.

Figura 9. *Tablas del archivo "mapping-auto.xlsx".*

Tabla1

codigo	Name	mitigacion
5.7	Threat intelligence	M1019
5.15	Access control	M1035, M1030, M1022, M1024, M1039, M1043
5.17	Authentication information	M1027
6.3	Information security awareness, education and training	M1017
8.1	User endpoint devices	M1033, M1034, M1037, M1040, M1041, M1049, M1053, M1021
8.2	Privileged access rights	M1026, M1052, M1018

Tabla2

target_id	target name	source_id
T1001	Data Obfuscation	M1031
T1001.001	Junk Data	M1031
T1001.002	Steganography	M1031
T1001.003	Protocol or Service Impersonation	M1031
T1003	OS Credential Dumping	M1015
T1003	OS Credential Dumping	M1040

Fuente: Elaboración propia.

b. El archivo "mapping-auto.xlsx" es procesado en el script "P1-map-controls-to-mitre.py" para generar una nueva tabla en el mismo archivo conteniendo cada técnica del MITRE ATT&CK y el control ISO 27001 asociado, su vista parcial se muestra en la Figura 10.

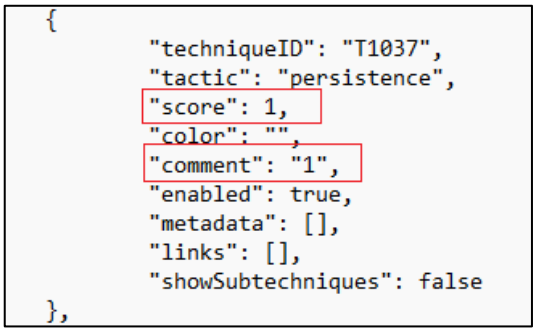
Figura 10. *Tabla generada por el script "P1-map-controls-to-mitre.py".*

target_id	target name	source_id	iso_id
T1001	Data Obfuscation	M1031	8.16
T1001.001	Junk Data	M1031	8.16
T1001.002	Steganography	M1031	8.16
T1001.003	Protocol or Service Impersonation	M1031	8.16
T1003	OS Credential Dumping	M1015	8.5, 8.9
T1003	OS Credential Dumping	M1040	8.1, 8.16

Fuente: Elaboración propia.

c. Del MITRE ATT&CK Navigator, se obtiene el archivo "mitre-data.json" el cual contiene las técnicas que cuentan con mitigación asociada (exceptuando las indicadas en el paso 5b), colocando un comentario y asignando un puntaje (score) de 1 a todas las técnicas seleccionadas, tal como se muestra en la Figura 11.

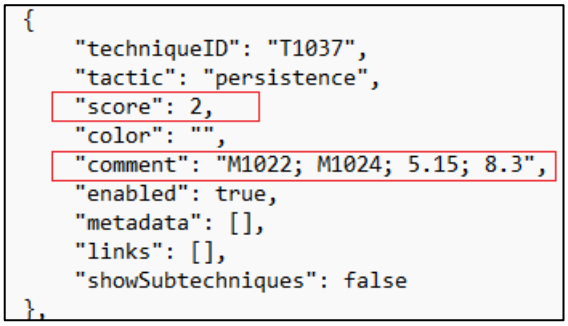
Figura 11. *Ejemplo de técnica en archivo "mitre-data.json".*



Fuente: Elaboración propia.

d. Se utiliza el script "P2-get-mitre-matrix.py" para generar el archivo "mapping-auto.json" a partir de los archivos de entrada "mapping-auto.xlsx" y "mitre-data.json". Este archivo resultante es un mapa de calor en MITRE Navigator, permitiendo visualizar las técnicas del marco MITRE ATT&CK mapeadas a controles ISO 27001. El proceso incluye la incorporación de comentarios en cada técnica, donde se detallan las mitigaciones y controles ISO asociados. Además, como se muestra en la Figura 12, el script ajusta el puntaje (score) de cada técnica en función del número de controles ISO relacionados.

Figura 12. *Ejemplo de técnica en archivo "mapping-auto.json".*

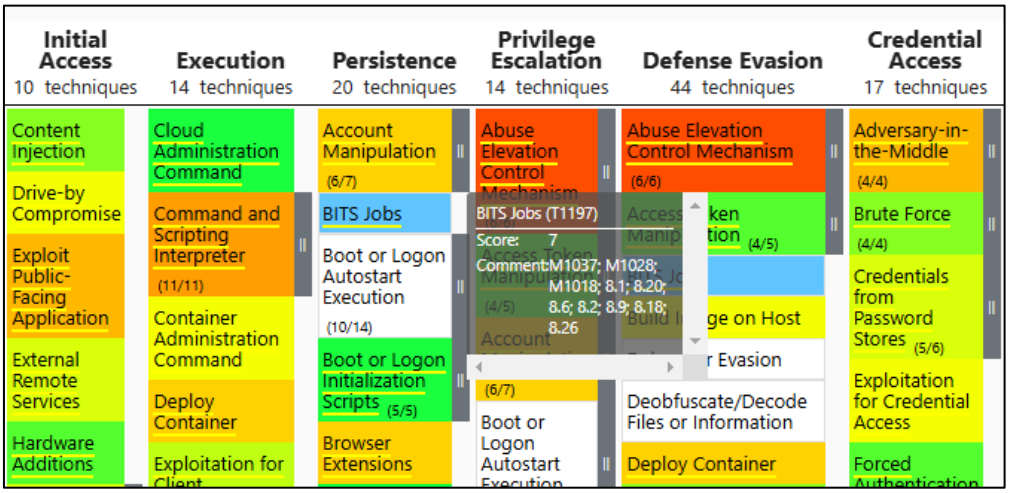


Fuente: Elaboración propia.

e. El archivo "mapping-auto.json" se carga en MITRE Navigator, donde se realizan las modificaciones finales, que incluyen la adición del título, descripción del archivo y la personalización de los colores del mapa de calor para facilitar su interpretación. A partir de esta configuración, se genera el archivo final

denominado “mitre-to-iso-27001.json”, que contiene el mapeo completo de las técnicas MITRE ATT&CK a los controles de la ISO 27001, el mapa obtenido se muestra en la Figura 13 (Revisar Anexo C para visualizar el mapa completo).

Figura 13. *Vista parcial del mapa de calor MITRE ATT&CK obtenido.*



Fuente: Elaboración propia.

4.1.5. Elección de la herramienta BAS

En base a la investigación realizada, a continuación, se presentan las diversas plataformas BAS actualmente disponibles:

1. Comerciales:
    a. Safebreach: De acuerdo con SafeBreach (2025), dentro de las funcionalidades de la plataforma BAS se encuentran:
        i. Plataforma SaaS.
        ii. Ataques predefinidos y customizables: Cuenta con una base de datos de ataques la cual se llama “Hacker’s Playbook”, con más de 30000 métodos de ataque. Asimismo, permite crear ataques personalizados y programar su ejecución.
        iii. Lista de vulnerabilidades por prioridad: Se integra con las herramientas de seguridad para poder listar las vulnerabilidades encontradas y priorizarlas para su mitigación.
        iv. Analizar con datos en tiempo real: Permite visualizar datos del proceso de testeo en tiempo real, obteniéndose así una visión cuantitativa de la

postura de seguridad actual que permite identificar brechas, agilizar remediación y reducir el riesgo.

v. Se integra con el marco MITRE ATT&CK para generar un mapa de calor en base al resultado de las simulaciones sobre las técnicas ATT&CK que se evalúan.
vi. Se integra con otras herramientas de seguridad para compartir datos de los resultados tales como SIEM o SOAR.
vii. Permite generar reportes, dashboards personalizados, provee un puntaje único sobre la postura de seguridad de la organización.
viii. Cuenta con una API que permite compartir datos dentro y fuera de la herramienta BAS.

b. Cymulate: De acuerdo con Cymulate (2025), las funcionalidades de la herramienta son:
    i. Plataforma SaaS.
    ii. Se integra con el framework MITRE ATT&CK para representar las técnicas ATT&CK disponibles, seleccionarlas y/o agruparlas de forma gráfica para sí poder definir templates de ataques.
    iii. Permite validar las siguientes herramientas de seguridad: EDR, NGFW, Proxy, Email Gateway, WAF, DLP; abarcando marcas como Qradar, Cortex XDR, Azure Sentinel, Splunk, Palo Alto, Trendmicro, Fortinet, Checkpoint Harmony Endpoint, etc.
    iv. Cuenta con una API disponible.
    v. Se integra con otras herramientas de seguridad como SIEM, SOAR, GRC.
    vi. Funciona en base a un agente instalado localmente en las máquinas sobre las cuales se ejecutan los ataques.
    vii. Permite generar reportes de los ataques simulados, visualizar el flujo de ataque y el número de máquinas afectadas.
    viii. Permite usar técnicas pre definidas y también customizar nuevas técnicas y crear escenarios de ataque.
c. Redscan: De acuerdo con Redscan (2025), este servicio BAS cuenta con las siguientes características:

i. Se trata de un servicio que crea simulaciones de ataque customizadas para las organizaciones, para ello crea las simulaciones en base al conocimiento de respuesta ante incidentes, casos atendidos y testeo de expertos de Redscan.
ii. Provee consultaría de expertos para las mitigaciones correspondientes post-simulación de ataques.
iii. Los expertos de Redscan pueden crear escenarios de exfiltración de datos, pruebas de phishing, movimiento lateral y ataques de malware en máquinas de pruebas.

d. Pentera: De acuerdo con Pentera (2025), las funcionalidades del producto son:
   i. Ofrece tres tipos de servicios: Pentera Core (Valida la seguridad en la red interna de la organización), Cloud (Valida la seguridad de los activos en la nube) y Surface (Valida la seguridad de los activos publicados en la red externa).
   ii. Su enfoque se basa en la ejecución de pruebas de pentesting.
   iii. Te permite definir la duración de las pruebas (por cuanto tiempo van a estar ejecutándose intentos de ataques) y la cantidad de activos a evaluar.
   iv. Genera un reporte al terminar las pruebas.
   v. Te muestra los tipos de ataque ejecutados y su clasificación en base al marco MITRE ATT&CK.
   vi. Realiza escaneo de vulnerabilidades, mostrando la lista de acuerdo a su prioridad: crítica, alta, media y baja.
   vii. Permite crear escenarios de ataques del tipo: Black Box, Gray Box, Custom Box (construir tu propio escenario) y de tipo Cloud.
   viii. Cuenta con un “Wiki-help”, el cual es una guía de mitigación por cada ataque que se ha ejecutado.

e. Fortitester: De acuerdo con Fortinet (2025), dentro de las funcionalidades del producto BAS, se encuentran:
   i. Es desarrollado en modelo hardware, software y consola cloud.
   ii. Solo cataloga las técnicas disponibles en base al marco MITRE ATT&CK.

iii. Permite la generación de tráfico DDoS (TCP, UDP y HTTP flood de sesiones).
iv. Ataques web: Soporta ataques del tipo Cross site scripting, SQL injection, Bad robots, Privilege escalation, etc.
v. Permite realizar PCAP replay: Esto permite simular una comunicación TCP/IP maliciosa enviando los paquetes recolectados de un ataque captura con Wireshark o tcpdump.
vi. Integración nativa con equipos Fortigate, también envía logs vía Syslog y SNMP.
vii. Cuenta con una API para ejecutar cambios en el equipo.

f. AttackIQ: De acuerdo con AttackIQ (2025), las funcionalidades del producto BAS son las siguientes:
   i. Ofrece las versiones “Flex” (Consola Cloud, sin uso de agentes), “Ready!” (Herramienta BAS como servicio, puede ser con agentes o sin agentes) y “Enterprise” (Herramienta BAS local, es con agentes).
   ii. PCAP replay: Permite simular tráfico malicioso para testear la seguridad del perímetro.
   iii. Cuentan con escenarios para testear técnicas de ransomware post-compromiso.
   iv. Atomic testing: Permite testear técnicas de MITRE ATT&CK, asimismo customizarlas y crear “templates” los cuales son los escenarios de ataque conformados por un grupo de técnicas.
   v. Flujos de ataques: Visualización en tiempo real de las fases del ataque que se ejecuta.
   vi. Gráficos de ataque: Indican el flujo en el cual se ejecutarán las fases del escenario de ataque escogido. Es similar a un diagrama de flujo donde dependiendo del resultado de una técnica, se deriva otra o no.
   vii. Permite hacer simulaciones de phishing, envío de adjuntos maliciosos, envío de archivos con macros, realizar spam, etc.
   viii. Cuenta con una API REST.
   ix. Integración con los equipos de seguridad: firewall, SIEM para recabar las alertas generadas por el ataque.

x. Por cada técnica te brinda un resumen, recomendaciones de mitigación, clasificación MITRE ATT&CK y customización del comando a ejecutar.
xi. Cuenta con un template integrado para la validación de los controles de la NIST 800-53.

2. Open-source:
    a. InfectionMonkey: De acuerdo con Akamai (2024), dentro de las funcionalidades de la herramienta BAS, se encuentran:
        i. Es una herramienta de emulación de ataques basado en el escaneo y auto propagación usando diferentes tipos de ataques.
        ii. Permite su uso en entornos locales, contenedores, nubes públicas y privadas.
        iii. Permite generar reportes sobre el rendimiento de las pruebas.
        iv. Cuenta con una lista de exploits y lista de fingerprinting de tipo HTTP, MSSQL, SMB y SSH. Tambien tiene la opción de configurar opciones como lista de usuarios, lista de contraseñas, hash LM, hash NTLM, pares SSH; finalmente, permite simular ransomware por medio de la especificación de una carpeta a la cual otorgas el permiso de encriptar sus archivos.
        v. A través de un “island” (paciente cero) se logra propagar los “agentes monkeys”.
        vi. Permite la generación de dos tipos de reportes: Security (Brinda detalle sobre los resultados de los ataques) y Ransomware (Brinda resultados sobre la simulación de ransomware).
        vii. No está integrado con MITRE ATT&CK.
    b. Atomic Red Team: De acuerdo con Red Canary (2023), se tienen las siguientes características:
        i. Es una librería de simulación de ataques, la cual sirve como base de datos para dichas simulaciones.
        ii. Categoriza las simulaciones de ataques de acuerdo al marco MITRE ATT&CK.

iii. Hace uso de del módulo powershell “Invoke Atomic Red Team” para ejecutar las simulaciones de ataque, sin embargo, también se pueden ejecutar copiando y pegando los comandos de cada técnica en la consola de la máquina de pruebas.
iv. El módulo powershell “Invoke Atomic Red Team” se puede ejecutar en máquinas Linux y macOS si es que se instala Powershell Core. Contando también con un archivo de logs de ejecución que permite saber la fecha/hora de ejecución de las pruebas y la máquina donde se ejecutó.
v. El BAS Caldera hace uso de esta librería.

c. Network Flight simulator: De acuerdo con AlphaSOC (2024), la herramienta BAS cuenta con las siguientes características:
   i. Herramienta de simulación de ataques que permite generar tráfico de red malicioso, simulaciones como DNS e ICMP tunneling, tráfico DGA, tráfico de criptominería, solicitudes hacia servidores C2 y exfiltración de datos por SFTP o SSH.
   ii. Puede ser instalado en dispositivos macOS, Linux, FreeBSD y Windows.
   iii. Cuenta con 11 módulos con ataques diferenciados.
   iv. Trabaja solo en línea de comandos
   v. Los ataques no están clasificados en base al marco MITRE ATT&CK.
d. APTSimulator: De acuerdo con Nextron (2022), dentro de las características de la herramienta BAS, se encuentran:
   i. Es un script de Windows, usa herramientas y archivos de salida para hacer que el sistema parezca haber sido comprometido.
   ii. No usa GUI, base de datos o agentes. Solo es necesario descargar el script y ejecutarlo como administrador en la máquina de prueba.
   iii. No permite la simulación de malware.
   iv. No clasifica los ataques en base al marco MITRE ATT&CK.
   v. No se recomienda ejecutarlo en ambientes de producción.
e. Caldera: De acuerdo con MITRE (2025a), la herramienta BAS cuenta con las siguientes características:

i. La herramienta consiste de 2 componentes: El sistema central (Servidor C2, REST API e interfaz web) y los plugins (Incluye funcionalidades como agentes, reportes y colecciones de tácticas ATT&CK).
ii. Compatible con Linux, macOS y Windows (En este último caso, solo en Docker).
iii. Cuenta con grupos de tácticas MITRE ATT&CK listos para ser usados, a las cuales los denomina “Adversaries” (Adversarios).
iv. Abilities: El apartado de “Abilities” (Habilidades) contiene la base de datos completa de las técnicas ATT&CK, asimismo se pueden crear habilidades personalizadas.
v. Realiza las simulaciones de ataques en base a agentes, los cuales pueden ser instalados en Linux, Windows y macOS.
vi. Operations: El apartado de “Operations” (Operaciones) permite automatizar las campañas del Red Team, pudiendo ejecutar los “Adversaries” a demanda y tener visibilidad en tiempo real del proceso.

En base a la revisión de las funcionalidades que ofrecen las herramientas BAS disponibles en la actualidad, se concluye lo siguiente:

- Si la organización desea adquirir una herramienta BAS comercial se recomienda AttackIQ, debido a su compatibilidad con MITRE ATT&CK, customización de ataques a evaluar, integración con herramientas de seguridad y generación de reportes.
- Si se desea adquirir una herramienta BAS open-source, se recomienda la adquisición de Caldera, ya que es compatible de igual forma con MITRE ATT&CK, permite customizar las técnicas a evaluar y generar reportes por cada uno, por lo que sus capacidades cubren de igual forma los objetivos y el alcance de la metodología, asemejándose en capacidades a herramientas BAS comerciales.

De acuerdo a lo concluido, en el presente trabajo se opta por el uso de la herramienta Caldera para la evaluación de los controles de la norma ISO 27001:2022.

4.2. Descripción de la metodología

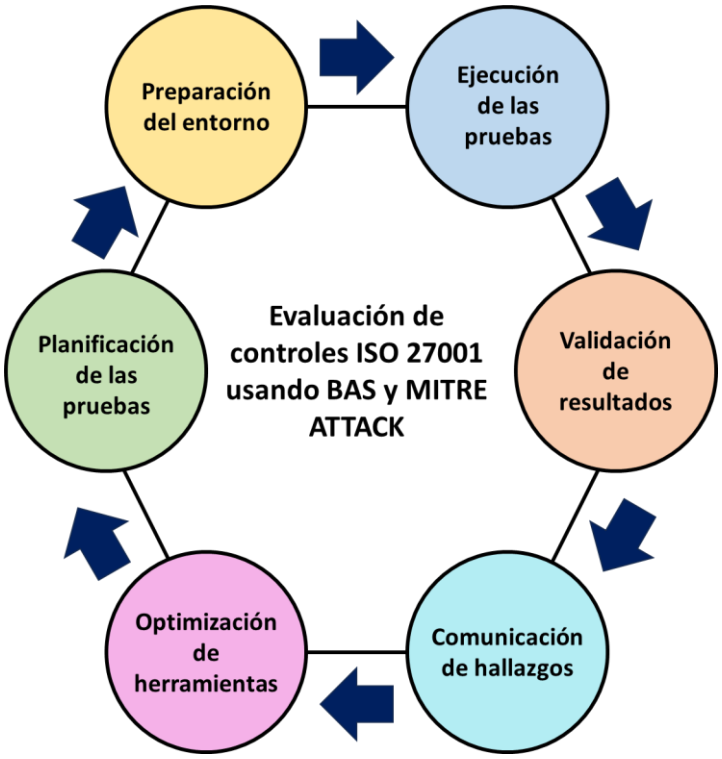
Teniendo en cuenta los pre requisitos desarrollados en los puntos anteriores, en el presente apartado se procede con la descripción de las fases de la metodología propuesta para la evaluación de los controles de la norma ISO 27001.

La metodología propuesta aborda la falta de un procedimiento específico para medir continuamente los controles de la norma ISO 27001:2022. Ya que, si bien el International Organization for Standardization (2022) establece en la norma que "la organización debe mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información" (p. 10), no proporciona directrices claras sobre cómo realizarlo, dejando el desarrollo de esta "mejora continua" a decisión de la organización. La presente metodología cubre este problema y busca desarrollar los pasos específicos necesarios para lograr la mejora continua a través de la evaluación de los controles ISO 27001 implantados en la organización.

La metodología esta desarrollada para ser un ciclo continuo, en el cual los resultados de la primera ejecución puedan servir como fuentes de cambio y mejora para la segunda. Esto garantiza que se cumpla la intención de evaluación continua de los controles de la ISO 27001:2022, viéndose reflejada en la fase de optimización de herramientas.

En la Figura 14 se muestra el esquema general de la metodología propuesta, la cual empieza con la fase de "Planificación de las pruebas" y finaliza con la de "Optimización de herramientas".

Figura 14. *Esquema de la metodología propuesta.*



Fuente: Elaboración propia.

La metodología cuenta con 6 fases diferenciadas, las cuales se detallan a continuación:

4.2.1. Fase I: Planificación de las pruebas

En esta primera fase se define:

1. **Asignación de roles:** El "Líder técnico" debe de asignar los roles descritos en el apartado 4.1.2 al personal calificado, los criterios de asignación se deben basar en los conocimientos técnicos que cuenten, para ello basarse en el apartado 4.1.3 y así escoger el personal idóneo para el rol.
2. **Inventario de activos a evaluar (alcance):** El "Líder técnico" en conjunto con el "Auditor interno de cumplimiento" y la "Alta Dirección" deben de revisar la lista de activos disponibles y escoger los que serán parte del entorno de evaluación, estos deben ser máquinas de trabajo (computadoras o laptops) y/o servidores.
3. **Definir lista de controles ISO 27001 a evaluar:** El "Líder técnico" en conjunto con el "Auditor interno de cumplimiento" y la "Alta Dirección" deben definir la lista de controles ISO 27001 que desean auditar en la evaluación.

4. **Definir lista de herramientas de seguridad involucradas:** El "Líder técnico" en conjunto con el "Administrador de infraestructura TI" deben de mapear las herramientas de seguridad existentes en la organización (firewall, EDR, IPS, DLP, SIEM, XDR, etc.).
5. **Definir la topología de pruebas:** De acuerdo a la lista de activos y al mapeo del punto anterior, el "Líder técnico" y el "Administrador de infraestructura TI" realizan la topología de pruebas con el fin de identificar las interacciones actuales entre las herramientas de seguridad y los activos escogidos.
6. **Establecer un cronograma de evaluación:** El "Líder técnico" en conjunto con la "Alta Dirección" definen si las pruebas de evaluación se realizaran de forma diaria, semanal, mensual, trimestral, etc. Así como también la fecha y hora en el cual se ejecutarán. Esto depende de los requerimientos de seguridad que tenga cada organización.

Finalizado los puntos de esta fase, se recomienda elaborar un documento de "Planificación de pruebas" en donde se evidencie el resultado de cada apartado en forma resumida.

4.2.2. Fase II: Preparación del entorno

En esta segunda fase se debe realizar:

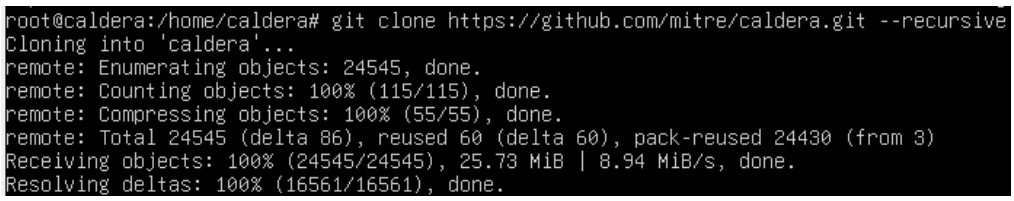
1. **Mapeo MITRE ATT&CK a controles ISO 27001 seleccionados:** Debido a que cada organización es diferente, se deberán seguir los pasos descritos en el apartado 4.1.4 con el fin de obtener el mapeo correspondiente. Sin embargo, se recomienda tomar como referencia el mapeo obtenido al final del mismo apartado (Revisar Anexo C) y modificarlo de acuerdo a los controles ISO 27001 que se desean evaluar en la organización.
2. **Instalación del BAS Caldera:** En este paso se realiza la instalación del BAS Caldera por parte del "Administrador de infraestructura TI" en una máquina local que cumpla con los siguientes requisitos mínimos:
    a. Memoria RAM mínima disponible de 8GB: Caldera recomienda que la máquina local tenga mínimo 8GB de RAM. Esto permite que no se agoten los recursos de la máquina durante el funcionamiento.
    b. Espacio en disco mínimo disponible de 10 GB: El BAS Caldera en su versión Docker (contenedor) ocupa un aproximado de 3.5 GB.

c. Sistema operativo Windows, Linux o macOS: Ya que se usará el archivo Docker de Caldera, permitiendo ejecutarlo en cualquier tipo de sistema.
d. Permisos necesarios de conectividad con los activos escogidos: Caldera usa el puerto HTTPS por defecto para comunicarse con los agentes.

A continuación, se describe el proceso de instalación realizado en una máquina virtual con sistema operativo Ubuntu Server 24.10 (GNU/Linux 6.11.0-13-generic x86_64):

1. Como se presenta en la Figura 15, se realiza la descarga del repositorio desde Github:
    a. Comando a ejecutar para la descarga:
    git clone https://github.com/mitre/caldera.git --recursive

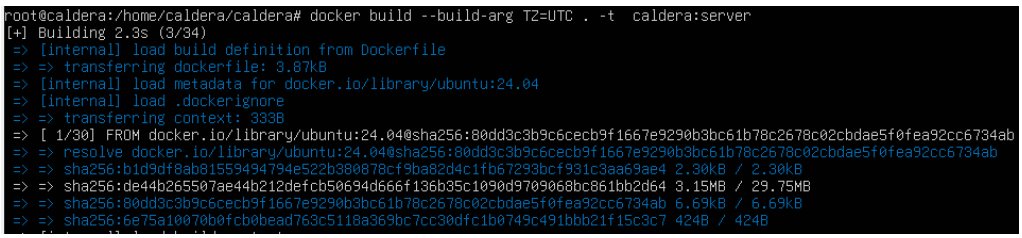
Figura 15. *Descarga de BAS Caldera.*



Fuente: Elaboración propia.

2. Tal como se muestra en la Figura 16, se ingresa a la carpeta creada y se construye la imagen Docker, asignándole un nombre. Para el presente trabajo, se colocó el nombre “caldera:server”.
    a. Comandos a ejecutar:
    cd caldera; docker build --build-arg TZ=UTC . -t caldera:server

Figura 16. *Construcción de imagen del contenedor BAS Caldera*



Fuente: Elaboración propia.

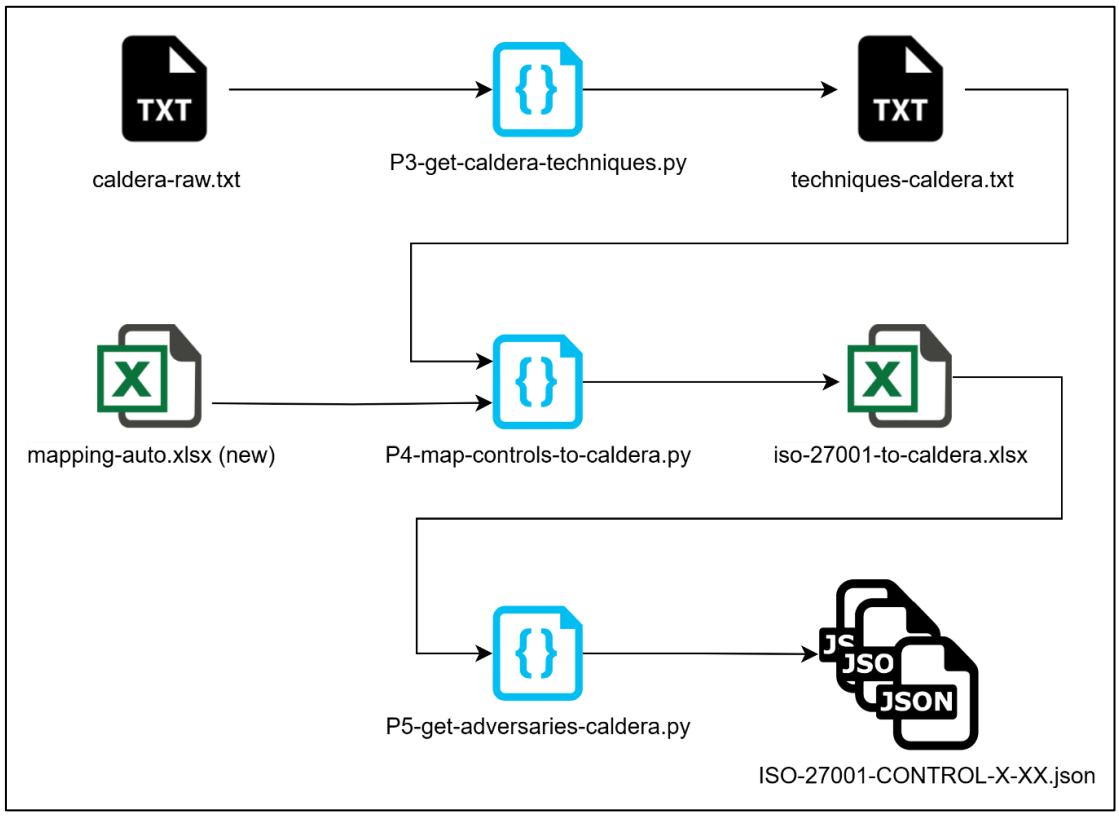
3. Finalmente, como se presenta en la Figura 17, se inicia el contenedor Docker en segundo plano y se valida su estado.
    a. Comandos a ejecutar:
    docker run -p 7010:7010 -p 7011:7011/udp -p 7012:7012 -p 8888:8888 -d caldera:server –insecure ; docker ps

Figura 17. *Ejecución del contenedor BAS Caldera.*

Fuente: Elaboración propia.

3. **Integrar los controles de la ISO 27001:2022 en el BAS Caldera:** En este punto se generan los archivos JSON asociados a cada control ISO 27001 y sus técnicas relacionadas, para posteriormente importarlos en el BAS Caldera y ser ejecutados en la Fase III. Los scripts usados se encuentran en el Anexo B, asimismo en la Figura 18 se muestra el diagrama de flujo del proceso:

Figura 18. *Diagrama de flujo para integrar controles ISO 27001 a técnicas BAS Caldera.*

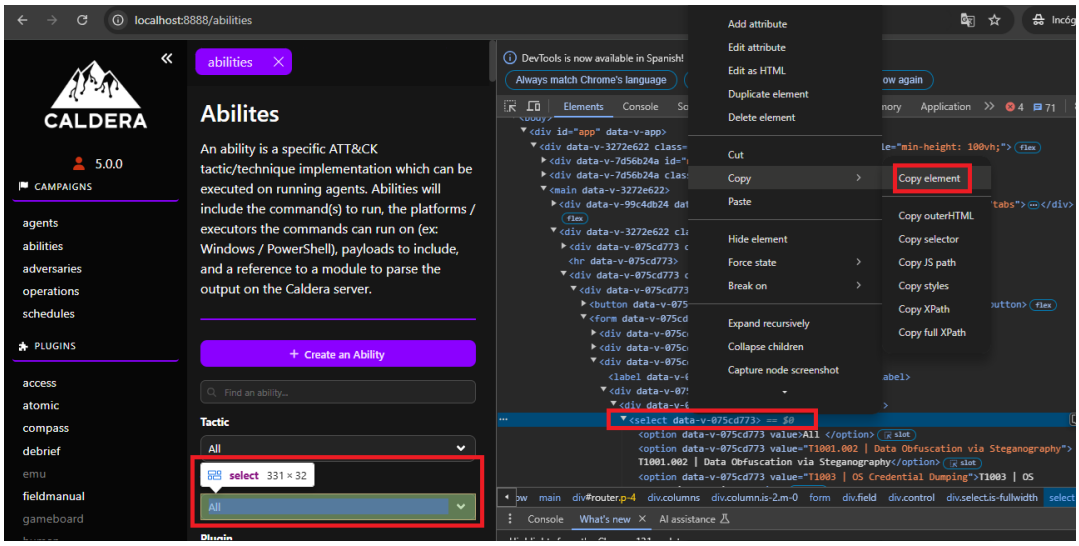


Fuente: Elaboración propia.

A continuación, se detallan los pasos:

a. Obtención de la lista de técnicas BAS Caldera: Aunque en MITRE (2025b) se puede descargar la lista de técnicas disponibles en Caldera, esta no se encuentra actualizada. Razón por la cual, se recomienda obtener la lista desde la interfaz web de Caldera. Para ello, según se muestra en la Figura 19, ir al apartado “Campaigns > Abilities” y usar la herramienta de desarrollo del navegador para copiar el fragmento HTML seleccionando la lista desplegable de técnicas, guardar lo obtenido en un archivo de texto titulado “caldera-raw.txt”.

Figura 19. *Obtención del fragmento HTML con las técnicas Caldera disponibles.*



Fuente: Elaboración propia.

b. Tratamiento de la lista de técnicas BAS Caldera: El archivo “caldera-raw.txt” es procesado por el script “P3-get-caldera-techniques.py” para obtener el archivo “techniques-caldera.txt”, el cual filtra solo las técnicas y las ordena una por una en cada línea del archivo. En la Figura 20 se muestra parte del archivo que se obtiene.

Figura 20. *Fragmento del archivo “caldera-raw.txt”.*

```
<select data-v-075cd773=""><option data-v-075cd773=""
value="">All </option><option data-v-075cd773=""
value="T1001.002 | Data Obfuscation via Steganography">T1001.002
| Data Obfuscation via Steganography</option><option
data-v-075cd773="" value="T1003 | OS Credential Dumping">T1003 |
OS Credential Dumping</option><option data-v-075cd773=""
value="T1003.001 | OS Credential Dumping: LSASS
Memory">T1003.001 | OS Credential Dumping: LSASS
Memory</option><option data-v-075cd773="" value="T1003.002 | OS
Credential Dumping: Security Account Manager">T1003.002 | OS
Credential Dumping: Security Account Manager</option><option
data-v-075cd773="" value="T1003.003 | OS Credential Dumping:
NTDS">T1003.003 | OS Credential Dumping: NTDS</option><option
data-v-075cd773="" value="T1003.004 | OS Credential Dumping: LSA
```

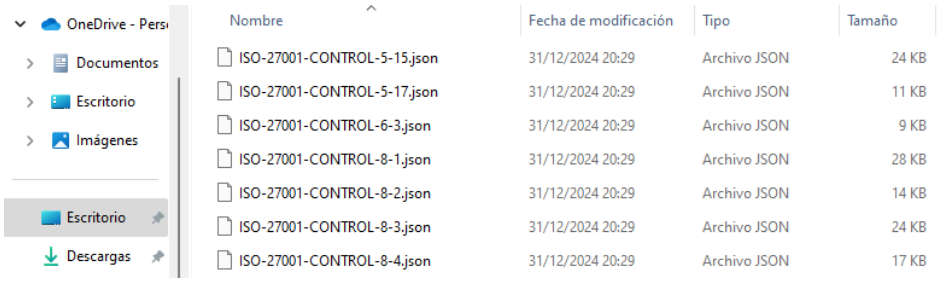
Fuente: Elaboración propia.

c. Mapeo de controles ISO 27001 a las técnicas de Caldera disponibles: Se utiliza el script “P4-map-controls-to-caldera.py” para que a partir de los archivos “mapping-auto.xlsx” y “techniques-caldera.txt” genere el archivo “iso-27001-

to-caldera.xlsx", el cual contiene la lista de controles ISO 27001 y las técnicas de Caldera asociadas.

d. Obtención de los archivos JSON por cada control ISO 27001: En la Figura 21 se muestran parte de los archivos JSON obtenidos en este paso. Para generarlos, se emplea el archivo "iso-27001-to-caldera.xlsx" en el script "P5-get-adversaries-caldera.py". Esto es necesario, ya que MITRE Navigator solo acepta este tipo de formato de archivo.

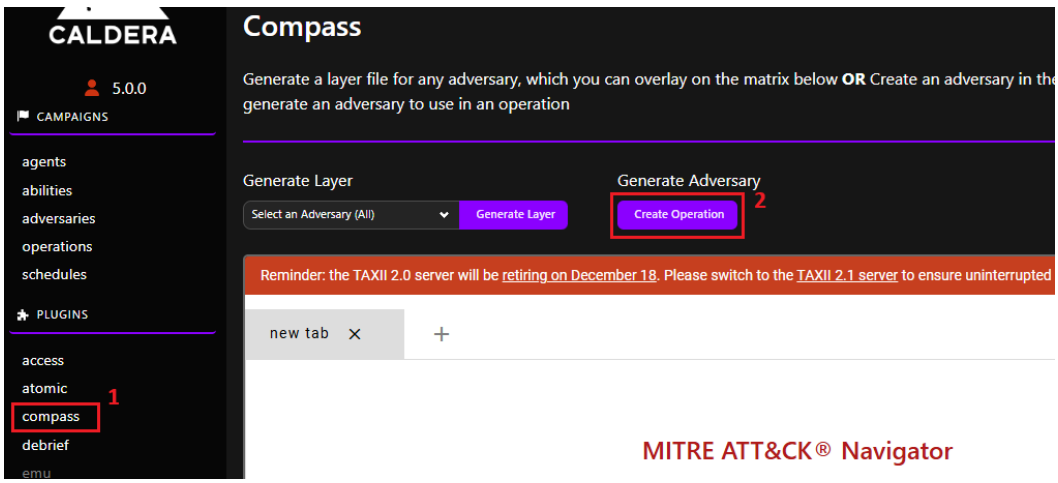
Figura 21. *Archivos JSON generados*



Fuente: Elaboración propia.

e. Importación de los archivos JSON al BAS Caldera: Según se muestra en la Figura 22, desde la interfaz web de Caldera ir al apartado "Plugins > Compass" y dar clic en la opción "Generate Adversary", aparecerá una ventana emergente al directorio de archivos local, el cual permitirá seleccionar los archivos JSON para la importación.

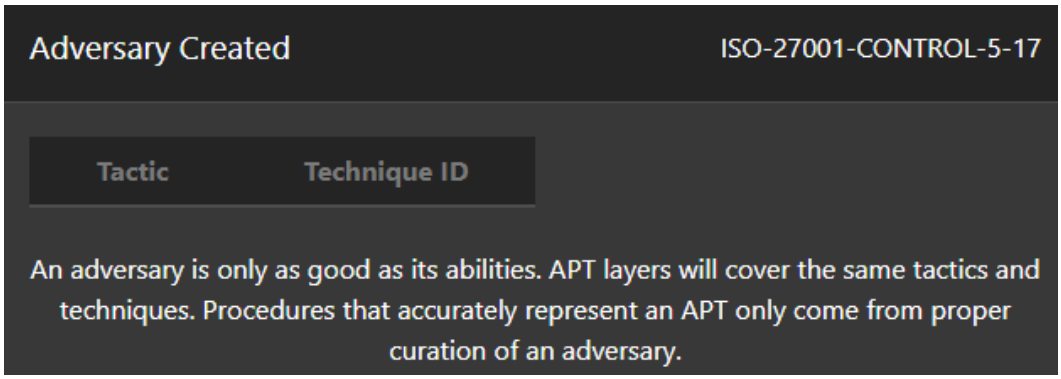
Figura 22. *Apartado en BAS Caldera para importar los archivos JSON generados.*



Fuente: Elaboración propia.

f. Validaciones post-importación: Como se muestra en la Figura 23, por cada archivo JSON importado, aparecerá una pestaña con el mensaje “Adversary created”.

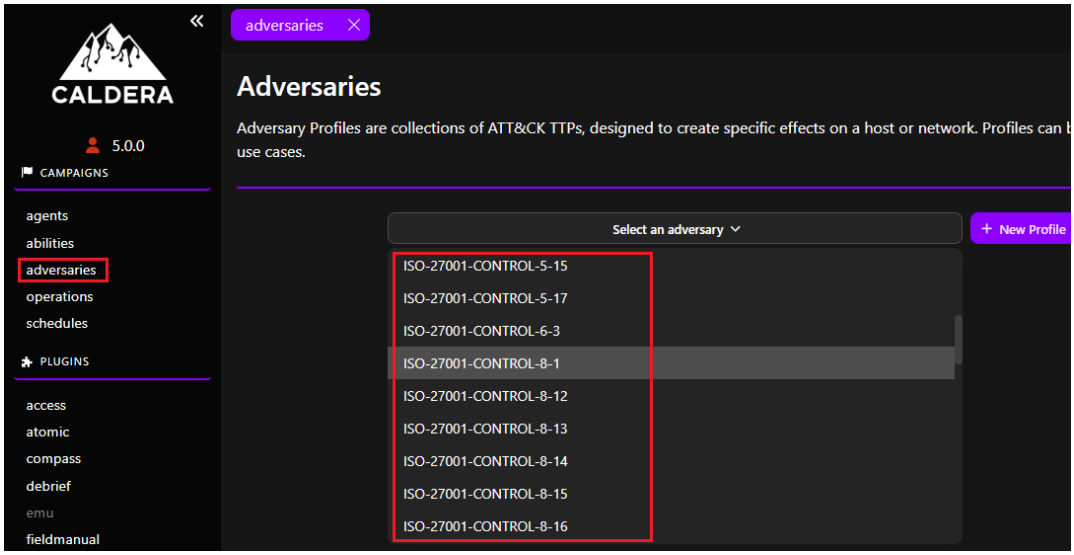
Figura 23. *Mensaje de validación post-importación de archivo JSON.*



Fuente: Elaboración propia.

Además, de acuerdo con la Figura 24, en el apartado “Campaigns > Adversaries” validar que aparezca en la lista desplegable el nombre del archivo importado.

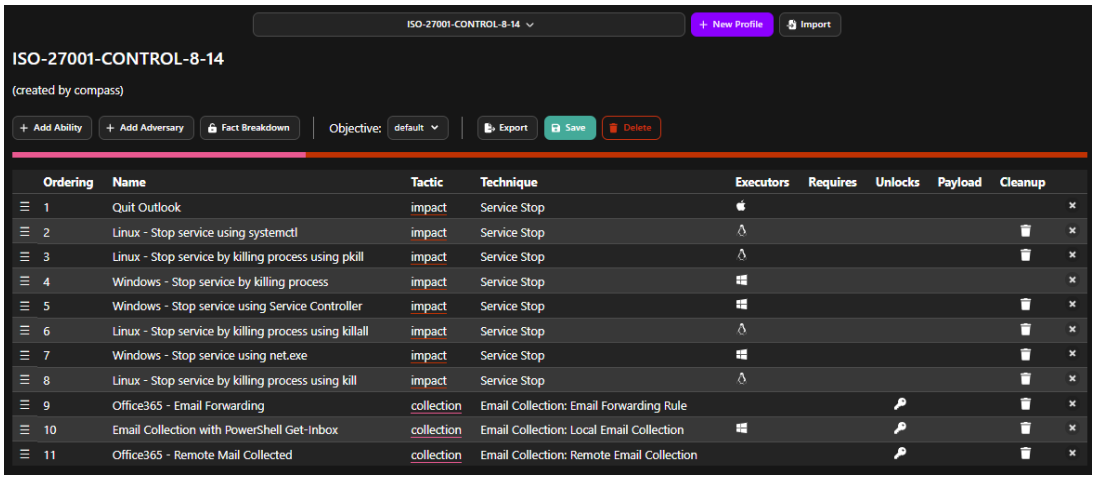
Figura 24. *Apartado en BAS Caldera para visualizar los controles importados.*



Fuente: Elaboración propia.

Finalmente, según se muestra en la Figura 25, comprobar que al escoger un control ISO 27001 aparezcan las técnicas asociadas.

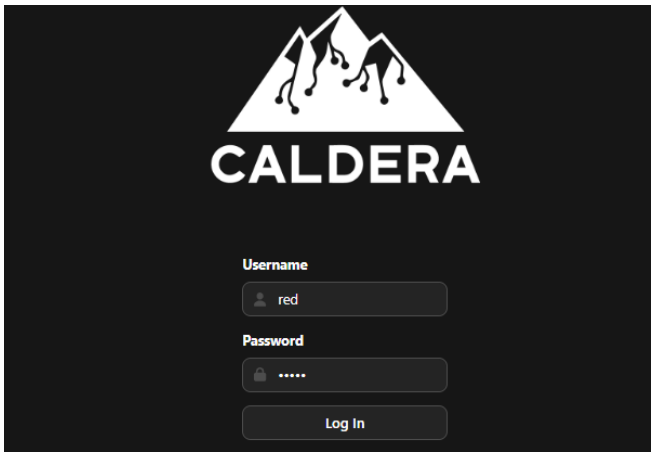
Figura 25. *Validación de importación de técnicas asociadas por cada control.*



Fuente: Elaboración propia.

4. **Revisión de técnicas ATT&CK por control ISO 27001**: En este paso, de acuerdo al mapeo realizado en el paso 1 y su posterior importación en el paso 3, se revisa en el BAS Caldera la lista de técnicas disponibles por control ISO 27001 y se escogen las que se van a utilizar para ejecutar las pruebas. Idealmente se escogerían todas, pero esto depende del criterio de la organización. Esta actividad debería llevarse a cabo por el "Líder técnico", "Evaluador de seguridad ofensiva" y la "Alta Dirección".
5. **Generación e instalación de agentes:** En este paso se explica el procedimiento para generar los agentes de Caldera desde la interfaz web, asimismo se explica el proceso de instalación de agentes en los activos escogidos.
    1. En cualquier navegador web, ingresar a la dirección IP del BAS Caldera instalado en el paso previo por el puerto 8888, en este caso se accede directamente desde localhost (https://localhost:8888/login)
    2. Aparecerá la pestaña de login, tal como se muestra en la Figura 26. Usar las siguientes credenciales para el acceso:
        a. Usuario: red
        b. Contraseña: admin

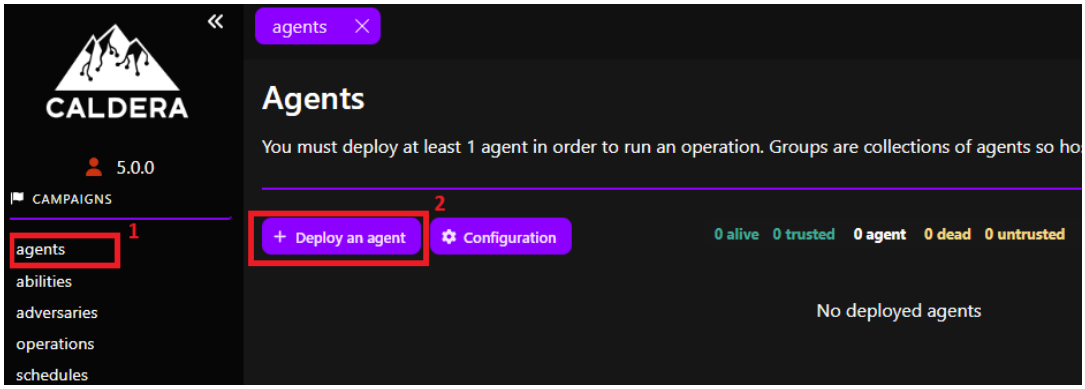
Figura 26. *Login de acceso a BAS Caldera.*



Fuente: Elaboración propia.

3. Como se detalla en la Figura 27, Ir al apartado “Campaigns > Agents” y dar clic en “Deploy an agent”.

Figura 27. *Acceso al apartado “Agents” en BAS Caldera.*



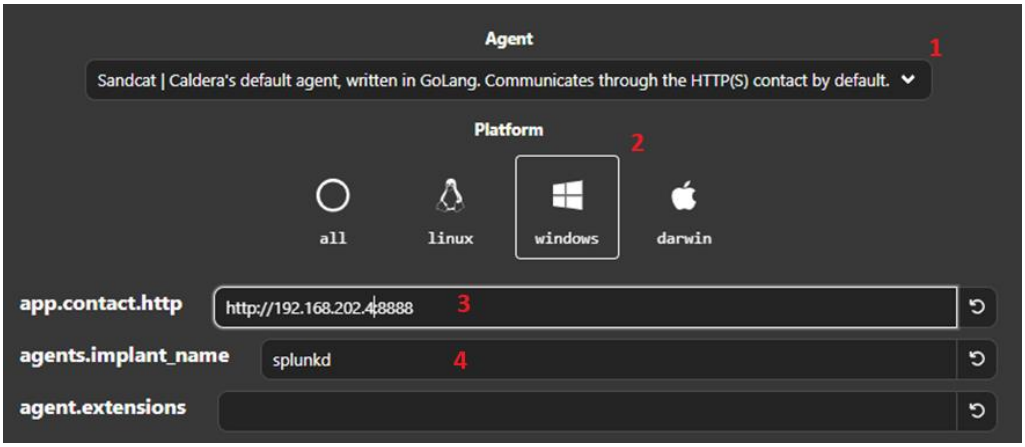
Fuente: Elaboración propia.

4. En la pestaña emergente, la cual se visualiza en la Figura 28, configurar las siguientes opciones:
    a. Tipo de agente: Escoger el agente Sandcat, este permite la comunicación por HTTP(S) entre el agente y el BAS.
    b. Platform: Seleccionar el sistema operativo en el cual se instalará el agente. Para el caso del presente ejemplo, se escogió Windows.

c. Apartado “app.contact.http”: Colocar la IP del BAS y el puerto HTTP. Para el caso del presente ejemplo, la IP es 192.168.202.4 y puerto 8888.

d. Apartado “agents.implant_name”: Colocar el nombre del proceso asociado al agente mientras está en ejecución. Para el caso del presente ejemplo, el nombre es “splunkd”.

Figura 28. *Opciones de despliegue agentes en BAS Caldera.*



Fuente: Elaboración propia.

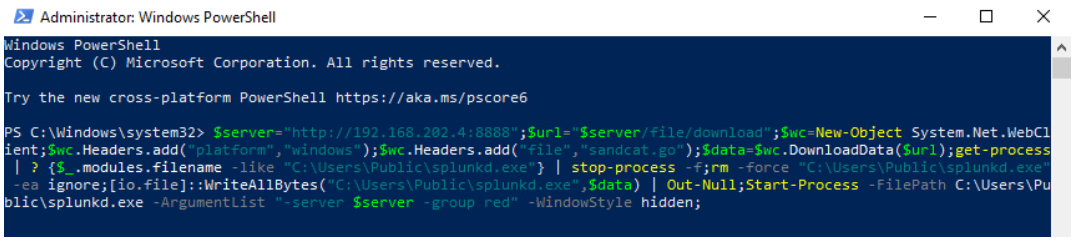
5. En la misma pestaña, desplazarse hacia la parte inferior y copiar el script tal como se muestra en la Figura 29, este script será ejecutado en las máquinas con el tipo de sistema operativo especificado para instalar el agente.

Figura 29. *Script generado para la instalación de agentes.*

Fuente: Elaboración propia.

6. En la máquina (computadora o laptop) donde se instalará el agente, según se muestra en la Figura 30, ejecutar el script generado con privilegios de administrador:

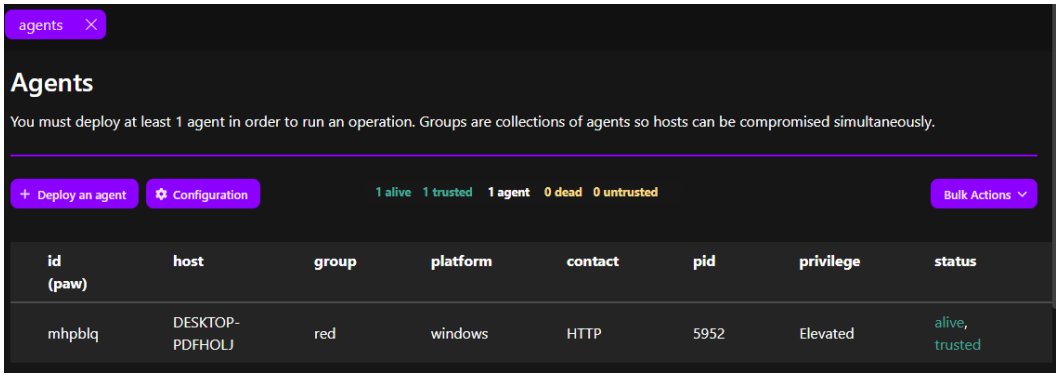
Figura 30. *Instalación de agente usando el script generado.*



Fuente: Elaboración propia.

7. Finalmente, en el mismo apartado “Campaigns > Agents” de la interfaz web del BAS Caldera, comprobar que el agente ya aparece conectado, tal como se observa en la Figura 31:

Figura 31. *Visualización de agente conectado a BAS Caldera.*



Fuente: Elaboración propia.

6. **Exclusión del agente en Antivirus local**: En este paso, se recomienda realizar una exclusión del agente Caldera en el Antivirus local de la máquina de pruebas. Para el caso del ejemplo, consistiría en excluir el archivo y proceso asociado “splunkd.exe”.

Finalizado la ejecución de todos los puntos de esta fase, se recomienda realizar un checklist de verificación de todos los activos que tienen los agentes Caldera instalados.

4.2.3. Fase III: Ejecución de las pruebas

En esta tercera fase, se procede a ejecutar la evaluación de los controles ISO 27001. Estas pruebas se realizan teniendo todas las protecciones activas en las máquinas de prueba escogidas y son ejecutadas en conjunto por el "Evaluador de seguridad ofensiva" en coordinación con el "Administrador de infraestructura TI" y "Líder técnico".

Se deben de ejecutar las pruebas en la(s) fecha(s) y hora(s) definidas en la "Fase I", asimismo el Evaluador de seguridad ofensiva debe de indicar la hora exacta cuando empezó con las pruebas, esto facilita la labor del Administrador de infraestructura TI para validar los logs de las herramientas de seguridad en el rango indicado.

El objetivo de estas pruebas es poder medir el nivel de cumplimiento de los controles ISO 27001 a través del resultado de ejecución de las técnicas MITRE ATT&CK usando el BAS Caldera.

Para la correcta categorización del resultado de las pruebas, considerar la Tabla 4, la cual presenta la equivalencia entre el resultado obtenido producto de la ejecución de la técnica y la validación realizada por el "Administrador de infraestructura TI":

Tabla 4. *Equivalencia en el resultado de evaluación.*

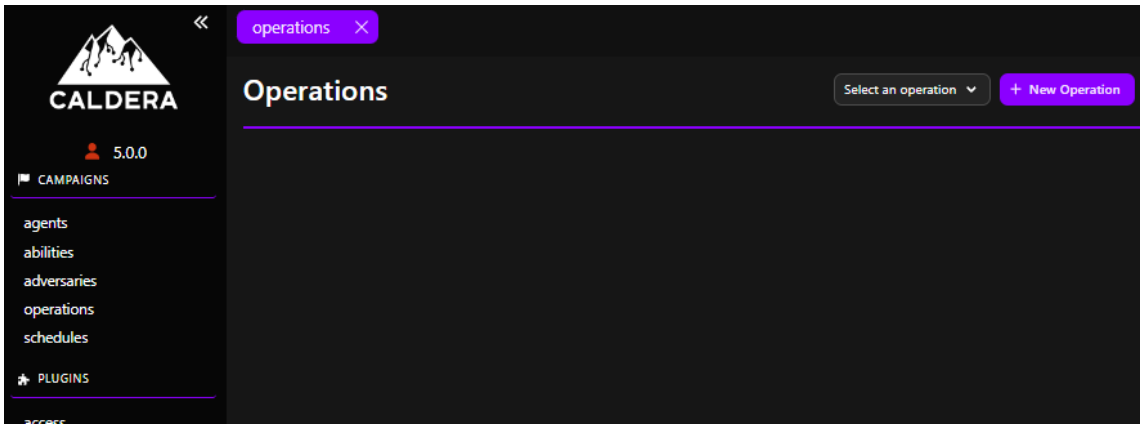
Resultado de técnica ejecutada	Significado de validación
Bloqueada	Se ha validado la herramienta de seguridad correspondiente y se encuentra un log asociado con acción de bloqueo.
Alertada	Se ha validado la herramienta de seguridad correspondiente y se encuentra un log asociado sin acción de bloqueo.
No detectada	Se ha validado la herramienta de seguridad correspondiente y no se encuentra un log asociado.
NA	No aplica. La técnica evaluada no corresponde ser detectada por la herramienta de seguridad ya que no forma parte del alcance de sus funciones de detección.

Fuente: Elaboración propia.

Los pasos para realizar la evaluación de los controles ISO 27001 usando el BAS Caldera son los siguientes:

1. Ir al apartado “Campaigns > Operations” y dar clic en la opción “New Operation”, como se muestra en la Figura 34.

   Figura 32. *Apartado para crear las pruebas en el BAS Caldera*

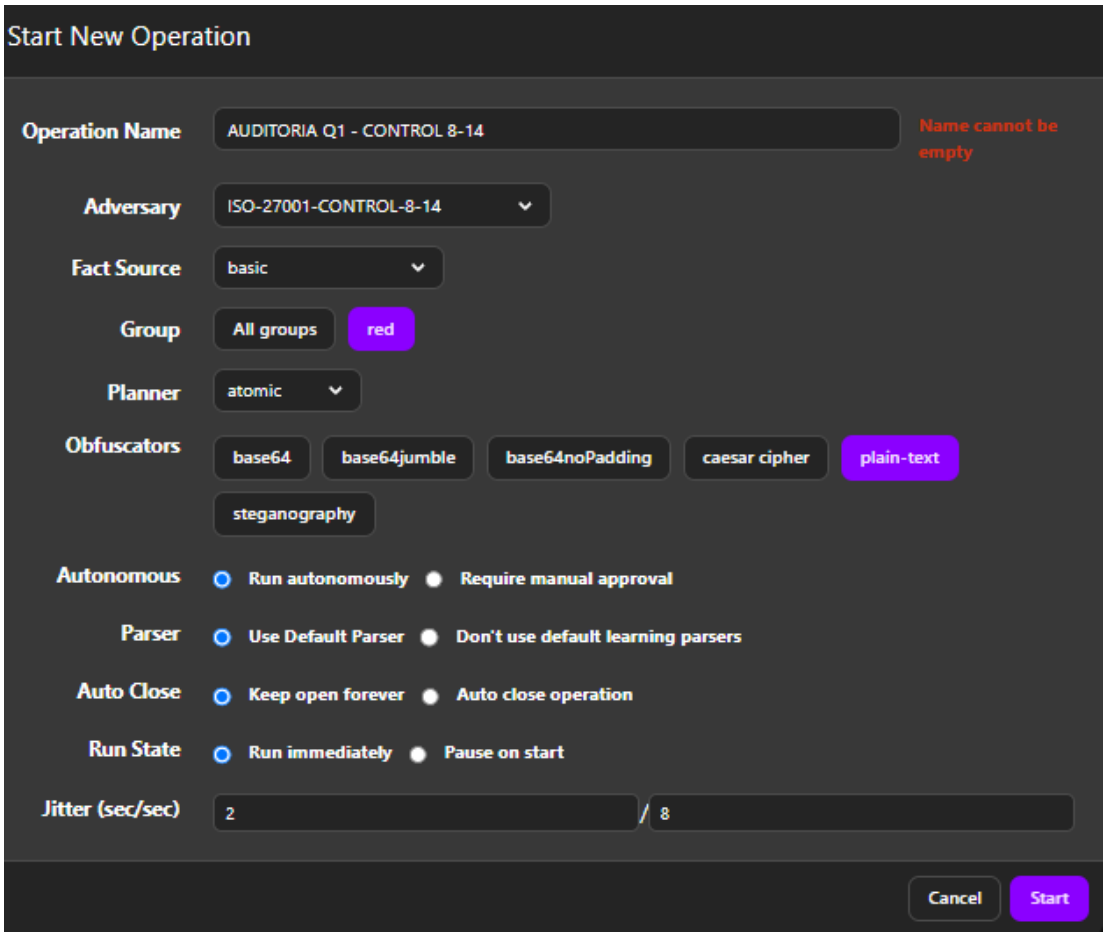


   Fuente: Elaboración propia.

2. En la ventana emergente, tal como se muestra en la Figura 35, configurar las siguientes opciones:
   a. Operation Name: Colocar el nombre a la operación. Se recomienda colocar el siguiente formato: AUDITORIA QX – CONTROL X_XX
   b. Adversary: Seleccionar de la lista desplegable, el control a evaluar en la prueba.
   c. Group: Escoger el grupo de activos creado en la plataforma.
   d. Los demás parámetros dejarlos por defecto.

   Hacer clic en “Start” para iniciar las pruebas.

Figura 33. *Opciones para crear las pruebas en el BAS Caldera*



Fuente: Elaboración propia.

3. En la nueva pestaña, mostrada en la Figura 34, validar que las técnicas asociadas al control escogido se estén ejecutando, asimismo para la columna “Status” considerar los estados detalladso en la Tabla 5:

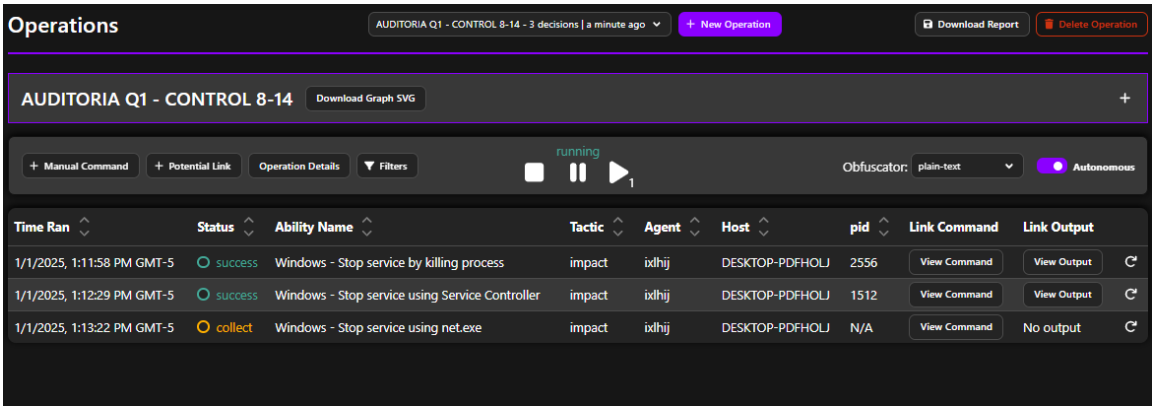
Tabla 5. *Estados de ejecución de técnicas en BAS Caldera.*

Estado	Explicación
success	La técnica escogida se ejecutó satisfactoriamente.
collect	BAS Caldera está intentando ejecutar la técnica escogida.
failed	La técnica escogida no se pudo ejecutar satisfactoriamente.

timeout	La técnica escogida no se completó durante los primeros 60 segundos (por defecto), se sugiere revisar los logs asociados.

Fuente: Elaboración propia.

Figura 34. *Ejemplo de ejecución de pruebas en el BAS Caldera*



Fuente: Elaboración propia.

4. Al finalizar la ejecución de las técnicas asociadas al control especificado, repetir el mismo procedimiento con los siguientes controles.

Finalizado los pasos descritos en esta fase, para propósitos de documentación de las pruebas por parte del “Evaluador de seguridad ofensiva”, se recomienda realizar el mapa ATT&CK por cada control ISO 27001 escogido y las técnicas asociadas usando MITRE Navigator.

4.2.4. Fase IV: Validación de resultados

En esta cuarta fase se realizan las revisiones de los resultados y la preparación para su presentación a la “Alta Dirección”. En esta fase los roles que intervienen son: “Auditor interno de cumplimiento”, “Administrador de infraestructura TI”, “Evaluador de seguridad ofensiva” y “Líder Técnico”.

Hay que tener en cuenta que inicialmente se ha escogido un grupo de activos a los cuales se les ha ejecutado las técnicas correspondientes, por lo que por cada activo se obtendrá un nivel de cumplimiento diferente en los controles ISO 27001 escogidos, dependiendo si las técnicas fueron o no ejecutadas satisfactoriamente.

Para el caso que el número de activos sea muy grande, como escenarios en los cuales la organización desee medir el cumplimiento a nivel de dispositivos endpoint de una red LAN con varios usuarios, si bien puede realizarse con una demora muy amplia en la ejecución y comunicación de resultados, se recomienda tomar como ejemplo 2 activos como máximo y en base a ellos realizar los pasos de esta metodología.

Para propósitos de visualización de resultados, la evaluación de cada control ISO 27001 se realiza en base a cada técnica ATT&CK asociada. Asimismo, cada técnica ATT&CK se aplica sobre un grupo determinado de herramientas de seguridad. Por lo cual, por cada herramienta de seguridad se debe aplicar el puntaje correspondiente de acuerdo a la Tabla 6:

Tabla 6. *Equivalencia en el resultado de evaluación.*

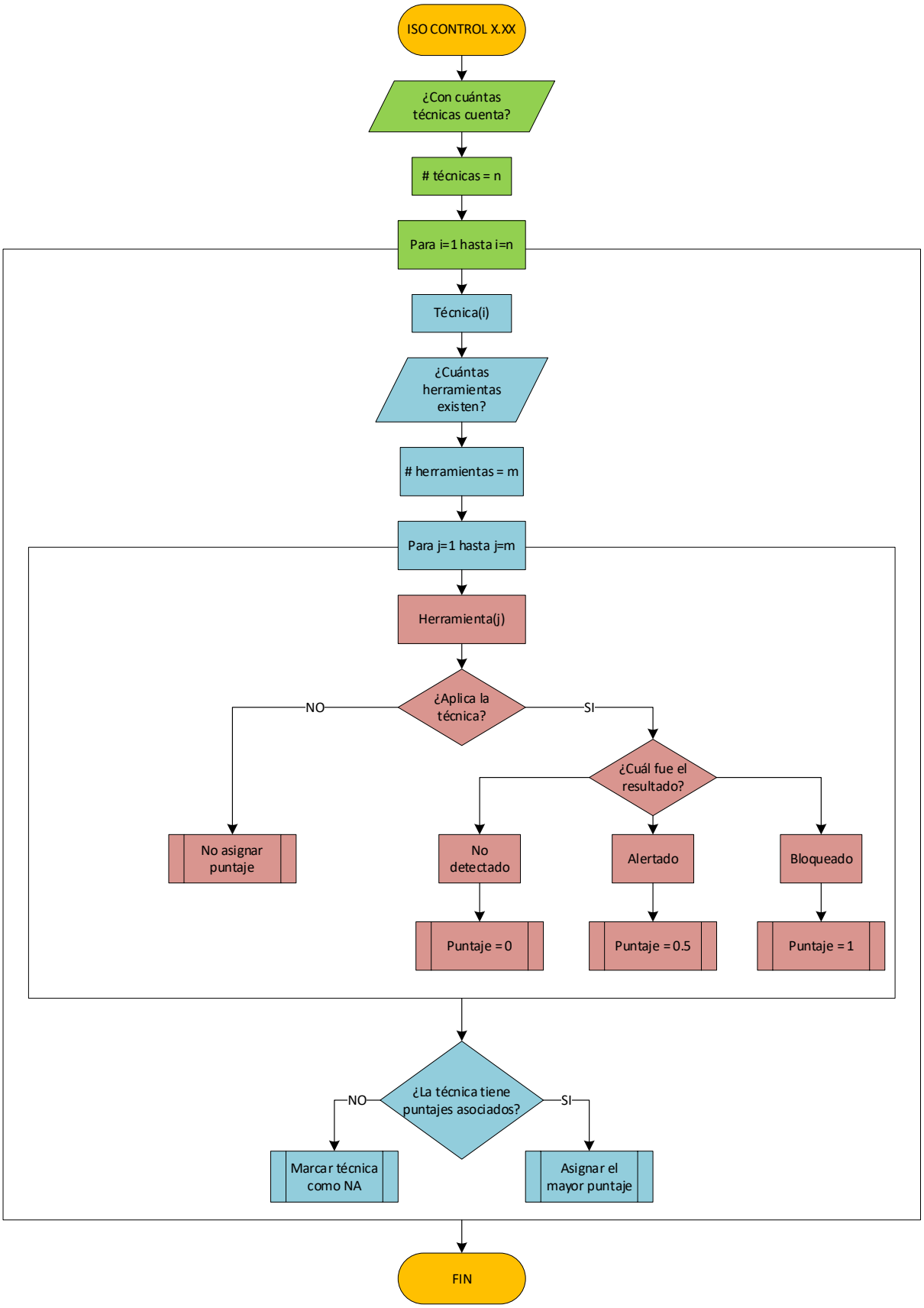
Resultado de técnica	Puntaje
Bloqueada	1
Alertada	0.5
No detectada	0
NA (No aplica)	Sin puntaje asociado

Fuente: Elaboración propia.

Si posterior a la revisión de todas las herramientas de seguridad, la técnica correspondiente no aplica a ninguna, no se toma en cuenta para el cálculo del cumplimiento del control ISO 27001 asociado. Además, como la técnica examinada obtiene varios puntajes dependiendo de las herramientas de seguridad, solo se tomará en cuenta el mayor puntaje obtenido.

A continuación, se muestra en la Figura 35 el diagrama de flujo correspondiente para asignar el puntaje a cada técnica:

Figura 35. *Diagrama de flujo para la asignación de puntaje.*



Fuente: Elaboración propia.

Para el cálculo del cumplimiento por cada control ISO 27001, el cual será expresado en porcentaje, se hará uso de la siguiente formula:

$$cumplimiento(\%) = \frac{Puntaje\ total\ obtenido}{\#\ técnicas\ totales\ aplicables}\ x\ 100\%$$

Donde:

- Puntaje total obtenido: Es la suma de cada puntaje individual de las técnicas asociadas al control ISO 27001 evaluado.
- # técnicas totales aplicables: Es la cantidad total de las técnicas que son aplicables, es decir la suma de las que tienen un puntaje asociado.

A continuación, se muestra un ejemplo de evaluación:

- Se escogió un activo ACT1 a evaluar.
- Se cuenta con 3 herramientas de seguridad (HA, HB y HC) que monitorean el activo.
- El control ISO 27001 8.1 asignado tiene 3 técnicas a evaluar (T1, T2 y T3).
- Los resultados son:
    - Técnica 1 (T1):
        - HA: NA, no aplica.
        - HB: Fue alertada, por lo cual su puntaje es 0.5.
        - HC: Fue bloqueada, por lo cual su puntaje es 1.
        - Resultado T1: Técnica es aplicable. Se toma el puntaje más alto entre las tres herramientas para T1, que es 1.
    - Técnica 2 (T2):
        - HA: Fue alertada, por lo cual su puntaje es 0.5.
        - HB: NA, no aplica.
        - HC: No detectado, por lo cual su puntaje es 0.
        - Resultado T2: Técnica es aplicable. Se toma el puntaje más alto entre las tres herramientas para T2, que es 0.5.
    - Técnica 3 (T3):
        - HA: NA, no aplica.
        - HB: NA, no aplica.

- HC: NA, no aplica.
- Resultado T3: Técnica es marcada como NA (No aplicable).

- Cumplimiento ISO 27001 8.1 para el activo ACT1:

$$cumplimiento(\%) = \frac{1 + 0.5}{2} x\ 100\%$$

$$cumplimiento(\%) = 75\%$$

Finalizada la recolección de evidencias, por cada activo evaluado se deben realizar las siguientes tablas para la presentación de resultados:

1. Tabla de resultados en herramientas de seguridad: La Tabla 7 se elabora por cada control ISO 27001, en la cual se presentan las técnicas ejecutadas, la lista de herramientas de seguridad y el resultado de la evaluación.

   Tabla 7. *Tabla de resultados en herramientas de seguridad.*

CONTROL ISO 27001 X.XX			
Técnica ejecutada	**Herramientas de seguridad**		
	EDR	**Firewall**	**Antivirus**
Técnica A	No detectado	Alertado	Bloqueado
Técnica B	Bloqueado	NA	Alertado

Fuente: Elaboración propia.

2. Tabla de cumplimiento ISO 27001: La Tabla 8 se elabora por cada control ISO 27001 y presenta la lista de técnicas, resultados, puntajes y el cumplimiento asociado.

   Tabla 8. *Tabla de cumplimiento ISO 27001.*

CONTROL ISO 27001 X.XX		
Técnica ejecutada	**Resultado**	**Puntaje**
Técnica A	Alertado	0.5
Técnica B	Bloqueado	1
Cumplimiento		75%

Fuente: Elaboración propia.

4.2.5. Fase V: Comunicación de hallazgos

En esta fase se comunican los resultados a la "Alta Dirección" con el fin de tomar decisiones en base a lo encontrado. Para ello, por cada activo evaluado se presentan los resultados de las tablas realizadas en la fase anterior, de esta forma se va mostrando adecuadamente el resultado de las herramientas de seguridad y su impacto en el cumplimiento del control ISO 27001 correspondiente.

Los objetivos de esta fase son:

- Lograr que la "Alta Dirección" comprenda que, para mejorar el cumplimiento de un activo en un determinado control ISO 27001, se deben tomar medidas correctivas en las herramientas de seguridad.
- Proponer y conseguir la aprobación de los cambios correspondientes en las herramientas de seguridad con el fin de mejorar el cumplimiento de la norma específica.

Las acciones a llevar a cabo dependen del resultado de las técnicas, que pueden ser:

- Resultado no detectado: Se debe proponer y aprobar la modificación técnica específica para lograr que mínimamente la herramienta de seguridad alerte la ejecución de la técnica correspondiente.
- Resultado Alertado: Se debe proponer y aprobar la modificación técnica específica para lograr que la herramienta de seguridad bloquee la ejecución de la técnica correspondiente.
- Resultado Bloqueado: En este caso se garantiza el cumplimiento de la técnica correspondiente, por lo que no se necesitan acciones adicionales.
- Resultado NA (No aplica): En este caso tampoco se necesitarían tomar acciones adicionales.

Finalmente, se debe elaborar una lista con los cambios acordados a realizar en las herramientas de seguridad.

4.2.6. Fase VI: Optimización de herramientas

En la presente fase final, lo que se debe buscar es realizar una optimización en las herramientas de seguridad y en las técnicas ATT&CK existentes en el BAS Caldera. Por lo que esta última fase es delegada a los roles de "Administrador de infraestructura TI" y "Evaluador de seguridad ofensiva".

A continuación, se detallan las acciones a realizar en esta fase:

1. En base a los resultados obtenidos en las pruebas y previa aprobación de cambios, se procede con los ajustes necesarios en la configuración de las herramientas de seguridad, con el objetivo de que el resultado final de la técnica que se ejecutó sea "Bloqueado".
2. Realizar la búsqueda de nuevas técnicas ATT&CK (Ya que el marco MITRE ATT&CK está en constante desarrollo y añaden nuevas técnicas con el tiempo) que no fueron cubiertas en las pruebas, de tal forma que se puedan mapear al control ISO 27001 correspondiente y posteriormente añadirlas a la herramienta BAS Caldera.
3. Si la organización lo considera necesario, las pruebas descritas en la presente metodología pueden realizarse una segunda vez, en este caso se desactivan las protecciones de las herramientas de seguridad que bloquearon la ejecución de la técnica y se vuelven a iniciar las simulaciones de ataques seleccionando solo las técnicas con estado "failed", esta prueba permitiría detectar si alguna otra herramienta de seguridad logra bloquearlas.

4.3. Evaluación

En el presente apartado se describe la evaluación de la metodología propuesta. Para ello, se implementó en un entorno empresarial, teniéndose el consentimiento para instalar la herramienta BAS Caldera y realizar las simulaciones de ataque.

Por motivos de confidencialidad el nombre de la empresa no se publicará en el presente trabajo, por lo que, si bien se mostrarán las evidencias y hallazgos, se tendrá cuidado de no publicar información privada.

La empresa acaba de homologar sus controles de la ISO 27001:2013 a los controles ISO 27001:2022. Dentro de su plan de auditoría de ciberseguridad contempla la revisión continua, pero esta se da en base a la revisión y actualización de los documentos presentados durante

la homologación. En vista de ello, se le propuso la implementación de la presente metodología, a fin de tener una visibilidad técnica y práctica del cumplimiento, lo cual les permitiría cumplir con su objetivo de revisión continua.

Para la implementación de la metodología, se aprobó hacer una "Prueba de concepto", en la cual se acordó instalar 1 agente en una máquina de la LAN y ejecutar los análisis. A continuación, se describe el desarrollo de las fases de la metodología en su ambiente de producción y los resultados obtenidos:

4.3.1. Fase I: Planificación de las pruebas

1. **Asignación de roles:** Se asignaron los roles respectivos en base a los conocimientos del personal interno, asumiendo mi persona los roles de "Líder técnico" y "Evaluador de seguridad ofensiva". Los demás roles ("Administrador de infraestructura TI", "Auditor interno de cumplimiento" y "Asistente técnico") fueron atribuidos al Administrador de sistemas, Auditor de cumplimiento y Asistente de operaciones de la empresa, respectivamente.
2. **Activos a evaluar:** Como se puede observar en la Figura 35 y Figura 36, las características y datos de red del activo escogido fueron: Computadora "HP ProDesk 400 G4" de 8 GB de RAM, con IP 172.16.100.46:

Figura 36. *Características del activo escogido*

```
PS C:\WINDOWS\system32> Get-CimInstance -ClassName Win32_ComputerSystem

Name            PrimaryOwnerName      Domain              TotalPhysicalMemory   Model                Manufacturer
----            ----------------      ------              -------------------   -----                ------------
DESKTOP-MIA74KJ [redacted]            WORKGROUP           8420900864            HP ProDesk 400 G4 DM HP
```

Fuente: Elaboración propia.

Figura 37. *Datos de red del activo escogido*

```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Dirección IPv4. . . . . . . . . . . . . . : 172.16.100.46
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 172.16.100.1
```

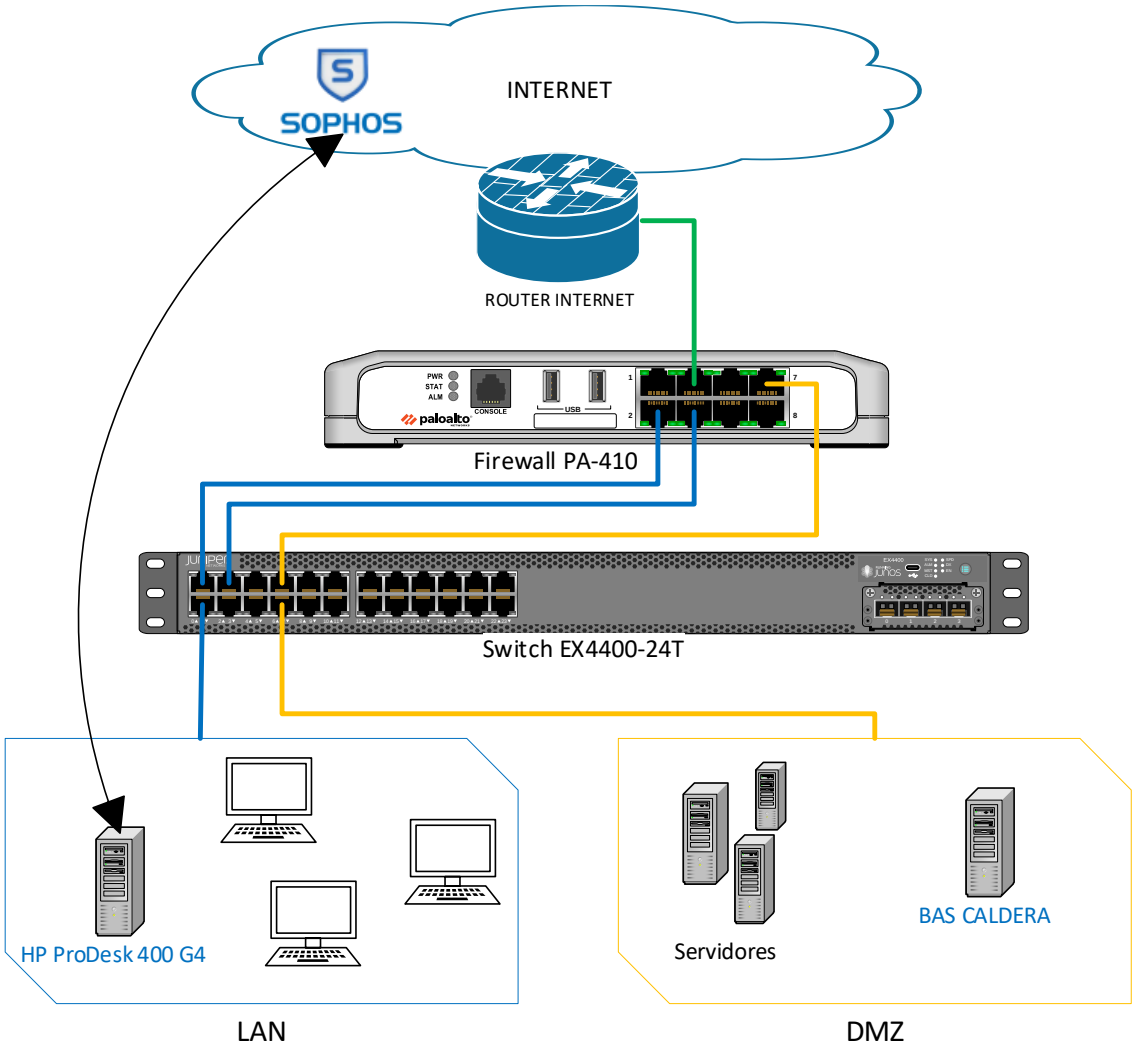
Fuente: Elaboración propia.

3. **Lista de controles ISO 27001:** Se decidió evaluar los siguientes controles:
   - CONTROL 8.20: Seguridad de redes

- CONTROL 8.7: Protección contra malware

4. **Herramientas de seguridad involucradas:** Se decidió evaluar el firewall Palo Alto modelo PA-410 y el EDR Sophos Endpoint.
5. **Topología de pruebas:** Para las presentes pruebas, se consideró la topología de la empresa mostrada en la Figura 37:

Figura 38. *Topología de la empresa como referencia para las pruebas*



Fuente: Elaboración propia.

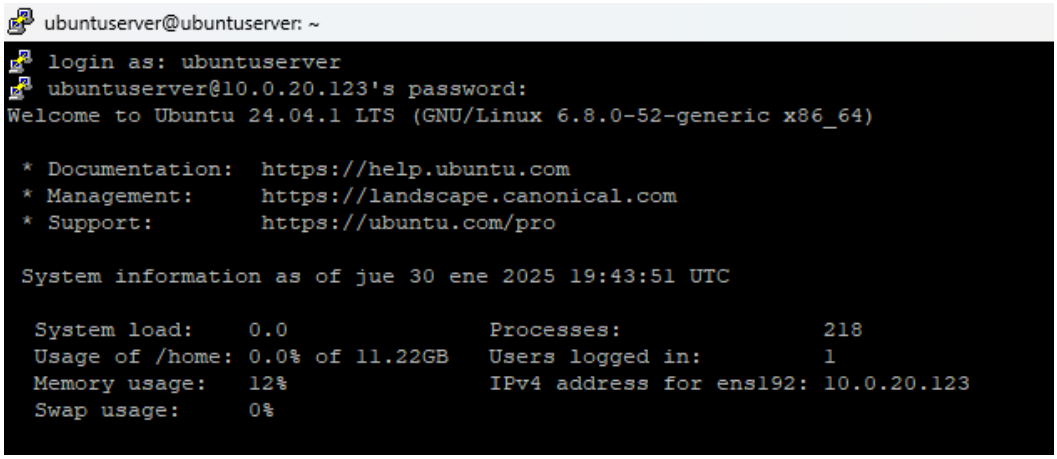
6. **Cronograma de evaluación:** Las pruebas se decidieron hacer de forma mensual, sin embargo, para el presente trabajo se detallará solo la primera prueba.

El documento de "Planificación de pruebas" se encuentra en el Anexo D.

4.3.2. Fase II: Preparación del entorno

1. **Mapeo MITRE ATT&CK a controles ISO 27001 seleccionados:** La empresa decidió hacer uso del mapeo MITRE ATT&CK realizado durante el desarrollo del presente trabajo.
2. **Instalación del BAS Caldera:** La empresa decidió usar la versión modificada del BAS Caldera que ya incluye los controles ISO 27001 a ser testeados. Para ello, se facilitó la versión en contenedor (Docker) del paso 3 perteneciente al apartado 4.2.2 (En el Anexo E se desarrolla el proceso de creación del contenedor personalizado). A continuación, se describen los pasos realizados para instalar la imagen Docker indicada en la infraestructura de la empresa:
    a. La empresa brindó las facilidades para la creación de un servidor Ubuntu virtualizado, cuyas características se detallan a continuación y se muestran en la Figura 39:
        i. Nombre: LAB-UbuntuServer
        ii. IP: 10.0.20.123
        iii. Zona de red: DMZ
        iv. Memoria RAM: 8GB
        v. Espacio en disco: 20 GB

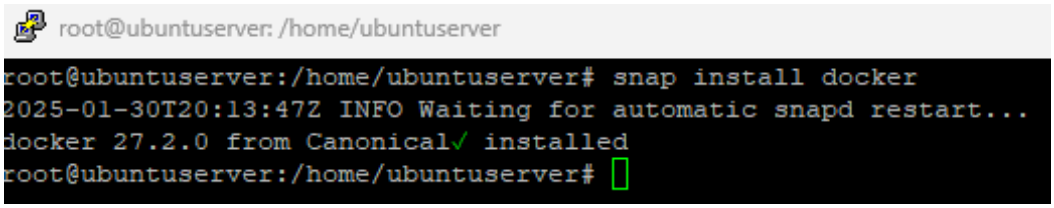
Figura 39. *Características del servidor Ubuntu virtualizado*



Fuente: Elaboración propia.

b. Como se observa en la Figura 40, se instala Docker con el comando: snap install docker

Figura 40. *Instalación Docker*

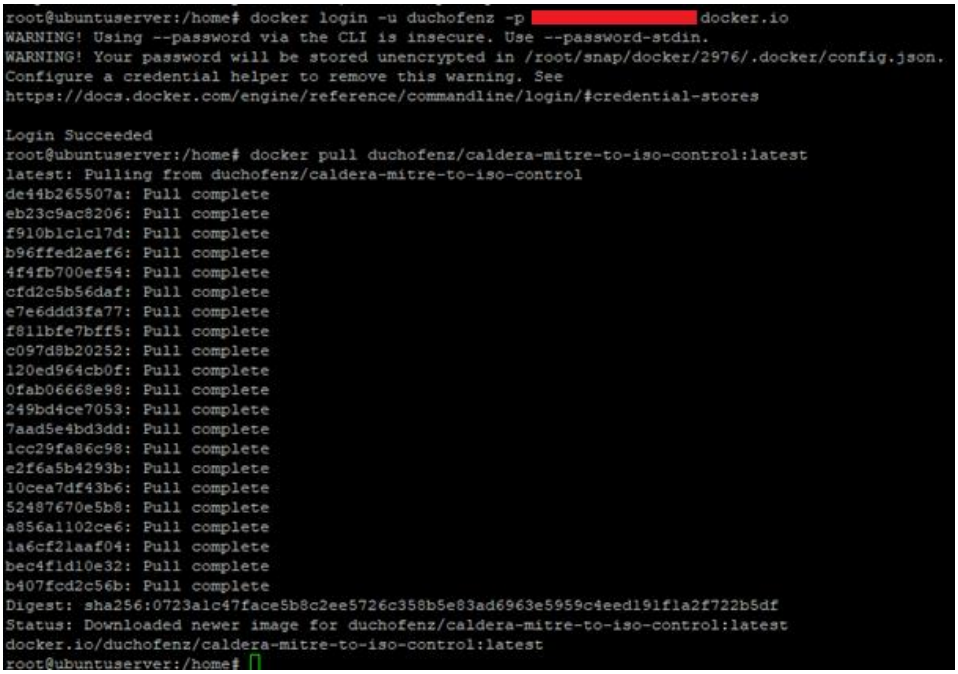


Fuente: Elaboración propia.

c. Login a DockerHub desde el servidor DMZ para descargar la imagen:

En la Figura 41 se muestra los comandos a ejecutar: docker login -u duchofenz -p <contraseña> docker.io; docker pull duchofenz/caldera-mitre-to-iso-control:latest

Figura 41. *Ejecución de comandos para descargar la imagen BAS Caldera*

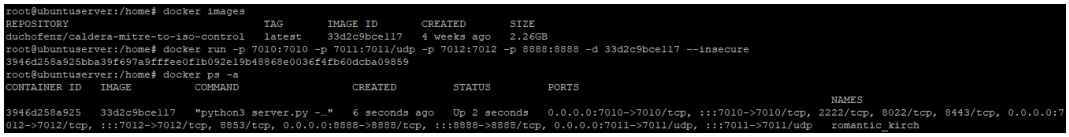


Fuente: Elaboración propia.

d. Se valida la descarga de la imagen y se inicia el contenedor:

La Figura 42 muestra los comandos a ejecutar: docker images; docker run -p 7010:7010 -p 7011:7011/udp -p 7012:7012 -p 8888:8888 -d <docker_id> --insecure

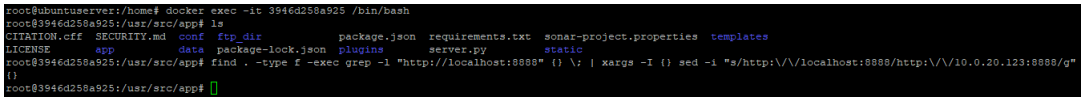
Figura 42. *Ejecución de comandos para iniciar el contenedor BAS Caldera*



Fuente: Elaboración propia.

e. Se inicia una Shell en el contenedor y se reemplaza el parámetro “localhost” con la IP asignada al servidor: 10.0.20.123, tal como se muestra en la Figura 43. Comandos a ejecutar: docker exec -it <docker_id> /bin/bash; find . -type f -exec grep -l "http://localhost:8888" {} \; | xargs -I {} sed -i "s/http:\/\/localhost:8888/http:\/\/10.0.20.123:8888/g" {}

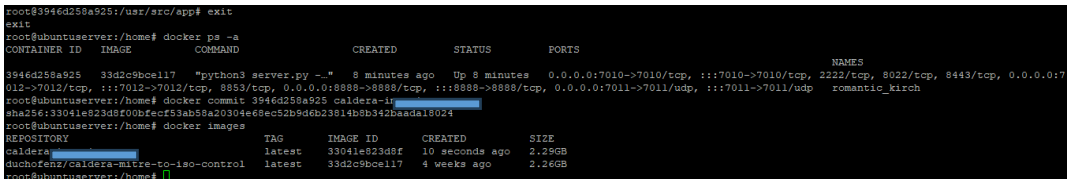
Figura 43. *Reemplazo del parámetro “localhost”*



Fuente: Elaboración propia.

f. Se construye la imagen Docker y se asigna un nombre como se observa en la Figura 44, se decidió colocar el nombre de la empresa:
Comandos: docker commit <docker_id> <nuevo_nombre>

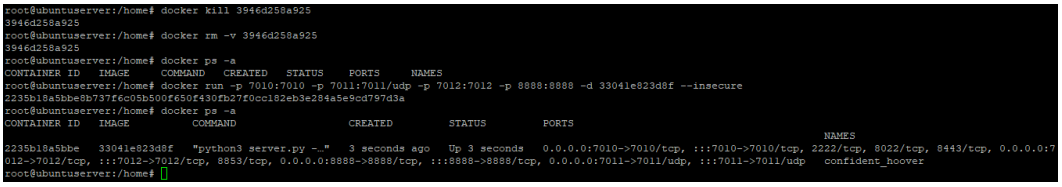
Figura 44. *Construcción de la imagen Docker*



Fuente: Elaboración propia.

g. Se elimina el contenedor inicial y se inicia el nuevo contenedor personalizado: La Figura 45 muestra el comando a ejecutar: docker kill <docker_id> ; docker rm -v <docker_id> ; docker run -p 7010:7010 -p 7011:7011/udp -p 7012:7012 -p 8888:8888 -d <nuevo_docker_id> --insecure

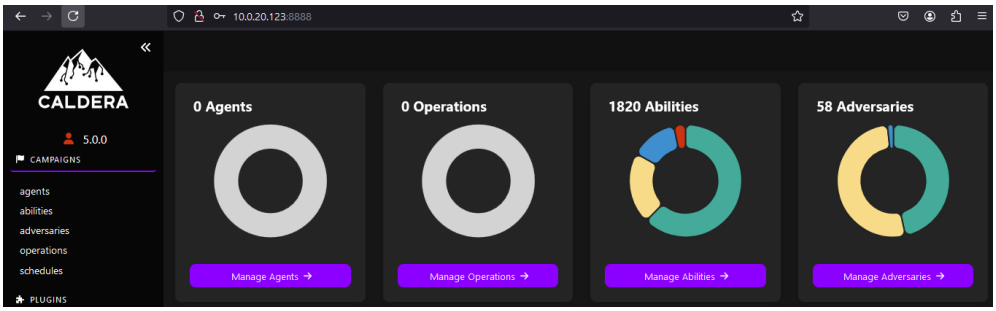
Figura 45. *Ejecución para el nuevo contenedor personalizado*



Fuente: Elaboración propia.

h. Como se observa en la Figura 46, se valida acceso a la plataforma satisfactoriamente:

Figura 46. *Plataforma BAS Caldera personalizada*



Fuente: Elaboración propia.

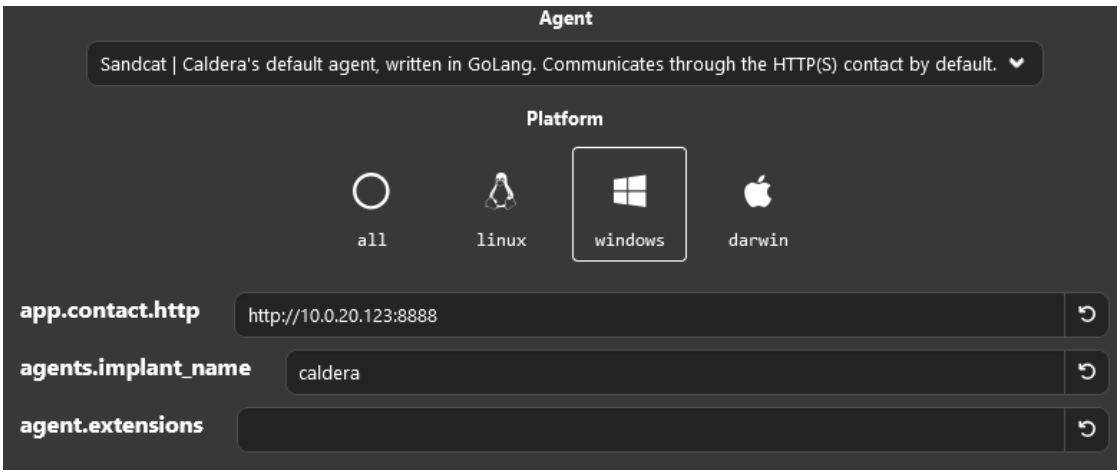
3. **Revisión de técnicas ATT&CK por control ISO 27001:** Se revisó en conjunto con la "Alta Dirección" las técnicas correspondientes a los controles ISO 27001 escogidos, se decidió lo siguiente:
   a. ISO 27001 CONTROL 8.20 – Seguridad de redes: Utilizar solo 10 técnicas para las pruebas.
   b. ISO 27001 CONTROL 8.7 – Protección contra malware: Utilizar solo 22 técnicas para las pruebas.
4. **Generación e instalación de agente:** De acuerdo con la Figura 47, se desplegó el agente Caldera con las siguientes opciones:
   a. Tipo de agente: Sandcat

b. Platform: Windows

c. app.contact.http: http://10.0.20.123:8888

d. agents.implant_name: caldera

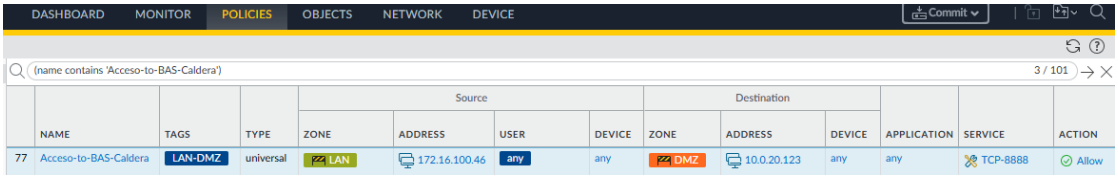
Figura 47. *Generación e instalación de agente Caldera*



Fuente: Elaboración propia.

Como se muestra en la Figura 48, se realizó la creación de la política de seguridad en el firewall Palo Alto para permitir la comunicación:

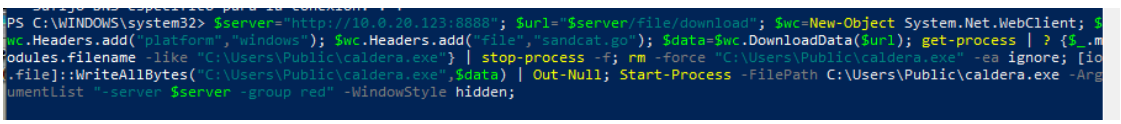
Figura 48. *Política de seguridad en el firewall Palo Alto*



Fuente: Elaboración propia.

Como se observa en la Figura 49, se ejecutó el script generado con privilegios de administrador:

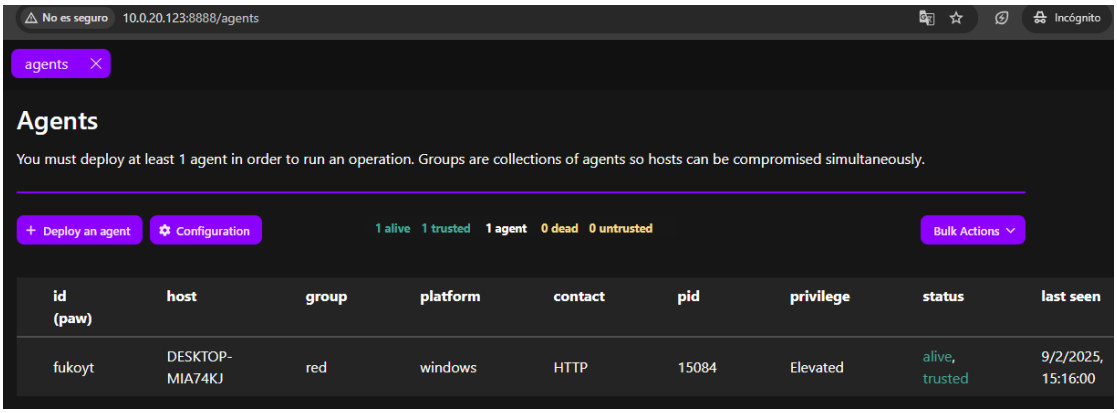
Figura 49. *Ejecución del script en la máquina escogida*



Fuente: Elaboración propia.

Finalmente, en la herramienta BAS se comprueba la correcta conexión con el agente, tal como se observa en la Figura 50:

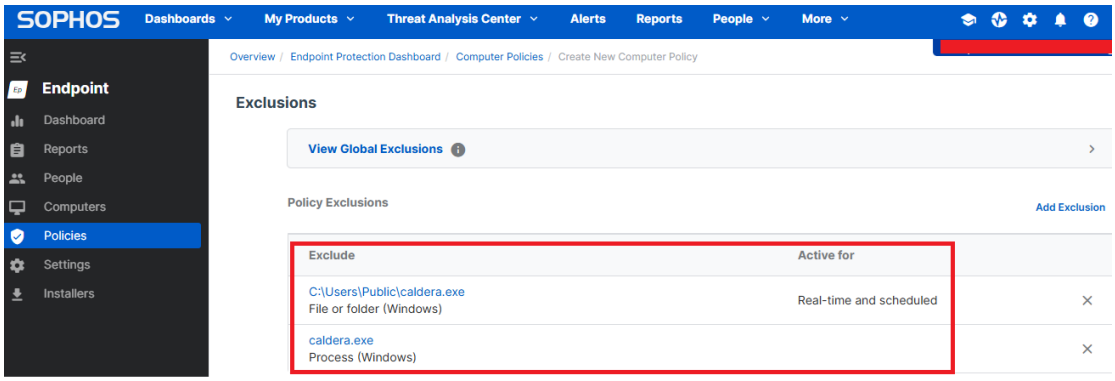
Figura 50. *Comprobación de la conexión con el agente instalado*



Fuente: Elaboración propia.

5. **Exclusión del agente en Antivirus local:** Se realizó la exclusión del proceso y archivo "caldera.exe", evidenciada en la Figura 51 y Figura 52, para evitar su eliminación desde el EDR Sophos Endpoint, el cual administra el Antivirus local de la máquina.

Figura 51. *Exclusión del proceso y archivo "caldera.exe"*



Fuente: Elaboración propia.

Figura 52. *Política de seguridad aplicada*

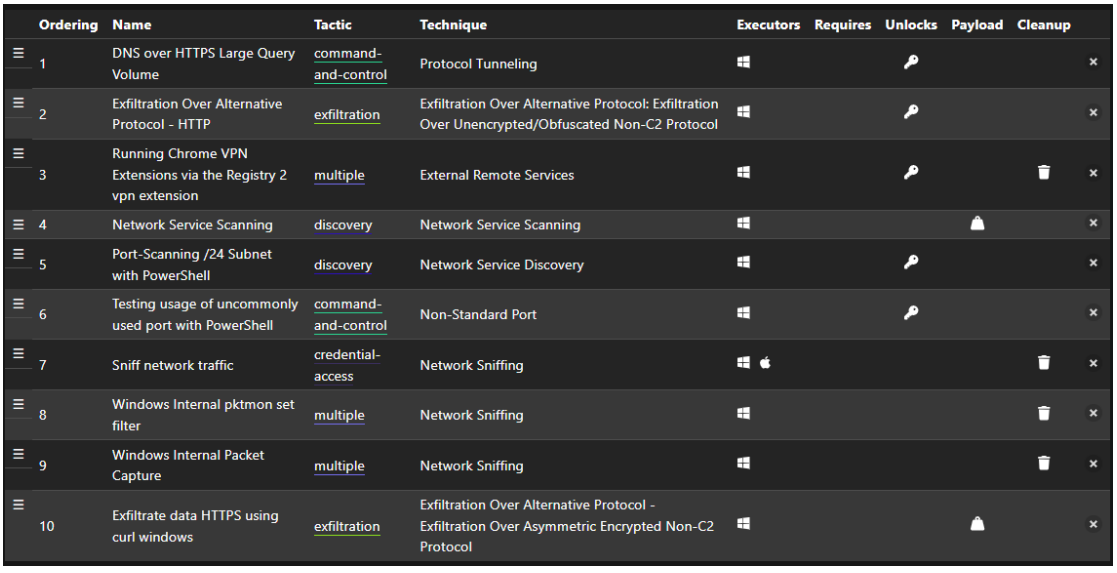
Fuente: Elaboración propia.

4.3.3. Fase III: Ejecución de las pruebas

A continuación, se detalla la ejecución de los 2 controles ISO 27001 escogidos:

- **ISO 27001 CONTROL 8.20 – Seguridad de redes:** En la Figura 53 se muestra la lista de las 10 técnicas escogidas en la plataforma BAS Caldera:

  Figura 53. *Lista de las técnicas relacionadas al control ISO 27001 8.20*

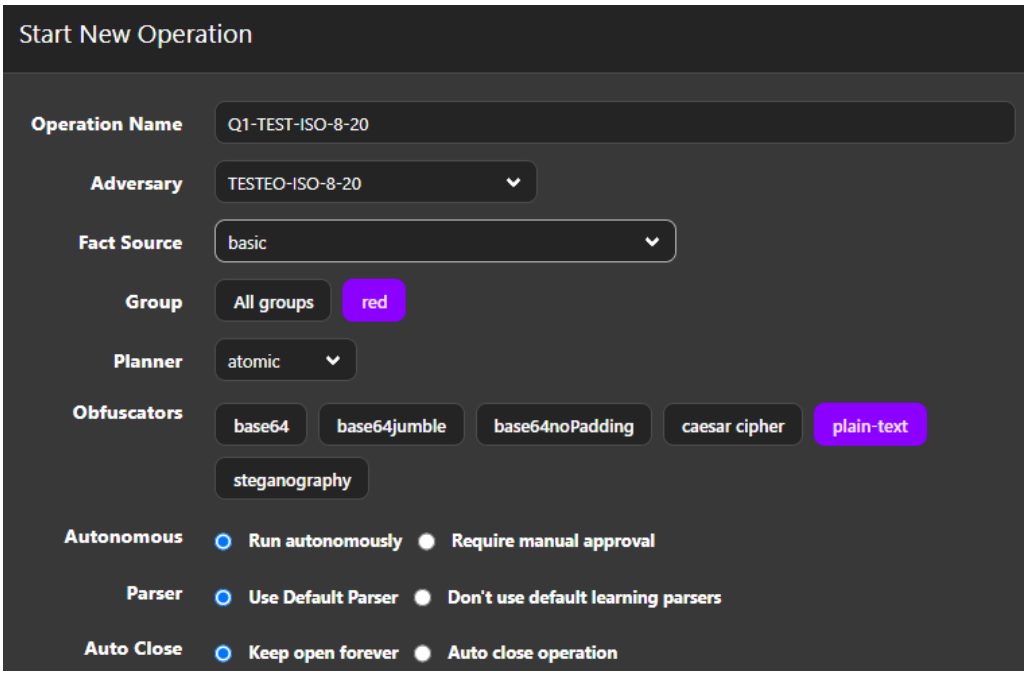


Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup
1	DNS over HTTPS Large Query Volume	command-and-control	Protocol Tunneling					
2	Exfiltration Over Alternative Protocol - HTTP	exfiltration	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol					
3	Running Chrome VPN Extensions via the Registry 2 vpn extension	multiple	External Remote Services					
4	Network Service Scanning	discovery	Network Service Scanning					
5	Port-Scanning /24 Subnet with PowerShell	discovery	Network Service Discovery					
6	Testing usage of uncommonly used port with PowerShell	command-and-control	Non-Standard Port					
7	Sniff network traffic	credential-access	Network Sniffing					
8	Windows Internal pktmon set filter	multiple	Network Sniffing					
9	Windows Internal Packet Capture	multiple	Network Sniffing					
10	Exfiltrate data HTTPS using curl windows	exfiltration	Exfiltration Over Alternative Protocol - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol					

Fuente: Elaboración propia.

En la Figura 54 se muestra la configuración de las opciones de ejecución indicadas en la metodología:

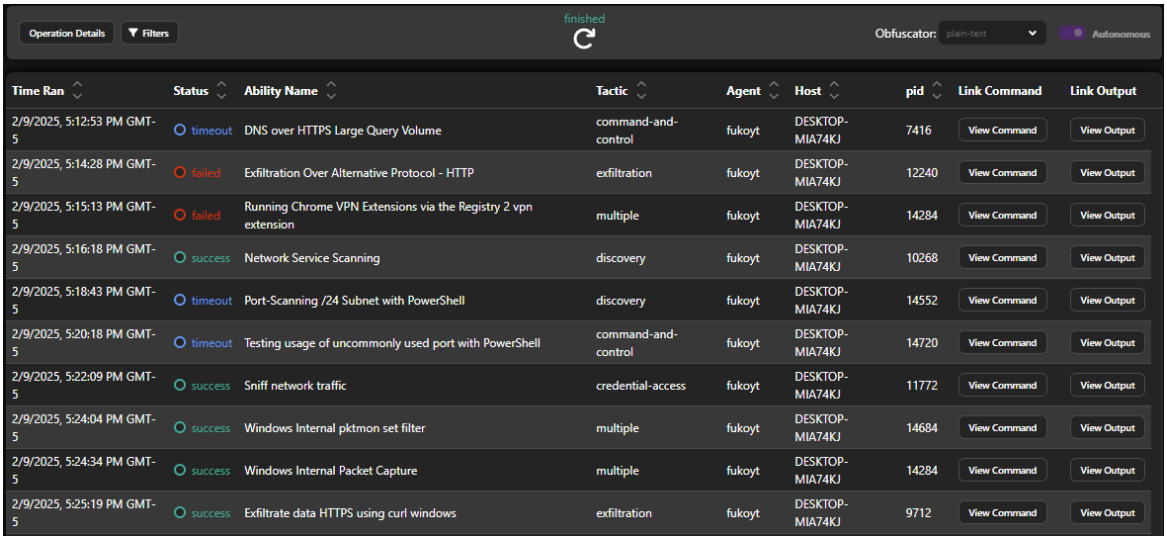
Figura 54. *Configuración de las opciones de ejecución para control ISO 27001 8.20*



Fuente: Elaboración propia.

Finalmente, como se muestra en la Figura 55, se valida que las técnicas asociadas fueron ejecutadas:

Figura 55. *Ejecución de técnicas asociadas al control ISO 27001 8.20*

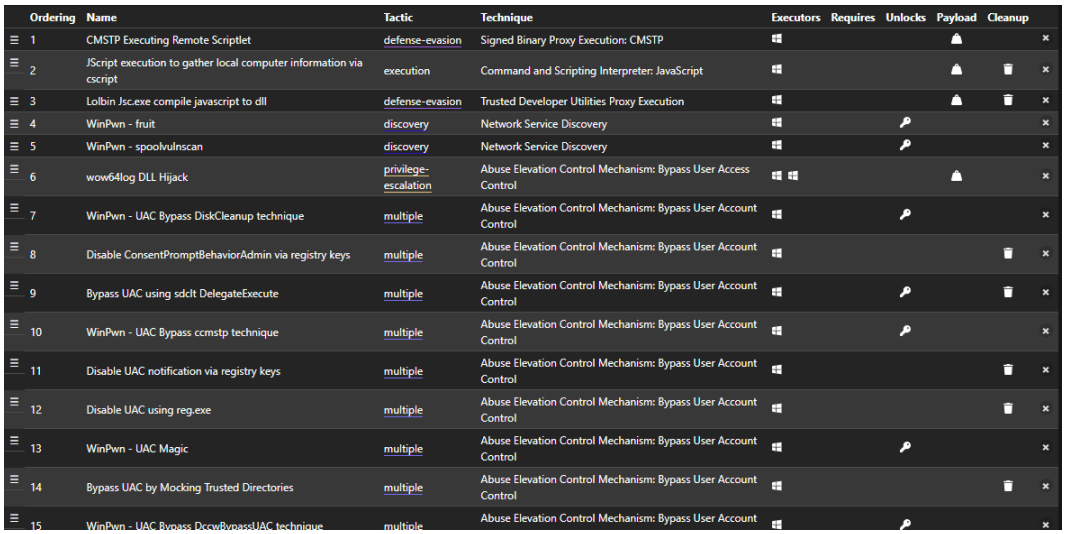


Time Ran	Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output
2/9/2025, 5:12:53 PM GMT-5	timeout	DNS over HTTPS Large Query Volume	command-and-control	fukoyt	DESKTOP-MIA74KJ	7416	View Command	View Output
2/9/2025, 5:14:28 PM GMT-5	failed	Exfiltration Over Alternative Protocol - HTTP	exfiltration	fukoyt	DESKTOP-MIA74KJ	12240	View Command	View Output
2/9/2025, 5:15:13 PM GMT-5	failed	Running Chrome VPN Extensions via the Registry 2 vpn extension	multiple	fukoyt	DESKTOP-MIA74KJ	14284	View Command	View Output
2/9/2025, 5:16:18 PM GMT-5	success	Network Service Scanning	discovery	fukoyt	DESKTOP-MIA74KJ	10268	View Command	View Output
2/9/2025, 5:18:43 PM GMT-5	timeout	Port-Scanning /24 Subnet with PowerShell	discovery	fukoyt	DESKTOP-MIA74KJ	14552	View Command	View Output
2/9/2025, 5:20:18 PM GMT-5	timeout	Testing usage of uncommonly used port with PowerShell	command-and-control	fukoyt	DESKTOP-MIA74KJ	14720	View Command	View Output
2/9/2025, 5:22:09 PM GMT-5	success	Sniff network traffic	credential-access	fukoyt	DESKTOP-MIA74KJ	11772	View Command	View Output
2/9/2025, 5:24:04 PM GMT-5	success	Windows Internal pktmon set filter	multiple	fukoyt	DESKTOP-MIA74KJ	14684	View Command	View Output
2/9/2025, 5:24:34 PM GMT-5	success	Windows Internal Packet Capture	multiple	fukoyt	DESKTOP-MIA74KJ	14284	View Command	View Output
2/9/2025, 5:25:19 PM GMT-5	success	Exfiltrate data HTTPS using curl windows	exfiltration	fukoyt	DESKTOP-MIA74KJ	9712	View Command	View Output

Fuente: Elaboración propia.

- **ISO 27001 CONTROL 8.7 – Protección contra malware:** En la Figura 56 se muestra la lista parcial de las 22 técnicas escogidas en la plataforma BAS Caldera:

Figura 56. *Lista de las técnicas relacionadas al control ISO 27001 8.7*

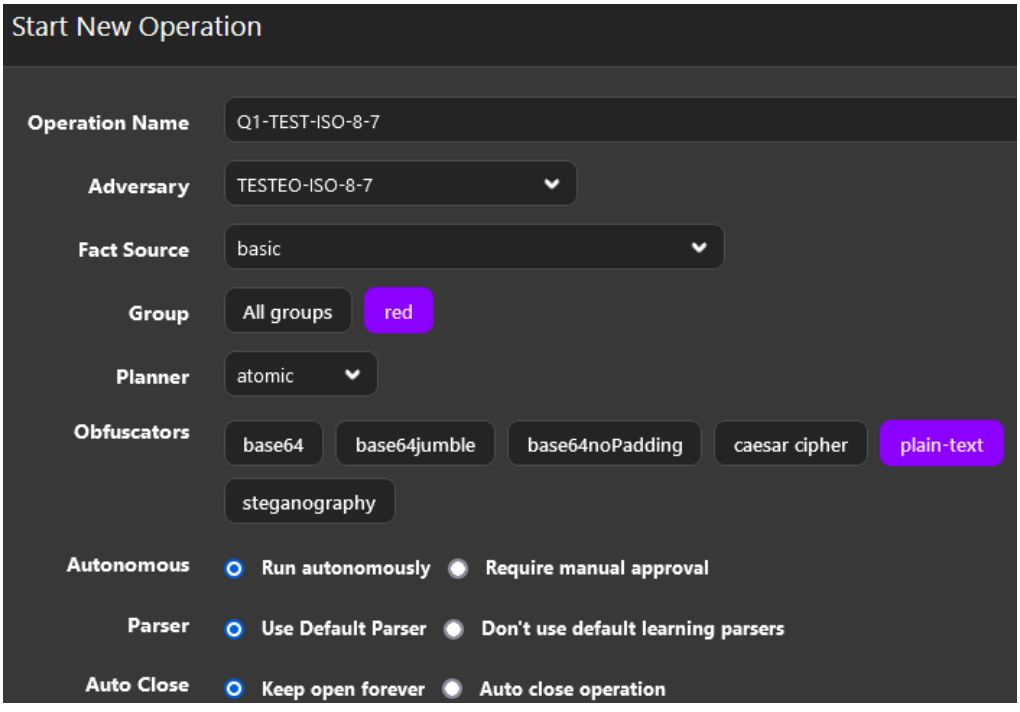


Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup
1	CMSTP Executing Remote Scriptlet	defense-evasion	Signed Binary Proxy Execution: CMSTP					
2	JScript execution to gather local computer information via cscript	execution	Command and Scripting Interpreter: JavaScript					
3	Lolbin Jsc.exe compile javascript to dll	defense-evasion	Trusted Developer Utilities Proxy Execution					
4	WinPwn - fruit	discovery	Network Service Discovery					
5	WinPwn - spoolvulnscan	discovery	Network Service Discovery					
6	wow64log DLL Hijack	privilege-escalation	Abuse Elevation Control Mechanism: Bypass User Access Control					
7	WinPwn - UAC Bypass DiskCleanup technique	multiple	Abuse Elevation Control Mechanism: Bypass User Account Control					
8	Disable ConsentPromptBehaviorAdmin via registry keys	multiple	Abuse Elevation Control Mechanism: Bypass User Account Control					
9	Bypass UAC using sdclt DelegateExecute	multiple	Abuse Elevation Control Mechanism: Bypass User Account Control					
10	WinPwn - UAC Bypass ccmstp technique	multiple	Abuse Elevation Control Mechanism: Bypass User Account Control					
11	Disable UAC notification via registry keys	multiple	Abuse Elevation Control Mechanism: Bypass User Account Control					
12	Disable UAC using reg.exe	multiple	Abuse Elevation Control Mechanism: Bypass User Account Control					
13	WinPwn - UAC Magic	multiple	Abuse Elevation Control Mechanism: Bypass User Account Control					
14	Bypass UAC by Mocking Trusted Directories	multiple	Abuse Elevation Control Mechanism: Bypass User Account Control					
15	WinPwn - UAC Bypass DccwBypassUAC technique	multiple	Abuse Elevation Control Mechanism: Bypass User Account					

Fuente: Elaboración propia.

Como se observa en la Figura 57, se configuraron las opciones de ejecución indicadas en la metodología:

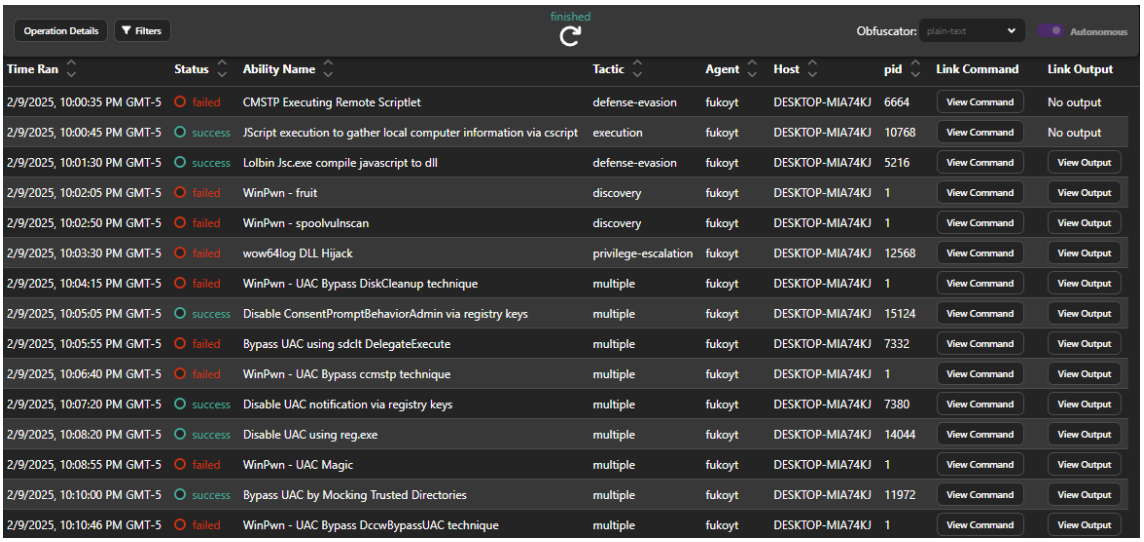
Figura 57. *Configuración de las opciones de ejecución para control ISO 27001 8.7*



Fuente: Elaboración propia.

Finalmente, como se observa parcialmente en la Figura 58, se valida que las técnicas asociadas fueron ejecutadas:

Figura 58. *Ejecución de técnicas asociadas al control ISO 27001 8.7*



Time Ran	Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output
2/9/2025, 10:00:35 PM GMT-5	failed	CMSTP Executing Remote Scriptlet	defense-evasion	fukoyt	DESKTOP-MIA74KJ	6664	View Command	No output
2/9/2025, 10:00:45 PM GMT-5	success	JScript execution to gather local computer information via cscript	execution	fukoyt	DESKTOP-MIA74KJ	10768	View Command	No output
2/9/2025, 10:01:30 PM GMT-5	success	Lolbin Jsc.exe compile javascript to dll	defense-evasion	fukoyt	DESKTOP-MIA74KJ	5216	View Command	View Output
2/9/2025, 10:02:05 PM GMT-5	failed	WinPwn - fruit	discovery	fukoyt	DESKTOP-MIA74KJ	1	View Command	View Output
2/9/2025, 10:02:50 PM GMT-5	failed	WinPwn - spoolvulnscan	discovery	fukoyt	DESKTOP-MIA74KJ	1	View Command	View Output
2/9/2025, 10:03:30 PM GMT-5	failed	wow64log DLL Hijack	privilege-escalation	fukoyt	DESKTOP-MIA74KJ	12568	View Command	View Output
2/9/2025, 10:04:15 PM GMT-5	failed	WinPwn - UAC Bypass DiskCleanup technique	multiple	fukoyt	DESKTOP-MIA74KJ	1	View Command	View Output
2/9/2025, 10:05:05 PM GMT-5	success	Disable ConsentPromptBehaviorAdmin via registry keys	multiple	fukoyt	DESKTOP-MIA74KJ	15124	View Command	View Output
2/9/2025, 10:05:55 PM GMT-5	failed	Bypass UAC using sdclt DelegateExecute	multiple	fukoyt	DESKTOP-MIA74KJ	7332	View Command	View Output
2/9/2025, 10:06:40 PM GMT-5	failed	WinPwn - UAC Bypass ccmstp technique	multiple	fukoyt	DESKTOP-MIA74KJ	1	View Command	View Output
2/9/2025, 10:07:20 PM GMT-5	success	Disable UAC notification via registry keys	multiple	fukoyt	DESKTOP-MIA74KJ	7380	View Command	View Output
2/9/2025, 10:08:20 PM GMT-5	success	Disable UAC using reg.exe	multiple	fukoyt	DESKTOP-MIA74KJ	14044	View Command	View Output
2/9/2025, 10:08:55 PM GMT-5	failed	WinPwn - UAC Magic	multiple	fukoyt	DESKTOP-MIA74KJ	1	View Command	View Output
2/9/2025, 10:10:00 PM GMT-5	success	Bypass UAC by Mocking Trusted Directories	multiple	fukoyt	DESKTOP-MIA74KJ	11972	View Command	View Output
2/9/2025, 10:10:46 PM GMT-5	failed	WinPwn - UAC Bypass DccwBypassUAC technique	multiple	fukoyt	DESKTOP-MIA74KJ	1	View Command	View Output

Fuente: Elaboración propia.

4.3.4. Fase IV: Validación de resultados

Los resultados obtenidos se resumen en las siguientes tablas:

1. **Tablas de resultados en herramientas de seguridad:** A continuación, en la Tabla 9 y Tabla 10, se presentan las tablas de resultados correspondientes a los controles ISO 27001 8.20 y 8.7, tomando en cuenta el resultado por cada herramienta de seguridad asociada.

Tabla 9. *Tabla de resultados ISO 27001 8.20 en herramientas de seguridad.*

CONTROL ISO 27001 8.20			
#	**Técnica ejecutada**	**Herramientas de seguridad**	
		EDR Sophos Endpoint	**Firewall PA-410**
1	DNS over HTTPS Large Query Volume	NA	Alertado
2	Exfiltration Over Alternative Protocol – HTTP	No detectado	Alertado
3	Running Chrome VPN Extensions via the Registry 2 vpn extension	NA	Alertado

4	Network Service Scanning	No detectado	No detectado
5	Port-Scanning /24 Subnet with PowerShell	No detectado	NA
6	Testing usage of uncommonly used port with PowerShell	NA	Alertado
7	Sniff network traffic	No detectado	NA
8	Windows Internal pktmon set filter	No detectado	NA
9	Windows Internal Packet Capture	No detectado	NA
10	Exfiltrate data HTTPS using curl windows	No detectado	Alertado

Fuente: Elaboración propia.

Tabla 10. *Tabla de resultados ISO 27001 8.7 en herramientas de seguridad.*

CONTROL ISO 27001 8.7			
#	**Técnica ejecutada**	**Herramientas de seguridad**	
		EDR Sophos Endpoint	**Firewall PA-410**
1	CMSTP Executing Remote Scriptlet	Bloqueado	NA
2	JScript execution to gather local computer information via cscript	No detectado	NA
3	Lolbin Jsc.exe compile javascript to dll	No detectado	NA
4	WinPwn-fruit	Bloqueado	Alertado
5	WinPwn-spoolvulnscan	Bloqueado	No detectado
6	Wow64log DLL Hijack	Bloqueado	NA
7	WinPwn – UAC Bypass DiskCleanup technique	Bloqueado	No detectado
8	Disable ConsentPromptBehaviourAdmin via registry keys	No detectado	NA
9	Bypass UAC using sdclt DelegateExecute	No detectado	NA
10	WinPwn - UAC Bypass ccmstp technique	Bloqueado	No detectado
11	Disable UAC notification via registry keys	No detectado	NA
12	Disable UAC using reg.exe	No detectado	NA
13	WinPwn - UAC Magic	Bloqueado	No detectado
14	Bypass UAC by Mocking Trusted Directories	No detectado	NA
15	WinPwn - UAC Bypass DccwBypassUAC technique	Bloqueado	Alertado

16	Bypass UAC using Event Viewer (PowerShell)	Bloqueado	NA
17	Launches an executable using Rundll32 and pcwutl.dll	No detectado	NA
18	PowerShell bitly Link Download	No detectado	Alertado
19	PowerShell Fileless Script Execution	Bloqueado	NA
20	Potentially Unwanted Applications (PUA)	Bloqueado	No detectado
21	File Extension Masquerading	No detectado	NA
22	UAC bypass registry	No detectado	NA

Fuente: Elaboración propia.

2. **Tablas de cumplimiento ISO 27001:** A continuación, en la Tabla 11 y Tabla 12, se presentan las tablas de cumplimiento correspondientes a los controles ISO 27001 8.20 y 8.7, tomando en cuenta el puntaje de cada técnica y el cumplimiento alcanzado.

Tabla 11. *Tabla de cumplimiento ISO 27001 8.20.*

CONTROL ISO 27001 8.20			
#	**Técnica ejecutada**	**Resultado**	**Puntaje**
1	DNS over HTTPS Large Query Volume	Alertado	0.5
2	Exfiltration Over Alternative Protocol – HTTP	Alertado	0.5
3	Running Chrome VPN Extensions via the Registry 2 vpn extension	Alertado	0.5
4	Network Service Scanning	No detectado	0
5	Port-Scanning /24 Subnet with PowerShell	No detectado	0
6	Testing usage of uncommonly used port with PowerShell	Alertado	0.5
7	Sniff network traffic	No detectado	0
8	Windows Internal pktmon set filter	No detectado	0
9	Windows Internal Packet Capture	No detectado	0
10	Exfiltrate data HTTPS using curl windows	Alertado	0.5
	Cumplimiento		25%

Fuente: Elaboración propia.

Tabla 12. *Tabla de cumplimiento ISO 27001 8.7.*

CONTROL ISO 27001 8.7			
#	**Técnica ejecutada**	**Resultado**	**Puntaje**
1	CMSTP Executing Remote Scriptlet	Bloqueado	1
2	JScript execution to gather local computer information via cscript	No detectado	0
3	Lolbin Jsc.exe compile javascript to dll	No detectado	0
4	WinPwn-fruit	Bloqueado	1
5	WinPwn-spoolvulnscan	Bloqueado	1
6	Wow64log DLL Hijack	Bloqueado	1
7	WinPwn – UAC Bypass DiskCleanup technique	Bloqueado	1
8	Disable ConsentPromptBehaviourAdmin via registry keys	No detectado	0
9	Bypass UAC using sdclt DelegateExecute	No detectado	0
10	WinPwn - UAC Bypass ccmstp technique	Bloqueado	1
11	Disable UAC notification via registry keys	No detectado	0
12	Disable UAC using reg.exe	No detectado	0
13	WinPwn - UAC Magic	Bloqueado	1
14	Bypass UAC by Mocking Trusted Directories	No detectado	0
15	WinPwn - UAC Bypass DccwBypassUAC technique	Bloqueado	1
16	Bypass UAC using Event Viewer (PowerShell)	Bloqueado	1
17	Launches an executable using Rundll32 and pcwutl.dll	No detectado	0
18	PowerShell bitly Link Download	Alertado	0.5
19	PowerShell Fileless Script Execution	Bloqueado	1
20	Potentially Unwanted Applications (PUA)	Bloqueado	1
21	File Extension Masquerading	No detectado	0
22	UAC bypass registry	No detectado	0
	Cumplimiento		52.27%

Fuente: Elaboración propia.

Para el cálculo del cumplimiento por cada control ISO 27001, se hace uso de la formula propuesta en la metodología:

$$cumplimiento(\%) = \frac{Puntaje\ total\ obtenido}{\#\ técnicas\ totales\ aplicables}\ x\ 100\%$$

- Cumplimiento para el control ISO 27001 8.20:

$$cumplimiento(\%) = \frac{2.5}{10}\ x\ 100\%$$

$$cumplimiento(\%) = 25\%$$

- Cumplimiento para el control ISO 27001 8.7:

$$cumplimiento(\%) = \frac{11.5}{22}\ x\ 100\%$$

$$cumplimiento(\%) = 52.27\%$$

En el Anexo F se presentan los resultados y las evidencias recopiladas de cada herramienta de seguridad, las cuales fueron utilizadas para categorizar, calificar y obtener los resultados mostrados en las tablas descritas en el presente apartado.

4.3.5. Fase V: Comunicación de hallazgos

Se derivaron los resultados obtenidos a la "Alta Dirección", posterior a la revisión, se aprobó y acordó ejecutar la siguiente lista de acciones:

- Cambios por realizar en el firewall PA-410:
  - Bloqueo de DNS sobre HTTPS: Bloquear la aplicación "dns-over-https" en toda la red, ya que no es usado por la empresa.
  - Bloqueo de escaneo de red: Habilitar el perfil de "Zone Proteccion" para bloquear ataques de reconocimiento, ataques de inundación TCP y basados en paquetes malformados.
  - Permitir solo puertos comunes: A las políticas de seguridad, adicional a la aplicación identificada, agregar el puerto correspondiente permitido.
  - Bloquear la descarga y subida de archivos en base al tipo: Habilitar el perfil "File Blocking" en las políticas de seguridad de navegación, bloqueando archivos batch, DLL, .lnk, jar, .exe, .zip, .rar, etc.

- Bloquear el uso de acortadores de url: Crear una categoría URL que contenga la lista de acortadores a bloquear, tales como bit.ly, ow.ly, etc.

- Cambios por realizar en el EDR Sophos Endpoint:
  - Bloquear el uso de cscript.
  - Habilitar protección contra script en Powershell (archivos ps1).
  - Habilitar política de Web Protection para bloquear descarga de archivos por HTTP y HTTPS.
  - Bloquear URL acortadora de enlaces.

4.3.6. Fase VI: Optimización de herramientas

Se realizaron los siguientes cambios en la herramienta de seguridad:

1. Evidencias de cambios aplicados en el firewall PA-410:
   a. Bloqueo de DNS sobre HTTPS: La Figura 59 muestra cómo se bloqueó la aplicación “dns-over-https” en toda la red, ya que no es usado por la empresa.

Figura 59. *Bloqueo de DNS sobre HTTPS*

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION
1	BLOCK_DoH	none	universal	any	any	any	any	any	any	any	dns-over-https	any	Deny

Fuente: Elaboración propia.

   b. Bloqueo de escaneo de red: Se habilitó el perfil de “Zone Proteccion” para bloquear ataques de reconocimiento en la zona LAN, DMZ y WAN, tal como se observa en la Figura 60.

Figura 60. *Bloqueo de escaneo de red*

Zone Protection Profile

Name: Proteccion_zona

Description:

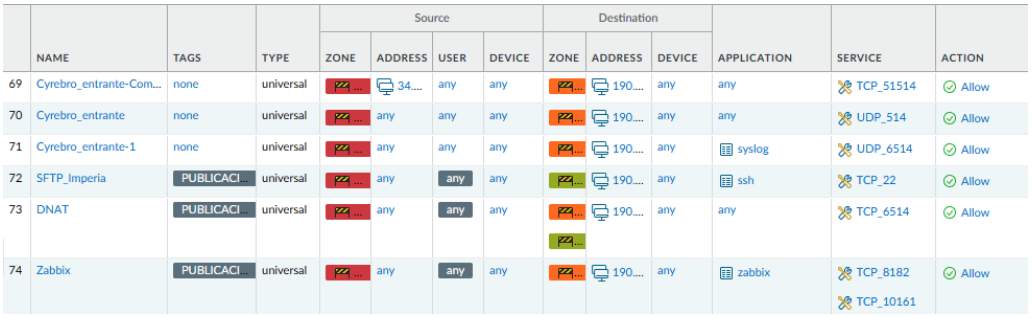
Flood Protection | Reconnaissance Protection | Packet Based Attack Protection | Protocol Protection | Ethernet SGT Pr

SCAN	ENABLE	ACTION	INTERVAL (SEC)	THRESHOLD (EVENTS)
TCP Port Scan	☑	block-ip	2	100
Host Sweep	☑	block-ip	10	100
UDP Port Scan	☑	block-ip	2	100

Fuente: Elaboración propia.

c. Permitir solo puertos comunes: Se modificaron las políticas de seguridad para agregarles el puerto correspondiente permitido. A continuación, en la Figura 61 se observa una muestra.

Figura 61. *Muestra de políticas con puertos comunes*

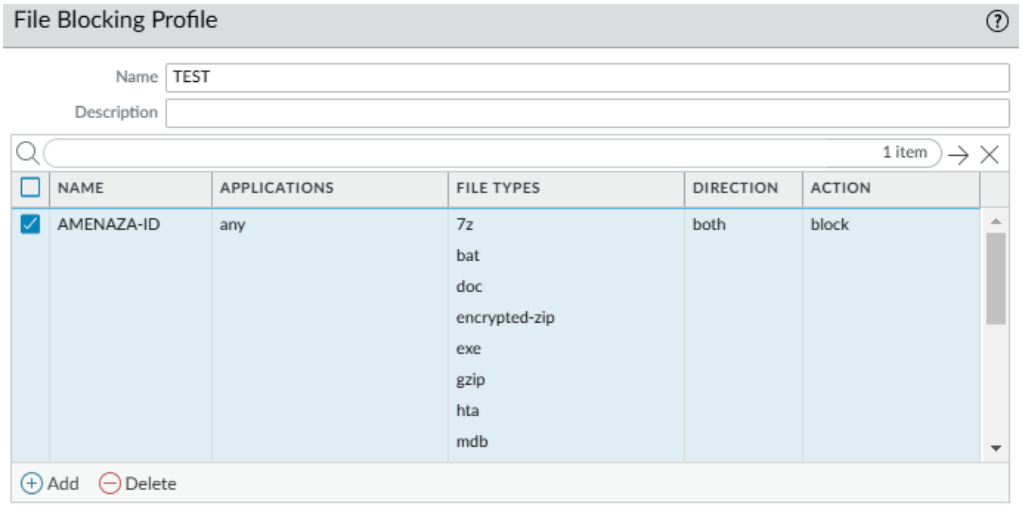


	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION
69	Cyrebro_entrante-Com...	none	universal	...	34....	any	any	...	190....	any	any	TCP_51514	Allow
70	Cyrebro_entrante	none	universal	...	any	any	any	...	190....	any	any	UDP_514	Allow
71	Cyrebro_entrante-1	none	universal	...	any	any	any	...	190....	any	syslog	UDP_6514	Allow
72	SFTP_Imperia	PUBLICACI...	universal	...	any	any	any	...	190....	any	ssh	TCP_22	Allow
73	DNAT	PUBLICACI...	universal	...	any	any	any	...	190....	any	any	TCP_6514	Allow
74	Zabbix	PUBLICACI...	universal	...	any	any	any	...	190....	any	zabbix	TCP_8182 TCP_10161	Allow

Fuente: Elaboración propia.

d. Bloquear la descarga y subida de archivos en base al tipo: Se habilitó el perfil "File Blocking", como se observa en la Figura 62, en las políticas de seguridad de navegación, bloqueando archivos 7z, bat, doc, encrypted-zip, exe, gzip, hta, etc.

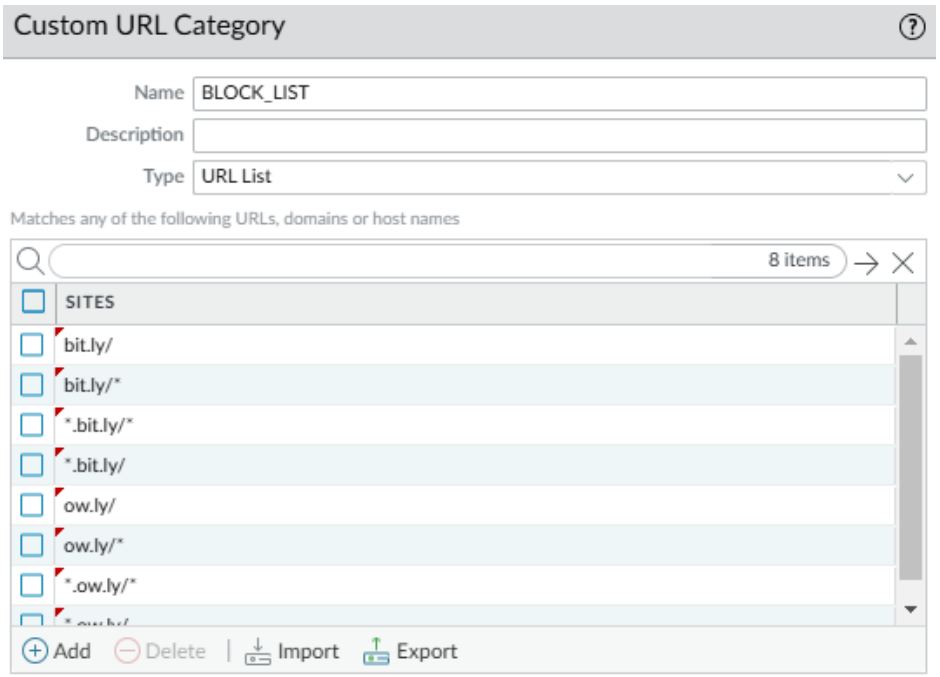
Figura 62. *Bloqueo de archivos en perfil "File Blocking"*



Fuente: Elaboración propia.

e. Bloquear el uso de acortadores de URL: La Figura 63 muestra que se configuró una categoría URL "BLOCK_LIST" en la cual se bloqueó acortadores de URL como "bit.ly" y "ow.ly".

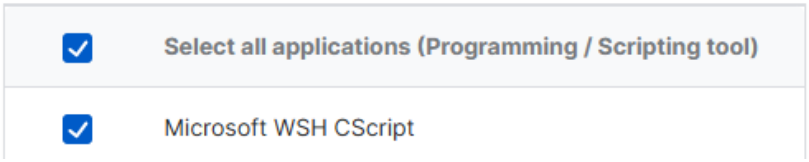
Figura 63. *Bloqueo de acortadores URL en "BLOCK_LIST"*



Fuente: Elaboración propia.

2. Evidencias de cambios aplicados en el EDR Sophos Endpoint:
    a. Bloquear el uso de cscript: La Figura 64 muestra el bloqueo de cscript (Microsoft WSH CScript) en la política "Application Control" de Sophos.

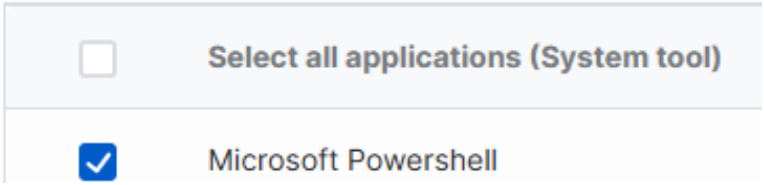
    Figura 64. *Bloqueo de Microsoft WSH cscript*



Fuente: Elaboración propia.

    b. Habilitar protección contra script en Powershell (archivos ps1): Como se muestra en la Figura 65, se bloqueó el uso de Powershell.

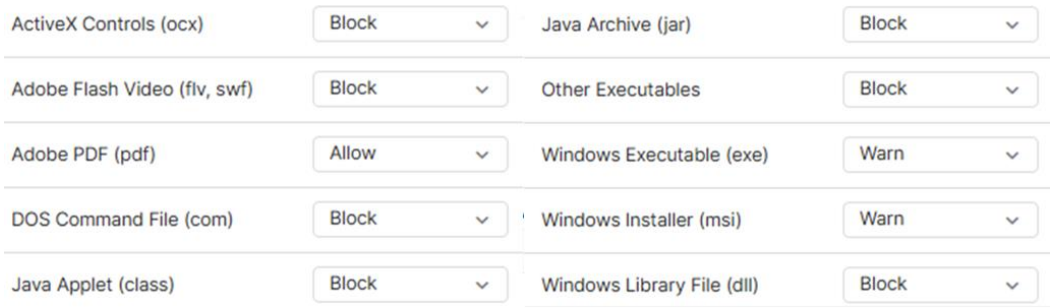
    Figura 65. *Bloqueo de Powershell para evitar el uso de scripts*



Fuente: Elaboración propia.

c. Habilitar política de Web Protection para bloquear descarga de archivos por HTTP y HTTPS: Se procedió con el bloqueo de la descarga de archivos, según lo mostrado en la Figura 66, donde se observan las opciones configuradas.

Figura 66. *Lista de archivos y su opción de descarga*



Fuente: Elaboración propia.

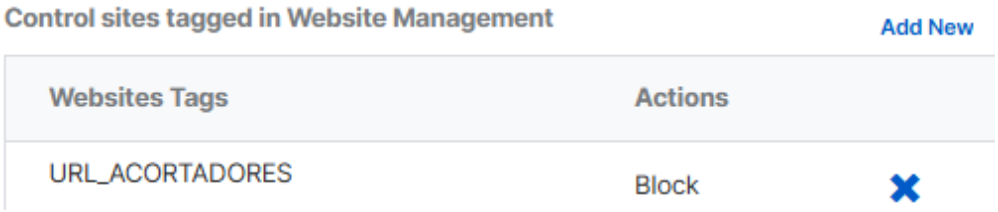
d. Bloquear URL acortadora de enlaces: Como se observa en la Figura 67 y Figura 68, se procedió con el bloqueo de los acortadores URL.

Figura 67. *Categoría de acortadores URL creada*

Website	Tagged As
bit.ly	URL_ACORTADORES
ow.ly	URL_ACORTADORES

Fuente: Elaboración propia.

Figura 68. *Bloqueo de acortadores URL*



Fuente: Elaboración propia.

Finalizada la ejecución de la metodología en la empresa, se identificaron los siguientes resultados al implementar las fases propuestas:

1. **Validación del proceso metodológico:** Durante la implementación de la metodología, los pasos a seguir fueron lo suficientemente detallados para poder ser replicados en la empresa, evidenciando que las fases propuestas son adecuadas y válidas para su adopción en las organizaciones.
2. **Auditoría continua de los controles:** La metodología permitió y facilitó la auditoría continua de los controles, los cuales fueron programados para realizarse de forma mensual, asegurando un monitoreo constante del cumplimiento.
3. **Alineación de técnicas y controles:** La empresa logró contar con un mapeo que les permitió alinear las técnicas del marco MITRE ATT&CK con los controles de la norma ISO 27001:2022, brindándoles visibilidad de las amenazas potenciales a las cuales están expuestas sus activos.
4. **Mejora en la medición del cumplimiento:** La empresa optimizó la medición del cumplimiento de sus controles ISO 27001:2022 al hacer uso de la fórmula de puntuación del cumplimiento, obteniendo visibilidad por cada prueba realizada.
5. **Mejora en la protección de herramientas de seguridad:** La empresa mejoró el estado de protección de sus herramientas de seguridad al poder identificar configuraciones deshabilitadas o no usadas correctamente, lo que le permitió tomar acciones correctivas para fortalecer su infraestructura.

5. Conclusiones y trabajo futuro

El presente trabajo ha abordado el problema de la deficiencia en las organizaciones para evaluar continuamente los controles de la norma ISO 27001:2022, para ello se ha desarrollado una metodología basada en la simulación de ataques, estructurada en seis fases, las cuales hacen uso de una herramienta BAS y el marco MITRE ATT&CK para poder brindar un marco metodológico que permita evaluar continuamente los controles y medir el cumplimiento de los mismos a demanda.

La metodología desarrollada no pretende reemplazar las auditorias tradicionales de los controles ISO 27001, las cuales son necesarias para comprobar que efectivamente los controles han sido implantados y se están cumpliendo. En cambio, busca servir como apoyo complementario para facilitar el cumplimiento continuo. Dado que la auditoría evalúa el estado de la organización en un momento especifico, esta metodología garantiza que el puntaje inicial se mantenga a lo largo del tiempo, permitiendo a las organizaciones preservar el cumplimiento inicial.

Su validez se verifica al implementar la metodología en un entorno empresarial, donde los resultados obtenidos evidencian su capacidad para cumplir con los objetivos planteados en el presente trabajo.

En primer lugar, se ha demostrado que es posible evaluar los controles de la norma ISO 27001:2022 usando una herramienta BAS y el marco MITRE ATT&CK, para ello se documentaron los pasos y uso de tecnologías específicas para realizar esta labor, contribuyendo con una guía clara para su implementación.

En segundo lugar, se ha comprobado que es posible realizar un mapeo entre técnicas ATT&CK y los controles ISO 27001:2022, sirviendo para propósitos de documentación, consulta y visibilidad de la cantidad de ataques que cubre la norma ISO 27001:2022, contribuyendo con un mapa de calor en MITRE Navigator que permite la comprensión del alcance de la norma en términos de seguridad ofensiva.

En tercer lugar, se ha logrado identificar a BAS Caldera como la herramienta más adecuada para la evaluación de los controles ISO 27001:2022. Su ventaja principal radica en ser open-source y ofrecer funcionalidades que permiten su integración nativa con el marco MITRE ATT&CK. Producto de la investigación, se contribuye con un archivo Docker de Caldera que

contiene los controles ISO 27001 mapeados, lo que facilita su instalación y personalización. Esto reduce tanto el tiempo necesario para evaluar los controles como los costos asociados.

En cuarto lugar, se ha elaborado el proceso metodológico para la evaluación de los controles ISO 27001:2022, garantizando su aplicabilidad y reproducibilidad. Este enfoque contribuye a mejorar el ciclo de evaluación continua, dado que sus seis fases conforman un proceso de retroalimentación constante. Permitiendo realizar evaluaciones a demanda sin procedimientos extensos.

En quinto lugar, se ha validado que la metodología es aplicable en entornos reales, contribuyendo con un ejemplo de implementación empresarial que demuestra su efectividad en la detección de configuraciones deficientes y en la mejora de la postura de seguridad de la organización. La implementación permitió revisar los resultados obtenidos en las herramientas de seguridad, mejorando su estado de protección, así como evaluar el porcentaje de cumplimiento por activo, proporcionando una escala de medición porcentual.

Por otra parte, una de las limitaciones de la metodología es que su alcance de medición queda restringido a los controles tecnológicos de la norma ISO 27001:2022, debido a que la herramienta BAS y el marco MITRE ATT&CK están enfocados en simulaciones de ataques dirigidos a activos tecnológicos, lo que impide su alcance en controles de tipo organizativos, de personas o físicos. Otra limitación es que la metodología se desarrolla utilizando el BAS Caldera, esto se dio en base al estudio de la herramienta más adecuada, por lo que, si la organización desea hacer uso de algún otro BAS, deberá adaptar el proceso de implementación según los requisitos específicos de dicha herramienta. Sin embargo, en términos generales, la metodología sigue siendo válida y cumple con su propósito.

Asimismo, el trabajo desarrollado podría ampliarse si el mapeo realizado entre las técnicas ATT&CK y los controles ISO 27001:2022 se extiende para incluir también los patrones de ataque de CAPEC. Esto permitiría obtener una visibilidad más completa de las vulnerabilidades que las amenazas pueden explotar, ya que CAPEC proporciona los CVE y CWE asociados.

También se podría investigar la posibilidad de ampliar la aplicación de la metodología propuesta para evaluar otros estándares de seguridad, como NIST 800-53, los controles CIS, entre otros. Esto permitiría adaptar la metodología a diferentes marcos de referencia y ampliar su utilidad en diversas organizaciones.

De igual forma, al proceso metodológico se le puede añadir la implementación de un SIEM (Sistema de gestión de información y eventos de seguridad), de tal forma que la fase de validación de resultados en las herramientas de seguridad se realice de manera centralizada, mediante la revisión exclusiva de los logs enviados hacia el SIEM.

Por último, se proyecta que el ciclo de evaluación continua desarrollado en el presente trabajo sea utilizado en futuras investigaciones sobre herramientas BAS relacionadas con el cumplimiento normativo. Por medio de la propuesta de un enfoque que integra el conocimiento en ciberseguridad ofensiva con las exigencias de cumplimiento normativo, uniendo dos áreas que generalmente se consideran separadas, se logra brindar una solución práctica para la validez continua de los controles de la ISO 27001:2022.

Referencias bibliográficas

ISC2 (2024). *2024 Cyberthreat Defense Report*. https://cloud.connect.isc2.org/cyberthreat-defense-report

A-LIGN (2024). *2024 Compliance Benchmark Report*. https://www.a-lign.com/resources/2024-compliance-benchmark-report-drata

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. En 2023 International Conference on Cyber Management and Engineering (CyMaEn) (pp. 117-122). Bangkok, Thailand. doi: 10.1109/CyMaEn57228.2023.10051114

CTX (2024). *¿Qué es el bastionado o hardening?*. https://ctxdetectives.com/que-es-el-bastionado-o-hardening/

Vectra (2024). *Detección y respuesta en red (NDR).* https://es.vectra.ai/topics/network-detection-and-response

IBM (2024). *¿Qué es la detección y respuesta de endpoints (EDR)?.* https://www.ibm.com/mx-es/topics/edr

Pilleux, G. (2021). *Sistema de pruebas de penetración automatizada para aplicaciones web.* [Tesis de pregrado, Universidad de Chile]. Repositorio académico de la Universidad de Chile. https://repositorio.uchile.cl/handle/2250/181748

Li, R., Abendroth, D., Lin, X., Guo, Y., Baek, H.-W., Eide, E., … Van der Merwe, J. (2015). Potassium. Proceedings of the Sixth ACM Symposium on Cloud Computing (SoCC) (pp. 30-42) Salt Lake City, UT, USA. doi:10.1145/2806777.2806935

Cano, J. (2019). *Análisis, diseño y desarrollo de una aplicación para la realización automática de pentesting.* [Trabajo Fin de Máster, Universidad de Alicante]. Repositorio Institucional de la Universidad de Alicante. https://rua.ua.es/dspace/handle/10045/93292

Ramiro, R. (2019). Conoce la tecnología "Breach and Attack Simulation" (BAS). *CIBERSEGURIDAD Blog*. https://ciberseguridad.blog/conoce-la-tecnologia-breach-and-attack-simulation-bas-y-resucita-tu-estrategia-de-ciberseguridad/#google_vignette

Ben-Yossef, A. (2024). *Automated Penetration Testing – How BAS killed the pen test*. https://cymulate.com/blog/automated-penetration-testing/

Engström, V., & Lagerström, R. (2022). Two decades of cyberattack simulations: A systematic literature review. Computers & Security, 116, 102681. https://doi.org/10.1016/j.cose.2022.102681

Kruck, G. P. (2023). *Combating Non-Compliance: Leveraging Breach & Attack Simulation Techniques to Continuously Validate Information Assurance Controls.* [Tesis doctoral, Marymont University]. Marymount University ProQuest Dissertations & Theses. https://www.proquest.com/openview/d78c3af49dbb84f51b9a635d2f529f99/1?pq-origsite=gscholar&cbl=18750&diss=y

AttackIQ (2022). AttackIQ-Breach and attack simulation. https://www.youtube.com/watch?v=iq5kOKtaiK0

Ferraz T. (2022). *Breach and attack simulator*. [Tesis de maestría, Universidade de Coimbra]. Repositório científico da UC. https://estudogeral.uc.pt/handle/10316/104723

MITRE (2024a). *Get Started*. MITRE. https://attack.mitre.org/resources/

IBM (2024). *Marco MITRE ATT&CK.* https://www.ibm.com/es-es/topics/mitre-attack

Rahman, M. R., & Williams, L. (2022). An investigation of security controls and MITRE ATT&CK techniques. *arXiv preprint arXiv:2211.06500*. doi:10.48550/arXiv.2211.06500

Hardey S. (2021). ATT&CK framework mapping methodology. https://github.com/center-for-threat-informed-defense/attack-control-framework-mappings/blob/main/docs/mapping_methodology.md

MITRE (2024b). *Enterprise Mitigations.* MITRE. https://attack.mitre.org/mitigations/enterprise/

MITRE (2024c). *ATT&CK Data & Tools* [Hoja de Excel]. MITRE. https://attack.mitre.org/resources/attack-data-and-tools/#excel-attack

SafeBreach (2025). SafeBreach Breach and Attack Simulation (BAS) Platform. https://www.safebreach.com/breach-and-attack-simulation-platform/

Cymulate (2025). Cymulate Breach and Attack Simulation (BAS). https://cymulate.com/data-sheet/bas-data-sheet/

Redscan (2025). Breach and attack simulation. https://www.redscan.com/services/breach-and-attack-simulation/

Pentera (2025). Pentera platform. https://pentera.io/platform/

Fortinet (2025) Fortitester Datasheet. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiTester.pdf

AttackIQ (2025). AttackIQ Products. https://www.attackiq.com/products/

Akamai (2024). Infection Monkey. https://github.com/guardicore/monkey/

Red Canary (2023). Atomic Red Team. https://github.com/redcanaryco/atomic-red-team/wiki/

AlphaSOC (2024). Network Flight Simulator. https://github.com/alphasoc/flightsim

Nextron (2022). APT Simulator. https://github.com/NextronSystems/APTSimulator

MITRE (2025a). MITRE Caldera. https://github.com/mitre/caldera

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection Information security management systems requirements* (estándar ISO 27001:2022). https://www.iso.org/es/norma/27001

MITRE (2025b). *Resources – Ability List* [Hoja de Excel]. Caldera Usage guide. https://caldera.readthedocs.io/en/latest/resources.html

Anexo A. Tabla Excel con mitigaciones ATT&CK

Tabla 13. *Controles ISO 27001 a mitigaciones MITRE ATT&CK.*

Código	Control	Mitigación
5.7	Inteligencia de amenazas	M1019
5.15	Control de acceso	M1035, M1030, M1022, M1024, M1039, M1043
5.17	Información de autenticación	M1027
6.3	Concienciación, educación y formación en seguridad de la información	M1017
8.1	Dispositivos de punto final de usuario	M1033, M1034, M1037, M1040, M1041, M1049, M1053, M1021
8.2	Derechos de acceso privilegiado	M1026, M1052, M1018
8.3	Restricción del acceso a la información	M1035, M1022, M1024, M1039, M1041, M1048
8.4	Acceso al código fuente	M1038, M1044
8.5	Autenticación segura	M1032, M1036, M1027, M1015
8.6	Gestión de la capacidad	M1042, M1028
8.7	Protección contra malware	M1033, M1021, M1016, M1046, M1042, M1034, M1051, M1017, M1053, M1049, M1050
8.8	Gestión de las vulnerabilidades técnicas	M1016, M1051, M1054
8.9	Gestión de la configuración	M1026, M1015, M1018
8.10	Eliminación de información	NA
8.11	Enmascaramiento de datos	NA
8.12	Prevención de fugas de datos	M1057
8.13	Copia de seguridad de la información	M1053
8.14	Redundancia de las instalaciones de tratamiento de la información	M1060
8.15	Registro	M1029
8.16	Actividades de monitoreo	M1031, M1040, M1020, M1038, M1050, M1025
8.17	Sincronización de relojes	NA
8.18	Uso de programas de utilidades privilegiadas	M1018, M1042
8.19	Instalación de software en sistemas operativos	M1033, M1051
8.20	Seguridad de las redes	M1037, M1030, M1048
8.21	Seguridad de los servicios de red	NA

8.22	Segregación de redes	M1030
8.23	Filtrado web	M1021, M1020
8.24	Uso de la criptografía	M1041
8.25	Ciclo de vida de desarrollo seguro	M1013, M1016, M1047
8.26	Requisitos de seguridad de las aplicaciones	M1018, M1045, M1041
8.27	Arquitectura de sistemas seguros y principios de ingeniería	NA
8.28	Codificación segura	M1051, M1013
8.29	Pruebas de seguridad en el desarrollo y la aceptación	M1047
8.30	Desarrollo externalizado	NA
8.31	Separación de los entornos de desarrollo, prueba y producción	M1030, M1051, M1053
8.32	Gestión del cambio	NA
8.33	Información de la prueba	NA
8.34	Protección de los sistemas de información durante las pruebas de auditoría	M1047

Fuente: Elaboración propia.

Anexo B. Scripts Utilizados

Tabla 14. *Script "P1-map-controls-to-mitre.py".*

```
import pandas as pd
from openpyxl import load_workbook

def cargar_tabla_por_nombre(ruta_excel, nombre_tabla):
    wb = load_workbook(ruta_excel, data_only=True)
    for ws in wb.worksheets:
        for tabla in ws._tables.values():
            if tabla.name == nombre_tabla:
                datos = ws[tabla.ref]
                columnas = [cell.value for cell in datos[0]]
                contenido = [[cell.value for cell in fila] for fila in datos[1:]]
                return pd.DataFrame(contenido, columns=columnas)

def actualizar_codigo_en_tabla3(ruta_excel):
    tabla1 = cargar_tabla_por_nombre(ruta_excel, "Tabla1")
    tabla2 = cargar_tabla_por_nombre(ruta_excel, "Tabla2")

    # Crear un diccionario para mapear 'mitigacion' a 'codigo'
    diccionario_mapeo = {}
    for mit, codigo in zip(tabla1["mitigacion"], tabla1["codigo"]):
        mit_list = mit.split(",")  # Dividir mitigaciones separadas por coma
        for m in mit_list:
            m = m.strip()  # Eliminar posibles espacios extra
            if m in diccionario_mapeo:
                diccionario_mapeo[m].append(codigo)
            else:
                diccionario_mapeo[m] = [codigo]

    # Función que encuentra todos los códigos para un 'source_id' en 'tabla2'
    def obtener_codigos(source_id):
        mit_list = source_id.split(",")  # Dividir el source_id en mitigaciones
        codigos = []
        for mit in mit_list:
            mit = mit.strip()  # Eliminar espacios extra
            if mit in diccionario_mapeo:
                codigos.extend(diccionario_mapeo[mit])  # Agregar todos los códigos
correspondientes
        return ', '.join(map(str, codigos))  # Unir todos los códigos con comas

    # Aplicar la función 'obtener_codigos' a la columna 'source_id' de 'tabla2'
    tabla2["iso_id"] = tabla2["source_id"].apply(obtener_codigos)

    # Guardar el DataFrame actualizado de vuelta en el archivo Excel
    with pd.ExcelWriter(ruta_excel, engine="openpyxl", mode="a", if_sheet_exists="overlay") as
writer:
        tabla2.to_excel(writer, sheet_name="Tabla3", index=False)

# Ruta del archivo Excel
ruta_excel = r"C:\Users\diego\OneDrive\Desktop\Maestria-ciberseguridad\TFM\TEST_JSON\mapping-
auto.xlsx"
actualizar_codigo_en_tabla3(ruta_excel)
```

Tabla 15. *Script "P2-get-mitre-matrix.py".*

```
import pandas as pd
import json
import re

# Cargar el archivo JSON
with open("mitre-data.json", "r") as json_file:
    json_data = json.load(json_file)

# Cargar el archivo Excel
excel_data = pd.read_excel("mapping-auto.xlsx", sheet_name="Tabla3")

# Normalizar los nombres de las columnas del archivo Excel para evitar errores
excel_data.columns = excel_data.columns.str.strip().str.lower().str.replace(' ', '_')

# Crear una lista para almacenar los resultados actualizados
updated_json = []

#---------------Iterar sobre las entradas del archivo JSON---------------
for entry in json_data:
    technique_id = entry.get("techniqueID")  # Obtener el valor de techniqueID
    if technique_id:
        # Filtrar filas en el archivo Excel donde target_id coincide con techniqueID
        matching_rows = excel_data[excel_data['target_id'] == technique_id]

        # Obtener los valores de source_id de las filas coincidentes
        source_ids = matching_rows['source_id'].dropna().astype(str).tolist()

        # Obtener los valores de iso_id de las filas coincidentes
        iso_values = matching_rows['iso_id'].dropna().astype(str).tolist()

        # Concatenar los valores de source_id e iso_id con comment en el JSON, esto permite
obtener en los comentarios las Mitigaciones y controles ISO 27001 asociados x c/tecnica
        if source_ids or iso_values:
            entry["comment"] = ""
            comment_id = entry.get("")  # Obtener comment del JSON, inicializa en blanco
            concatenated_values = ""
            # Concatenar source_ids
            if source_ids:
                concatenated_values += "; ".join(source_ids)
            # Concatenar iso_values
            if iso_values:
                if concatenated_values:
                    concatenated_values += "; "  # Agregar separación si ya hay source_ids
                concatenated_values += "; ".join(iso_values)

            # Actualizar el comentario
            entry["comment"] = comment_id + "; " + concatenated_values if comment_id else
concatenated_values

    # Agregar la entrada actualizada a la lista
    updated_json.append(entry)

#---------------Procesar, limpiar los comentarios y calcular score---------------
for entry in updated_json:
```

```
    comment = entry.get("comment", "")
    if comment:
        # Separar por ";" o ",", eliminar duplicados y reconstruir el comentario
        comment_parts = [part.strip() for part in comment.replace(",", ";").split(";")]
        unique_comments = list(dict.fromkeys(comment_parts))
        entry["comment"] = "; ".join(unique_comments)

        # Contar ocurrencias de valores numéricos (regex para detectar números como 8.14, 8.1,
etc.)
        numeric_values = [value for value in unique_comments if re.match(r"^\d+\.\d+$",
value)]
        entry["score"] = len(numeric_values)  # Guardar el conteo en el campo "score"
    else:
        entry["score"] = 0  # Si no hay comentario, el score es 0

# Mostrar el menor y mayor valor de "score"
scores = [entry["score"] for entry in updated_json]
min_score = min(scores)
max_score = max(scores)

print(f"El menor valor de 'score' es: {min_score}")
print(f"El mayor valor de 'score' es: {max_score}")

# Guardar resultados
# Guardar el archivo JSON actualizado
with open("mapping-auto.json", "w") as output_file:
    json.dump(updated_json, output_file, indent=4)

print("El archivo JSON actualizado se ha guardado como 'mapping-auto.json'.")
```

Tabla 16. *Script "P3-get-caldera-techniques.py".*

```
import re

# Función para leer el archivo y extraer los valores del atributo 'value'
def extraer_valores(archivo_entrada):
    valores = []

    # Abrir y leer el archivo de entrada
    with open(archivo_entrada, 'r', encoding='utf-8') as f:
        contenido = f.read()

    # Buscar todos los valores de los atributos 'value' en el archivo
    valores_raw = re.findall(r'value="([^"]+)"', contenido)

    # Filtrar los valores que siguen el patrón "T1XXX" o "T1XXX.XXX"
    patron = r'T1\d{3}(\.\d{3})?'

    # Aplicar la expresión regular para filtrar los valores válidos
    valores = [valor for valor in valores_raw if re.match(patron, valor)]

    # Procesar los valores para quedarnos solo con la parte antes del "|" y eliminar espacios
en blanco
    valores_procesados = [valor.split('|')[0].strip() for valor in valores]
```

```
    return valores_procesados

# Función para guardar los valores extraídos en un nuevo archivo
def guardar_valores(valores, archivo_salida):
    # Eliminar duplicados usando un set
    valores_unicos = list(set(valores))  # Convertimos el set nuevamente a lista para poder
ordenar

    # Opcional: Si quieres ordenar los valores
    valores_unicos.sort()

    # Guardar los valores únicos en el archivo
    with open(archivo_salida, 'w', encoding='utf-8') as f:
        for valor in valores_unicos:
            f.write(valor + '\n')

#----------------------
archivo_entrada = 'caldera-raw.txt'  # El archivo de entrada extraido de Caldera
archivo_salida = 'techniques-caldera.txt'  # El archivo de salida con las técnicas extraídas

# Extraer los valores del archivo de entrada
valores = extraer_valores(archivo_entrada)

if not valores:
    print("No se encontraron técnicas.")
else:
    # Guardar los valores extraídos en el archivo 'techniques-caldera.txt'
    guardar_valores(valores, archivo_salida)
```

Tabla 17. *Script "P4-map-controls-to-caldera.py".*

```
import pandas as pd
import re

# Leer los valores de los technique_id desde el archivo .txt usando expresiones regulares
with open('techniques-caldera.txt', 'r', encoding='utf-8') as file:
    # Leer cada línea del archivo y eliminar los saltos de línea
    technique_ids = [line.strip() for line in file]

# Leer el archivo Excel 'mapping_auto.xlsx', hoja 'Tabla3'
mapping_df = pd.read_excel('mapping-auto.xlsx', sheet_name='Tabla3')

# Crear un diccionario para mapear 'iso_id' a 'technique_id'
iso_to_techniques = {}

# Iterar sobre las filas de 'mapping_df' para realizar el mapeo
for _, row in mapping_df.iterrows():
    target_id = row['target_id']
    iso_values = str(row['iso_id']).split(',')  # Los valores de 'iso_id' pueden estar
separados por comas
    iso_values = [test.strip() for iso_id in iso_values]  # Limpiar espacios alrededor de cada
valor de 'iso_id'

    if target_id in technique_ids:
```

```
        for iso_id in iso_values:
            if iso_id not in iso_to_techniques:
                iso_to_techniques[iso_id] = []
            if target_id not in iso_to_techniques[iso_id]:
                iso_to_techniques[iso_id].append(target_id)

# Eliminar duplicados en las listas de 'target_id' y 'iso_id'
for iso_id in iso_to_techniques:
    iso_to_techniques[iso_id] = list(set(iso_to_techniques[iso_id]))  # Eliminar duplicados de
'target_id'

# Crear un DataFrame con los resultados
output_data = []
for iso_id, technique_ids in iso_to_techniques.items():
    output_data.append([iso_id, ', '.join(technique_ids)])  # Unir los 'technique_id' con coma
en la misma celda

output_df = pd.DataFrame(output_data, columns=['iso_id', 'technique_id'])

# Guardar el DataFrame en un nuevo archivo Excel
output_df.to_excel('iso-27001-to-caldera.xlsx', index=False)

print("El archivo 'iso-27001-to-caldera.xlsx' ha sido generado exitosamente.")
```

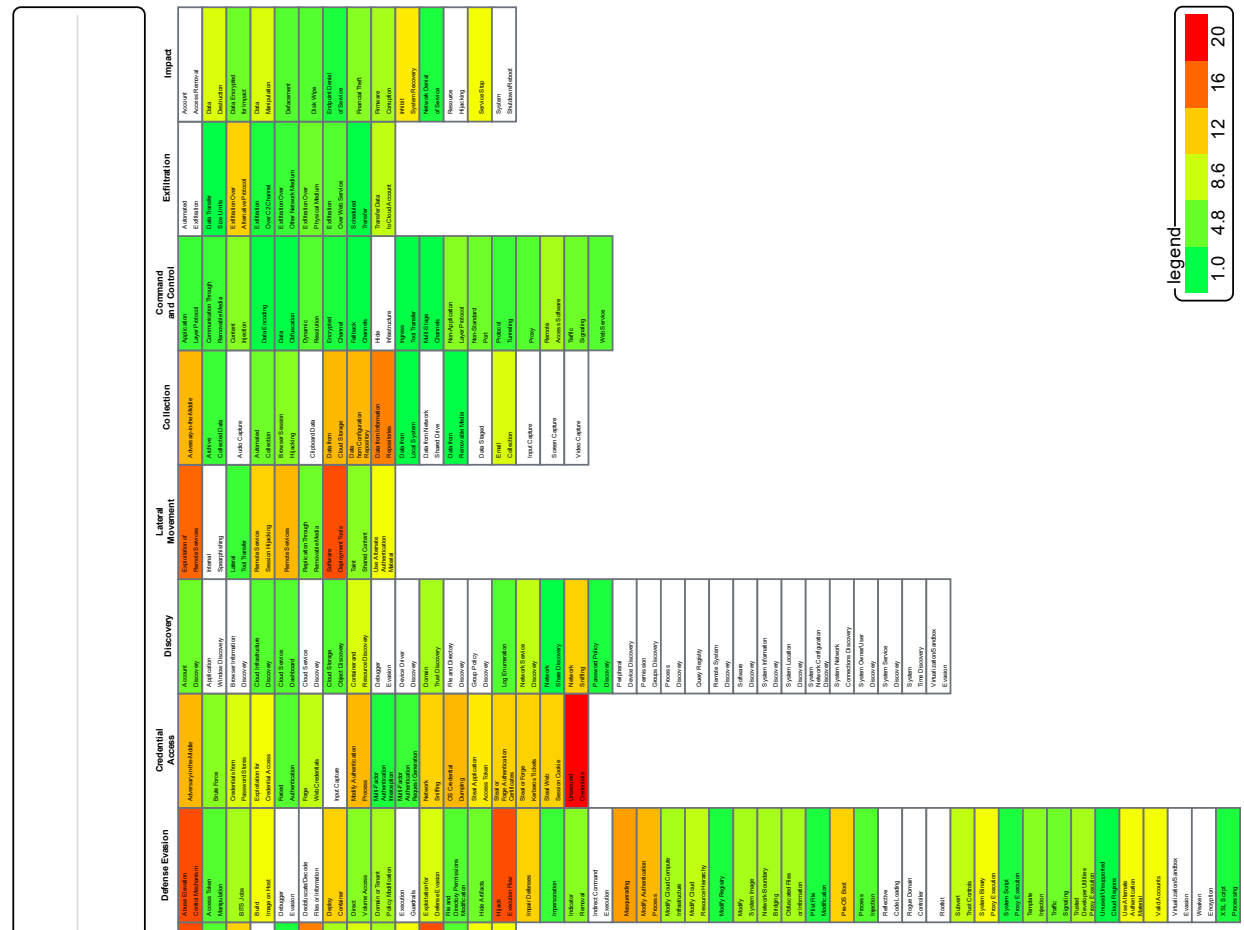
Tabla 18. *Script "P5-get-adversaries-caldera.py".*

```
import os
import pandas as pd
import json

def generar_archivos_json(archivo_excel):
    # Leer el archivo Excel
    df = pd.read_excel(archivo_excel, dtype={"iso_id":str})

    # Crear la carpeta "resultados" si no existe
    carpeta_resultados = "resultados"
    if not os.path.exists(carpeta_resultados):
        os.makedirs(carpeta_resultados)

    # Iterar sobre las filas del DataFrame
    for _, fila in df.iterrows():
        # Obtener el valor de la celda "iso_id"
        valor_iso = str(fila["iso_id"]).replace(".", "-")
        # Crear el nombre del archivo JSON
        nombre_archivo = f"ISO-27001-CONTROL-{valor_iso}.json"
        ruta_archivo = os.path.join(carpeta_resultados, nombre_archivo)

        # Crear el encabezado del archivo JSON
        encabezado = {
            "name": f"ISO-27001-CONTROL-{valor_iso}",
            "versions": {
                "attack": "16",
                "navigator": "5.1.0",
                "layer": "4.5"
```

```
            },
            "domain": "enterprise-attack",
            "description": "",
            "filters": {
                "platforms": [
                    "Windows",
                    "Linux",
                    "macOS",
                    "Network",
                    "PRE",
                    "Containers",
                    "IaaS",
                    "SaaS",
                    "Office Suite",
                    "Identity Provider"
                ]
            },
            "sorting": 0,
            "layout": {
                "layout": "side",
                "aggregateFunction": "average",
                "showID": False,
                "showName": True,
                "showAggregateScores": False,
                "countUnscored": False,
                "expandedSubtechniques": "none"
            },
            "hideDisabled": False,
            "techniques": []
        }

        # Obtener los valores de "technique_id" asociados al valor de "iso_id"
        technique_ids = fila["technique_id"].split(",") if pd.notna(fila["technique_id"]) else
[]

        for technique_id in technique_ids:
            entrada = {
                "techniqueID": technique_id.strip(),
                "tactic": "",
                "score": 1,
                "color": "",
                "comment": "",
                "enabled": True,
                "metadata": [],
                "links": [],
                "showSubtechniques": False
            }
            encabezado["techniques"].append(entrada)

        # Agregar el pie al archivo JSON
        pie = {
            "gradient": {
                "colors": [
                    "#00ff45ff",
                    "#feff00ff",
                    "#ff0000ff"
                ],
```

```
                "minValue": 1,
                "maxValue": 20  # Valores máximo y mínimo generados en el código P4
            },
            "legendItems": [],
            "metadata": [],
            "links": [],
            "showTacticRowBackground": False,
            "tacticRowBackground": "#dddddd",
            "selectTechniquesAcrossTactics": True,
            "selectSubtechniquesWithParent": False,
            "selectVisibleTechniques": False
        }

        # Combinar encabezado, técnicas y pie
        contenido_json = {**encabezado, **pie}

        # Escribir el archivo JSON
        with open(ruta_archivo, "w", encoding="utf-8") as archivo:
            json.dump(contenido_json, archivo, indent=4)

    print(f"Archivos JSON generados en la carpeta '{carpeta_resultados}'.")

# Ruta al archivo Excel
archivo_excel = "iso-27001-to-caldera.xlsx"

# Llamar a la función
generar_archivos_json(archivo_excel)
```

Anexo C. Mapa de calor técnicas ATT&CK a controles ISO 27001



Anexo D. Ficha de planificación de pruebas

Tabla 19. *Ficha de planificación de pruebas elaborada.*

FICHA DE PLANIFICACION DE PRUEBAS				
1. Asignación de roles				
Líder técnico	**Administrador de infraestructura TI**	**Auditor interno de cumplimiento**	**Evaluador de seguridad ofensiva**	**Asistente técnico**
Diego Uchofen	Asignado	Asignado	Diego Uchofen	Asignado
2. Activos a evaluar				
Hostname	**Modelo**	**IP**	**Encargado**	**Área**
DESKTOP-MIA74KJ	HP ProDesk 400 G4	172.16.100.46	Administrador de sistemas	Soporte
3. Controles ISO 27001:2022 a evaluar				
ISO CONTROL 8.20, ISO CONTROL 8.7				
4. Herramientas de seguridad				
Nombre	**Tipo**	**Modelo**	**IP**	
FW-PRI-PALOALTO	Firewall	PA-410	14.14.14.2	
SOPHOS ENDPOINT	EDR	CLOUD	NO APLICA	
5. Cronograma de evaluación				
Periodicidad	Diario	Semanal	Mensual	Trimestral
			X	
Consideraciones	Se realizarán el 09 de cada mes			

Anexo E. Proceso de creación del contenedor BAS personalizado con los controles ISO 27001 agregados

A continuación, se describen los pasos realizados para crear la imagen Docker de la herramienta BAS, la cual contiene importado los controles ISO 27001 mapeados a técnicas ATT&CK de acuerdo al desarrollo del presente trabajo.

1. Habiendo realizado la importación de los controles ISO 27001 en el contenedor Caldera creado, se procede a detener el contenedor y generar la nueva imagen Docker, como se observa en la Figura 69.
    a. Comandos a ejecutar: docker stop <docker_id> ; docker commit <docker_id> <nuevo_nombre>

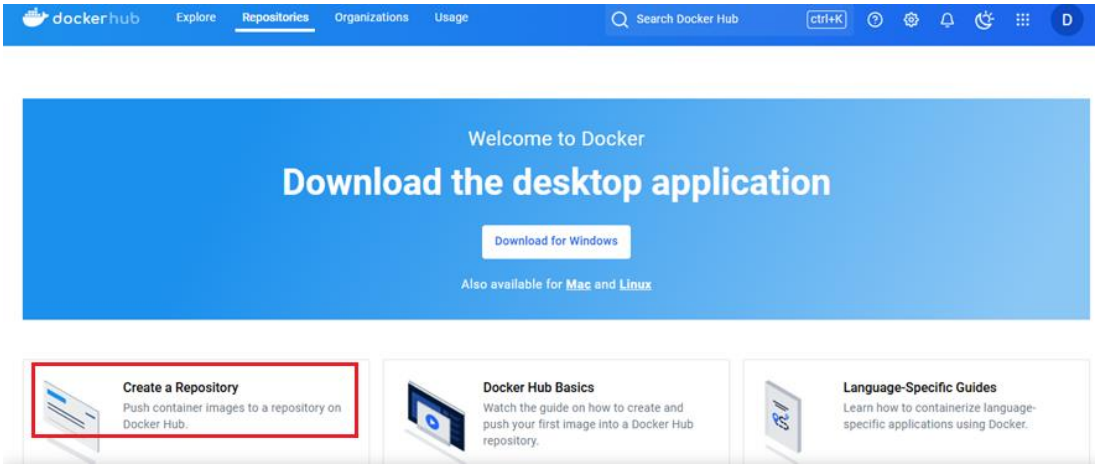
Figura 69. *Construcción de nueva imagen del contenedor BAS Caldera.*

```
root@caldera:/home/caldera# docker commit 42a3bc1ed7dc caldera-iso-controls
sha256:33d2c9bce1174d9d5f760953a4366b5ac958f622a918970a055820370c091b25
root@caldera:/home/caldera# docker images
REPOSITORY            TAG       IMAGE ID       CREATED          SIZE
caldera-iso-controls  latest    33d2c9bce117   10 seconds ago   2.26GB
caldera               server    675f46fd9e88   3 days ago       2.18GB
root@caldera:/home/caldera#
```

Fuente: Elaboración propia.

2. Se crea un repositorio en Dockerhub (https://hub.docker.com/), tal como se observa en la Figura 70:

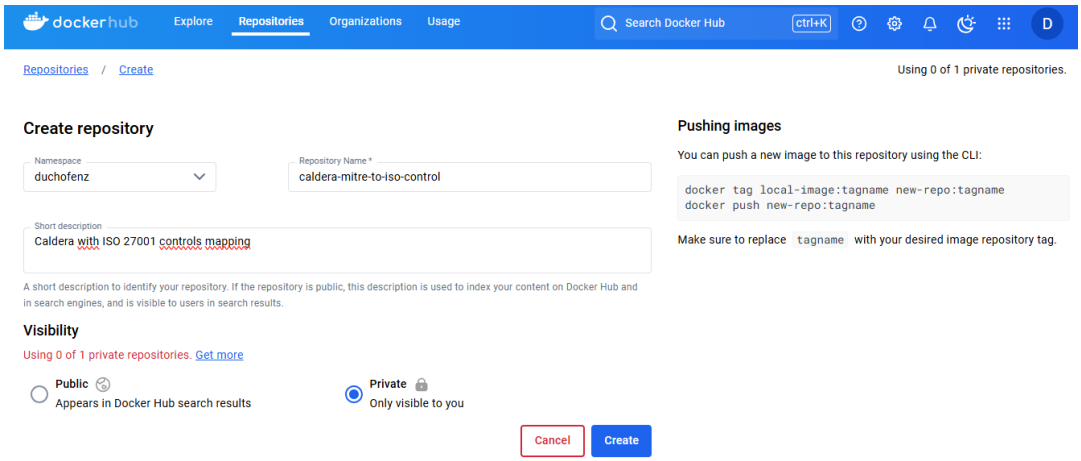
Figura 70. *Creación de repositorio en Docker Hub.*



Fuente: Elaboración propia.

3. Se configuran las opciones del nuevo repositorio, así como se observa en la Figura 71 y se da clic en “Create”:
    a. Namespace: Nombre de usuario asociado.
    b. Repositorio Name: Nombre del repositorio, en este caso es: “caldera-mitre-to-iso-control”
    c. Visibility: Private (Only visible to you). Esto hace que el repositorio no sea de uso público.

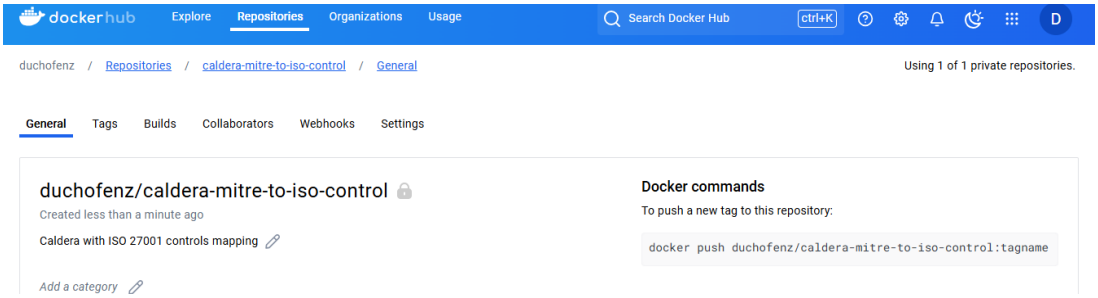
Figura 71. *Creación de repositorio en Docker Hub.*



Fuente: Elaboración propia.

4. Se valida la creación del repositorio exitosamente como se muestra en el Figura 72:

Figura 72. *Validación de creación repositorio en Docker Hub.*



Fuente: Elaboración propia.

5. A la nueva imagen creada se le asigna el nombre del repositorio y tag asociado (en este caso es “duchofenz/caldera-mitre-to-iso-control:latest”):
    a. Comando a ejecutar: docker tag <nombre-imagen-actual>:<nombre-tag> <repositorio>:<nombre-tag>, mostrado en la Figura 73.

Figura 73. *Cambio de nombre y tag asociado.*

Fuente: Elaboración propia.

6. Se procede con el login a Dockerhub desde el servidor que contiene Caldera, como se muestra en la Figura 74, para importar la nueva imagen creada:
    a. Comando a ejecutar: docker login -u <usuario> -p <contraseña> docker.io

Figura 74. *Login en DockerHub desde el servidor*

Fuente: Elaboración propia.

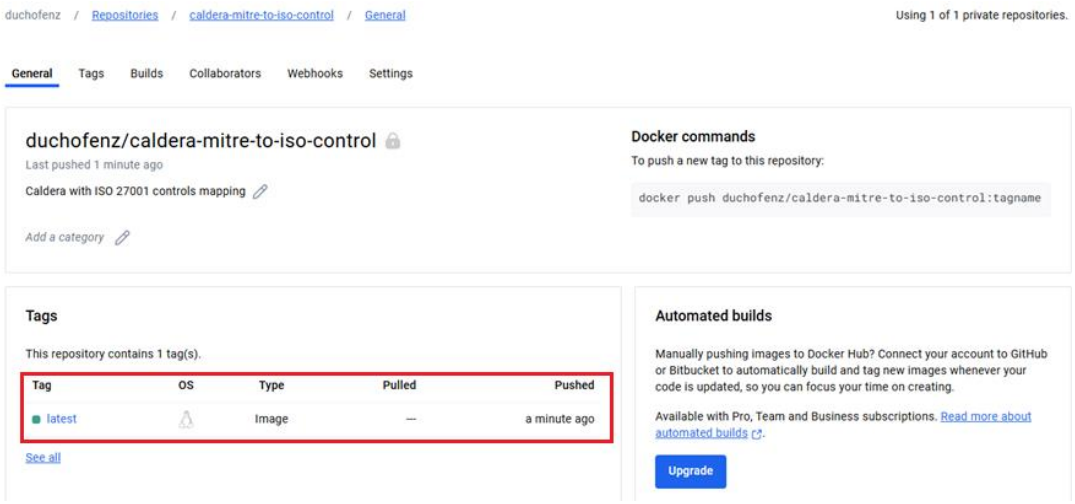
7. Se importa el archivo docker al repositorio en Dockerhub, tal como se observa en la Figura 75:
    a. Comando a ejecutar: docker push <repositorio>:<nombre_tag>

Figura 75. *Ejecución del contenedor BAS*

Fuente: Elaboración propia.

8. Validar que aparezca en el repositorio como en la Figura 76: Ingresar a la web de DockerHub y validar que el nuevo contenedor haya sido importado satisfactoriamente.

Figura 76. *Validación importación de nuevo archivo BAS Caldera*

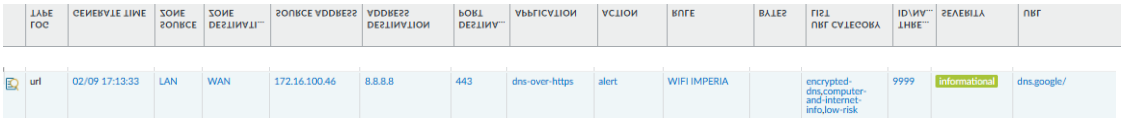


Fuente: Elaboración propia.

Anexo F. Resultados en herramientas de seguridad

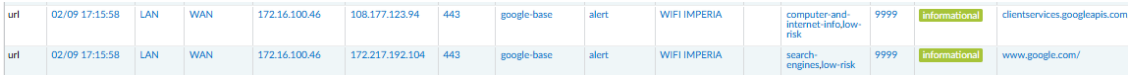
Para el control ISO 27001 8.20:

- DNS over HTTPS Large Query Volume: Alertado.



- Exfiltration Over Alternative Protocol – HTTP: Alertado.

- Running Chrome VPN Extensions via the Registry 2 vpn extension: Alertado.



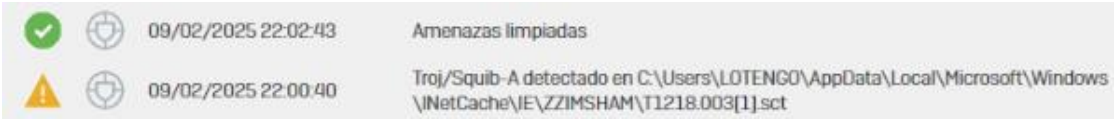
- Network Service Scanning: No detectado. El escaneo abarca el firewall, ejecuta un archivo ps1.
- Port-Scanning /24 Subnet with PowerShell: No detectado. El tráfico es dentro de la misma red por lo que no llega al firewall, además se trata de un conjunto de comandos ejecutados en Powershell.
- Testing usage of uncommonly used port with PowerShell: Alertado.

- Sniff network traffic: No detectado,
- Windows Internal pktmon set filter: No detectado.
- Windows Internal Packet Capture: No detectado.
- Exfiltrate data HTTPS using curl windows: Alertado.

SOURCE ZONE	DESTINATI... ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	DESTINA... PORT	APPLICATION	ACTION	RULE	BYTES	URL CATEGORY LIST	THRE... ID/NA...	SEVERITY	URL
LAN	WAN	172.16.100.46	104.21.66.52	443	ssl	alert	WIFI IMPERIA		online-storage-and-backup,medium-risk	9999	informational	file.io/

Para el control ISO 27001 8.7:

- CMSTP Executing Remote Scriptlet: Bloqueado.

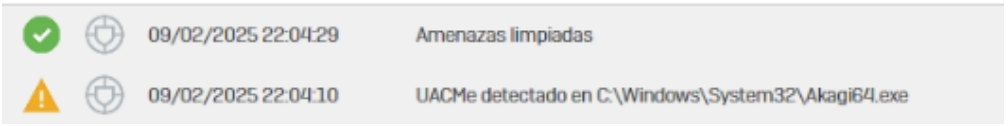


- JScript execution to gather local computer information via cscript: No detectado
- Lolbin Jsc.exe compile javascript to dll: No detectado.
- WinPwn-fruit: Bloqueado.

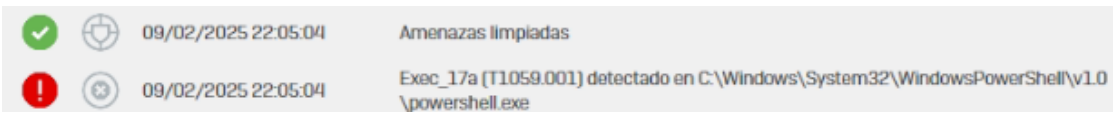
SOURCE ZONE	DESTINATI... ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	DESTINA... PORT	APPLI...	ACTIO...	RULE	BYTES	URL CATEGORY LIST	THRE... ID/NA...	SEVERITY	URL
LAN	WAN	172.16.100.46	185.199.111.133	443	ssl	alert	WIFI IMPERIA		shareware-and-freeware,low-risk	9999	informational	raw.githubusercontent.com/

- WinPwn-spoolvulnscan: Bloqueado.

- Wow64log DLL Hijack: Bloqueado.



- WinPwn – UAC Bypass DiskCleanup technique: Bloqueado.



- Disable ConsentPromptBehaviourAdmin via registry keys: No detectado.
- Bypass UAC using sdclt DelegateExecute: No detectado.
- WinPwn - UAC Bypass ccmstp technique: Bloqueado.

- Disable UAC notification via registry keys: No detectado.
- Disable UAC using reg.exe: No detectado.
- WinPwn - UAC Magic: Bloqueado.

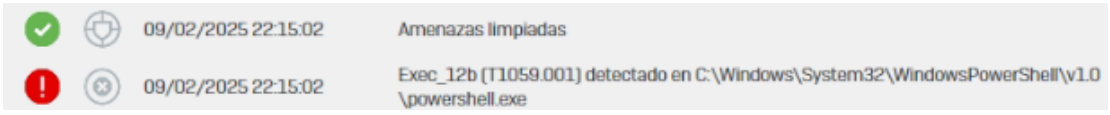
- Bypass UAC by Mocking Trusted Directories: No detectado.
- WinPwn - UAC Bypass DccwBypassUAC technique: Bloqueado.

- Bypass UAC using Event Viewer (PowerShell): Bloqueado.

- Launches an executable using Rundll32 and pcwutl.dll: No detectado.
- PowerShell bitly Link Download: Alertado.

SOURCE ZONE	DESTINATI... ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	DESTINA... PORT	APPLI...	ACTIO...	RULE	BYTES	URL CATEGORY LIST	THRE... ID/NA...	SEVERITY	URL
LAN	WAN	172.16.100.46	67.199.248.10	443	ssl	alert	WIFI IMPERIA		computer-and-internet-info,low-risk	9999	informational	bit.ly/

- PowerShell Fileless Script Execution: Bloqueado.



- Potentially Unwanted Applications (PUA): Bloqueado.

- File Extension Masquerading: No detectado, pero la política de Powershell impidió su ejecución.
- UAC bypass registry: No detectado.