Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad | 3 | “Proyecto Final: Plan de Acción”

Seguridad Informática I

Ingeniería en Desarrollo de Software

academiaglobal

TUTOR: Jessica Hernández Romero tutor.etica@umi.edu.mx

ALUMNA: Sarahi Jaqueline Gómez Juárez.

FECHA: lunes, 15 de agosto de 2025.

Índice:

Introducción:

El presente proyecto constituye la **Etapa 3 del Plan de Acción en Seguridad Informática**, desarrollado con el propósito de fortalecer la protección de los activos tecnológicos, usuarios y procesos críticos, en esta fase, el énfasis se centra en la **implementación práctica de dichas recomendaciones**, garantizando un enfoque integral que abarque dimensiones humanas, lógicas, físicas, de almacenamiento y de comunicación, en esta fase, el énfasis se centra en la **implementación práctica de dichas recomendaciones**, garantizando un enfoque integral que abarque dimensiones humanas, lógicas, físicas, de almacenamiento y de comunicación.

Este proyecto busca garantizar la **disponibilidad, integridad y confidencialidad de la información** institucional, fortaleciendo la confianza en las operaciones diarias del Instituto Veracruzano y promoviendo una cultura de ciberseguridad que prepare a la comunidad para enfrentar con eficacia los retos de un mundo digital en constante transformación,

El desarrollo inicia con la **selección de herramientas tecnológicas** que resultan idóneas por su costo, compatibilidad y funcionalidad, entre ellas destacan PhishTool para capacitación contra phishing, BitLocker para cifrado de discos, Google Drive para gestión de accesos en la nube, Malwarebytes para detección de malware, Nessus Essentials como escáner de vulnerabilidades, y Snort IDS para monitoreo de red, entre otras, estas soluciones fueron seleccionadas no solo por su accesibilidad, sino porque resuelven de manera directa la mayoría de los factores de riesgo diagnosticados, cubriendo así la brecha entre teoría y práctica.

Posteriormente, se establece un **plan de acción estructurado** es un documento estratégico que organiza, de manera estructurada y secuencial, las medidas preventivas y

correctivas necesarias para **proteger los sistemas, datos y recursos tecnológicos** de una institución u organización, su finalidad es reducir riesgos y mitigar vulnerabilidades mediante actividades definidas, responsables asignados, herramientas tecnológicas y un cronograma de ejecución.

Este plan integra acciones de **capacitación, políticas de acceso, uso de software de protección, monitoreo de red, respaldo de información y protocolos de contingencia**, garantizando así la **confidencialidad, integridad y disponibilidad** de la información, en otras palabras, es la guía práctica que transforma el diagnóstico de riesgos en soluciones aplicables y medibles, asegurando la continuidad operativa y la resiliencia frente a amenazas internas o externas.

Dentro de este plan de acción se divide en responsables, apoyos y herramientas para cada actividad, desde la capacitación del personal en ingeniería social, hasta la implementación de protocolos de respaldo bajo la estrategia 3-2-1, pasando por la configuración de roles de acceso, segmentación de red, monitoreo de energía y establecimiento de planes de contingencia como el uso de hotspot móvil, así mismo se implementa un cronograma, porque la claridad del cronograma asegura la organización temporal de las medidas, evitando improvisaciones y garantizando que cada área cumpla su papel en la seguridad institucional, durante esta tercera fase, se exploraron diversas herramientas y estrategias para resolver las incidencias detectadas en la fase 1 de nuestro proyecto, las herramientas y soluciones sean seleccionado con especial cuada para que aquellas que mejor se adapten a las necesidades específicas de nuestra institución sean implementadas, además, el cronograma que se a establecido se ha detallado para que que indique ¿cuándo? y ¿cómo se llevarán a cabo las diferentes acciones planificadas?, asegurando así una implementación eficiente y oportuna.

A lo largo de este proceso, nos hemos centrado en la importancia de proteger la integridad y confidencialidad de la información, así como en garantizar la continuidad de las operaciones académicas y administrativas.

Asimismo, se incorpora la **práctica del plan de acción**, ejemplificada mediante capturas de pantalla que documentan el uso real de algunas de las herramientas seleccionadas, estas evidencias muestran cómo las soluciones propuestas no se quedan en el plano teórico, sino que se aplican en entornos concretos: respaldos en Google Drive, análisis con Malwarebytes, monitoreo con BatteryCare, entre otros, con ello se refuerza la validez de la propuesta al demostrar su funcionalidad operativa.

Finalmente, la **evaluación** confirma que la elección de cada herramienta fue adecuada para responder a amenazas específicas, ya sean ataques de phishing, intrusiones no autorizadas, malware, desastres físicos o fallas de comunicación, el proyecto, en su conjunto, refleja la importancia de integrar medidas preventivas, controles técnicos y protocolos organizacionales para alcanzar los tres pilares fundamentales de la seguridad informática: **disponibilidad, integridad y confidencialidad**, constituyendo un modelo práctico y fácilmente replicable que puede aplicarse en cualquier organización educativa o administrativa, su enfoque integral permite anticiparse a los riesgos, optimizar recursos y consolidar una **cultura institucional de ciberseguridad**, indispensable en un mundo digital cada vez más vulnerable y complejo.

Descripción:

El presente proyecto es un plan de acción en seguridad informática, tiene como finalidad fortalecer la protección de los activos tecnológicos, usuarios y procesos críticos del Instituto Veracruzano, a través de una metodología organizada en siete pasos, se busca garantizar la disponibilidad, integridad y confidencialidad de la información institucional, estableciendo lineamientos claros y medidas preventivas frente a amenazas humanas, lógicas, físicas, de almacenamiento y comunicación.

Cada fase está diseñada para dar respuesta a vulnerabilidades específicas: desde el levantamiento de información inicial, la identificación y clasificación de riesgos, hasta la selección de herramientas tecnológicas, la preparación y la implementación de controles de seguridad, de esta manera, se promueve un entorno seguro y confiable para la comunidad académica y administrativa, optimizando recursos y asegurando el cumplimiento de normativas vigentes.

El plan involucra a diversas áreas como Sistemas, Recursos Humanos, Seguridad Física, Jurídico y Dirección Administrativa, quienes de manera conjunta contribuyen a mitigar riesgos y establecer una cultura de ciberseguridad, con ello, no solo se protegen los recursos tecnológicos de la institución, sino que también se refuerza la confianza en sus operaciones diarias.

El **paso uno** será el **Diagnóstico Inicial**, donde se realiza un levantamiento de información sobre los activos tecnológicos, usuarios y procesos críticos, elaborando un inventario de equipos, redes y aplicaciones utilizadas en la institución, el responsable directo es el Administrador de Sistemas y como su apoyo directo es el Analista de Ciberseguridad, la amenaza que resuelve es el desconocimiento del entorno y falta de control sobre los recursos

tecnológicos.

El **segundo paso** es la identificación de riesgos, detectar amenazas humanas, lógicas, físicas, de almacenamiento y comunicación en el entorno, construir una matriz de riesgos para cada factor identificado, el responsable directo es el Analista de Ciberseguridad,y como su apoyo directo es RRHH y el Encargado de Seguridad Física, su principal objetivo es resolver la falta de visibilidad de vulnerabilidades y posibles incidentes.

El **tercer paso** es la clasificación y priorización, asignando niveles de probabilidad e impacto a cada riesgo detectado, clasificando riesgos en críticos, altos, medios y bajos, el responsable principal es el Coordinador de TI y su apoyo directo es la Dirección Administrativa, resolviendo la priorización incorrecta que llevaría a invertir recursos en amenazas menores.

El **cuarto paso** es la definición de políticas de seguridad, redactar lineamientos para el uso de contraseñas, accesos físicos y digitales, es sumamente vital para la seguridad del Instituto Veracruzano por lo que establecer protocolos para manejo de información sensible, el responsable directo es el Dirección de TI y para el apoyo del mismo es el Analista de Ciberseguridad mas el Jurídico, resolviendo el uso inadecuado de sistemas e incumplimiento de normas.

El **quinto paso** es la selección de herramientas tecnológicas evaluar soluciones disponibles y elegir las más adecuadas según costo, eficacia y compatibilidad es parte de lo que trata este documento por lo que gracias a sus características se ha seleccionado: PhishTool, BitLocker, Google Drive, Malwarebytes, Nessus, Snort IDS, Acronis Backup, BatteryCare, Google Home, Hotspot móvil y Google Keep, el responsable directo es el especialista en Seguridad y apoyo es el Administrador de Sistemas más Responsable de Compras físicas y tecnológicas que por lo usual es el administrador del instituto Veracruzano o el contador, la

amenaza que resuelve es el uso de software no confiable y ausencia de herramientas preventivas.

El **sexto paso** es la identificación y preparación, realizar diagnóstico de riesgos y vulnerabilidades como lo son el:

Detectar amenazas humanas, lógicas, físicas, de almacenamiento y de comunicación.

Documentar cada riesgo en una matriz con responsable, herramienta y solución.

Capacitar al personal contra phishing.

Uso de PhishTool para entrenar y concientizar el responsable es el Analista de Ciberseguridad más RRHH.

Adquirir licencias oficiales de software y seguridad, usar un antivirus empresarial, firewall, herramientas de respaldo y monitoreo, el encargado es el Especialista en Seguridad y su apoyo directo son Responsable de Compras y el Administrador de Sistemas.

Establecer políticas de acceso físico y digital por lo que se instalan controles de acceso biométrico, cámaras y registros digitales, cifrando discos duros con BitLocker.

Definir protocolos de respaldo y recuperación, aplicando estrategias 3-2-1 (copias locales, externas y en la nube), realizando una verificación de la restauración mensual con Acronis Backup y Google Drive.

Configurar segmentación de red y medidas de comunicación, creando VLANs por áreas, por lo que se habilita el firewall y monitoreo con Snort IDS y se establece una red de invitados y rotación de claves Wi-Fi.

El **séptimo paso** es la implementación del plan de acción, por lo que es fundamental la capacitación contra phishing e ingeniería social, mediante el uso de PhishTool para entrenar y concientizar, el responsable directo es el Analista de Ciberseguridad y apoyo: RRHH, disminuyendo las probabilidades de Amenazas Humanas en especial por el personal de la

universidad algunas de **sus principales acciones a realizar son**:

La protección de datos locales en equipos institucionales, cifrando los discos duros con BitLocker, responsable directo es el Administrador de Sistemas y apoyo el Especialista en Seguridad, disminuyendo las Amenazas Físicas.

Gestión de accesos y trazabilidad en la nube, usando Google Drive con roles, permisos e historial, el responsable principal es el Administrador de Red, apoyo: Encargado de Compras/Soporte, resolviendo la vulnerabilidad de almacenamiento.

Escaneo y eliminación de amenazas ocultas, usando Malwarebytes Free, su responsable directo es el Técnico de Soporte TI y su apoyo: Administrador de Red, la amenaza que resuelve: Amenazas Lógicas.

Evaluación de vulnerabilidades en software y configuraciones, escaneado con Nessus Essentials, con el Auditor de Seguridad TI, responsable encargado y su apoyo el Administrador de Sistemas, la amenaza que resuelve: Vulnerabilidades Lógicas y de Almacenamiento.

Monitoreo de tráfico de red y ataques externos, usando Snort IDS con Firewall Windows, su responsable principal es el Administrador de Red y su apoyo: Analista de Seguridad, la amenaza que resuelve: Vulnerabilidades de Comunicación.

Respaldos bajo estrategia 3-2-1, usando Acronis Backup con Google Drive, su responsable: Administrador de Sistemas y su apoyo: Encargado de Compras, la vulnerabilidad que resuelve es la falta de almacenamiento.

Prevención de pérdida de datos por fallas eléctricas o batería, monitoreada con BatteryCare, el responsable es el Técnico de Soporte TI y su apoyo el Administrador de Red, la amenaza que resuelve: Amenazas Físicas.

Monitoreo ambiental y accesos físicos, usando Google Home más Sensores, su

responsable encargado es el Encargado de Seguridad Física, con el apoyo de protección Civil, la amenaza que resuelve: Amenazas Físicas.

Segmentación de red y seguridad Wi-Fi, configuración de VLANs, SSID invitados y claves WPA3 en router, el responsable: Administrador de Red y su apoyo: Técnico de Soporte TI, la vulnerabilidad que resuelve es la falta de comunicación.

Plan de contingencia de conexión a Internet, usando un Hotspot móvil (Android), su responsable es Administrador de Sistemas y su apoyo: Dirección/Usuarios clave, la vulnerabilidad que resuelve los problemas de comunicación, porque se caiga la línea de internet.

Es sumamente importante llevar y tener una documentación y protocolos preventivos ordenados, usando Google Keep (Checklist), su responsable es el Analista de Datos y el Coordinador TI, con apoyo de todo el personal, resolviendo la falta organizacional que es una amenaza para nuestro proyecto.

Justificación:

El objetivo es porque la necesidad creciente de proteger la información y los recursos tecnológicos frente a amenazas que comprometen la continuidad de las operaciones y la confianza institucional, dentro de en un entorno académico y administrativo como el del Instituto Veracruzano, la seguridad digital no puede considerarse un lujo, sino una obligación indispensable para garantizar la disponibilidad, integridad y confidencialidad de los datos.

La adopción de medidas preventivas y correctivas que vienen ejemplificadas dentro de este proyecto proporciona una capa adicional de seguridad, lo que resulta vital en un panorama donde la ciberdelincuencia es una amenaza constante, al emplear este tipo de solución, la universidad puede fortalecer sus defensas cibernéticas y proteger sus activos de información crítica, incluidos los datos estudiantiles, académicos y administrativos, este proyecto responde a la importancia de transformar la identificación de riesgos en medidas concretas, organizadas y aplicables, que permitan anticiparse a los incidentes en lugar de reaccionar únicamente cuando estos ocurren, la implementación de herramientas como **PhishTool, BitLocker, Google Drive, Malwarebytes, Nessus, Snort IDS y Acronis Backup** asegura que cada vulnerabilidad detectada sea tratada con una solución específica y efectiva, reforzando la protección tanto en el ámbito lógico como físico y organizacional, la implementación de un plan de acción específico permite no solo mitigar los riesgos asociados con posibles ataques cibernéticos, sino también garantizar la continuidad de las operaciones académicas y administrativas de la universidad.

La ciberseguridad no solo protege la infraestructura tecnológica, sino que también contribuye a mantener la **credibilidad institucional y la confianza de los usuarios**, la pérdida de datos, la fuga de información o una intrusión no autorizada pueden afectar de manera crítica

la reputación y la estabilidad de cualquier organización, por ello, contar con protocolos claros, cronogramas definidos y responsables asignados permite optimizar los recursos disponibles y minimizar los riesgos de forma integral, la aplicación de un plan de acción bien diseñado y ejecutado demuestra el compromiso de la institución con la seguridad informática y la protección de la privacidad de sus miembros, esto no solo preserva la reputación de la universidad, sino que también fomenta la confianza entre los estudiantes, profesores y personal administrativo, creando un entorno educativo más seguro y protegido para todos los involucrados, este tipo de solución es esencial para salvaguardar la universidad contra las crecientes amenazas cibernéticas y garantizar su funcionamiento continuo en el mundo digital actual.

Es decir este es una estrategia para que la institución, mediante ha ella, esta es sólida para enfrentar los desafíos de un mundo digital en constante evolución, con ello, se garantiza no solo la protección de los activos tecnológicos, sino también la formación de una cultura de seguridad informática entre todos los miembros de la comunidad educativa.

Desarrollo:

Proyecto Final - Etapa 3 - Plan de Acción

Contextualización: Después de identificar los factores de riesgo en la actividad 1 y realizar las recomendaciones en la actividad 2 ahora es importante que aplicar estos conocimientos demostrando cómo resolver esos eventos, es importante también revisar los videos del contenido de la materia y navegar entre las herramientas de seguridad para encontrar la que se adecue a resolver la mayoría de las amenazas y vulnerabilidades.

Actividad: Con base a las Actividades 1 y 2 diseñar y establecer un plan de acción en donde se indiquen los pasos a seguir para implementar las recomendaciones implicadas en la actividad 2.

En este sentido, dicho análisis deberá dar solución a la mayoría de las incidencias y amenazas encontradas en ambas actividades.

Selección de software:

Se eligen las herramientas tecnológicas más adecuadas según las **necesidades, requisitos y presupuesto**, involucrando el identificar lo que se busca, comparar opciones, evaluar funciones y costos, hacer pruebas y finalmente decidir la solución más rentable y compatible por lo cual se han escogido las siguientes herramientas y plataformas para desarrollar nuestro plan de acción:

Figura 1

PhishTool:

Nota: La siguiente imagen muestra la plataforma de inicio de PhisTool, este se integra en nuestro flujo de trabajo existente, sin interrupciones ni configuraciones complejas, ya que los correos electrónicos de phishing denunciados llegan a la consola de PhishTool, donde se analizan, enriquecen y presentan automáticamente para una investigación estructurada, de la bandeja de entrada a la información en segundos.

Extrae correos electrónicos reportados desde cualquier lugar: clientes, buzones de correo

de reporteros, SIEM o integraciones de API ayudando a la ingesta de correo electrónico: que es el **proceso de capturar, recibir y almacenar correos electrónicos** dentro de un sistema o aplicación para su posterior **procesamiento, análisis o archivado**.

Otra de sus principales características es la decodificación de encabezados, enlaces, archivos adjuntos y metadatos, sin trabajo manual, es decir el análisis automatizado que **examinar datos, documentos o eventos mediante software o algoritmos**, sin necesidad de intervención humana constante, su objetivo es **ahorrar tiempo, reducir errores y detectar patrones** que serían difíciles o muy lentos de encontrar manualmente también brinda a los analistas una vista estructurada para investigar cada informe en contexto completo.

Beneficiando a un Informes de resultados que presentan de manera clara y ordenada los **hallazgos, métricas, conclusiones y recomendaciones** obtenidas tras un análisis, proyecto o proceso, cerrando los casos de forma limpia con comentarios estructurados automatizados y/o integraciones posteriores, una herramienta de análisis forense gratuita para que los analistas individuales investiguen los correos electrónicos de phishing denunciados ayudando a cargar y analizar correos electrónicos de phishing, al análisis completo del encabezado y del cuerpo, inspección de enlaces y accesorios a su vez la detección y notas de analistas dentro de su versión gratuita.

Por su arte en la versión de paga sus principales caracteristicas:

Acceso al equipo multiusuario

Colaboración y visibilidad en equipo

Integraciones de API y buzones

Complemento de Outlook (informe a PhishTool)

Comentarios automatizados de los informadores

Alertas personalizadas y webhooks

Inicio de sesión único/SAML 2.0

Los correos electrónicos de phishing son una de las amenazas más reportadas, pero siguen siendo una de las más difíciles de investigar de manera eficiente.

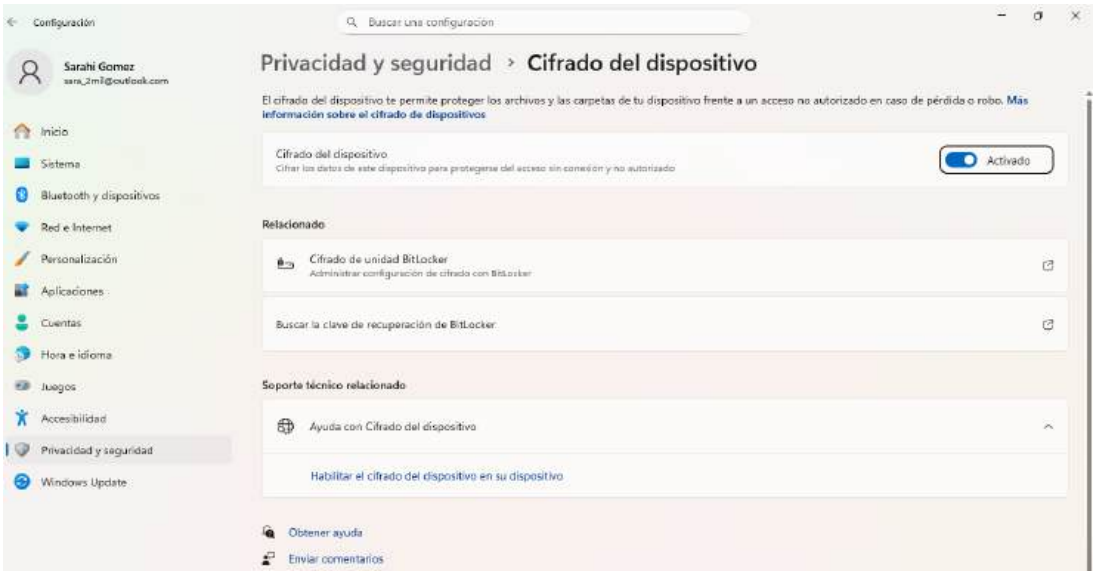
Los analistas pierden horas buscando encabezados, decodificando enlaces y saltando entre herramientas que no fueron creadas para el trabajo.

PhishTool cambia eso, convierte los correos electrónicos sin procesar en investigaciones forenses estructuradas, rápidamente, cada encabezado, enlace y archivo adjunto se analiza y se presenta para la acción, para que su equipo pueda clasificar más rápido, responder de manera más inteligente y cerrar casos con confianza, el enlace para su acceso:

https://www.phishtool.com/

Figura 2

BitLocker:



Nota: La imagen muestra BitLocker que es una herramienta de **cifrado de disco completo** incluida en las versiones profesionales y empresariales de **Windows** (desde Windows

Vista en adelante), su función principal es **proteger la información almacenada en un disco duro o unidad externa** frente a accesos no autorizados, incluso si alguien extrae físicamente el disco del equipo, ayuda al **cifrado completo**: protege todo el contenido de la unidad (archivos, configuraciones, datos temporales) con **algoritmos de cifrado**: usa AES (Advanced Encryption Standard) con claves de 128 o 256 bits, gracias a su **inicio seguro**, antes de arrancar Windows, valida que el sistema no haya sido manipulado, por eso hace una **autenticación** que pede PIN, contraseña o usar el chip **TPM (Trusted Platform Module)** para validar la integridad del arranque.

A continuación se describen algunas de sus principales ventajas y desventajas:

Ventajas:

Seguridad: si un dispositivo es robado, los datos quedan ilegibles sin la clave de recuperación.

Integración nativa: no requiere instalar software adicional.

Administración centralizada: en empresas, se puede gestionar con **Active Directory** o **Microsoft Intune**.

Protección offline: evita que un atacante acceda a los archivos desde otro sistema operativo.

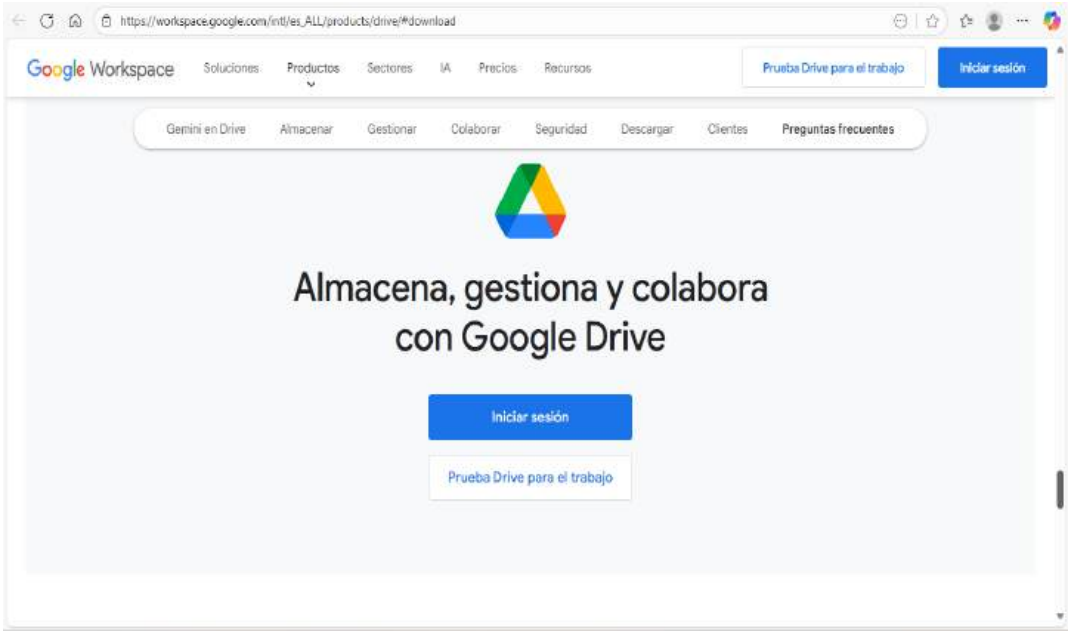
Desventajas:

Solo disponible en **Windows Pro, Enterprise y Education** (no en Home), puede afectar mínimamente el rendimiento (aunque en equipos modernos casi no se nota), si se pierde la clave de recuperación, **los datos no se pueden recuperar**, el enlace para su acceso es:

[Windows 11/10] Encriptación del dispositivo (BitLocker) | Soporte técnico oficial | ASUS México

Figura 3

Google Drive:

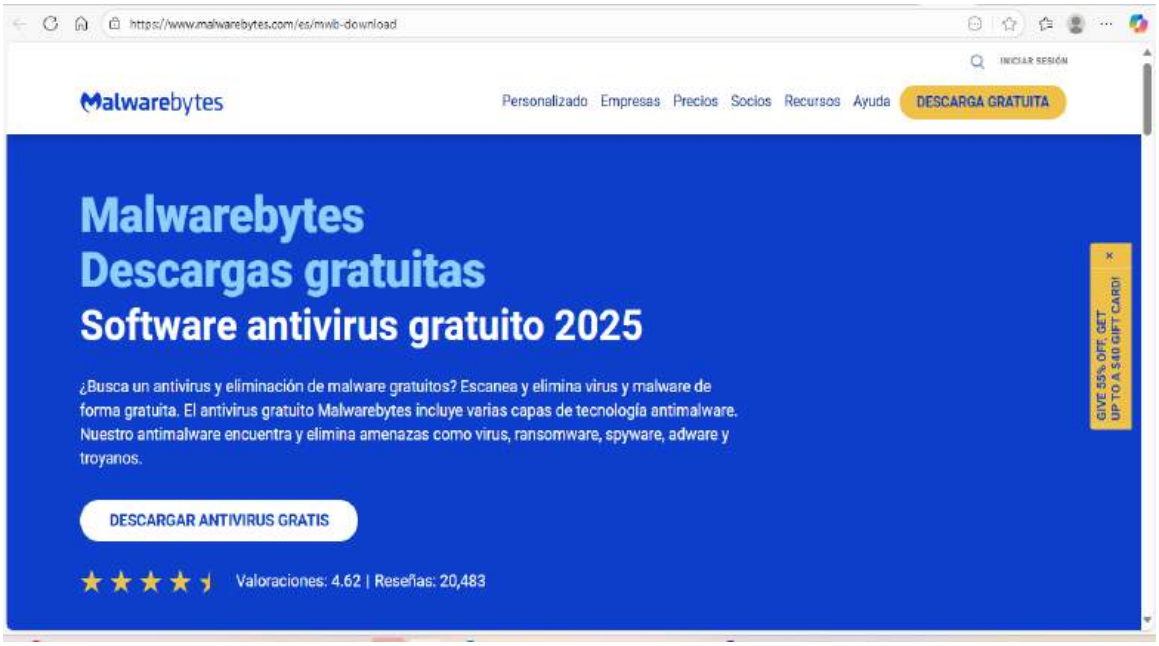


Nota: La imagen muestra una parte del ecosistema de **Google, Google Drive**, es un servicio de **almacenamiento en la nube de Google** que permite **guardar, sincronizar y compartir archivos** desde cualquier dispositivo con internet. Ofrece 15 GB gratis, integración con Google Docs, Sheets y Slides, y facilita la **colaboración en tiempo real** entre varias personas. los **permisos y roles** son la forma en la que decides **quién puede ver, comentar, editar o administrar** tus archivos y carpetas compartidas, esto es clave para mantener el **control y la seguridad** de tu información, el enlace para su acceso es:

https://workspace.google.com/intl/es_ALL/products/drive/#download

Figura 4

Malwarebytes Free:



Nota: **Malwarebytes Free** es un programa de seguridad que detecta y elimina malware, spyware y programas no deseados, funciona solo como **escáner bajo demanda**, es decir, revisa tu equipo cuando tú lo ejecutas, es útil para limpiar una computadora ya infectada o hacer análisis adicionales, no ofrece **protección en tiempo real**, por lo que no bloquea amenazas mientras navegas, la versión completa (Premium) incluye defensa activa contra ransomware, sitios web maliciosos y exploits, el enlace para su acceso es: https://www.malwarebytes.com/es/mwb-download

Figura 5

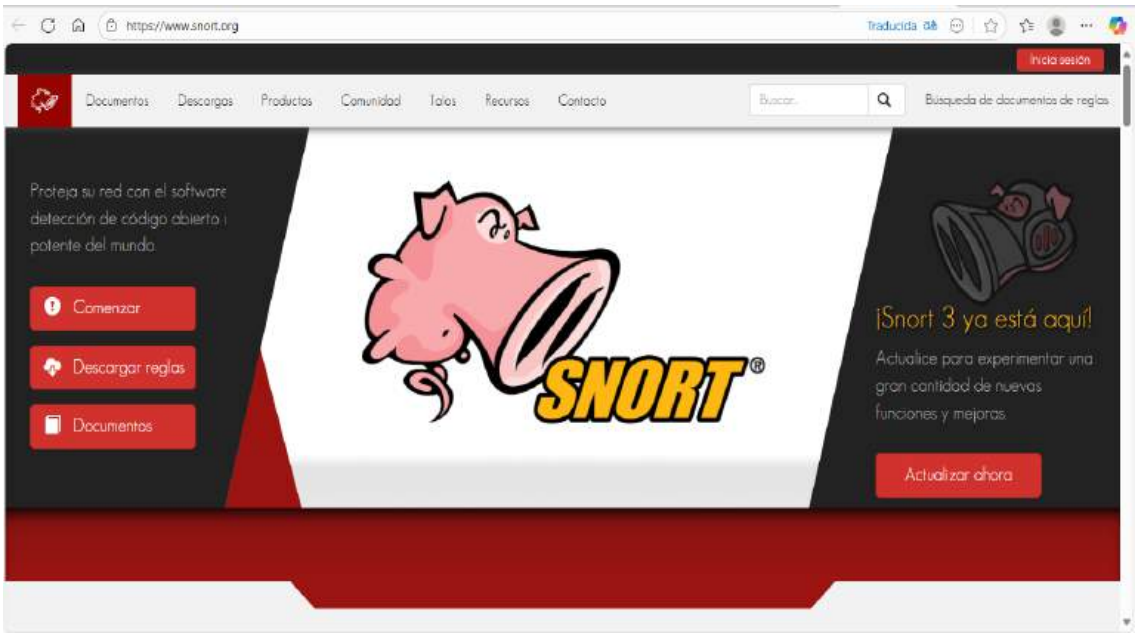
Nessus Essentials:

Nota: La imagen muestra la plataforma de **Nessus® Professional** que es un escáner de vulnerabilidades usado en ciberseguridad, que permite detectar fallas, configuraciones incorrectas y software obsoleto en sistemas y redes, que genera informes con el nivel de riesgo y recomendaciones de corrección, cuenta con una base de datos de más de 75,000 vulnerabilidades actualizadas, es utilizado por administradores y auditores para fortalecer la seguridad de las organizaciones, el enlace para su acceso es:

https://es-la.tenable.com/products/nessus/nessus-professional/evaluate

Figura 6

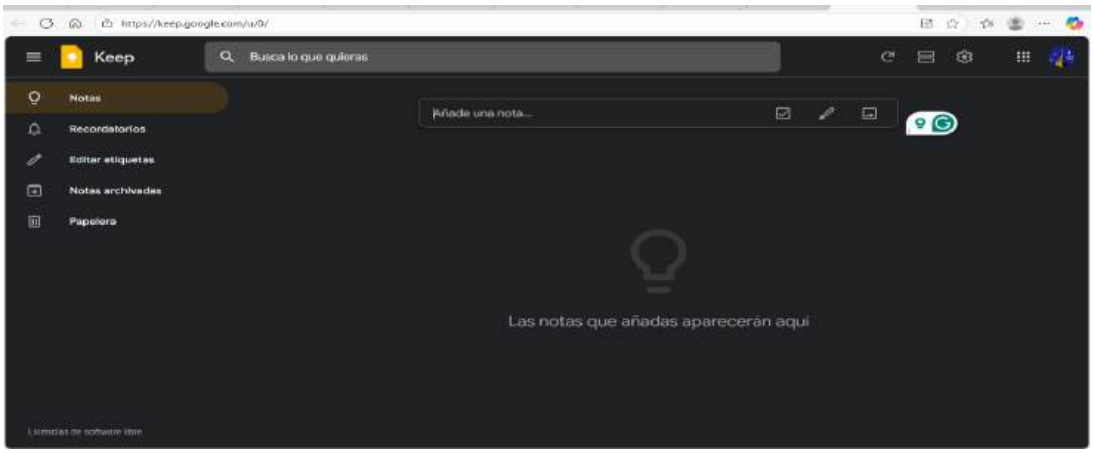
Snort IDS:



Nota: La siguiente imagen muestra a Snort IDS Snort IDS este es un sistema de detección de intrusos en red de código abierto, analiza el tráfico en tiempo real para identificar ataques y anomalías, usa reglas (signaturas) que se pueden personalizar según la red, funcionando como IDS y puede configurarse como IPS para bloquear amenazas, es gratuito y ampliamente usado en seguridad informática, el enlace para su acceso es: https://www.snort.org

Figura 7

Google Keep



Nota: La siguiente imagen muestra a **Google Keep**, es una aplicación de Google para tomar notas y crear listas, permite agregar texto, voz, imágenes y recordatorios, las notas se sincronizan, en la nube y se acceden desde cualquier dispositivo, ofrece organización con etiquetas, colores y búsqueda rápida, se pueden compartir notas para colaborar en tiempo real, el enlace para su acceso es: https://keep.google.com/u/0/

Figura 8

Acronis Backup:

Nota: La siguiente imagen muestra **Acronis Backup**, un software de respaldo y recuperación de datos que permite hacer copias de seguridad automáticas de sistemas, archivos y aplicaciones, ofrece almacenamiento local o en la nube con cifrado seguro, incluye protección contra malware y ransomware, facilita la recuperación rápida para minimizar pérdidas y tiempos de inactividad, el enlace para su acceso es: https://www.acronis.com/es/products/true-image/

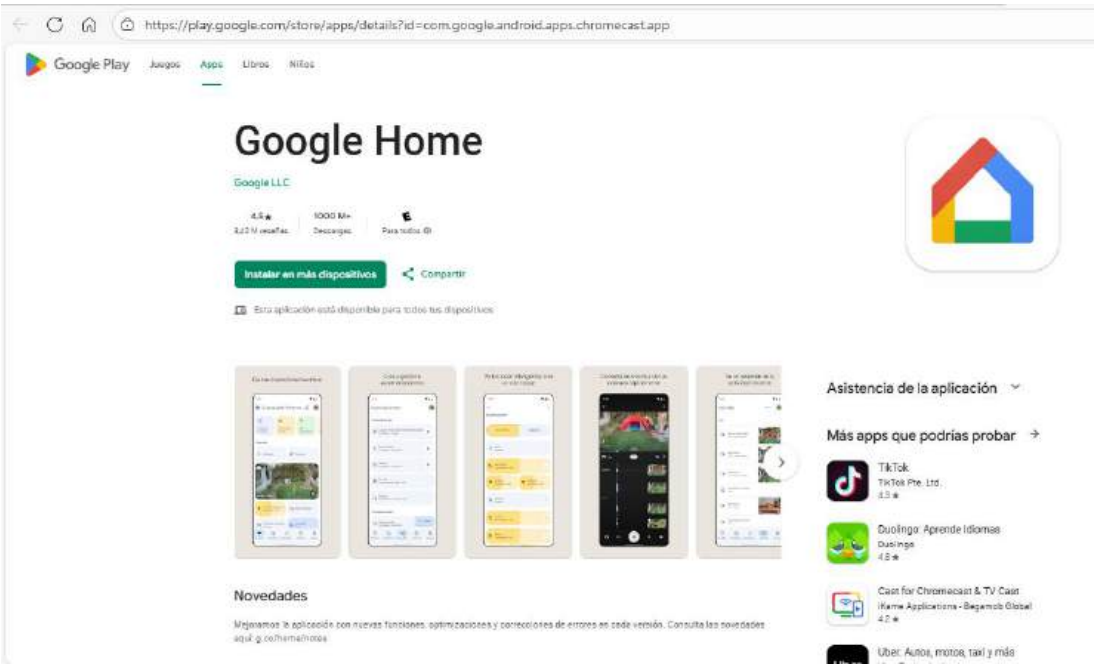
Figura 9

BatteryCare (Windows):

Nota: La siguiente imagen muestra el programa **BatteryCare,** es un programa gratuito para Windows que optimiza la batería de portátiles, monitorea ciclos de carga y descarga para dar estadísticas precisas, recomienda calibraciones para mantener el buen estado de la batería, permite cambiar planes de energía de forma automática, es ligero, fácil de usar y consume pocos recursos, el enlace para su acceso es: https://www.acronis.com/es/products/true-image/

Figura 10

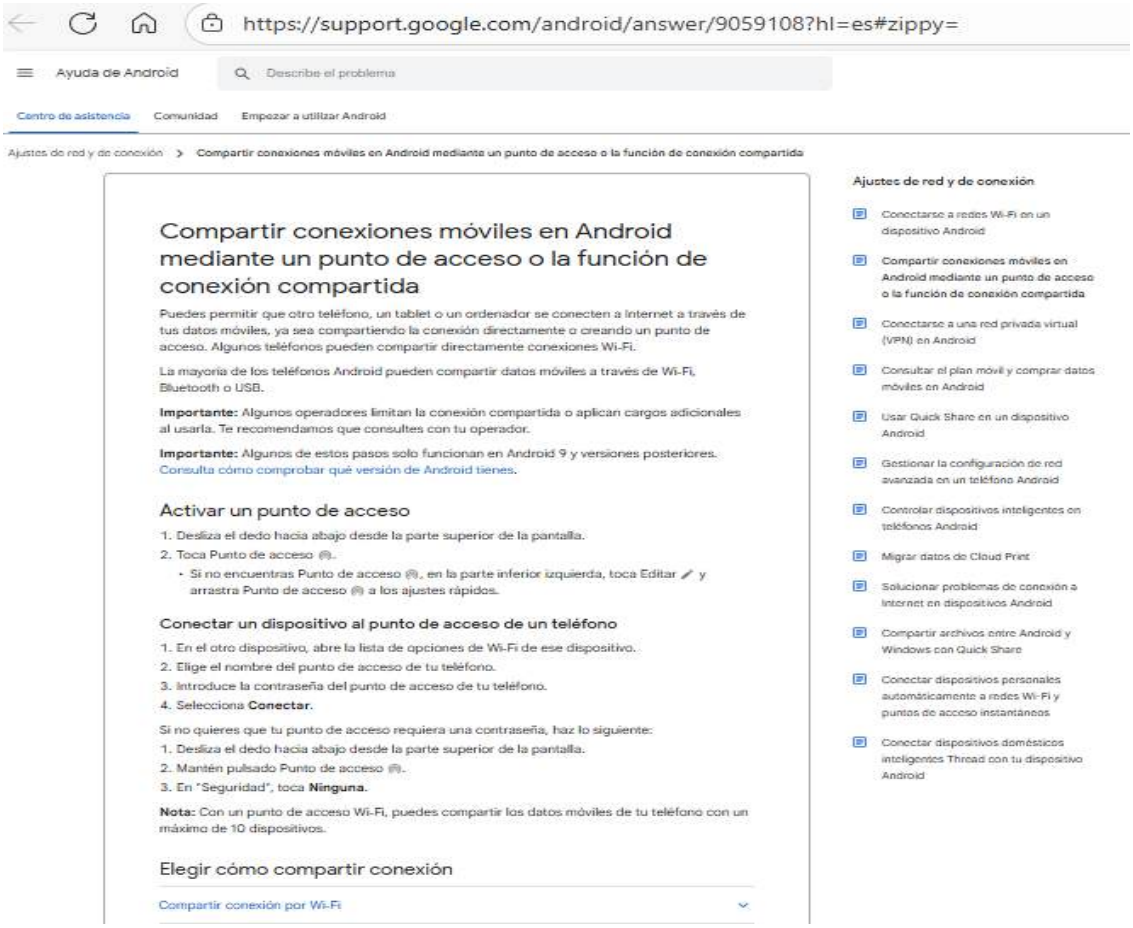
Google Home:



Nota: La siguiente imagen muestra **Google Home**, es una app de Google para controlar dispositivos inteligentes, permite manejar luces, cámaras, termostatos y más desde el celular, se integra con **Google Assistant** para usar comandos de voz, ofrece rutinas automatizadas para simplificar tareas del hogar, convierte la casa en un **hogar inteligente** accesible desde cualquier lugar, el enlace para su acceso es: https://www.acronis.com/es/products/true-image/

Figura 11

Hotspot móvil:



Nota: La imagen muestra una serie de instrucciones para efectuar el **Hotspot móvil**, esta es la función que permite compartir internet desde un celular, convierte el dispositivo en un punto de acceso Wi-Fi, Bluetooth o USB, otros equipos como laptops y tablets se conectan a esa red, usa contraseña y cifrado para mantener la conexión segura, consume datos del plan y más batería del teléfono, se establece como Plan B en nuestro plan de acción, utilizando datos móviles como respaldo en caso de una caída del enlace principal. el enlace para su acceso es: https://support.google.com/android/answer/9059108?hl=es#zippy=

Figura 12

Tabla de la Selección de software:

INSIDENCIA	1.Ingeniería social (phishing en correo, WhatsApp, llamadas)	2.Acceso físico deficiente (entradas abiertas, bitácoras manuales fáciles de falsificar, poca supervisión).	3.Fuga de información confidencial por personal interno	4.Malware /Ransomware por antivirus gratuito y firewall deshabilitado	5.Software no confiable descargado en Servidor 2	6.Saturación/DDoS al enlace comercial	7.Incendio	8.Inundación / Huracán / Sismo	9.Cortes y picos eléctricos	10.Sin alarma de seguridad en acceso	11.Espacio insuficiente y falta de gestión de capacidad	12.Sin respaldos 3-2-1 ni retención probada	13.Sin cifrado en reposo ni control granular de roles	14.Segmentación nula (planta baja directa a módem)	15.Wi-Fi sin controles avanzados	16.Firewall deshabilitado y sin IDS/IPS	17.Único enlace sin redundancia/failover
Responsable	Analista de Ciberseguridad + Responsable de Capacitación de RRHH	Administrador de Sistemas + Encargado de Seguridad Física + Jefe de Protección Civil	Administrador de Red + Analista de Datos	Especialista en Seguridad Informática	Auditor de seguridad / Ingeniero de redes	Administrador de Red	Coordinador de Seguridad Física + Jefe de Protección Civil	Administrador de Bases de Datos +Director Académico	Técnico de Soporte de Infraestructura	Técnico en instalaciones / Seguridad física	Administrador de Bases de Datos	Administrador de Base de Datos + Administrador de Sistemas	Administrador de Base de Datos + Especialista en Seguridad	Administrador de Red	Administrador de Red	Administrador de Servidores	Usuario final / Coordinador de TI
Herramanta/s	PhishTool	BitLocker (Windows)	Google Drive (permisos y roles)	Malwarebytes Free	Nessus Essentials	Snort IDS	Checklist en Google Keep	Acronis Backup + Google Drive	BatteryCare (Windows)	Sensores simples + Google Home	Nessus Essentials	Acronis Backup + Google Drive	BitLocker + Google Drive	Cambio manual en router	Cambio manual en router	Snort IDS + Firewall de Windows	Hotspot móvil
Paso a Seguir para el plan de Accion	Usar PhishTool para entrenar al personal	Cifrar discos duros para proteger datos locales mas Control de accesos físicos (biometría, cámaras, registros digitales)	Configurar roles de acceso y activar historial de actividad mas NDA + monitoreo de accesos a carpetas críticas	Escanear y eliminar amenazas ocultas	Detectar software vulnerable y configuraciones inseguras	Detectar tráfico anómalo y ataques de red	Crear protocolo de prevención y simulacros	Respaldar documentos críticos en nube y disco externo	Monitorear batería y evitar pérdida de datos	Usar sensores simples conectados a Google Home	Detectar servicios innecesarios que consumen recursos y gestiónar el almacenamiento (NAS, cuotas, alertas)	Crear rutina de respaldo semanal	Cifrar archivos y limitar accesos	Configurar red de invitados desde el panel del módem	Acceder a 192.168.1.1 y cambiar clave WPA2 segura	Activar firewall y usar Snort para monitoreo básico	Se establece como Plan B, utilizando datos móviles como respaldo en caso de una caída del enlace principal
Amenaza o vulnerabilidades encontradas	Amenazas Humanas	Amenazas Humanas	Amenazas Humanas	Amenazas Lógicas	Amenazas Lógicas	Amenazas Lógicas	Amenazas Físicas	Amenazas Físicas	Amenazas Físicas	Amenazas Físicas	Vulnerabilidades de Almacenamiento	Vulnerabilidades de Almacenamiento	Vulnerabilidades de Almacenamiento	Vulnerabilidades de Comunicación	Vulnerabilidades de Comunicación	Vulnerabilidades de Comunicación	Vulnerabilidades de Comunicación

Nota: La imagen muestra la selección de estas herramientas como BitLocker, Google Drive y Acronis Backup es porque se usa

para la Seguridad de la información y protección de datos, ya que BitLocker cifra discos duros para evitar accesos no autorizados, Google Drive almacena y protege archivos críticos con control de roles y cifrado en reposo, al igual que Acronis Backup realiza respaldos automáticos en nube y disco externo.

Estos programas enlistados ayudan a la Prevención y detección de amenazas:

PhishTool: Entrena al personal contra ataques de phishing e ingeniería social.

Malwarebytes Free: Escanea y elimina malware, ransomware y spyware.

Nessus Essentials: Detecta vulnerabilidades en software y configuraciones inseguras.

Snort IDS más Firewall de Windows: Monitorean tráfico de red y bloquean accesos maliciosos.

Para la Gestión de infraestructura y continuidad operativa **BatteryCare** es una herramienta que monitorea el estado de la batería para evitar pérdida de datos por apagones y Google Home más los sensores detectan condiciones físicas como incendios o intrusiones, además, configurar redes seguras y segmentadas y Hotspot móvil (Android) proporciona conexión alternativa ante caída del servicio principal.

Google Keep (Checklist) ayuda a la organización y documentación en las cuales se pueden registra protocolos, simulacros y tareas preventivas, permitiendo quedar guardados en linea, evitando perdidas de documentos importantes en caso de que el equipo ya no funcione.

Estas herramientas fueron seleccionadas por su eficacia, accesibilidad y compatibilidad con el entorno institucional, y están alineadas con las amenazas y vulnerabilidades identificadas en el proyecto.

Figura 13

Plan de acción:

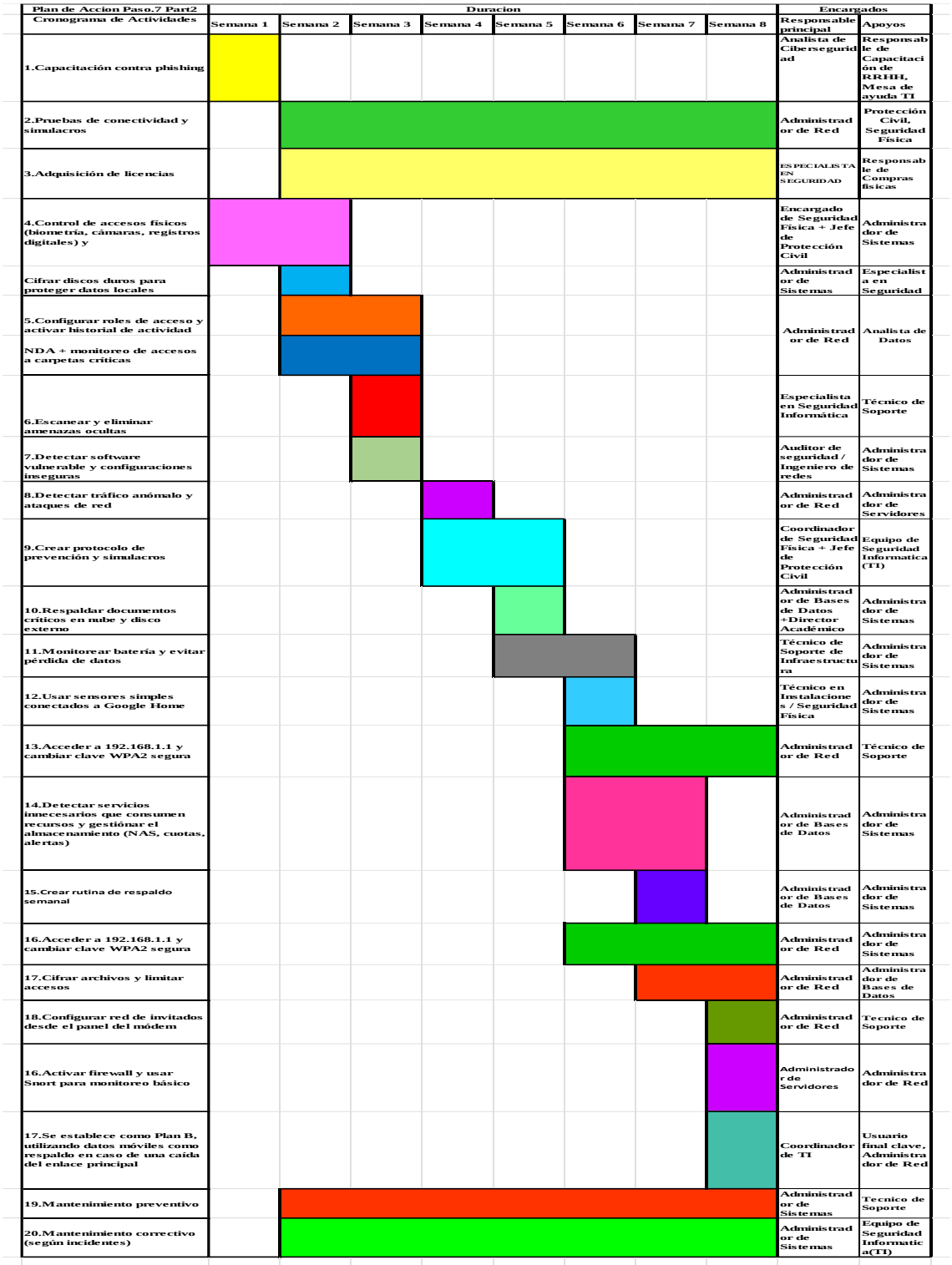
Plan de Accion Paso.7	Amenazas Humanas			Amenazas Lógicas			Amenazas Físicas				Vulnerabilidades de Almacenamiento			Vulnerabilidades de Comunicación			
Insidencia	Phishing / Ingeniería social	Intrusión física por personas no autorizadas, robo de equipos, manipulación directa de servidores o acceso a información sensible.	Abuso de privilegios, fuga de información, manipulación o borrado de datos sensibles por personal interno.	Descarga de malware, ejecución de ransomware, acceso remoto no autorizado y cifrado malicioso de archivos.	Instalación de malware, backdoors o exploits que comprometan la disponibilidad y la integridad del servidor.	Ataques de denegación de servicio distribuido (DDoS), interrupción de red y caída de los servicios institucionales.	Incendio en áreas críticas que provoque pérdida de equipos, interrupción académica y daños a la infraestructura.	Desastres naturales (inundaciones, huracanes, sismos) que provoquen interrupción prolongada, pérdida de equipos y afectación directa a la infraestructura escolar.	Cortes eléctricos prolongados, sobrecargas o variaciones de voltaje que interrumpan clases, dañen servidores y ocasionen pérdida de datos.	Intrusión física por terceros o personal interno, robo de documentos sensibles, manipulación de servidores y sustracción de recursos materiales.	Interrupción de servicios por falta de espacio, pérdida de información crítica, corrupción de archivos y fallos en respaldos automáticos.	12.Sin respaldos 3-2-1 ni retención probada	13.Sin cifrado en reposo ni control granular de roles	14.Segmentación nula (planta baja directa a módem)	15.Wi-Fi sin controles avanzados	16.Firewall deshabilitado y sin IDS/IPS	Caída del servicio por saturación, fallas del proveedor o ataques DDoS que afecten la continuidad académica y administrativa.
Semana de Inico y Semana de Fin	Semana 1 -1	Semana 1 -2	Semana 2 -2	Semana 2 -3	Semana 3 -3	Semana 3 -4	Semana 4-4	Semana 4 -5	Semana 5 -5	Semana 5-6	Semana 6-6	Semana 6 -7	Semana 7 -7	Semana 7 -8	Semana 8 -8	Semana 6 -8	Semana 7 -8
Responsables	Analista de Ciberseguridad + Responsable de Capacitación de RRHH	Administrador de Sistemas + Encargado de Seguridad Física + Jefe de Protección Civil	Administrador de Red + Analista de Datos	Especialista en Seguridad Informática	Auditor de seguridad / Ingeniero de redes	Administrador de Red	Coordinador de Seguridad Física + Jefe de Protección Civil	Administrador de Bases de Datos +Director Académico	Técnico de Soporte de Infraestructura	Técnico en instalaciones / Seguridad física	Administrador de Bases de Datos	Administrador de Base de Datos + Administrador de Sistemas	Administrador de Base de Datos + Especialista en Seguridad	Administrador de Red	Administrador de Red	Administrador de Servidores	Usuario final / Coordinador de TI
Herramanta/s	PhishTool	BitLocker (Windows)	Google Drive (permisos y roles)	Malwarebytes Free	Nessus Essentials	Snort IDS	Checklist en Google Keep	Acronis Backup + Google Drive	BatteryCare (Windows)	Sensores simples + Google Home	Nessus Essentials	Acronis Backup + Google Drive	BitLocker + Google Drive	Cambio manual en router	Cambio manual en router	Snort IDS + Firewall de Windows	Hotspot móvil
Solucion	Usar PhishTool para entrenar al personal	Cifrar discos duros para proteger datos locales mas Control de accesos físicos (biometría, cámaras, registros digitales)	Configurar roles de acceso y activar historial de actividad mas NDA + monitoreo de accesos a carpetas críticas	Escanear y eliminar amenazas ocultas	Detectar software vulnerable y configuraciones inseguras	Detectar tráfico anómalo y ataques de red	Crear protocolo de prevención y simulacros	Respaldar documentos críticos en nube y disco externo	Monitorear batería y evitar pérdida de datos	Usar sensores simples conectados a Google Home	Detectar servicios innecesarios que consumen recursos y gestiónar el almacenamiento (NAS, cuotas, alertas)	Crear rutina de respaldo semanal	Cifrar archivos y limitar accesos	Configurar red de invitados desde el panel del módem	Acceder a 192.168.1.1 y cambiar clave WPA2 segura	Activar firewall y usar Snort para monitoreo básico	Se establece como Plan B, utilizando datos móviles como respaldo en caso de una caída del enlace principal
Enlaces de las herramientas	https://www.phishtool.com/	[Windows 11/10] Encriptación del dispositivo (BitLocker) | Soporte técnico oficial | ASUS México	Google Drive: comparte archivos online con almacenamiento seguro en la nube | Google Workspace	https://www.malwarebytes.com/es/mwb-download	https://es-la.tenable.com/products/nessus/nessus-professional/evaluate	Snort - Sistema de detección y prevención de intrusiones en la red	https://keep.google.com/u/0/	https://drive.google.com/drive/home tambien esta: https://www.acronis.com/es/products/true-image/	https://batterycare.net/en/download.html	Google Home - Aplicaciones en Google Play	https://es-la.tenable.com/products/nessus/nessus-professional/evaluate	https://www.acronis.com/es/products/true-image/	[Windows 11/10] Encriptación del dispositivo (BitLocker) | Soporte técnico oficial | ASUS México	https://vimeo.com/611217188/9f83380a29	https://vimeo.com/611217188/9f83380a29	Snort - Sistema de detección y prevención de intrusiones en la red	Compartir conexiones móviles en Android mediante un punto de acceso o la función de conexión compartida - Ayuda de Android

Nota: La figura es el plan que se organiza en ocho semanas para solucionar los diecisiete factores de riesgo, agrupados en

Amenazas Humanas, Lógicas, Físicas, y Vulnerabilidades de Almacenamiento y Comunicación, cada una de ellos indica los responsables, las herramientas para implementar la solución, como la acción concreta como por ejemplo la capacitación anti-phishing; acceso físico más BitLocker; permisos y trazabilidad en Google Drive; escaneo de malware y vulnerabilidades con (Malwarebytes/Nessus), Snort para tráfico anómalo, simulacros, respaldo 3-2-1 (Acronis/Drive), monitoreo/UPS, segmentación y SSID de invitados, firewall activo y Plan B con datos móviles, el principal objetivo es la reducción de CVEs, alertas IDS y 2FA activo, el resultado esperado es disminuir la probabilidad e impacto de incidentes y asegurar la disponibilidad, integridad y confidencialidad del entorno escolar

Figura 14

Cronograma de actividades:



Nota: Es un cronograma de actividades en formato Gantt, en el que se planifican las tareas de prevención, seguridad informática, respaldo de datos y mantenimiento de la infraestructura tecnológica de un colegio/organización, cada una de las filas corresponde a una actividad específica por ejemplo la capacitación contra phishing, pruebas de conectividad, adquisición de licencias, control de accesos físicos, respaldos, se consideró el monitoreo, protocolos, mantenimiento preventivo y correctivo porque es vital tenerlos en cuenta, en las columnas de semanas de la 1 a la 8 se muestra con colores el tiempo de ejecución de inicio y final de cada una de las actividades, la última columna asigna responsables principales y apoyos, incluyen los roles como analista de ciberseguridad, administrador de red, especialista en seguridad informática, técnicos de soporte, protección civil, administrador de sistemas, entre otros, en pocas palabras, es un plan de acción calendarizado que integra actividades técnicas, físicas y organizacionales, asegurando la continuidad operativa, la protección de la información y la reducción de riesgos.

Práctica de plan de acción:

A continuación, se incluyen figuras que ejemplifican la operación de ciertas plataformas y programas seleccionados, los cuales abordan de forma disruptiva diversas amenazas y vulnerabilidades, aunque no se representan todas las herramientas descritas en el documento, esta sección cumple una función aclaratoria mediante la demostración práctica:

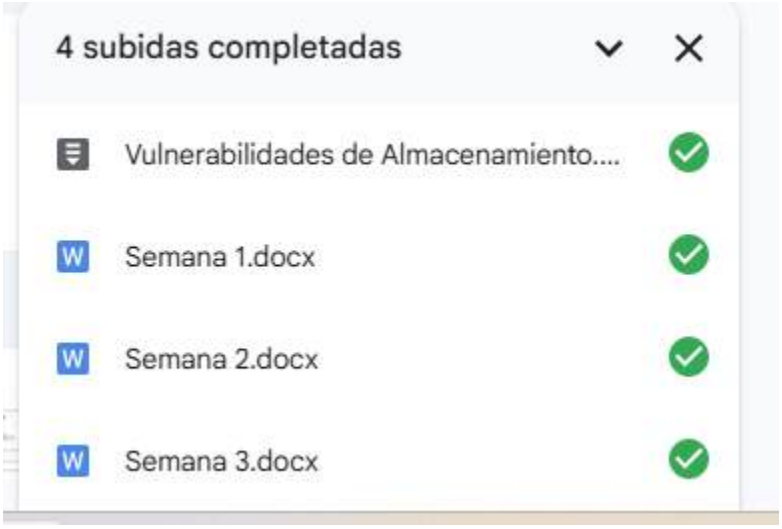
Figura 15

Subida de archivos en Google Drive

Nota: En esta imagen se muestra en Google Drive cubriendo la vulnerabilidad de la Falta de respaldos 3-2-1, la solución aplicada es la subida de archivos semanales (Semana 1, Semana 2, Semana 3) como parte de una rutina de respaldo.

Figura 16

Archivos organizados en Drive:



Nota: La presente imagen presenta la vulnerabilidad de ausencia de respaldos periódicos, solucionada con la organización de documentos por semana en Google Drive, lo que asegura continuidad de la información.

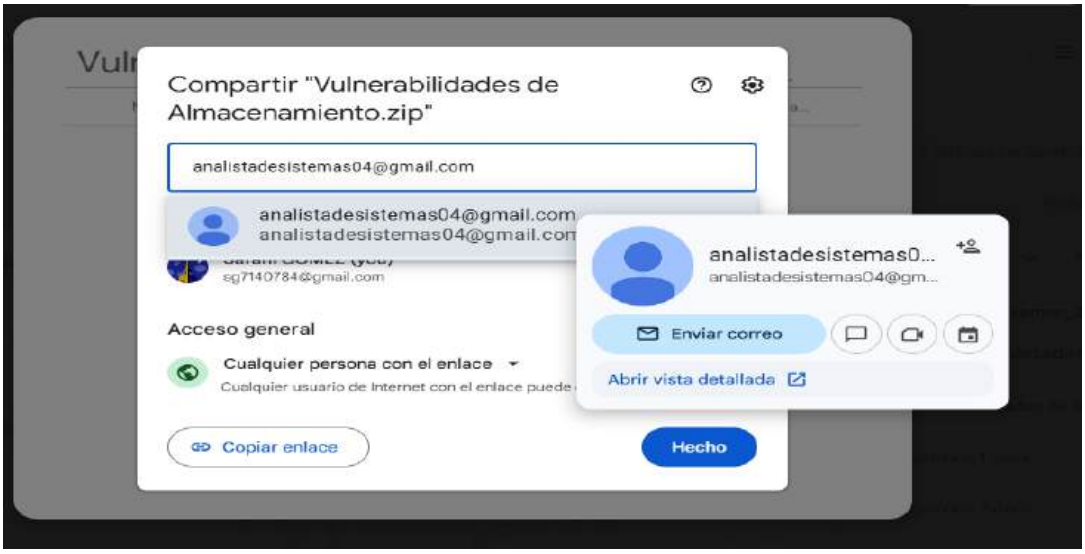
Figura 17

Archivo comprimido en Drive (.zip):

Nota: Esta imagen cubre la vulnerabilidad de guardar archivos sin cifrado, en reposo ni control granular de roles, la solución aplicada fue subir un archivo ZIP protegido con contraseña a Google Drive, añadiendo seguridad adicional.

Figura 18

Compartición de archivo por correo:



Nota: En esta imagen se cubre la vulnerabilidad de los accesos sin control, aplicando la solución que otorga acceso únicamente a usuarios autorizados mediante correo específico.

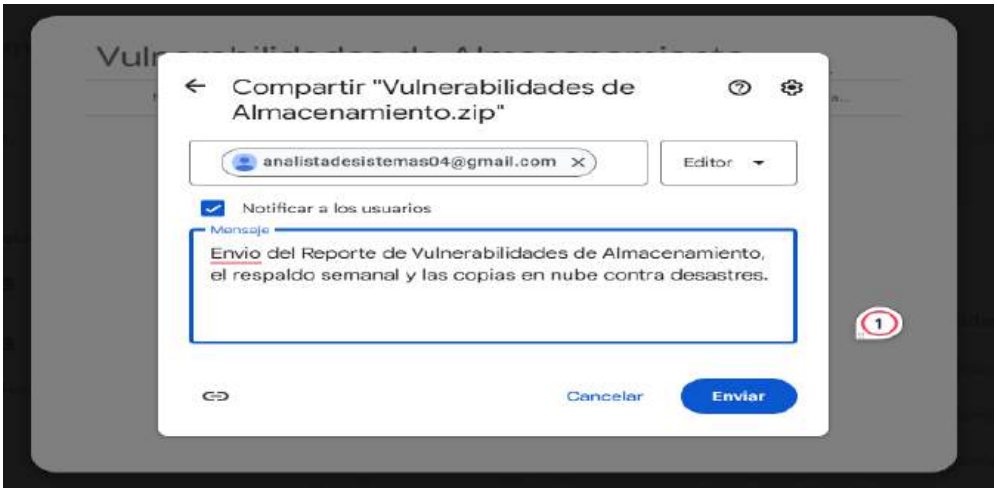
Figura 19

Acceso restringido confirmado con la configuración de roles de acceso:

Nota: La imagen muestra la vulnerabilidad cubierta: Roles sin granularidad en almacenamiento, y los archivos expuestos públicamente, aplicando el acceso restringido solo al propietario y al analista de sistemas, es un claro ejemplo de la configuración de permisos en Google Drive: restringido o solo usuarios con enlace controlado.

Figura 20

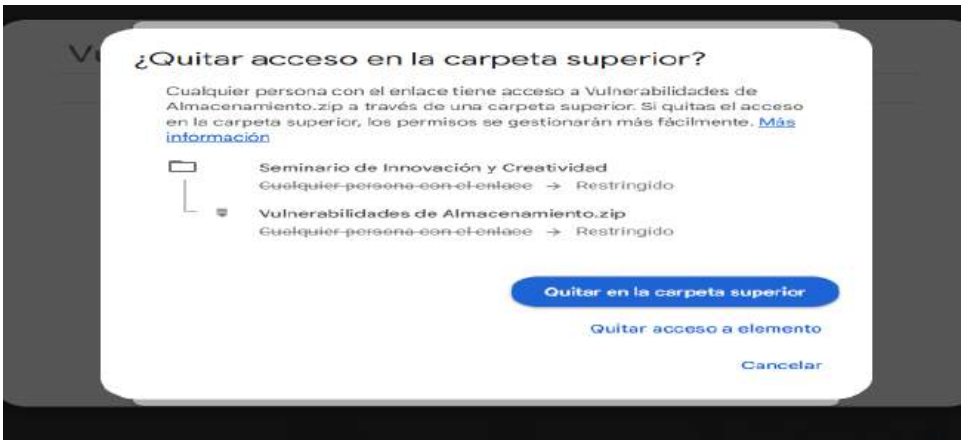
Envío de archivo con mensaje ayudando a una comunicación más efectiva:



Nota: La imagen cubre la vulnerabilidad de un respaldo sin comunicación ni evidencia, con la documentación de la acción mediante envío del archivo con mensaje: “Respaldo semanal y copias en nube contra desastres”.

Figura 21

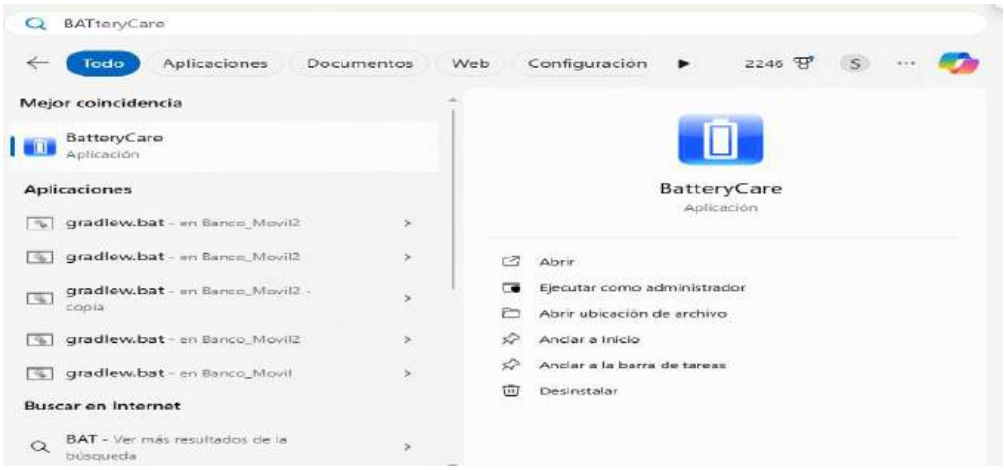
Restricción de permiso en los archivos:



Nota: La imagen cubre la vulnerabilidad de permisos inseguros desde carpetas principales y archivos, la solución aplicada es la eliminación de accesos heredados, dejando la seguridad gestionada únicamente en el archivo crítico.

Figura 22

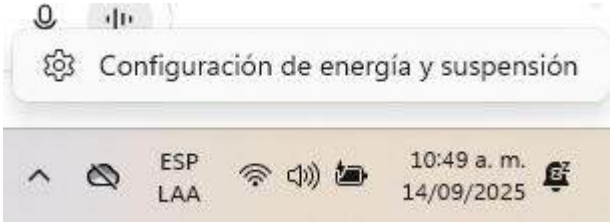
BatteryCare (Aplicación detectada en Windows):



Nota: En esta figura se muestra la aplicación **BatteryCare** lista para abrirse desde el menú de Windows, con ella puedes monitorear en tiempo real el nivel de batería, estado de salud, ciclos de carga y recibir alertas configurables, esto permite anticiparse a un corte eléctrico o descarga inesperada, evitando pérdida de datos al poder guardar tu trabajo antes de que se apague el equipo, en las siguientes figuras se muestra brevemente de lo que sea escrito aquí.

Figura 23

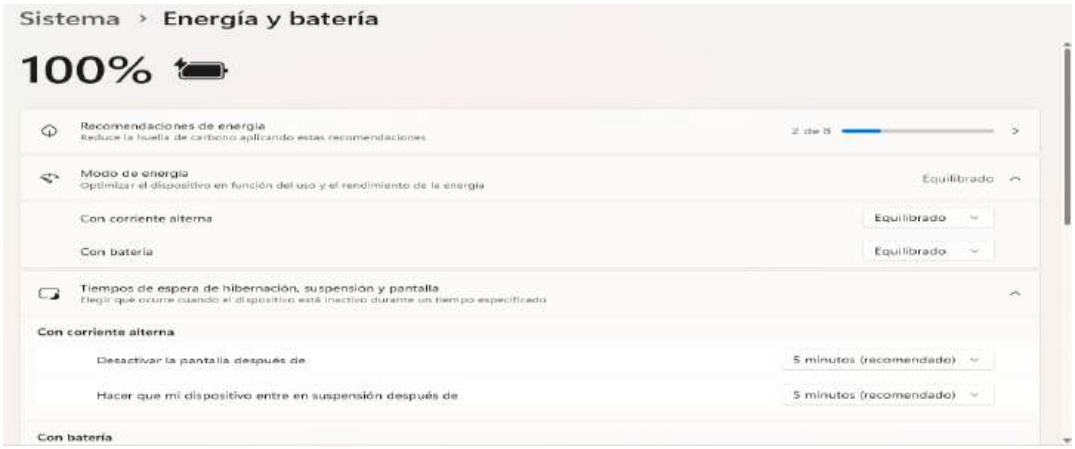
***Apertura de BatteryCare en Windows*:**



Nota: Esta ventana muestra la aplicación **BatteryCare** lista para ejecutarse, permite acceder al panel principal donde se monitorean el nivel de batería, tiempo estimado de duración y estado de salud, **c**ontribuyendo al monitoreo de batería (control del estado y alertas de la batería para evitar apagados inesperados).

Figura 24

Recomendaciones de energía en Windows:



Nota: En esta sección se configuran opciones como brillo automático, suspensión y ahorro energético, permitiendo aplicar ajustes que reducen el consumo y protegen el sistema ante fallos de energía, previniendo la pérdida de datos (evita que la batería se agote rápidamente y previene interrupciones).

Figura 25

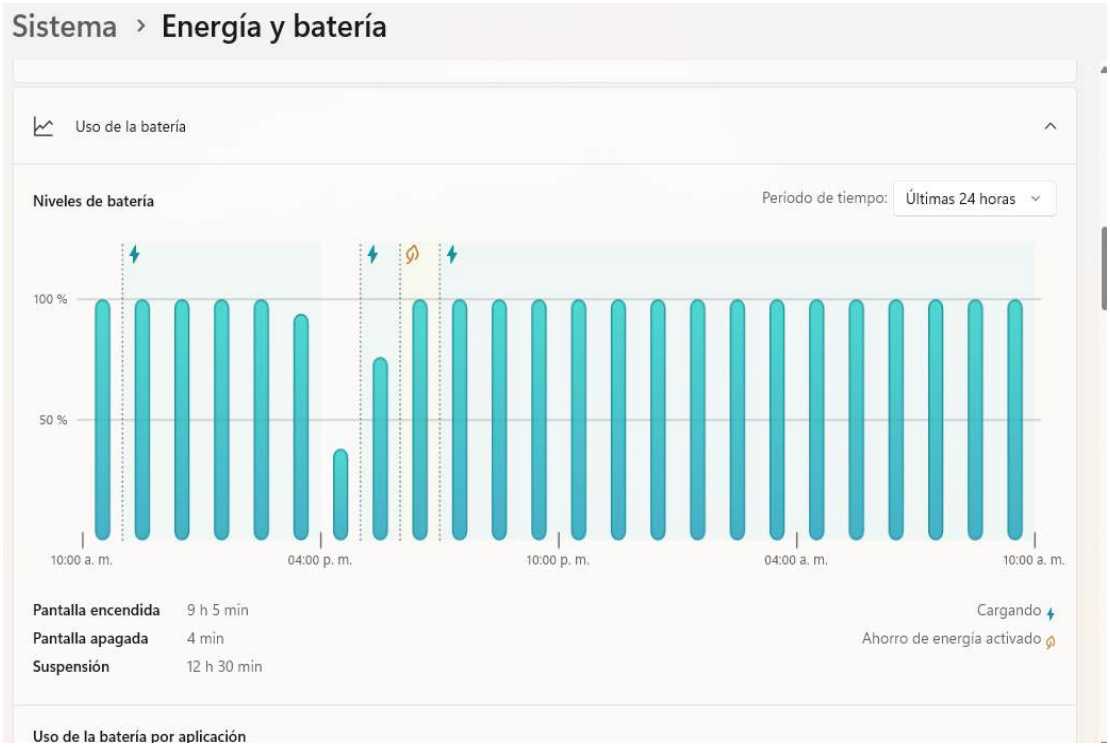
Configuración de notificaciones en Windows:

Nota: En esta imagen se activan notificaciones prioritarias y alertas visibles en pantalla, esto garantiza que el usuario sea advertido antes de que la batería se descargue por completo, ayudando a la prevención de pérdida de datos (permite reaccionar a tiempo ante advertencias de

batería baja).

Figura 26

Configuración de energía y batería en Windows:



Nota: Esta imagen muestra el nivel actual de batería y las opciones de modo de energía (equilibrado, alto rendimiento, ahorro). También define los tiempos de suspensión y apagado de pantalla, su **contribución** es el monitoreo de batería (control del consumo y administración de energía para extender su duración).

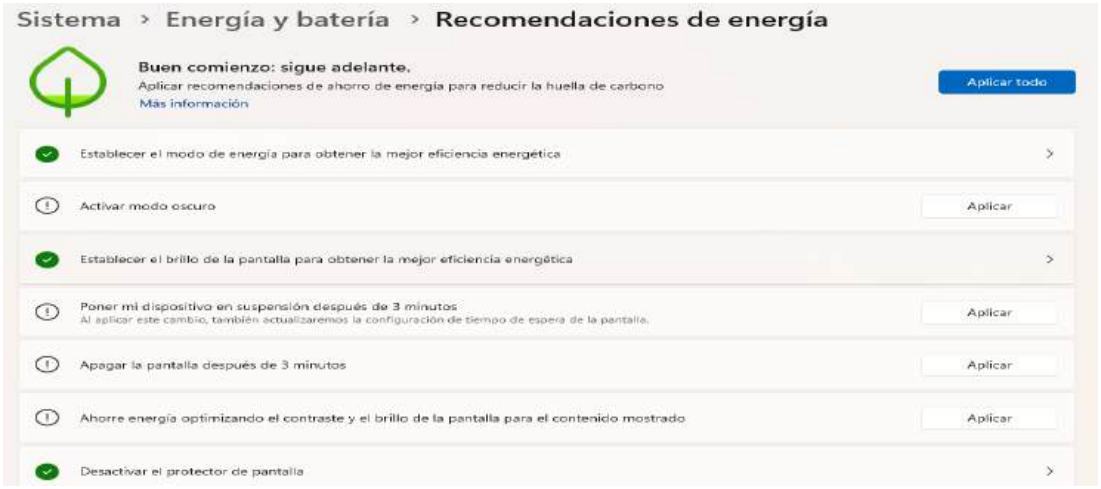
Figura 27

Suspensión y pantalla en batería/corriente:

Nota: Esta imagen muestra la configuración de tiempos de espera para suspender el equipo o apagar la pantalla al trabajar con corriente o batería, evita pérdidas en caso de descuido prolongado, su **contribución** es el monitoreo de batería (control del consumo y administración de energía para extender su duración, evitando apagados inesperados).

Figura 28

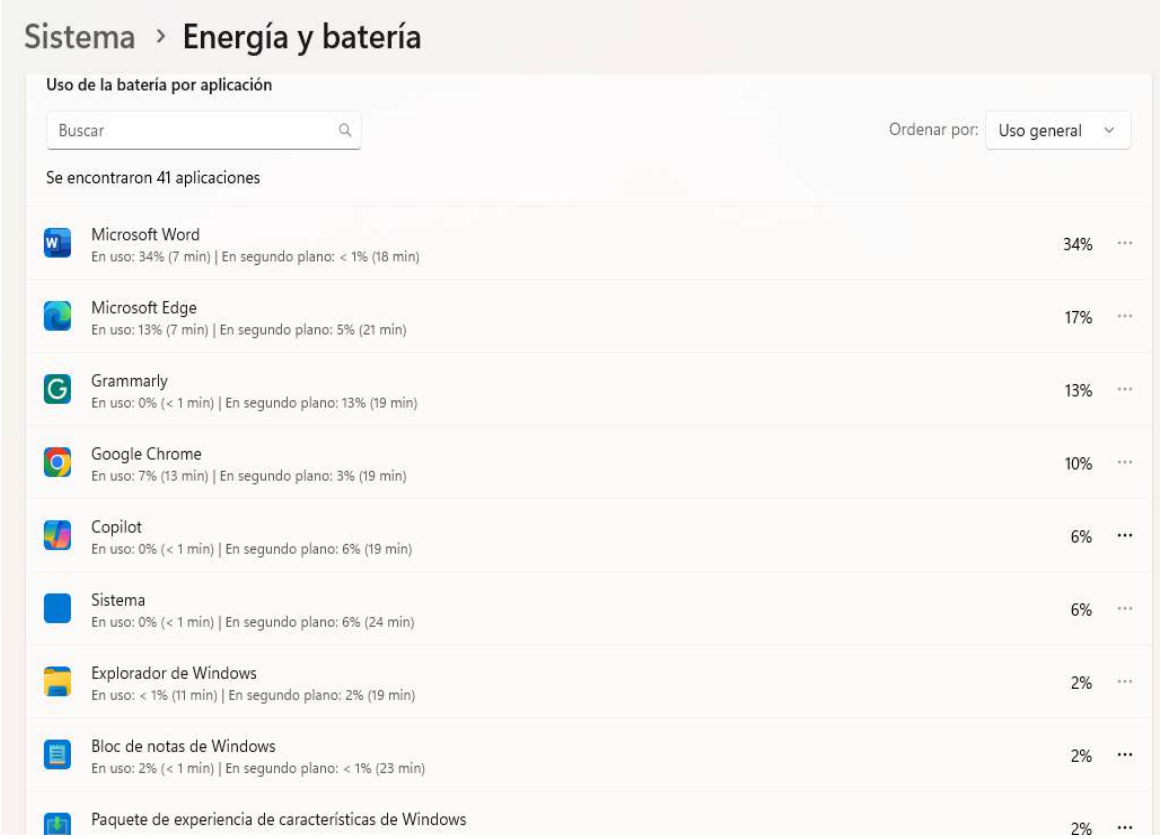
***Opciones de ahorro de energía*:**



Nota: La imagen muestra la activación automática del ahorro de energía al llegar a cierto porcentaje de batería y la reducción de brillo cuando está en uso, ayudando al monitoreo de batería (gestiona el uso de batería y extiende la autonomía del equipo).

Figura 29

Uso de la batería por aplicación:



Nota: La imagen identifica el consumo energético de cada aplicación instalada, permitiendo cerrar programas que desgastan la batería innecesariamente, previene la pérdida de datos (reduce riesgos de apagado por consumo excesivo).

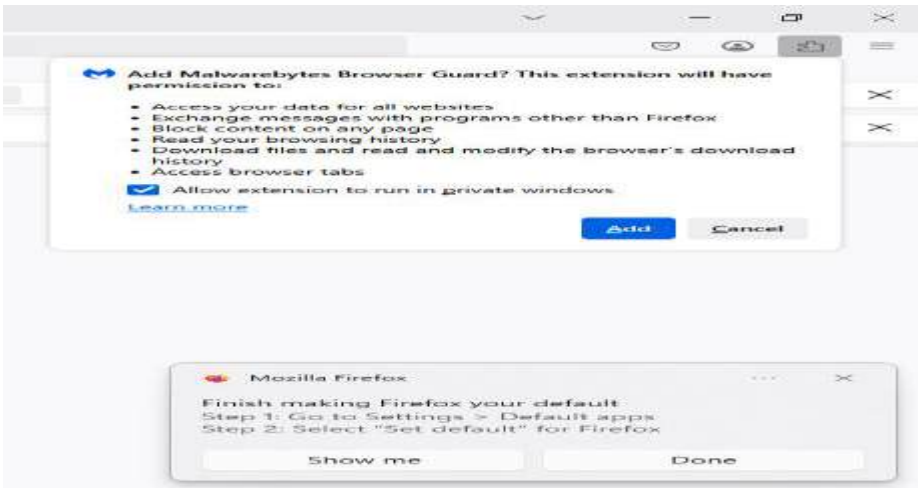
Figura 30

Configuración de acciones al cerrar tapa o botón:

Nota: La imagen permite definir qué ocurre al cerrar la tapa o presionar el botón de encendido (suspender, hibernar, apagar), así se evitan interrupciones y pérdida de documentos, previendo la pérdida de datos (asegura un cierre controlado y evita cortes abruptos).

Figura 31

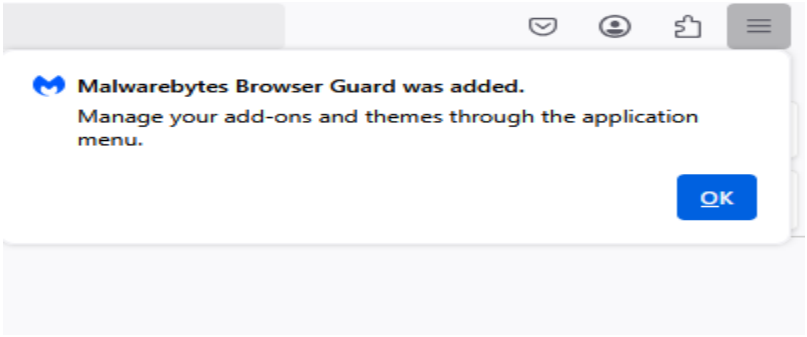
Instalación de la extensión (Browser Guard)



Nota: La imagen muestra el momento de agregar la protección en el navegador, ayuda a cubrir la amenaza al **bloquear descargas sospechosas y accesos no autorizados desde la web**, mediante la prevención activa contra malware antes de que llegue al sistema.

Figura 32

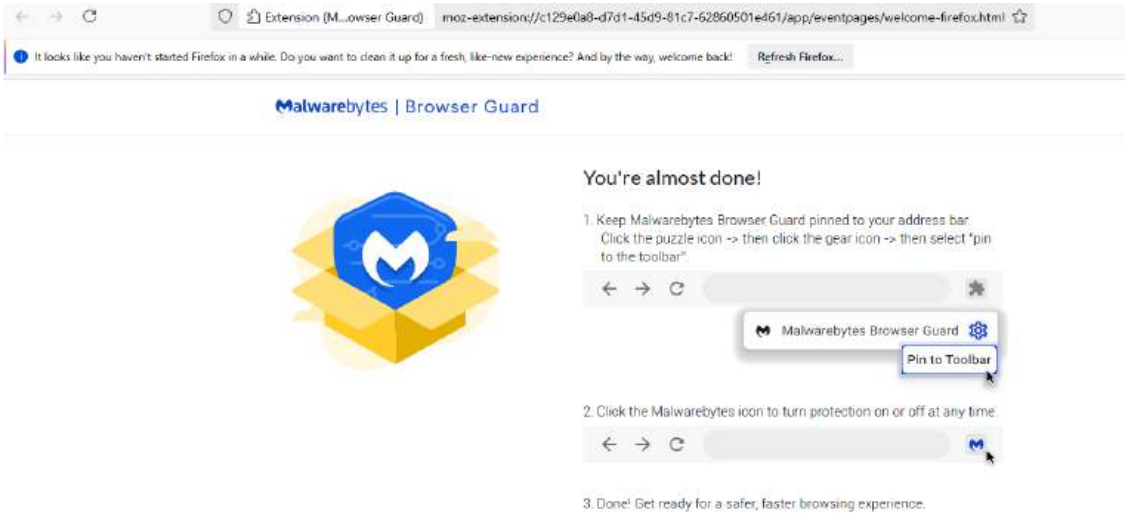
Confirmación de extensión añadida:



Nota: La imagen muestra la extensión fue instalada correctamente en Firefox, indicando que el navegador ya tiene una capa adicional de protección, ayuda a evitar la ejecución de ransomware descargado por sitios maliciosos.

Figura 33

Pin a la barra del navegador (Browser Guard activo)



Nota: La imagen representa la extensión **Malwarebytes Browser Guard** está activa en la barra, permite al usuario controlar el bloqueo en tiempo real, gracias a que el programa realiza el monitoreo continuo de descargas y accesos remotos no autorizados**.**

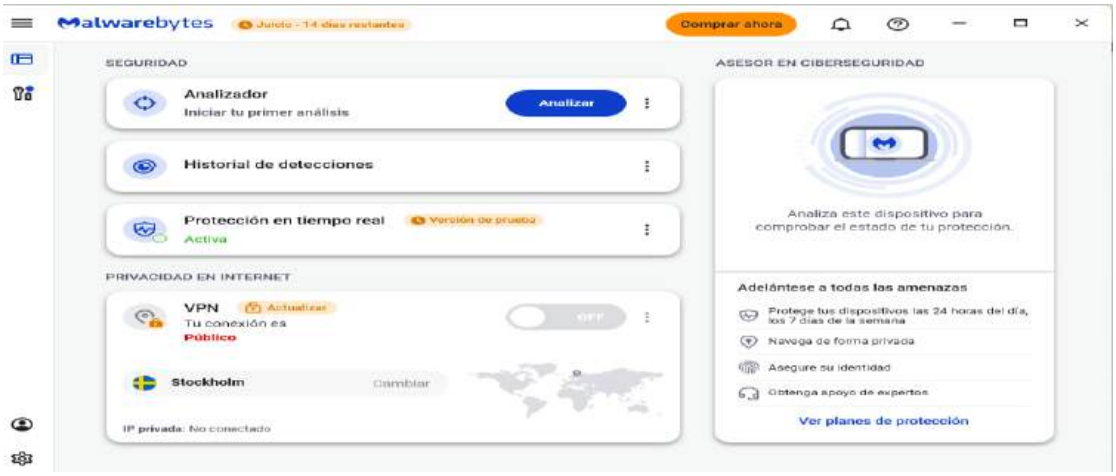
Figura 34

Pantalla de bienvenida a Malwarebytes Desktop

Nota: La imagen aquí presente del programa se prepara en el programa de escritorio, como la base para ejecutar análisis completos del sistema**,** la solución aplicada es eliminar malware y cifrados ocultos en archivos.

Figura 35

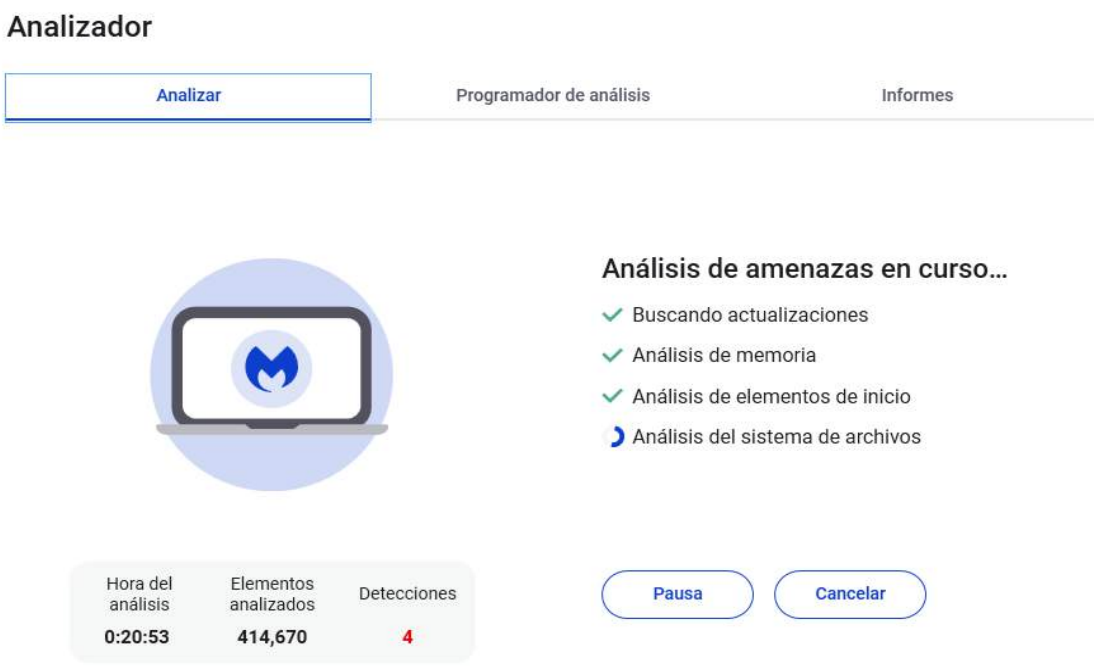
Pantalla principal de Malwarebytes Free:



Nota: La imagen muestra la interfaz principal del programa, con opciones como Analizador, Historial de detecciones *y* Protección en tiempo real, usar **Malwarebytes Free** permite iniciar análisis de amenazas en el dispositivo y activar medidas de protección para detectar y eliminar software malicioso, cubriendo el riesgo de descarga de malware, ransomware y accesos remotos no autorizados**.**

Figura 36

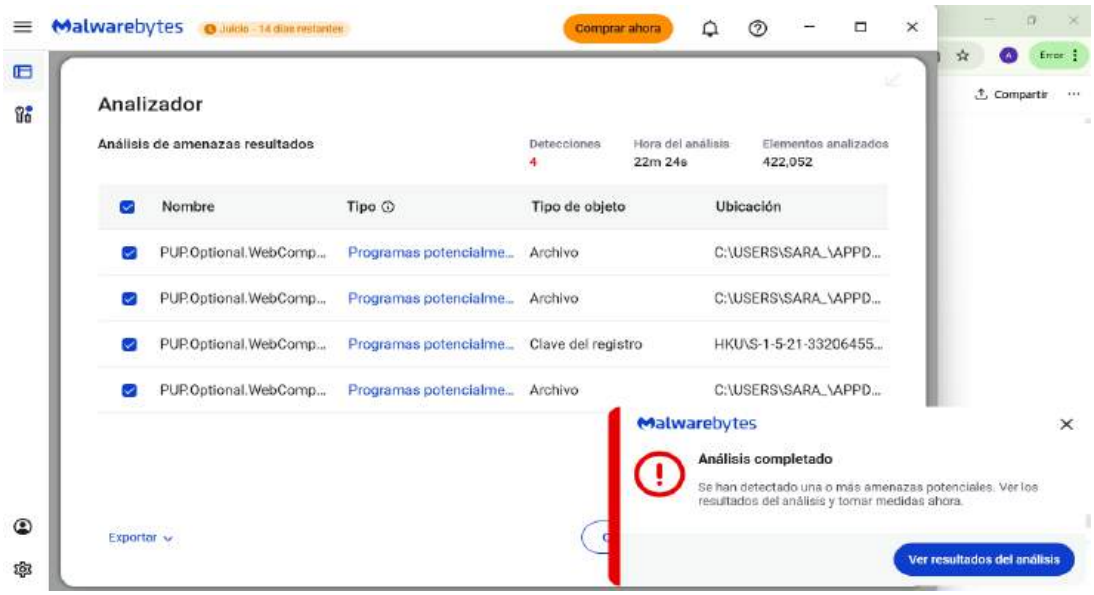
Análisis en curso:



Nota: La imagen muestra que el sistema está siendo analizado (memoria, inicio, sistema de archivos), detectando las amenazas como ransomware en ejecución, solucionando mediante la identificación activa de amenazas ocultas en segundo plano**.**

Figura 37

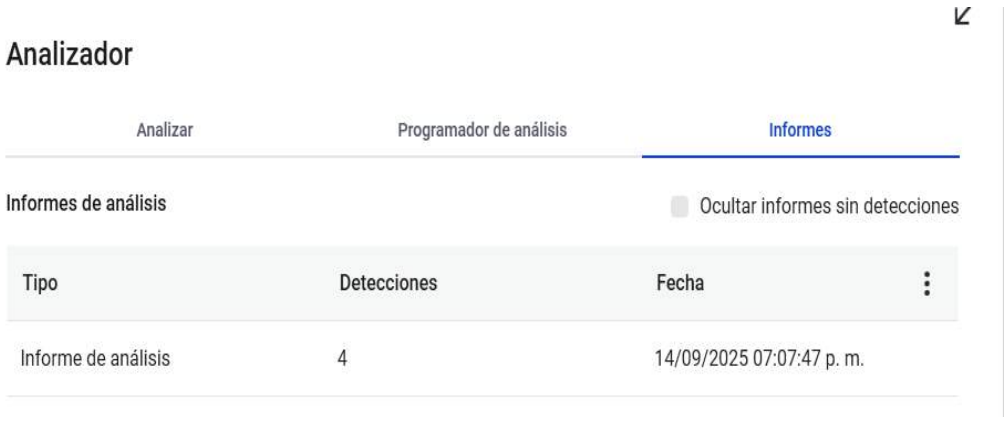
Resultados del análisis (detecciones encontradas):



Nota: La imagen muestra que el sistema detectó programas potencialmente maliciosos, dentro de esta imagen se ve la acción de escaneo en práctica, confirma que Malwarebytes identifica archivos sospechosos relacionados con malware**,** elimina programas que podrían usarse para cifrar datos o permitir acceso remoto.

Figura 38

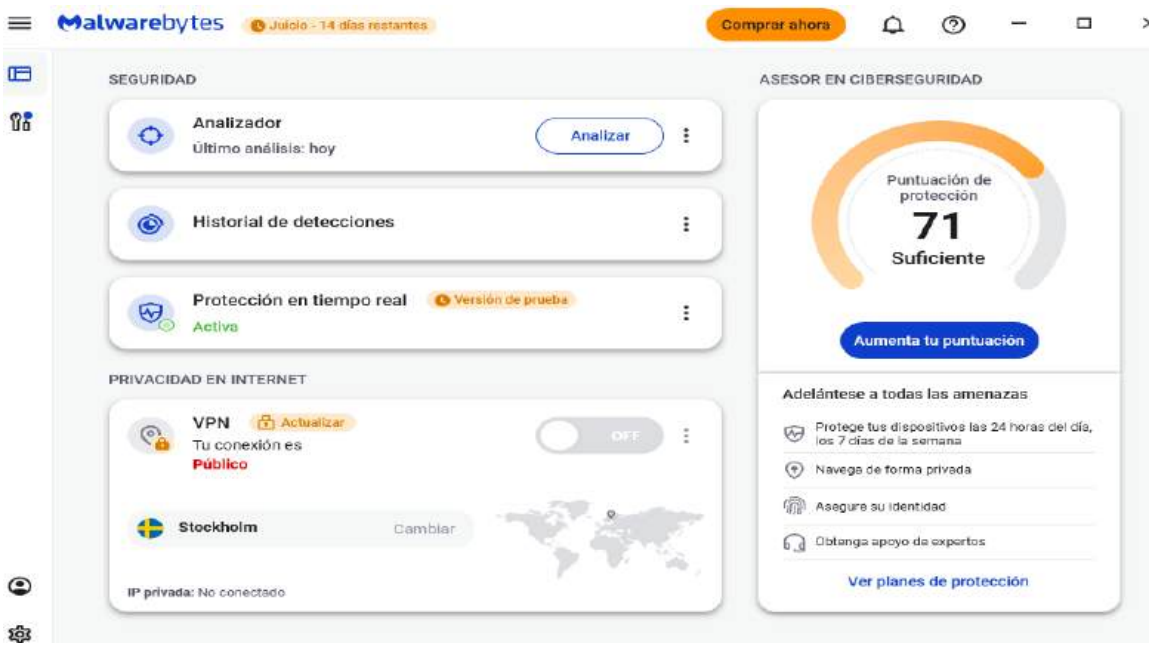
Informe de detecciones



Nota: La imagen muestra el registro de análisis realizado con resultados, permitiendo evidenciar la gestión de amenazas, facilitando el control documental de incidentes de seguridad.

Figura 39

Panel general de protección:



Nota: La imagen muestra la vista del estado de seguridad, protección en tiempo real y puntaje de protección, confirmando que la protección sigue activa, permitiendo la prevención constante contra nuevas descargas de malware y ransomware**.**

Evaluación:

La selección de estas herramientas tecnológicas utilizadas para mitigar las vulnerabilidades identificadas en la etapa 1, en concordancia con las recomendaciones de la etapa 2, cada herramienta ha sido evaluada en función de su aplicabilidad, eficacia y compatibilidad con el entorno institucional, y se integra como parte del plan de acción técnico.

La herramienta de **PhishTool** es una plataforma de simulación de ataques de ingeniería social y phishing, su función en el plan de acción es la capacitación del personal para detectar correos fraudulentos, ayudando a mitigar amenazas humanas mediante entrenamiento activo, por su parte **BitLocker (Windows)** es un sistema de cifrado de discos duros integrado en Windows, la función en el plan de acción es la protección de datos locales ante robo físico o acceso no autorizado, previniendo la fuga de información y pérdida de datos sensibles por lo cual se usa **Google Drive** ya que este es una herramienta de almacenamiento en la nube con control de permisos, historial y roles, es un **ecosistema de servicios y productos**, entre los que destacan:

Gmail para correo electrónico gratuito, **Google Drive** es el encargado del almacenamiento en la nube, **Google Maps utilizado** para mapas y navegación, **Google Chrome** es un navegador web, **Google Fotos, YouTube, Google Docs, Google Meet**, entre muchos otros, la función en el plan de acción es la gestión de accesos, respaldo de información y cifrado en reposo, ya que asegura disponibilidad y control granular de datos críticos.

Así mismo **Malwarebytes Free** es un antivirus gratuito para escaneo y eliminación de malware, en nuestro plan de acción está la detección de amenazas ocultas como ransomware y spyware, reduciendo los riesgos lógicos mediante limpieza preventiva, por lo cual también se ha utilizado **Nessus Essentials** que es un escáner que detecta las vulnerabilidades del software y configuraciones inseguras, en nuestro plan de acción este realiza una evaluación de sistemas y

detección de fallos técnicos, fortaleciendo la seguridad lógica y de almacenamiento.

Es fundamental considerar un sistema de detección de intrusos basado en análisis de tráfico de red por lo cual se ha seleccionado **Snort IDS**, en nuestro plan de acción lleva a cabo el monitoreo de ataques DDoS, tráfico anómalo y vulnerabilidades de comunicación, protegiendo la infraestructura de red ante amenazas externas, así mismo se utiliza un filtro de tráfico entrante/saliente integrado en el sistema operativo denominado **Firewall de Windows** concede el bloqueo de accesos no autorizados y protección de servicios, complementando el monitoreo de red y refuerza la seguridad lógica.

Acronis Backup es un software que ayuda tener copias de seguridad locales y en la nube, en nuestro plan de acción es un programa que se utilizara pare el respaldo de documentos críticos y recuperación ante fallos, mitigando vulnerabilidades de almacenamiento y garantizando la continuidad operativa.

BatteryCare este software que monitorea el estado de la batería en laptops, previniendo la pérdida de datos por cortes eléctricos o sobrecargas que no hayan sido guardados previamente, reduciendo riesgos físicos y protegiendo la integridad de los equipos, al sumarlo con **Google Home más Sensores,** que es un ecosistema de automatización para monitoreo ambiental, beneficiando la prevención ante incendios, intrusión física o condiciones ambientales adversas, que refuerza la seguridad física mediante alertas tempranas.

Se realizará el **Cambio Manual en router** en el cual se **configura la red de invitados desde el panel del módem y se cambia la clave WPA2** a una más segura, para esta ocasión se utiliza el panel de configuración de red doméstica **(Router (192.168.1.1))** la segmentación de red, configuración de invitados y seguridad Wi-Fi, mejora la seguridad de comunicación y evita accesos no autorizados.

En caso que la señal de Internet caiga se ha considerado **Hotspot móvil (Android)** que es una función para compartir conexión móvil como respaldo, es decir en nuestro plan de acción se utiliza como plan B ante caída del enlace principal o interrupción de red, garantizando la continuidad académica y administrativa en caso de falla del proveedor, por último se consideró **Google Keep (Checklist)** como aplicación para crear listas y protocolos, registro de simulacros, protocolos de prevención y seguimiento de tareas dentro nuestro plan de acción, facilitando la gestión organizacional y la documentación de acciones preventivas.

Conclusión:

El desarrollo de este plan de acción en seguridad informática permitió consolidar una estrategia integral que responde de manera efectiva a las amenazas y vulnerabilidades identificadas en etapas previas, a través de la selección adecuada de herramientas tecnológicas, la definición de políticas y protocolos, así como la calendarización de actividades en un cronograma, se logró establecer un marco preventivo y correctivo que garantiza la continuidad operativa y la protección de la información institucional, cada solución implementada desde el uso de PhishTool para la capacitación contra phishing, BitLocker para el cifrado de datos, Google Drive para la gestión de accesos, hasta Malwarebytes, Nessus y Snort IDS para la detección de amenazas y monitoreo de red contribuye de manera específica a reforzar los tres pilares fundamentales de la seguridad informática: **confidencialidad, integridad y disponibilidad**. Asimismo, herramientas complementarias como Acronis Backup, BatteryCare, Google Home y Hotspot móvil aportan resiliencia y aseguran la capacidad de respuesta ante incidentes imprevistos.

En suma, este proyecto constituye una guía práctica aplicable en contextos reales, capaz de optimizar recursos, anticiparse a los riesgos y fortalecer una cultura institucional de ciberseguridad, su implementación representa un paso decisivo hacia la construcción de entornos tecnológicos confiables, resilientes y preparados para enfrentar los retos de un mundo digital en constante evolución.

En la actualidad, vivimos en un entorno altamente digitalizado donde la información personal, académica y laboral circula constantemente a través de dispositivos y redes, esta realidad ha generado la necesidad de adquirir habilidades en **seguridad informática**, no solo

como un conocimiento técnico, sino como una competencia fundamental para desenvolverse con responsabilidad en la vida cotidiana y alcanzar un mejor desempeño en el ámbito laboral, aprender estas herramientas no solo protege la información, sino que también ofrece ventajas significativas en términos de prevención, continuidad y competitividad profesional.

El aprendizaje de habilidades en **seguridad informática** ofrece múltiples beneficios que trascienden el ámbito académico, impactando tanto la vida cotidiana como el desarrollo profesional, en un mundo digital cada vez más expuesto a amenazas, contar con estos conocimientos se convierte en una ventaja competitiva y en una herramienta esencial de protección personal y organizacional.

La elaboración de un plan de acción en seguridad informática, basado en la identificación de amenazas y vulnerabilidades, es de suma importancia tanto en el ámbito laboral como en la vida cotidiana, en el entorno laboral, este plan garantiza la protección de los activos de información de la empresa, preservando su integridad y minimizando los riesgos de sufrir ataques cibernéticos que podrían comprometer su funcionamiento y reputación, además, contribuye a mantener la confianza de los clientes y la credibilidad de la organización en el mercado, por otro lado, en la vida cotidiana, la seguridad informática se vuelve cada vez más relevante debido al uso generalizado de dispositivos digitales y la conexión a internet en múltiples aspectos de nuestra rutina diaria, un plan de acción bien diseñado nos permite proteger nuestra información personal y privacidad contra posibles amenazas cibernéticas,

En la vida cotidiana, la **protección de la información personal** es fundamental, saber crear contraseñas seguras y aplicar autenticación de dos factores evita accesos indebidos a cuentas bancarias, redes sociales o correos electrónicos, por ejemplo: configurar contraseñas robustas en aplicaciones móviles previene el robo de datos al perder un celular, en caso de perder

el teléfonos o sufrir un robo a mano armada al delincuente le costara más esfuerzo acceder a datos de alta delicadeza, así como previene el fraude digital.

La capacidad de reconocer correos de phishing o enlaces sospechosos reduce el riesgo de ser víctima de estafas, al saber identificar un correo falso que suplanta a un banco antes de proporcionar datos personales.

De igual manera, crear un respaldo y continuidad de la información es vital, el saber usar herramientas de respaldo como Google Drive o Acronis Backup garantiza que documentos importantes (fotos, tareas, comprobantes, certificados) no se pierdan ante fallas técnicas, como un ejemplo básico es el simple hecho de recuperar una tesis universitaria desde la nube tras el formateo inesperado de la computadora.

En la vida laboral actual existe una mayor competitividad profesional, se valoran a los empleadores que saben implementar medidas de seguridad, ya que reducen riesgos en la organización, por decidir un solo ejemplo, un analista de TI que configura VLANs y firewalls protege los sistemas de la empresa frente a intrusiones externas, al tener la capacidad de respuesta ante incidentes, porque conoce herramientas como Malwarebytes o Snort IDS que permite detectar y responder rápidamente a amenazas con la ayuda un técnico de soporte logra aislar un malware antes de que afecte toda la red corporativa, asegurando la continuidad operativa.

El dominio de estrategias es sumamente importante implementarlas, como por ejemplo la copia de seguridad 3-2-1 garantiza que los procesos de la empresa continúen sin interrupciones, dentro de la vida laboral en una firma contable, los respaldos automáticos permiten seguir trabajando aún después de un corte eléctrico o un ataque de ransomware.

Aprender y aplicar estas habilidades fortalece la autonomía digital en la vida diaria y

refuerza la credibilidad profesional en el ámbito laboral, desde proteger datos personales hasta implementar planes de seguridad en una organización, estas competencias convierten al individuo en un agente capaz de prevenir, mitigar y responder de manera efectiva a los desafíos de la era digital.

En conclusión, el aprendizaje de habilidades en seguridad informática representa un puente entre la teoría y la práctica, con un impacto directo en la vida cotidiana y en el entorno laboral, no se trata únicamente de instalar programas o seguir protocolos, sino de desarrollar una cultura de prevención y conciencia digital que permita anticiparse a los riesgos y enfrentar los desafíos de un mundo interconectado, al aplicarlas, las personas no solo protegen su información personal, sino que también se convierten en agentes de cambio dentro de las organizaciones, aportando valor y asegurando la estabilidad tecnológica en una era donde la información es el recurso más valioso.

Referencias:

Acronis True Image (antes Cyber Protect Home Office) - Copia de seguridad integrada y protección contra malware. (s. f.-a). Acronis. https://www.acronis.com/es/products/true-image/

Acronis True Image (antes Cyber Protect Home Office) - Copia de seguridad integrada y protección contra malware. (s. f.-b). Acronis. https://www.acronis.com/es/products/true-image/

BatteryCare - download. (s. f.). https://batterycare.net/en/download.html

Cid, M. (2024, 18 junio). 192.168.1.1 o 192.168.0.1: cómo entrar en el router y configurar la conexión. Xataka Móvil. https://www.xatakamovil.com/tutoriales/192-168-1-1-como-entrar-en-el-router-y-configurar-la-conexion

Compartir conexiones móviles en Android mediante un punto de acceso o la función de conexión compartida - Ayuda de Android. (s. f.). https://support.google.com/android/answer/9059108?hl=es

Google Home - Apps on Google Play. (s. f.). https://play.google.com/store/apps/details?id=com.google.android.apps.chromecast.app&pli=1

Herramientas de análisis del tráfico de red. (s. f.).

Malwarebytes. (2025, 3 febrero). Malwarebytes Gratis: Antivirus gratuito 2025 | 100% gratuito y de fácil instalación. https://www.malwarebytes.com/es/mwb-download

Porto, J. P. (2023, 30 octubre). Ciberseguridad - Qué es, historia, origen y ejemplos. Definición.de. https://definicion.de/ciberseguridad/

Sign in - Google Accounts. (s. f.). https://keep.google.com/u/0/

SNORT - Network Intrusion Detection & Prevention System. (s. f.). https://www.snort.org/

Tenable Nessus Essentials Vulnerability Scanner. (s. f.). Tenable®. https://es-la.tenable.com/products/nessus/nessus-essentials

UNIDAD 3 Configuración del Ruter. (s. f.). Vimeo. https://vimeo.com/611217188/9f83380a29

Video conferencing, web conferencing, webinars, screen sharing. (s. f.-a). Zoom. https://academiaglobal-mx.zoom.us/rec/play/yB3gFUhR6wB9TEdos7BdwZzKW0OVvjaHz99jTBBleDGe4ytgWLbPPD1PGlPGi1HMJSHsWYsjsRgeQgx0.SPqgR0l3OG6tpBJR?eagerLoadZvaPages=sidemenu.billing.plan_management&accessLevel=meeting&canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FQqNd34qtzPbhEV0wubkdwWqAzkiAC5mqW4ntsiDUvNzlYkZivO3E21aODjF3FiIo.W7OAryYHFGMJeEtF

Video conferencing, web conferencing, webinars, screen sharing. (s. f.-b). Zoom. https://academiaglobal-mx.zoom.us/rec/play/SLDjQaRhGqYifRnNxLKdxxlVKZW60C9cClNINICcPmQUgbId6fQE0KgV3fV-bSofnWaSMJV0Fikg8Yj_.61EZKNXmcC8HNYTH?eagerLoadZvaPages=sidemenu.billing.plan_management&accessLevel=meeting&canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FSPjM56MonfOvcPHkWxnE_fmCLvRqXmo02o6dHyb19KAvZi-PGZx3fU61ljycEqB5.OYh6kMfigK3Azuu5

Video conferencing, web conferencing, webinars, screen sharing. (s. f.-c). Zoom. https://academiaglobal-mx.zoom.us/rec/play/SLDjQaRhGqYifRnNxLKdxxlVKZW60C9cClNINICcPmQUgbId6fQE0KgV3fV-bSofnWaSMJV0Fikg8Yj_.61EZKNXmcC8HNYTH?eagerLoadZvaPages=sidemenu.billing.plan_management&accessLevel=meeting&canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FSPjM56MonfOvcPHkWxnE_fmCLvRqXmo02o6dHyb19KAvZi-PGZx3fU61ljycEqB5.OYh6kMfigK3Azuu5

Video conferencing, web conferencing, webinars, screen sharing. (s. f.-d). Zoom. https://academiaglobal-mx.zoom.us/rec/play/uF6UBy1_AEc7zcvS4R4lGh-lToY2QvD-tt9T31p5GWL_dTpfeB-Gs-tJB1Xz8dx0S4n734ZEA6l0_6ur.K3ojZTRWloep6eDI?eagerLoadZvaPages=sidemenu.billing.plan_management&accessLevel=meeting&canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FUTS-2zbbPx6124MVQ3Y1ZGoeyBXUe_kee8Y4XAt2ZHxvHrhw9ZdgeWeWT5ANyhyu.ukXpdmnSVKB1wcVN

[Windows 11/10] Encriptación del dispositivo (BitLocker) | Soporte técnico oficial | ASUS. (2022a, septiembre 1). Soporte Técnico Oficial | ASUS. https://www.asus.com/cl/support/faq/1044341/

[Windows 11/10] Encriptación del dispositivo (BitLocker) | Soporte técnico oficial | ASUS. (2022b, septiembre 1). Soporte Técnico Oficial | ASUS. https://www.asus.com/cl/support/faq/1044341/

[Windows 11/10] Encriptación del dispositivo (BitLocker) | Soporte técnico oficial | ASUS México. (2022a, septiembre 1). Soporte Técnico Oficial | ASUS México. https://www.asus.com/mx/support/faq/1044341/

[Windows 11/10] Encriptación del dispositivo (BitLocker) | Soporte técnico oficial | ASUS México. (2022b, septiembre 1). Soporte Técnico Oficial | ASUS México. https://www.asus.com/mx/support/faq/1044341/