

Proyecto Final - Etapa 3 - Plan de Acción

Seguridad Informática I

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: José Luis Pacheco González

Fecha: 14 de septiembre de 2024

Índice

Introducción	3
Descripción	4
Justificación	5
Desarrollo.....	6
• Selección de software.....	6
• Plan de acción	7
• Práctica de plan de acción.....	11
• Evaluación.....	12
Conclusión	14
Referencias.....	15

Introducción

El proyecto final tiene como objetivo presentar un plan de acción integral para fortalecer la seguridad informática de una institución educativa ubicada en la costa de Veracruz. Dado el contexto actual, en el que la institución carece de un departamento de TI formal y su infraestructura tecnológica muestra vulnerabilidades significativas, se ha desarrollado un plan basado en las actividades 1 y 2 del curso, enfocadas en el análisis de amenazas y vulnerabilidades.

A través de un análisis exhaustivo de los sistemas, la infraestructura física y las prácticas de seguridad, se identificaron amenazas lógicas, físicas y humanas que podrían comprometer la integridad de los datos y la operación cotidiana de la institución. Además, se diagnosticaron vulnerabilidades en la comunicación y el almacenamiento de información crítica.

El plan propone soluciones prácticas y específicas, como la implementación de herramientas gratuitas y eficientes, por ejemplo, VirusTotal, además de la capacitación del personal administrativo y docente para cubrir las necesidades de seguridad. Asimismo, se presentan recomendaciones de mejora en el control de accesos, el uso de contraseñas seguras, y la protección de la red interna.

Descripción

La actividad plantea el desafío de aplicar los conocimientos adquiridos en las actividades previas, enfocándose en la implementación de soluciones para las amenazas y vulnerabilidades identificadas. Después de realizar un análisis detallado de los factores de riesgo en la actividad 1 y proponer recomendaciones en la actividad 2, ahora es necesario diseñar un plan de acción concreto que permita resolver esos eventos de manera efectiva.

El plan debe abordar las principales incidencias detectadas, siguiendo un enfoque estructurado que incluya pasos específicos para aplicar las medidas recomendadas, como el uso de herramientas de seguridad adecuadas y la adopción de buenas prácticas de ciberseguridad en la institución educativa.

Además, es esencial explorar las herramientas de seguridad disponibles para seleccionar las más adecuadas a las necesidades identificadas en el análisis previo. La navegación entre estas herramientas y la revisión de los recursos audiovisuales del curso ayudarán a encontrar soluciones que se ajusten a las características y limitaciones del entorno escolar.

Justificación

El proyecto se basa en la necesidad urgente de proteger la infraestructura tecnológica de la institución educativa, dada la falta de un departamento de TI formal y la exposición a múltiples amenazas y vulnerabilidades. El análisis realizado en las actividades 1 y 2 ha identificado riesgos significativos tanto a nivel lógico, como físico y humano, los cuales comprometen la seguridad de la información y la operatividad de la institución. Estos riesgos incluyen el uso de contraseñas débiles, software no verificado, acceso no controlado a la red y la falta de mecanismos de detección y respuesta a incidentes.

Este plan de acción es esencial para mitigar las vulnerabilidades detectadas y garantizar que las operaciones diarias de la institución no se vean interrumpidas por fallas de seguridad. Además, se busca mejorar la cultura de ciberseguridad entre el personal docente y administrativo, quienes, dada la ausencia de un equipo de TI especializado, deben asumir un papel activo en la implementación de medidas de seguridad.

Desarrollo

- **Selección de software**

1. **Snort:** Sistema de detección y prevención de intrusiones que analiza el tráfico de red y detecta actividades sospechosas.
2. **Cisco Umbrella:** Solución basada en la nube para bloquear el acceso a sitios web no deseados y proteger contra amenazas en línea.
3. **pfSense:** Firewall y router de código abierto, permite la configuración detallada de reglas de tráfico y características de seguridad.
4. **Bitdefender Premium:** Antivirus con capacidades avanzadas de protección, escaneo en tiempo real y prevención de amenazas.
5. **Cisco Catalyst:** Switches gestionables para crear y administrar VLANs, mejorando la seguridad y el rendimiento de la red.
6. **AppLocker:** Herramienta de Windows para gestionar qué aplicaciones pueden ejecutarse, creando políticas de seguridad.
7. **VirusTotal:** Servicio en línea para analizar archivos y URLs en busca de malware y verificar su seguridad.
8. **Unifi Ubiquiti:** Solución de red para configurar el cifrado WPA3 y gestionar el acceso a la red Wi-Fi.
9. **OpenVPN:** Solución de VPN para cifrar comunicaciones externas y asegurar el acceso remoto.
10. **SSL/TLS:** Protocolos para cifrar las comunicaciones internas y proteger la integridad de los datos en tránsito.

Plan de acción

Uso de VirusTotal

VirusTotal es una plataforma en línea que analiza archivos y URLs con más de 70 motores antivirus, lo que permite detectar malware y amenazas que podrían pasar desapercibidas con un solo software antivirus.

Auditoría de software existente:


Verificar los programas instalados, especialmente aquellos descargados de fuentes no confiables (como el sistema de control en el servidor 2).

Los archivos ejecutables del software sospechoso se suben a VirusTotal para su análisis, permitiendo identificar posibles amenazas.

Verificación de URLs:

Antes de descargar nuevos programas, el personal puede analizar las URLs en VirusTotal para comprobar si el sitio es seguro, previniendo infecciones desde la web.

Interpretación de resultados:



VirusTotal genera un informe detallado; si algún motor antivirus marca el archivo como malicioso, se debe eliminar o evitar instalar. Si no se encuentran amenazas, se puede continuar su uso con precaución.

Política de uso continuo:

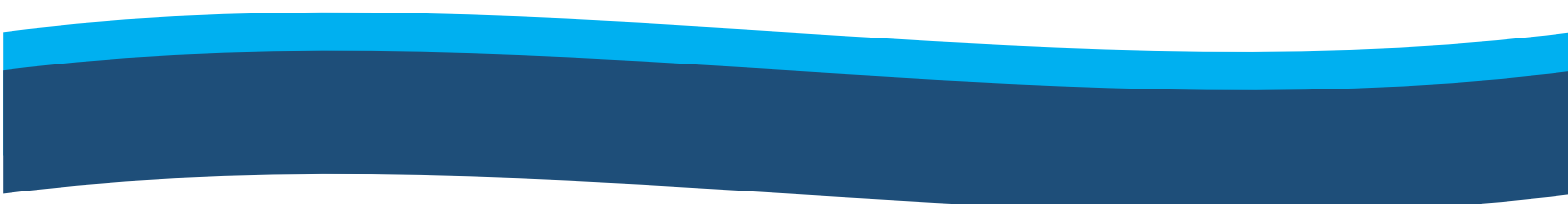
Se recomienda que el Docente de Informática implemente una política donde todo nuevo software sea revisado por VirusTotal, asegurando que solo programas verificados se instalen en la red de la institución.

Ventajas:

Detección múltiple: Mayor probabilidad de identificar malware gracias a la variedad de motores antivirus.

Prevención: Verificación rápida de archivos y sitios antes de usarlos.

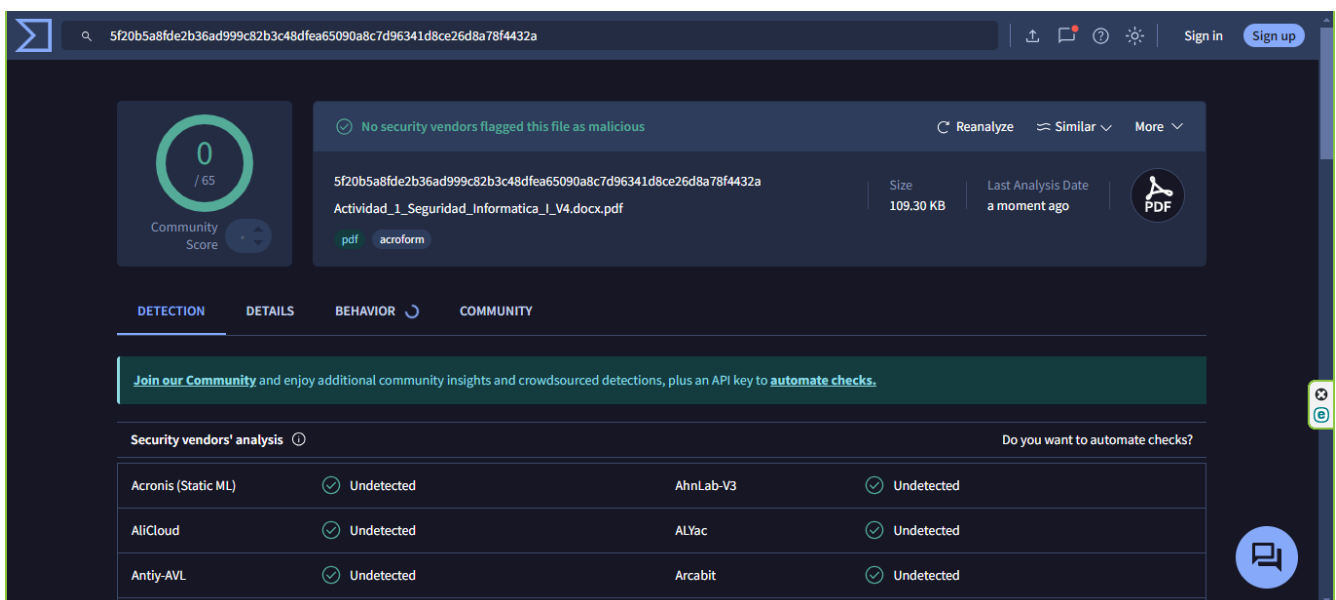
Fácil uso: No requiere instalación y permite obtener resultados de manera inmediata.



A continuación, se agregan capturas de la herramienta, aquí se muestra la interfaz inicial, donde podemos ver las opciones para analizar un archivo y una url.



En esta otra se realizo el análisis de un pdf, el cual no representa ningún tipo de amenaza.



En esta última captura se analizó el enlace de una página poco confiable para descargar la herramienta app locker, el cual muestra una alerta sospechosa.

https://applocker.softonic.com/

0 / 96
Community Score

✓ No security vendors flagged this URL as malicious

Reanalyze Search Graph API

https://applocker.softonic.com/
applocker.softonic.com

Status: 406
Last Analysis Date: 28 days ago

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ Do you want to automate checks?

URLQuery	ⓘ Suspicious	Abusix	✓ Clean
Acronis	✓ Clean	ADMINUSLabs	✓ Clean
AllLabs (MONITORAPP)	✓ Clean	AlienVault	✓ Clean

Práctica de plan de acción

Semana	Incidencia	Solución	Fechas	Herramienta	Encargado
1	Uso de contraseñas débiles por los usuarios.	Establecer una política de contraseñas seguras que incluya: mínimo 8 caracteres, uso de mayúsculas, minúsculas, números y símbolos. Forzar cambio de contraseña cada 90 días y habilitar autenticación multifactor (MFA) en los accesos críticos.	6 - 10 septiembre 2024	LastPass (gestor de contraseñas para usuarios), Google Authenticator (MFA para accesos).	Coordinador de Desarrollo Académico: Responsable de supervisar y aplicar la política de contraseñas con los docentes y alumnos.
	Acceso no autorizado a equipos para actividades personales (redes sociales, correo personal, etc.).	Implementar reglas en el firewall que bloqueen el acceso a sitios no autorizados durante horario laboral y monitorear el tráfico de red en busca de comportamientos inusuales.	11 - 14 septiembre 2024	Snort (sistema de detección de intrusiones para monitorear tráfico), Cisco Umbrella (control de acceso a internet).	Encargado del Centro de Cómputo: Gestiona la implementación de las reglas de acceso a internet en los equipos.
2	Falta de firewall habilitado en la red.	Configurar el firewall interno y establecer reglas específicas para permitir solo el tráfico necesario, bloquear puertos no esenciales y activar funciones de detección de intrusiones en tiempo real.	15 - 17 septiembre 2024	pfSense (configuración de firewall robusto con reglas personalizadas y monitoreo de tráfico).	Encargado del Centro de Cómputo: Se asegura de que el firewall se configure correctamente y lo monitorea periódicamente.
	Antivirus gratuito y obsoleto, no adecuado para amenazas avanzadas.	Migrar a una solución de antivirus empresarial con análisis en tiempo real, protección contra malware avanzado y capacidad de análisis de comportamiento.	18 - 19 septiembre 2024	Bitdefender Premium (antivirus con protección avanzada, análisis en tiempo real y prevención de amenazas).	Secretario Administrativo: Gestiona la compra e implementación del antivirus en todos los equipos de la institución.
3	Servidor espejo vulnerable en la misma red que los usuarios.	Segmentar la red mediante la creación de VLANs dedicadas para servidores y usuarios, lo que limita el acceso entre ambos y protege los servidores de posibles ataques desde los dispositivos de los usuarios.	20 - 25 septiembre 2024	Cisco Catalyst (switches gestionables para VLANs), pfSense (configuración de VLANs en el firewall).	Encargado del Centro de Cómputo: Realiza la configuración de VLANs para proteger los servidores.
	Uso de software descargado de fuentes no confiables sin verificación previa.	Auditar todos los programas instalados y eliminar aquellos que no cuenten con una fuente verificada. Implementar una lista blanca de aplicaciones permitidas para evitar la instalación de software no autorizado.	26 - 27 septiembre 2024	AppLocker (herramienta para gestionar aplicaciones permitidas en Windows), VirusTotal (verificación de archivos).	Docente de Informática: Revisa y audita el software instalado en los equipos y elimina programas no verificados.
4	Red Wi-Fi insegura con acceso limitado a WPA2 y sin autenticación adicional.	Configurar la red Wi-Fi con cifrado WPA3 y habilitar una autenticación de dos pasos para los accesos. Además, establecer una red separada para invitados para evitar el acceso a la red principal.	28 septiembre - 2 octubre 2024	Unifi Ubiquiti (configuración de red con cifrado WPA3 y control de acceso), Google Authenticator (MFA para usuarios).	Encargado del Centro de Cómputo: Responsable de configurar la seguridad de la red Wi-Fi.
	Falta de cifrado en las comunicaciones internas, lo que las hace vulnerables a interceptaciones.	Implementar cifrado SSL/TLS en todas las conexiones internas y configurar una VPN para los accesos remotos, asegurando que toda la comunicación esté cifrada de extremo a extremo.	3 - 5 octubre 2024	OpenVPN (VPN para cifrar comunicaciones externas), SSL/TLS (para proteger las comunicaciones internas).	Secretario Administrativo: Coordina la implementación del cifrado en las comunicaciones internas y remotas.

Evaluación

VirusTotal fue seleccionada como herramienta clave para este proyecto debido a su capacidad de analizar archivos y Urls utilizando múltiples motores antivirus, lo que permite una detección más amplia de posibles amenazas y malware que podrían no ser detectados por una sola solución antivirus. Es una plataforma gratuita, accesible y fácil de usar, lo que la convierte en una excelente opción para una institución educativa con limitaciones de recursos y sin un departamento de TI especializado.

Amenazas y Vulnerabilidades que VirusTotal Ayuda a Resolver

Amenazas lógicas:

Software malicioso descargado de fuentes no confiables: En el escenario presentado, se municiona un sistema de control descargado de Internet, del cual se desconoce la fuente. Permite analizar este software en busca de malware antes de ejecutarlo, previniendo infecciones que comprometan la seguridad de los datos.

Archivos infectados: En una red donde el uso personal de los equipos no está restringido, como el acceso a redes sociales o correo electrónico, los archivos pueden infectarse fácilmente a través de descargas inseguras. Detecta estos archivos maliciosos y evita que se propaguen.

Vulnerabilidades de almacenamiento:

Instalación de software sin verificación previa: Ayuda a mitigar el riesgo de instalar programas que podrían contener malware, evitando que comprometan los servidores o los equipos de la red.

Vulnerabilidades de comunicación:

Enlaces maliciosos en correos electrónicos o sitios web: También permite verificar URLs, por lo que los enlaces sospechosos enviados por correo electrónico o accedidos en la red pueden ser analizados antes de que los usuarios los abran, evitando ataques de phishing o la descarga de malware desde sitios inseguros.

Conclusión

Este proyecto ha logrado identificar, analizar y proponer soluciones a las amenazas y vulnerabilidades de seguridad informática presentes en la institución educativa. A través de las actividades 1 y 2, se diagnosticaron riesgos relacionados con la infraestructura tecnológica, las prácticas de los usuarios y la falta de mecanismos de protección adecuados. En respuesta, se desarrolló un plan de acción enfocado en mitigar estos riesgos mediante el uso de herramientas accesibles, como VirusTotal, y la implementación de medidas básicas de ciberseguridad.

El plan propuesto tiene como objetivo garantizar la protección de los datos y la continuidad operativa de la institución, abordando tanto vulnerabilidades lógicas como físicas. Además, al involucrar al personal docente y administrativo en la aplicación de estas soluciones, se fomenta una cultura de ciberseguridad que es fundamental para el éxito del proyecto, especialmente ante la ausencia de un equipo de TI especializado.

Este enfoque práctico y adaptado a las necesidades del entorno no solo permite resolver los problemas identificados, sino que también prepara a la institución para enfrentar futuros desafíos en el ámbito de la seguridad informática.

Referencias

Ciberseguridad en los colegios, una inversión ineludible. (2023, January 24). Grupo AE; Grupo AE S.L. <https://grupo-ae.com/ciberseguridad-colegios/4899063377/>

Flores, V. (2023, June 6). Hablemos de ciberseguridad: Recomendaciones para instituciones de educación superior. Proctorizer. <https://proctorizer.com/ciberseguridad-para-instituciones-de-educacion-superior/>



Enlace Github