

Actividad 3 - Plan de acción

Seguridad Informática I

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: José Domingo Reyes Arroyo

Fecha: 5 de enero de 2024

1 Índice

1	Índice	2
1	Introducción.....	3
2	Descripción.....	3
3	Justificación.....	4
4	Desarrollo	5
4.1	Selección de Software	5
4.2	Plan de acción.....	9
4.3	Practica de plan de acción	11
4.4	Evaluación.....	11
5	Conclusión.....	14
6	Referencias	15

1 Introducción

Para realizar el proyecto final, después de haber evaluado en la actividad 1 las vulnerabilidades, que se define como una debilidad existente en un sistema, red o aplicación que puede ser utilizada por una persona malintencionada a menudo llamados Hacker, con la intención de comprometer la seguridad de dicho sistema y las amenazas, que son propiamente la acción maliciosa encaminada a aprovechar esa vulnerabilidad para hacer daño a ese sistema o a una empresa en general. Para la segunda actividad se tomó en cuenta el comportamiento de los ciberataques de los últimos años y de la actualidad en que podemos estar expuestos a ataques personales como ingeniería social, colaboradores malintencionados, propagación de datos confidenciales, extravió o hurto de dispositivos personales, poco control en las empresas o dependencias y para esto se propuso hacer una planificación, mejora o implementación que eliminara o disminuyera las amenazas y vulnerabilidades detectadas. Por lo cual y para continuar con este proyecto final se realizará la ejecución de dichas planeaciones, mejoras e implementaciones para garantizar que se eliminen las amenazas y vulnerabilidades detectadas.

2 Descripción

Así pues, para finalizar este proyecto se realizará la ejecución de dichas mejoras propuestas para resolver los eventos detectados siguiendo un cronograma de actividades donde se identificarán las herramientas que se han de utilizar para la elaboración del plan de acción para este proyecto final, para la elaboración del plan de acción se dará respuestas a las preguntas

principales que son: ¿Qué se realizará para resolver estas incidencias?, ¿Cuándo se realizará? y ¿Con que se realizará? Con la finalidad realizar posteriormente el cronograma de dichas actividades definiendo así la estructura general del plan de acción, con lo cual se eliminarán estas vulnerabilidades y amenazas. Después de la ejecución del plan de acción y del cronograma se enviará evidencia que pruebe que la ejecución de estas herramientas es la mas viable para eliminar las situaciones encontradas dentro de la institución y evitar que esta sea o este a merced de ataques cibernéticos o físicos y ponga en peligro la integridad de los estudiantes, docentes y administrativos.

3 Justificación

Considerando dentro de la institución que la seguridad de la información y la integridad de las personas que trabajan y estudian en la institución, son la principal prioridad de esta, se considera de suma importancia que como analista de seguridad desarrollemos propuestas de mejora e implementación de sistemas de seguridad tanto físicos como informáticos que garanticen la seguridad de la información que maneja la institución y sobre todo garantice la integridad de las personas que trabajan o estudian en dicha institución. Ejecutando el proyecto final aseguraremos a la institución que las propuestas de mejora aquí descritas, son la mejor opción para disminuir el riesgo y garantizar la seguridad de la información y la integridad personal de los alumnos, docentes y administrativos.

Esta es la razón más importante que como encargados de la seguridad informática debemos comprender y debemos poner especial atención en esta para evitar posibles fraudes, intrusiones, bloqueos y eliminación de información, así como el hackeo de equipos, pero sobre todo lo mas importante, debemos entender que, como analistas de seguridad, debemos estar muy atentos de cada mínimo detalle para proceder adecuadamente y cuidar la integridad de toda la institución.

4 Desarrollo

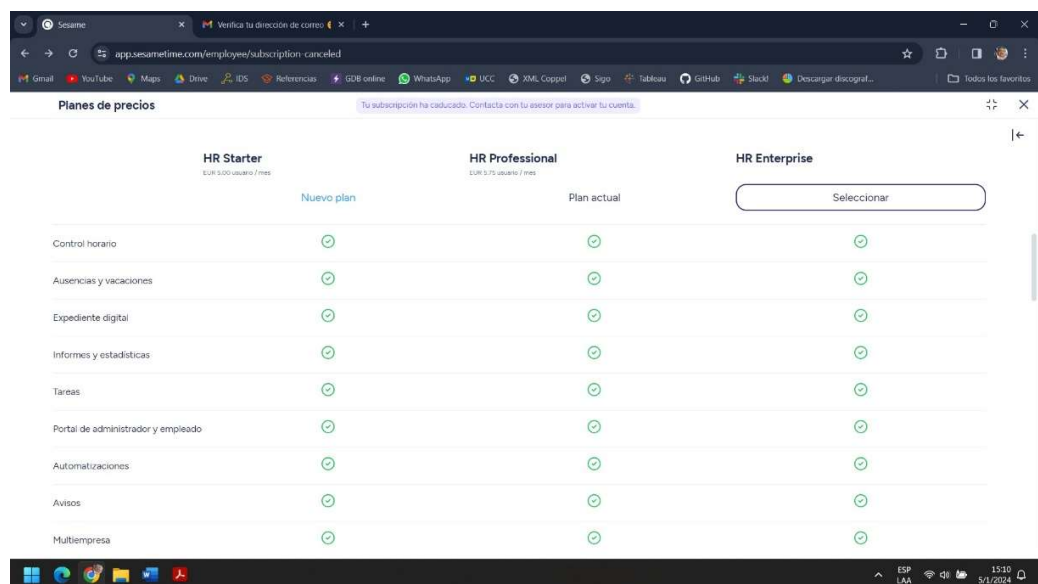
Para este proyecto final se presenta la tabla de vulnerabilidades y amenazas de ejecución requeridos para su implementación:

4.1 Selección de Software

Para eliminar la mayoría de las vulnerabilidades encontradas, se sugiere el uso de 2 herramientas específicas que ya se han testeado con anterioridad en proyectos anteriores y que pueden ayudar a la institución a eliminar dichas vulnerabilidades, estas herramientas son:

Primeramente un software en línea que permite detectara los empleados que ingresan y salen de la institución, así como también permite a los empleados registrarse a través de su dispositivo móvil y mientras estos lo hacen desde su aplicación, permite a la aplicaciones monitorear en

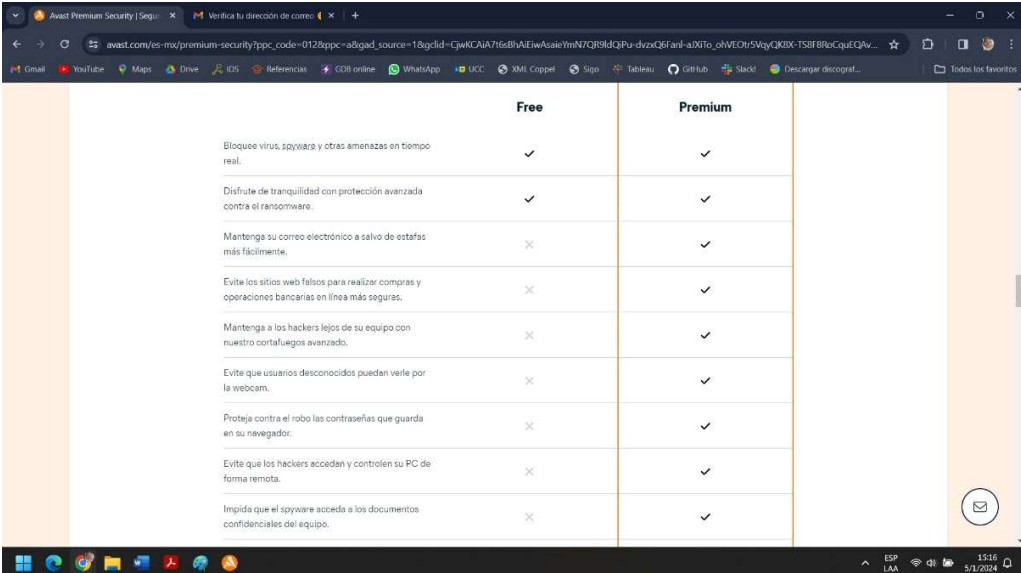
tiempo real si los empleados están realmente dentro de la empresa, en cuestiones de seguridad, en caso de algún desastre natural como inundación, sismo, huracán, etc. La aplicación proporcionara un escanea en tiempo real para detectar si alguien esta dentro del edificio en esos casos imprevistos para poderle salvar la vida o incluso para hacer una correcta evacuación del edificio. A continuación, se proporciona evidencia de la herramienta:



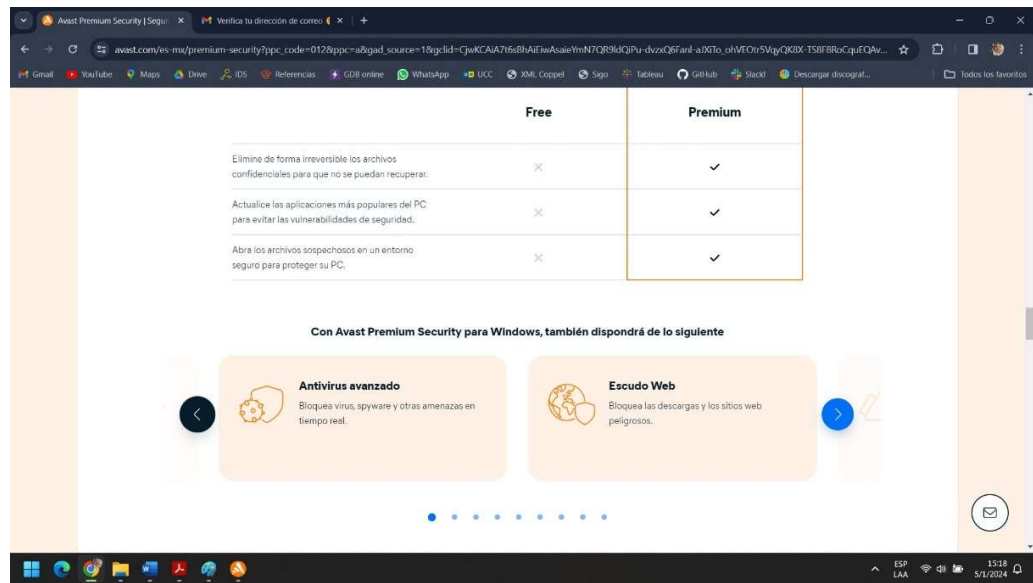
Esta es la pagina de la herramienta la cual proporcionara todos los requerimientos que en ella especifican.

A continuación, para la segunda herramienta se propone un antivirus muy poderoso que tiene incluso versión free y versión premium, para su versión free es una herramienta muy conocida y selecta por mas del 60% de usuario de computadoras, este es un antivirus del cual se muestra su opción premium que seria de gran ayuda para administrar la información de los equipos de cómputo de la institución:

Esta herramienta incluye las protecciones que se muestran a continuación según su versión premium:



	Free	Premium
Bloquee virus, spyware y otras amenazas en tiempo real.	✓	✓
Disfrute de tranquilidad con protección avanzada contra el ransomware.	✓	✓
Mantenga su correo electrónico a salvo de estafas más fácilmente.	✗	✓
Evite los sitios web falsos para realizar compras y operaciones bancarias en línea más seguras.	✗	✓
Mantenga a los hackers lejos de su equipo con nuestro cortafuegos avanzado.	✗	✓
Evite que usuarios desconocidos puedan verle por la webcam.	✗	✓
Proteja contra el robo las contraseñas que guarda en su navegador.	✗	✓
Evite que los hackers accedan y controlen su PC de forma remota.	✗	✓
Impida que el spyware acceda a los documentos confidenciales del equipo.	✗	✓



Aparte de estas protecciones también incluye: Antivirus avanzado, escudo web, alertas de hackeo, inspector de red, sitios web legítimos, modo de banco, cortafuegos avanzado, escudo de ransomware, escudo de datos confidenciales, escudo de web cam, destructor de datos, actualizador de software automático, modo pasivo, modo no molestar, actualización en tiempo real, protección de contraseñas, escudo de acceso remoto y más.

Con estas herramientas se puede disminuir o eliminar la mayoría de las eventualidades encontradas que son susceptibles a amenazas.

4.2 Plan de acción

A continuación, se presenta un plan de acción donde se retoma la tabla de la actividad 1 y 2 para contestar a las preguntas antes descritas, el que, como y cuando:

Factores	Amenazas/Vulnerabilidades	Solución	Herramientas	Página	Fechas
Ubicación	Se encuentra en la ciudad de Veracruz cerca de la costa	se recomienda implementar un sistema de seguridad ante inundaciones, promover que los equipos de computo sean resguardados en el segundo piso.	Sesame con la geolocalización ayuda a saber donde esta el personal	https://www.sesamehr.mx/	8 al 14 de enero 2024
Infraestructura	Tiene 3 departamentos, 1 centro de computo y 1 biblioteca, cuenta con 2 pisos y 18 salones	cambiar la estructura de los departamentos, donde los servidores y equipos de computo de escritorio se ubiquen en el segundo piso y tener un área de resguardo para los equipos portátiles en el mismo piso por cuestiones de inundación	no hay herramienta, la sugerencia es cambiar los equipos al segundo piso, modificación de planos		15 al 21 de enero 2024
Movilidad	Tiene 4 escaleras y un ascensor	colocar letreros para rutas de evacuación en escaleras, ubicando la vía mas corta, para acceso a los salones recomendar el uso de la escalera mas cercana al aula para evitar el Axeso de flujo de estudiantes, el ascensor solo usarlo para personas discapacitadas o para cuando se transporta material pesado	Sesame con la geolocalización ayuda a saber donde esta el personal ayuda a evacuar mas rápido el edificio y saber sino hay personal adentro mientras esta el desastre natural	https://www.sesamehr.mx/	8 al 14 de enero 2024
Accesos al edificio	Presenta 1 entrada principal, 2 laterales y una salida posterior a la cancha principal	dejar solo un acceso a las instalaciones, el cual se sugiere la entrada principal en caso de contar con 2 turnos, proponer la salida posterior, mientras el acceso para el segundo turno se realiza por el acceso principal, registrando a toda persona que entra o sale del edificio, contratar seguridad para acceso principal y salida posterior.	Sesame ayuda a controlar las entradas y salidas y proporciona un reporte cada que se requiera	https://www.sesamehr.mx/	8 al 14 de enero 2024
Entrada/Salida de personal	Los docentes se registran en una libreta y los administrativos con tarjeta	implementar que todos los docentes y administrativos cuenten con tarjeta o se implemente acceso por huella o chip en tarjeta de identificación, esta implementación también permitiría que el acceso de los alumnos sea por este medio para tener mas control de la cantidad de personas que alberga.	Sesame ayuda a controlar las entradas y salidas y proporciona un reporte cada que se requiera	https://www.sesamehr.mx/	8 al 14 de enero 2024
Seguridad en áreas financieras	El área administrativa y financiera no cuentan con alarma de seguridad	instalar alarmas de seguridad para acceso, ya sea con huella o clave (panel digital) para las áreas de riesgo	Sesame ayuda a controlar las entradas y salidas y proporciona un reporte de quienes acceden a dichas áreas	https://www.sesamehr.mx/	8 al 14 de enero 2024
seguridad ante contingencias	Cuenta con 2 extintores clase A y 1 clase B	contratar proveedor de extintores e hidrantes, quien hará una planeación de los extintores e hidrantes que sean requeridos para todo el edificio, es mucho mejor con proveedor ya que se encargan de toda la planeación y garantía de los equipos así como su recarga y mantenimiento cada año	no hay herramienta, la sugerencia es contratar proveedor para temas de extinguidores e hidrantes, además de proponer la creación de una Unidad Interna de Protección y una Comisión de Seguridad con el mismo personal		15 al 21 de enero 2024
Salidas de emergencia	Cuenta con 1 salida de emergencia	implementar punto de reunión, el cual sea intermedio entre la entrada y la salida del edificio, para que ambas puedan fungir como salidas de emergencia, incluir en el tablero de acceso por huella o chip, la consulta de emergencia de la población total dentro del edificio para poder hacer un conteo rápido y validar si alguien no se quedo atrapado dentro del inmueble.	no hay herramienta, la sugerencia es contratar proveedor para temas de extinguidores e hidrantes, además de proponer la creación de una Unidad Interna de Protección y una Comisión de Seguridad con el mismo personal		15 al 21 de enero 2024
dispositivos de alarma	No se tiene detectores de humo, movimiento, impacto, etc.	con el mismo proveedor de extintores e hidrantes se hace la instalación de este tipo de sensores y la planificación de los que se requieren, en cuestión de los acceso se recomienda un sensor por entrada o salida para monitorear en horario no laborales si hay accesos no permitidos.	no hay herramienta, la sugerencia es contratar proveedor para temas de extinguidores e hidrantes, además de proponer la creación de una Unidad Interna de Protección y una Comisión de Seguridad con el mismo personal		15 al 21 de enero 2024
Servidores físicos	solo tiene 1 servidor	se recomienda la instalación de otro servidor para la cantidad de información que se maneja, dejar 1 exclusivo para administrativos y otro para alumnos. Implementar la creación de una base de datos en cada servidor con la información de cada docente y alumno necesarios.	Avast instalación en cada servidor para protección de la información delicada	https://www.avast.com/es-mx/premium-security#pc	2 al 7 de enero 2024
Servicio de internet	1 servicio de internet de 20 GB comercial	aumentar la capacidad del internet de comercial a empresarial para mejorar el servicio y la velocidad de transferencia.	No hay herramienta se sugiere cambio de plan de internet		15 al 21 de enero 2024
Equipos de escritorio	Cuenta con 10 equipos de escritorio	determinar la necesidad de equipos de escritorio según la cantidad de personas que trabajan en cada departamento para asegurar que cada administrativo cuente con un equipo.	Avast instalación en cada equipo de computo para protección de la información delicada	https://www.avast.com/es-mx/premium-security#pc	2 al 7 de enero 2024
Laptops	cuenta con 5 laptop	adquirir un equipo portátil para cada docente, el cual pueda ser usado tanto dentro de la institución como fuera de ella para que cada uno de los docentes pueda tener la información de los alumnos en su equipo.	Avast instalación en cada equipo de computo para protección de la información delicada	https://www.avast.com/es-mx/premium-security#pc	2 al 7 de enero 2024
Servidor espejo	cuenta con 1 servidor espejo	eliminar el servidor espejo y en su lugar contratar un servidor en la nube para tener la información respaldada en caso de alguna situación de desastre natural.	Avast instalación con cada servidor para protección de la información delicada	https://www.avast.com/es-mx/premium-security#pc	2 al 7 de enero 2024
Conexión de los equipos	en planta baja es con conexión directa al modem por cable y en planta alta Wi-Fi	eliminar la conexión directa al modem e implementar que todos los equipos se conecten a través de Wi-Fi instalando VPN para mejorar la seguridad de la información, instalar repetidores para facilitar que la señal sea la misma en cualquier punto del edificio.	Avast proporciona un cortafuegos seguro para las conexiones en red	https://www.avast.com/es-mx/premium-security#pc	2 al 7 de enero 2024
Condición de los equipos	Equipos lentos y sin espacio de almacenamiento	depurar los equipos de ser posible reiniciarlos de fabrica, para instalar software de limpieza y antivirus actualizados a todos los equipos.	Avast instalación de herramienta alterna para evitar saturación de los discos duros, viene incluida en la versión premium.	https://www.avast.com/es-mx/premium-security#pc	2 al 7 de enero 2024
Seguridad de los equipos	Usuario y contraseña básicos (Equipo-1, 1234abc)	implementar un administrador de contraseñas para implementar un usuario por departamento y una contraseña que cumpla con los requisitos de seguridad establecidos, además de generar un usuario por cada docente dependiendo de la materia y de la misma manera generar una contraseña segura	Avast permite la creación y administración de contraseñas seguras para cada equipo de computo o para cada departamento	https://www.avast.com/es-mx/premium-security#pc	2 al 7 de enero 2024

4.3 Practica de plan de acción

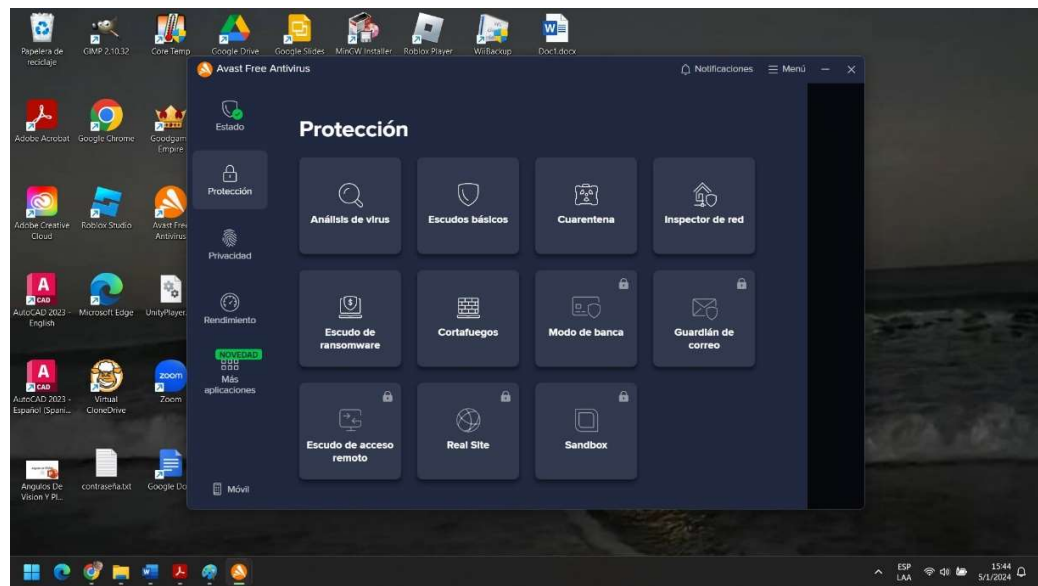
Para continuar se muestra el plan de acción en ejecución en las fechas especificadas en un cronograma de actividades:

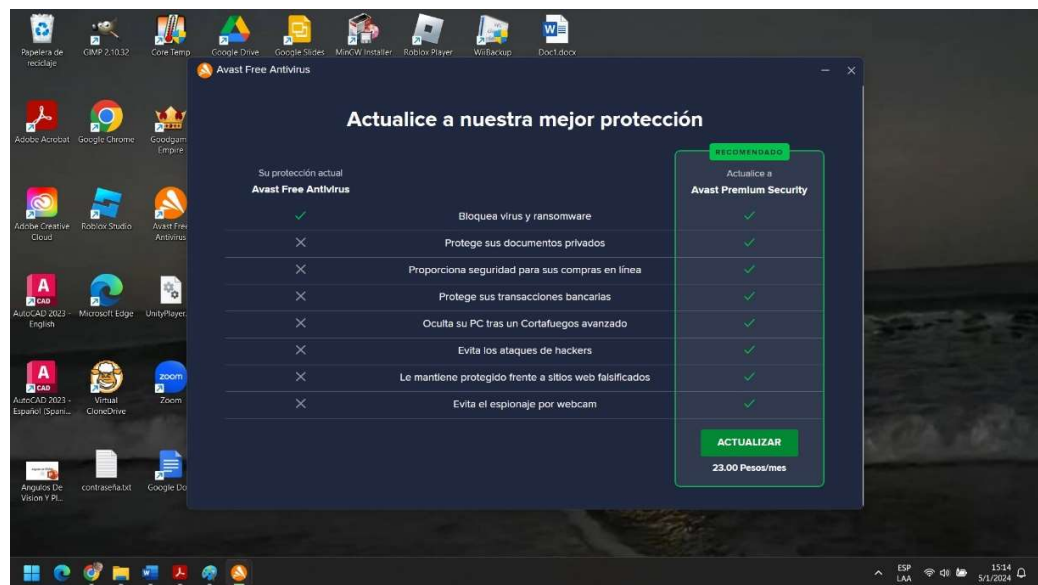
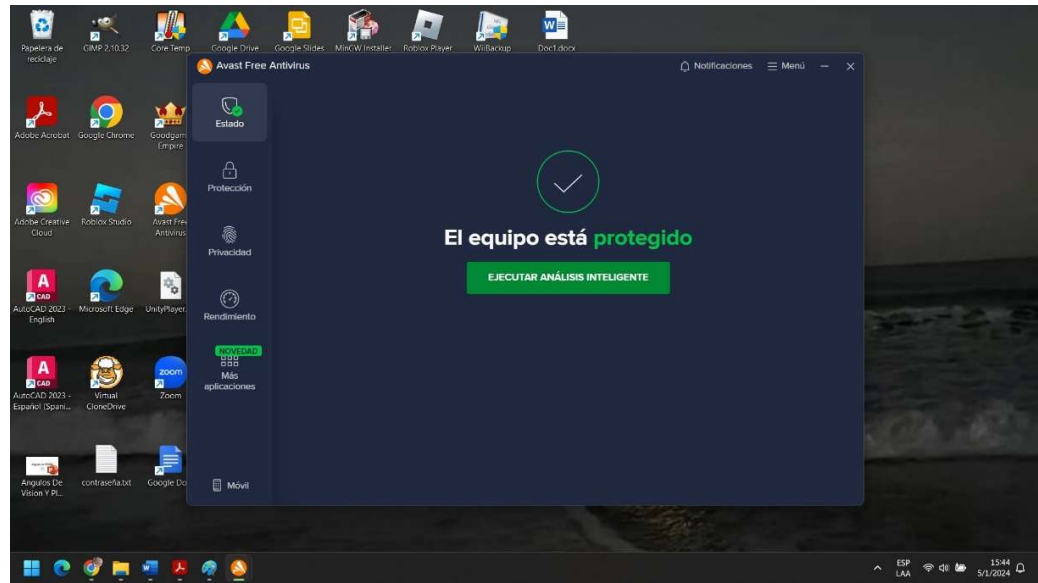
Factores	Amenazas/Vulnerabilidades	Fechas	Semana1	Semana 2	Semana 3
Ubicación	Se encuentra en la ciudad de Veracruz cerca de la costa	8 al 14 de enero 2024			
Infraestructura	Tiene 3 departamentos, 1 centro de computo y 1 biblioteca, cuenta con 2 pisos y 18 salones	15 al 21 de enero 2024			
Movilidad	Tiene 4 escaleras y un ascensor	8 al 14 de enero 2024			
Accesos al edificio	Presenta 1 entrada principal, 2 laterales y una salida posterior a la cancha principal	8 al 14 de enero 2024			
Entrada/Salida de personal	Los docentes se registran en una libreta y los administrativos con tarjeta	8 al 14 de enero 2024			
Seguridad en áreas financieras	El área administrativa y financiera no cuentan con alarma de seguridad	8 al 14 de enero 2024			
seguridad ante contingencias	Cuenta con 2 extintores clase A y 1 clase B	15 al 21 de enero 2024			
Salidas de emergencia	Cuenta con 1 salida de emergencia	15 al 21 de enero 2024			
dispositivos de alarma	No se tiene detectores de humo, movimiento, impacto, etc.	15 al 21 de enero 2024			
Servidores físicos	solo tiene 1 servidor	2 al 7 de enero 2024			
Servicio de internet	1 servicio de internet de 20 GB comercial	15 al 21 de enero 2024			
Equipos de escritorio	Cuenta con 10 equipos de escritorio	2 al 7 de enero 2024			
Laptops	cuenta con 5 laptop	2 al 7 de enero 2024			
Servidor espejo	cuenta con 1 servidor espejo	2 al 7 de enero 2024			
Conexión de los equipos	en planta baja es con conexión directa al modem por cable y en planta alta Wi-Fi	2 al 7 de enero 2024			
Condición de los equipos	Equipos lentos y sin espacio de almacenamiento	2 al 7 de enero 2024			
Seguridad de los equipos	Usuario y contraseña básicos (Equipo-1, 1234abc)	2 al 7 de enero 2024			

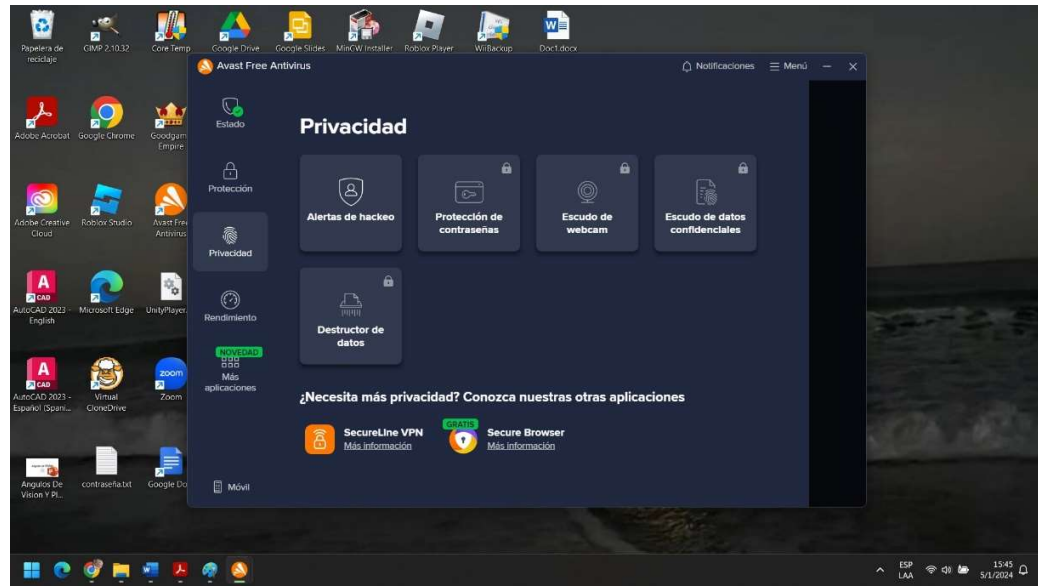
4.4 Evaluación

En esta etapa se demuestran las capacidades de la herramienta propuesta para la mejora de la seguridad informática, en el caso de la primera herramienta por ser de paga y por ser en línea no se cuenta con acceso a la misma, de la segunda herramienta se cuenta con la

instalación free, pero esta muestra las opciones premium con las cuales pudiera contar en caso de contratar:







5 Conclusión

Con el desarrollo de este proyecto se asegura la obtención de las habilidades necesarias para fungir como analista de seguridad de una empresa o institución, para detectar vulnerabilidades que puedan tener los sistemas de cualquier empresa, como ingenieros en desarrollo de software debemos estar a la par de la seguridad informática, ya que es un tema que sin duda alguna es relevante para cualquier área de la informática a la que se enfoque un ingeniero en desarrollo de software, cabe destacar que estas actividades que permiten atender temas de seguridad informática y física para cualquier situación que se pueda presentar son cruciales para el aprendizaje personal y ayudan a poder detectar cualquier situación de vulnerabilidad dentro de la empresa incluso permiten tener una visión mas amplia de cualquier situación que pueda atentar contra la seguridad personal, física y de cualquier sistema

informático, hoy en día las hackers no se enfocan solamente en sistemas operativos vulnerables, se enfocan en encontrar cualquier error en cualquier sistema operativo sea o no sea seguro, la idea es encontrar cualquier falla en los sistemas y hay quienes las usan para mejorar los sistemas y ayudar a perfeccionar el sistema operativo, pero también hay personas que se dedican a crear afectaciones en pequeña gran escala, es por ello que debemos estar preparados para cualquier situación en cuanto al tema de seguridad se refiera.

6 Referencias

De Seguridad Informática, S. (2023, 28 septiembre). *Vulnerabilidades y amenazas informáticas*. DragonJAR - Servicios de Seguridad Informática.

<https://www.dragonjar.org/vulnerabilidades-y-amenazas-informaticas.xhtml> 11

Santander, B. (s. f.). *Vulnerabilidad*. Banco Santander.

<https://www.bancosantander.es/glosario/vulnerabilidad-informatica>

Ortiz, A. E. (2020, 13 julio). ¿Qué es una amenaza informática? ¿Cómo contenerla? | Blog HostDime Latinoamérica, Servidores dedicados. *Blog HostDime*

Latinoamérica, servidores dedicados. <https://www.hostdime.la/blog/que-es-una-amenaza-informatica-como-contenerla/>

Legro, A. (2023, 29 diciembre). Ataques informáticos: causas y 12 tipos de ciberataques. *Win Empresas*. <https://winempresas.pe/blog/ataques-informaticos-causas-y-12-tipos-de-ciberataques>

What is Intrusion Prevention System? | VMware Glossary. (2023, 26 noviembre). VMware. <https://www.vmware.com/es/topics/glossary/content/intrusion-prevention-system.html>

Prevención y detección de intrusiones. (s. f.). <https://www.fortra.com/es/soluciones/seguridad-informatica/infraestructura/deteccion-y-prevencion-de-intrusiones>

Actividad subida al repositorio de GitHub: <https://github.com/drcksug/Seguridad-Informatica-I>