Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad |3| Plan de Acción.

Seguridad Informática I.

Ingeniería en Desarrollo de Software.

TUTOR: Jessica Hernández Romero.

ALUMNO: Ramón Ernesto Valdez Felix.

FECHA: 10/01/2025.

Introducción.

En esta actividad final de la materia de Seguridad Informática I, realizaremos la documentación del plan de acción de las recomendaremos de las soluciones para las vulnerabilidades presentadas en el análisis de la primera actividad, la contextualización de la actividad final es la siguiente: 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. Ya con el contexto de la actividad sin más que decir realizaremos la documentación del plan de acción para que se lleve a cabo un plan de mitigación en cualquier colegio o escuela pública de cualquier nivel que sufra de estos escenarios por no contar con ningún tipo de seguridad física o informática en el plantel.

Descripción.

En esta actividad final de la materia de Seguridad Informática I, realizaremos la documentación del plan de acción del análisis realizado al colegio de educación superior de la ciudad de Veracruz, el cual nos permitirá dar la solución o mitigar las recomendaciones de cada una de las vulnerabilidades y amenazas presentadas en dicho plantel ya que con esto daremos a conocer que afectaciones tiene el no tener ninguna tipo de seguridad física, informática y así implementar la solución de las vulnerabilidades y amenazas. Con el análisis de la información de las vulnerabilidades y amenazas que se presentan en el colegio de educación superior, realizaremos una tabla del plan de acción donde se anexara la evidencia de la solución de cada una de las recomendaciones de los riesgo o hallazgo detectado en el análisis de la actividad anterior, estos nos servirán para que cualquier plantel del pais de mexico que no cumpla con ningún tipo de acciones de seguridad físicas o informáticas puedan utilizar el material e implementar sus soluciones, así queden libres de amenazas y vulnerabilidades.

Justificación.

En esta actividad trabajaremos con la documentación del plan de acción de la solución de las vulnerabilidades y amenazas detectadas en el colegio de educación superior donde utilizaremos las documentaciones de las dos actividad anterior el cual servirá para realizar el plan de acción de las recomendar el como solucionar cada uno de los riegos o hallazgos obtenidos en el análisis creando una tabla identificando y plasmando la información de la duración del tiempo que se llevará para la implementación de solución de las vulnerabilidades y amenazas trabajadas en las actividades anteriores de la materia de Seguridad Informática I análisis y algunos puntos a tomar en cuenta para el llenado de la documentación de esta actividad que son los siguientes:

- PDF de está actividad en el portafolio GitHub.
- Anexar el archivo comprimida .zip en el portafolio de GitHub.
- Anexa link de GitHub en documento.
- Tabla del plan de acción de las recomendaciones de las amenzas y vulnerabilidades.
- 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.

Desarrollo:

En este punto realizaremos la documentación de la actividad de plan de acción del colegio de educación superior de la ciudad de Veracruz, estas información nos servirá para la entrega de la actividad de la materia en curso de Seguridad Informática I, como información adicional se realizará la mitigación o solución de las recomendaciones por cada de vulnerabilidad y amenazas detectadas en el análisis de las actividades de la materia en curso.

Link: GitHub

Selección de software.

Se anexará el listado de los software o herramientas que serán utilizados en las solución completa de la mitigación de las amenazas y vulnerabilidades presentadas en al análisis del colegio de educación superior de la ciudad de Veracruz las cuales no tiene un orden en especial.

Listado de herramientas utilizadas:
GSuite de Google (Gmail, Meet, Site y Drive).
Zoom (Videoconferencias).
IDS: AlienVault OSSIM.
IPS: Fortinet
Software House Win-PAK
Veeam Data Platform.

Plan de acción.

Se anexará la evidencia con las tablas de plan de acción, con las preguntas asignadas en la documentación: ¿Qué se realizará para resolver estas incidencias ?, ¿Cuándo se realizará?,¿Con qué se realizará?.con el análisis de vulnerabilidades y amenazas detectadas en la actividad del colegio de educación superior de la ciudad de veracruz, crearemos las tabla del plan de acción y el cronograma de solución o mitigación de cada vulnerabilidad o amenaza encontrada y así se apliquen las mejoras de la seguridad informática en el colegio.

Empleado Insatisfecho.				
	Semana 3	**Semana 2**		**Semana 1 y 2**
Incidencia	Concientización.	Canales de comunicación.	Auditoría de acceso.	Sistemas de detección de intrusiones.

Solucion	Realizar una campaña de capacitación al personal para darles la concientización de un empleado.	Realizar buzón de correo y foros de quejas anónimas para que muestren sus inconformidades a si sus actividades de una organización.	Tener auditorías con el objetivo de garantizar que solo las personas autorizadas tengan acceso a los recursos y datos de una organización.	Una plataforma de seguridad integral que incluye un IDS, un SIEM y otras herramientas de seguridad. Ofrece una visión unificada de la seguridad de la red.
Fecha	13 al 17 de enero de 2025	7 al 11 de enero de 2025		1 al 11 de enero de 2025
Herramienta.	Videoconferências Zoom o meet de google.	Correo electrónico y sitio de foro de gsuite de google.	OSSIM genera alertas en tiempo real sobre posibles intrusiones.	IDS: AlienVault OSSIM

Denegación de servicio.			
	Semana 2 y 3	**Semana 4**	**Semana 3 y 4**
Incidencia	Implementar medidas de seguridad básicas.	Monitoreo constante de red.	Colabora con un proveedor de servicios de Internet (ISP) Confiable.

Solucion	Para mitigar estos ataques, es fundamental implementar una combinación de medidas de seguridad tanto a nivel de red como de aplicación.	El monitoreo constante de una red es esencial para detectar y mitigar los ataques DDoS de manera proactiva.	El colaborar con un ISP confiable es una estrategia eficaz para proteger tu organización contra los ataques DDoS. Al aprovechar la experiencia y los recursos de un ISP, puedes mejorar significativamente la seguridad de tu red y garantizar la continuidad de tus servicios.
Fecha	7 al 17 de enero de 2025	20 al 24 de enero de 2025	12 al 24 de enero de 2025
Herramienta.	IDS AlienVault OSSIM, IPS Fortinet	IDS AlienVault OSSIM, IPS Fortinet	Telmex**:** Como uno de los proveedores más grandes, Telmex cuenta con una amplia infraestructura y ofrece soluciones de seguridad avanzadas, incluyendo protección contra DDoS.

Hurto de equipos y documentos.				
	Semana 5	**Semana 5**	**Semana 6**	**Semana 6**
Incidencia	Control de accesó.	Vigilancia.	Almacenamiento seguro.	Identificación de equipos.

Solucion	Un sistema de control de acceso es un conjunto de medidas de seguridad que restringen el acceso físico a instalaciones, áreas o recursos específicos. Estos sistemas pueden ser mecánicos, electrónicos o una combinación de ambos.	La implementación de un sistema de vigilancia integral, combinado con medidas de seguridad adicionales, es fundamental para prevenir el hurto de equipos y documentos.	El almacenamiento seguro es esencial para proteger tus equipos, documentos y otros bienes valiosos de robos, daños y pérdidas. Al implementar las medidas adecuadas, puedes garantizar la integridad de tus activos y tener tranquilidad.	La identificación clara y precisa de todos los equipos y documentos es un paso fundamental para prevenir y mitigar el hurto. Al asignar un identificador único a cada elemento, se facilita su seguimiento, recuperación y, en caso de robo, se agiliza la denuncia y la investigación.
Fecha	27 al 31 de Enero del 2025.	27 al 31 de Enero del 2025.	3 al 7 de Febrero del 2025.	3 al 7 de Febrero del 2025.
Herramienta.	Software House Win-PAK:	Software House Win-PAK:	Drive de GSuite de google es un almacenamientos seguro para los documentos.	InvGate Asset Management.

Falta de sistemas centralizados.				
	Semana 3 y 4	**Semana 2**	**Semana 3**	**Semana 1**
Incidencia	Diversidad de medios de almacenamiento	Políticas de Retención de Datos	Pruebas de Restauración	Concientización del Personal
Solucion	Utilizar una combinación de medios de almacenamiento, como discos duros externos, cintas magnéticas y almacenamiento en la nube, para reducir el riesgo de pérdida de datos por falla de un solo medio.	Conjunto de reglas y procedimientos que establecen cuánto tiempo debe conservarse determinada información dentro de una organización. Esta política es fundamental para cumplir con las regulaciones, optimizar el almacenamiento y proteger la privacidad de los datos.	proceso crítico en cualquier plan de recuperación ante desastres (DRP). Consiste en verificar de manera práctica que los sistemas, aplicaciones y datos respaldados pueden ser restaurados de manera exitosa en caso de una interrupción del servicio.	Realizar una campaña de capacitación al personal para darles la concientización de buen uso de sistemas de la organización.

Fecha	13 al 24 de enero de 2025	7 al 11 de enero de 2025	20 al 24 de enero de 2025	1 al 6 de enero de 2025
Herramienta.	Veeam Data Platform.	Veeam Data Platform.	Veeam Data Platform.	Videoconferências Zoom o meet de google.

Red local insegura.				
	Semana 6 y 7	**Semana 7 y 8**	**Semana 5 y 6**	**Semana 4**
Incidencia	Contraseñas robustas.	Cifrado.	Segmentación de redes.	Actualizaciones constantes.
Solucion	La seguridad de tus cuentas en línea depende en gran medida de la fortaleza de tus contraseñas. Al combinar generadores de contraseñas, gestores de contraseñas y buenas prácticas,	El cifrado de red es una herramienta esencial para proteger la confidencialidad de los datos transmitidos a través de una red. Sin embargo, la seguridad de este cifrado depende de varios factores,	La segmentación de redes es una estrategia de seguridad que consiste en dividir una red en múltiples subredes más pequeñas, cada una con sus propias políticas de seguridad y acceso. Esta práctica es	Las actualizaciones constantes son esenciales para mantener una red segura, pero en un entorno inseguro, pueden presentar desafíos adicionales.

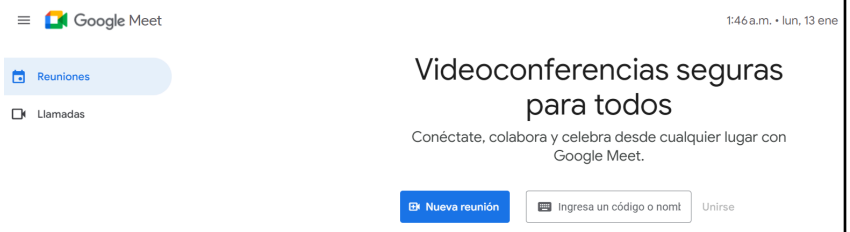
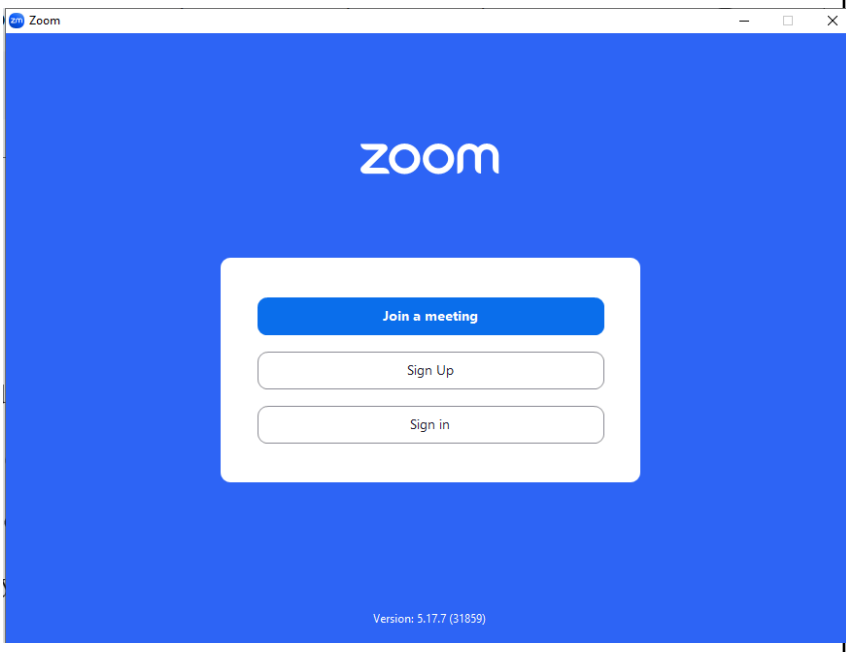
	puedes crear un muro de protección impenetrable contra los ciberdelincuentes.	desde la elección del algoritmo hasta la implementación correcta.	crucial para limitar el impacto de una brecha de seguridad, ya que al contener un ataque a un segmento específico, se evita que se propague a toda la red.	
Fecha	10 al 21 de Febrero de 2025	17 al 28 de Febrero de 2025	27 de Enero al 7 de Febrero del 2025.	10 al 28 de Febrero de 2025
Herramienta.				

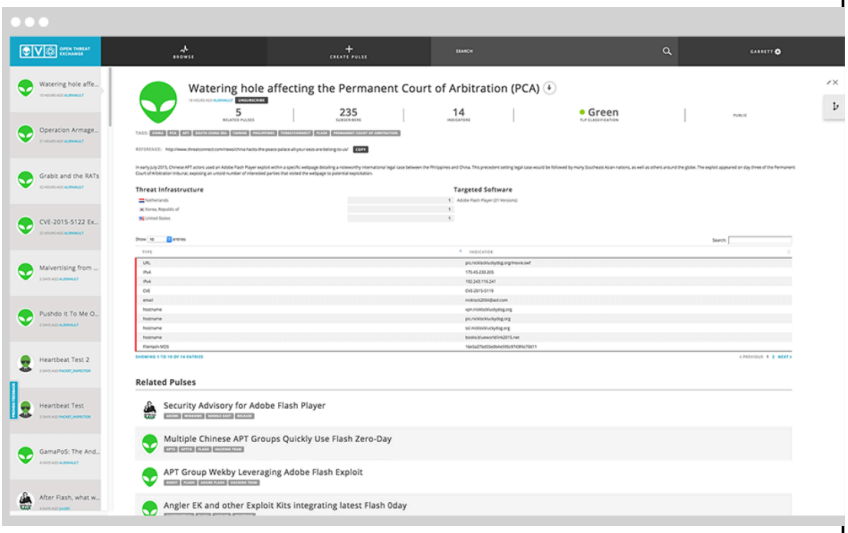
Cronograma de Plan de accion:

Cronograma del Plan de Acción (Amenazas y Vulnerabilidades).									
Mes	Enero				Febrero				Marzo
Semanas	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7	Semana 8	Semana 9
Empleados insatisfechos.									
Concientización.									
Canales de comunicación.									
Auditoria de acceso.									
Sistemas de detección de intrusiones.									
Denegación de servicio.									
Implementar medidas de seguridad básicas.									
Monitoreo constantemente de red.									
Colabora con un proveedor de servicios de Internet (ISP) Confiable.									
Hurto de equipos y docementos.									
Control de accesó.									
Vigilancia									
Almacenamiento seguro									
Identificación de equipos									
Falta de un sistema de respaldo Centralizado.									
Diversidad de medios de almacenamiento									
Pruebas de Restauración									
Políticas de Retención de Datos									
Concientización del Personal									
Seguridad de las Copias de Seguridad									
Red local insegura									
Contraseñas robustas.									
Cifrado.									
Segmentación de redes.									
Actualizaciones constantes.									
Inventarios de dispositivos:									

Práctica de plan de acción.

Se anexará la evidencia de las imágenes de las herramientas utilizadas para la solución de las mitigación de algunas vulnerabilidades y amenazas presentadas en el análisis de el colegio de educación superior de la ciudad de Veracruz.

Aplicacion	Imagen evidencia.
Videoconferencias Meet.	
Videoconferencias Zoom.	

IDS: AlienVault OSSIM.	

Evaluación.

En este punto agregaremos como evidencia el por qué recurrimos a las herramientas principales de mitigación de las vulnerabilidades y amenazas presentadas en el análisis del colegio de educación superior de la ciudad de Veracruz.

Aplicacion	**Breve descripcion**
GSuite Google	Seleccionamos esta herramienta de trabajo por varias soluciones de vulnerabilidades que se presentaron una de ella fue la capacitación de los empleados de la organización como también un buzón, un sitio de quejas y sugerencias.
Zoom	Esta herramienta la escogimos como segunda opción para capacitación del personal de la organización.
IDS: AlienVault OSSIM.	Por ser una poderosa plataforma de gestión de seguridad de la información (SIEM) de código abierto que ha ganado gran popularidad en el sector. Combina múltiples herramientas de seguridad en una única interfaz, lo que la convierte en

	una solución integral para proteger tus sistemas y datos.

Conclusion.

En conclusión: La implementación de este plan de acción es solo el comienzo de nuestro viaje hacia una mayor seguridad cibernética. A medida que evoluciona el panorama de las amenazas, seguiremos evaluando y mejorando nuestras medidas de protección. La revisión periódica de este plan nos permitirá identificar nuevas vulnerabilidades y adaptar nuestras estrategias en consecuencia. Nuestro objetivo es garantizar que nuestra organización esté siempre preparada para enfrentar cualquier desafío que pueda surgir. Esperamos reducir en un 50% los incidentes de seguridad en los próximos seis meses. Agradecemos a nuestro equipo de TI por su dedicación en la creación de este plan. Juntos, hemos construido una base sólida para proteger nuestra organización y nuestros datos. Invitamos a todos a seguir participando en capacitaciones y reportando cualquier actividad sospechosa. En esta materia aprendimos cómo detectar las amenazas y vulnerabilidades que se puedan presentar en cualquier parte de las organizaciones en las que estemos laborando.

Referencias.

Gemini - chat to supercharge your ideas. (n.d.). Gemini. Retrieved January 9, 2025, from https://gemini.google.com/

Ingeniería en desarrollo de software. (n.d.). Edu.Mx. Retrieved January 9, 2025, from https://umi.edu.mx/coppel/IDS/login/index.php

#1 global leader in data resilience. (n.d.). Veeam Software. Retrieved January 13, 2025, from https://www.veeam.com/