Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad 3 – Plan de Acción.

Seguridad Informatica1.

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: Homero Ramirez Hurtado

Fecha:02 de Enero del 2024

Índice.

Introducción.

La seguridad informática es un aspecto crítico en el mundo digital actual. Un plan de acción de seguridad informática es un conjunto de medidas diseñadas para proteger los sistemas de información contra amenazas y vulnerabilidades. Este plan se basa en una evaluación de riesgos que identifica los activos de información, las amenazas a esos activos y las vulnerabilidades que podrían explotar. El plan también incluye políticas y procedimientos para minimizar los riesgos, así como estrategias de respuesta a incidentes para manejar cualquier brecha de seguridad. Además, un plan de acción de seguridad informática efectivo requiere una formación continua del personal para garantizar que comprendan y sigan las políticas de seguridad. En última instancia, el objetivo de un plan de acción de seguridad informática es garantizar la confidencialidad, integridad y disponibilidad de la información, protegiendo así los activos de información valiosos de una organización.

Descripción.

Un plan de acción de seguridad informática es un conjunto de medidas diseñadas para proteger los sistemas de información de una organización. Comienza con una evaluación de riesgos para identificar posibles amenazas y vulnerabilidades. Luego, se desarrollan políticas y procedimientos para mitigar estos riesgos. Estos pueden incluir la implementación de firewalls y software antivirus, la realización de copias de seguridad regulares de datos y la capacitación del personal en prácticas seguras de TI.

Además, el plan debe incluir una estrategia de respuesta a incidentes para manejar cualquier violación de seguridad que ocurra. Esto puede implicar la identificación y contención del incidente, la erradicación de la amenaza, la recuperación de los sistemas y la revisión de las políticas para prevenir futuros incidentes.

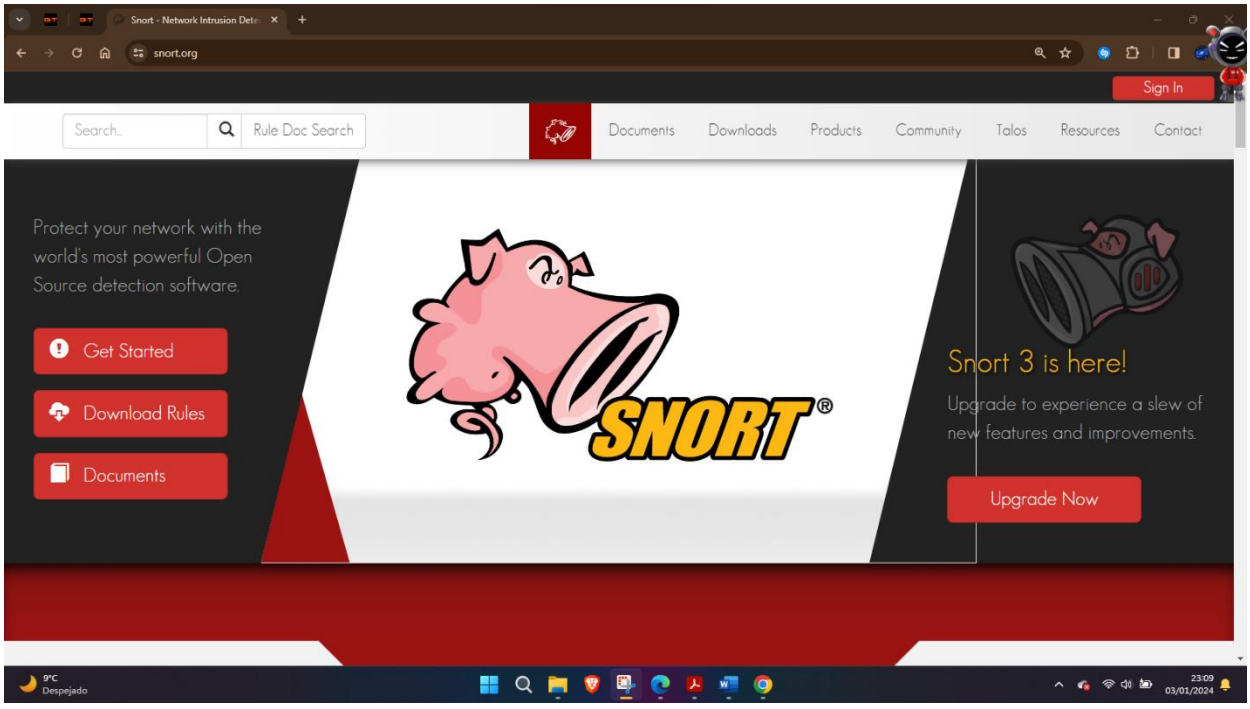
Finalmente, el plan debe ser revisado y actualizado regularmente para adaptarse a las nuevas amenazas y tecnologías. La seguridad informática es un proceso continuo que requiere un compromiso constante para ser efectivo.

Justificación.

La seguridad informática es esencial en el mundo digital actual. Un plan de acción sólido para la seguridad informática es crucial para proteger los datos y la información confidencial. Este plan garantiza la integridad, confidencialidad y disponibilidad de los datos, evitando el acceso no autorizado y las amenazas cibernéticas. Además, un plan de acción eficaz puede prevenir la pérdida de datos y minimizar el tiempo de inactividad del sistema, lo que puede tener un impacto significativo en la productividad y la reputación de una organización. También es importante para cumplir con las regulaciones y normativas de privacidad de datos. En resumen, un plan de acción para la seguridad informática es una inversión necesaria que proporciona una defensa robusta contra las amenazas cibernéticas, protege los activos valiosos de la organización y mantiene la confianza de los clientes y socios comerciales. Por lo tanto, es fundamental para el éxito y la sostenibilidad a largo plazo de cualquier organización en la era digital.

Desarrollo.

Selección de Software.



Plan de Acción.

1. Políticas de seguridad:

- Establecer políticas claras sobre el uso de los equipos y el acceso a Internet. Esto incluiría restricciones sobre el uso de redes sociales, correo electrónico y WhatsApp para fines personales.
- Implementar políticas de contraseñas fuertes. Las contraseñas deben ser únicas y complejas, no tan simples como “1234abc”.

2. Protección de la red:

- Habilitar el firewall en todos los equipos para proteger la red interna de amenazas externas.
- Considerar la implementación de una red privada virtual (VPN) para proporcionar una capa adicional de seguridad.

3. Software y hardware:

- Actualizar todos los equipos a la última versión de su sistema operativo y aplicaciones.
- Considerar la posibilidad de actualizar el hardware si los equipos están funcionando lentamente o se están quedando sin espacio de almacenamiento.
- Asegurarse de que todos los equipos tengan un software antivirus instalado y actualizado. Considerar la posibilidad de actualizar a una versión de pago para obtener una protección más completa.
- Revisar el origen del software descargado de Internet y asegurarse de que proviene de una fuente confiable.

4. Acceso físico:

- Instalar una alarma de seguridad en el área administrativa financiera.
- Implementar un sistema de registro electrónico para los docentes, en lugar de una libreta.

5. Capacitación:

- Proporcionar capacitación regular a todo el personal sobre las mejores prácticas de seguridad informática.

6. Plan de respuesta a incidentes:

- Desarrollar un plan de respuesta a incidentes de seguridad informática. Esto debería incluir quién debe ser notificado, cómo se debe contener el incidente y cómo se debe recuperar.

7. Copias de seguridad y recuperación:

- Implementar un plan de copias de seguridad y recuperación para proteger los datos importantes. Esto es especialmente importante para el servidor que contiene la base de datos general.

8. Auditorías de seguridad:

- Realizar auditorías de seguridad regulares para identificar y corregir cualquier vulnerabilidad.

Practica de Plan de Acción.

Semana	Incidencia	Solución	Fechas	Herramientas
Semana 1	Falta de alarma de seguridad en el área administrativa financiera	Instalar un sistema de alarma de seguridad	1-7 Enero	Sistema de alarma
Semana 2	Equipos lentos y con poco espacio de almacenamiento	Realizar una limpieza de archivos y optimización del sistema	8-14 Enero	Software de limpieza y optimización
Semana 3	Firewall deshabilitado y antivirus gratuito	Habilitar el firewall y actualizar a un antivirus de pago	15-21 Enero	Firewall integrado, Antivirus de pago
Semana 4	Contraseñas básicas y uso personal de los equipos	Implementar políticas de contraseñas seguras y restricciones de uso personal	22-28 Enero	Políticas de seguridad de la red

Evaluación.

Semana 1:

- **Día 1-2:** Limitar acceso a la base de datos (BD).
- **Día 3-4:** Identificar datos sensibles en todos los sistemas.
- **Día 5-7:** Iniciar el proceso de cifrado de información.

Semana 2:

- **Día 1-2:** Actualizar el sistema y verificar las licencias de software.
- **Día 3-4:** Configurar conexiones seguras y cifradas.
- **Día 5-7:** Actualizar antivirus y firewall en todos los equipos.

Semana 3:

- **Día 1-2:** Implementar el uso de un gestor de contraseñas.
- **Día 3-4:** Actualizar el sistema operativo (S.O) en todos los equipos.
- **Día 5-7:** Instalar software Anti-Spy en todos los equipos.

Semana 4:

- **Día 1-2:** Configurar correos empresariales para mayor seguridad.
- **Día 3-4:** Instalar software de bloqueo a accesos no autorizados.
- **Día 5:** Aplicar filtros anti-spam en los correos electrónicos.
- **Día 6-7:** Actualizar contraseñas en el sistema.

Conclucion.

Un plan de acción sobre seguridad informática es esencial en el mundo digital actual. La creciente dependencia de la tecnología ha hecho que la seguridad informática sea una prioridad para las organizaciones. Un plan de acción efectivo puede ayudar a prevenir, detectar y responder a las amenazas de seguridad. La prevención implica la implementación de medidas de seguridad como firewalls y software antivirus. La detección se logra mediante el monitoreo constante de la red y los sistemas para identificar cualquier actividad sospechosa. La respuesta a las amenazas incluye la contención del incidente y la recuperación de los sistemas afectados. Además, la educación y la formación de los empleados en prácticas seguras de TI son fundamentales para minimizar los riesgos de seguridad. Un plan de acción también debe incluir políticas claras y procedimientos para manejar incidentes de seguridad. En conclusión, un plan de acción sobre seguridad informática es una herramienta vital para proteger los activos digitales de una organización. Su implementación y mantenimiento requieren un compromiso constante y una inversión en recursos, pero los beneficios superan con creces los costos. La seguridad informática no es un destino, sino un viaje continuo.

Referencias: Bing y Video de la Tutoría 3.