SEGURIDAD INFORMÁTICA SEGURIDAD DE LA INFORMACIÓN

Trabajo Realizado por: Emilio Corona Muñoz, Armando Lara Romero 6A

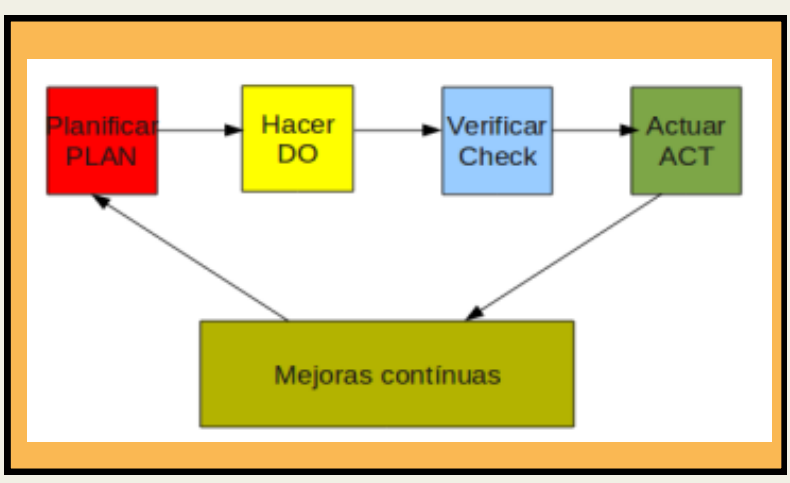
¿QUÉ ES LA SEGURIDAD INFORMATICA?

La seguridad informática (abreviada para la seguridad de la tecnología de la información) es la práctica de proteger los sistemas informáticos, redes, dispositivos digitales, datos de acceso no autorizado, filtraciones de datos, ataques cibernéticos y otras actividades maliciosas.

SEGURIDAD DE LA INFORMACIÓN: MODELO PDCA

LLa organización del tema de la seguridad debe tener un Sistema de Gestión de la seguridad de la Información (SGSI) cuyo objetivo es el proteger la información, pero primero lo que se debe hacer es identificar los activos de información los cuales son los que tienen que ser protegidos y el grado de protección.

Aplicacion del plan PDCA ('PLAN-DO-CHECK-ACT) lo que seria Planificar, hacer, verificar, actuar y volcer a repetir el ciclo. Un SGSI simple cumple cuatro niveles repetitivos mejorando la seguridad.



Planificar: establecer el contexto, creando políticas de seguridad, análisis de riesgos. Hacer; implementar el sistema de gestión de seguridad. Verificar: monitorizar actividades. Actuar: ejecutar tareas de mantenimiento.

BASES DE LA SEGURIDAD INFORMÁTICA

- **Confiabilidad:** La probabilidad de que un sistema se comporte tal y como se espera de él.
- **Confidencialidad:** Garantizar que la información sensible esté protegida contra el acceso no autorizado. Esto implica el uso de controles de acceso, cifrado de datos y políticas de privacidad adecuadas.
- **Disponibilidad:** La información debe de estar disponible cuando se necesite. Implica la implementación de medidas para prevenir y mitigar interrupciones del servicio, como la redundancia de sistemas, la copia de seguridad de datos y la planificación de la continuidad del negocio.
- **Integridad:** La integridad de los datos (el volumen de la información). La integridad del origen (la fuente de los datos, llamada autenticación). Es importante hacer hincapié en la integridad del origen, ya que puede afectar a su exactitud, credibilidad y confianza que las personas ponen en la información.

MECANISMOS BÁSICOS DE SEGURIDAD

- **Autenticación:** Verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.
- **Autorización:** Proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización.
- **Administración:** establece, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema.
- **Auditoría y registro:** la Auditoría es continua vigilancia de los servicios en producción y para ello se recaba información y se analiza. Este proceso permite a los administradores verificar que las técnicas de autenticación y autorización utilizadas se realizan según lo establecido y se cumplen los objetivos fijados por la organización.

VULNERABILIDADES DE UN SISTEMA INFORMÁTICO

- **Hardware**: elementos físicos del sistema informático, tales como procesadores, cableado de red, medios de almacenamiento (cabinas, discos, cintas, usb, DVDs,...).
- **Software**: elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones.
- **Datos:** comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red.

Las vulnerabilidades de los sistemas informáticos las podemos agrupar en función de:

Diseño:

- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficiente e inexistente.

Implementación:

- Errores de programación.
- Existencia de "puertas traseras" en los sistemas informáticos.

Vulnerabilidad del día cero:

- Se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución "conocida", pero se sabe cómo explotarla.

Vulnerabilidades conocidas:

Vulnerabilidad de condición de carrera (race condition).

POLÍTICAS DE SEGURIDAD

Lo primero que se debe hacer es un análisis de las posibles amenazas que el sistema pueda tener y saber cuál de esas amenazas podrían perder y las probabilidades que ocurran.

Las políticas deben hacer lo siguiente:

- Definir qué es seguridad de la información, cuáles son sus objetivos principales y su importancia dentro de la organización
- Mostrar el compromiso de sus altos cargos con la misma
- Definir la filosofía respecto al acceso a los datos.
- Establecer responsabilidades inherentes al tema.
- Clasificar los datos y controlarlos.
- Tener un plan de contingencia.
- Administrar las computadoras.

Y lo último, pero no menos importante es que la seguridad debe ir más allá del conocimiento de los empleados como tener un mecanismo de seguridad física y lógica, como tener estrategias de copias de seguridad o un plan de recuperación en caso de un incidente

CONCLUSIONES

Tanto los usuarios (sin importar el nivel de conocimiento) como las organizaciones, son cada vez más dependientes de Internet y de las tecnologías de información, lo que también los expone constantemente a diferentes amenazas, en las que se utilizan estas condiciones para cometer acciones delictivas con fines económicos.

la seguridad informática y la seguridad de la información son aspectos fundamentales en el mundo digital actual, y su importancia solo seguirá creciendo a medida que la tecnología avance y las amenazas cibernéticas continúen evolucionando.