Laboratorio #2

La **confidencialidad, integridad y disponibilidad** (CID) son principios fundamentales en la seguridad de la información:

- **Confidencialidad**: Asegura que la información solo sea accesible para aquellos autorizados a verla, protegiendo los datos contra accesos no autorizados.
- **Integridad**: Garantiza que la información se mantenga precisa y completa, protegiéndola de modificaciones no autorizadas.
- **Disponibilidad**: Asegura que la información y los recursos estén accesibles y utilizables cuando se necesiten, garantizando la continuidad del negocio.

Pregunta 1

¿Qué concepto consideras más crítico en una empresa de salud? ¿Y en una empresa de comercio electrónico?

R/

En una empresa de salud, **la confidencialidad** es probablemente el principio más crítico debido a la naturaleza sensible de los datos que se manejan, como historiales médicos, diagnósticos, tratamientos, y datos personales de los pacientes.

En una empresa de comercio electrónico, el principio más crítico suele ser **la disponibilidad**, ya que se depende de que el sitio web o la plataforma esté siempre accesible para los clientes.

Pregunta 2

¿Como podrías priorizar la implementación a una empresa con recursos limitados?

R/enfocado la más importante a la empresa según el caso, implementando todos pero dándole mas prioridades a la empresa.

Defina y ejemplos

Virus: es una aplicación o código malintencionado que se emplea para ejecutar actividades destructivas en un dispositivo o red local. La actividad malintencionada de este código puede dañar el sistema local de archivos, robar datos, interrumpir servicios, descargar más malware o cualquier otra acción que esté codificada en el programa.

Ejemplo: MyDoom Este virus fue uno de los más rápidos en propagarse por Internet. Se enviaba a través de correos electrónicos y utilizaba vulnerabilidades en los sistemas operativos Windows para propagar el malware y realizar ataques DDoS (denegación de servicio distribuida).

Gusano: es un tipo de malware similar al virus, pero el gusano se replica y se propaga automáticamente a través de redes, explotando vulnerabilidades en sistemas, sin necesidad de intervención del usuario.

Ejemplo: blaster es un gusano que exploto una vulnerabilidad en Windows en 2003

Troyano: es un tipo de malware que se disfraza de software legítimo para engañar al usuario y, una vez ejecutado, permite a los atacantes obtener acceso no autorizado al sistema, robar información o instalar otros tipos de malware. es un tipo de malware que se disfraza de software legítimo para engañar al usuario y, una vez ejecutado, permite a los atacantes obtener acceso no autorizado al sistema, robar información o instalar otros tipos de malware.

Ejemplo: Emotet se disfraza de un archivo adjunto en un correo electrónico legítimo, como una factura o un documento importante. Cuando el usuario lo abre, el troyano se instala y permite a los atacantes robar contraseñas y datos personales.

Ransonwares: es un tipo de malware que bloquea el acceso a archivos o sistemas de la víctima y exige un rescate (generalmente en criptomonedas) para liberarlos.

Ejemplo: WannaCry Este malware explotó una vulnerabilidad en sistemas Windows y cifró los archivos de las víctimas, pidiendo un rescate en Bitcoin para desbloquearlos. Afectó a miles de organizaciones en todo el mundo, incluyendo hospitales y empresas.

Spyware: es un tipo de malware diseñado para espiar las actividades del usuario, recopilar información personal sin su consentimiento y enviarla a un atacante, generalmente con fines maliciosos o para publicidad no deseada.

Ejemplo: Pegasus Este malware espía a través de vulnerabilidades en teléfonos móviles, permitiendo a los atacantes acceder a mensajes, llamadas y otras actividades del dispositivo sin que el usuario lo sepa.

Resultado de prueba de ciberseguridad