DEFINICION Y EJEMPLOS

Comprender los principios de Confidencialidad, Integridad y Disponibilidad.

Confidencialidad: Es aquella que nos garantiza que los datos y todo tipo de información este o sea solo disponible para aquellas personas con las credenciales correctas o solo las personas autorizadas.

Integridad: Esta nos asegura que ninguno de los datos que tengamos guardado ya sea en un disco duro o cualquier otro lugar no sea alterado por personas que no tengan esa autorización y así mismo toda esa información se mantenga correcta.

Disponibilidad: Esta nos asegura que todo sistema o datos este siempre disponible cada vez que un usurario lo necesite.

Pregunta 1: ¿Qué concepto consideras mas critico en una empresa de salud? ¿y en una empresa de comercio electrónico?

¿Qué concepto consideras más critico en una empresa de salud?

Considero el concepto de confidencialidad ya que esta nos permite una mayor seguridad al momento de nosotros como usuarios, ya que aquí lo que guardamos son datos personales y queremos que todo este tipo de datos sean lo más confiable posible.

¿y en una empresa de comercio electrónico?

Considero que así sea la disponibilidad ya que como hablamos de comercio pues estamos hablando de una venta y si las ventas no están disponibles la empresa comienza a perder dinero en este caso y eso es lo que nunca se quiere en una empresa, es por eso que siempre tiene que estar disponible.

Pregunta 2: ¿Cómo podrías priorizar la implementación a una empresa con recursos?

Podemos hacerlo evaluando los riesgos de manera rigurosa, de esta forma podemos priorizar el que recurso mas necesario, claro que también depende la empresa en si por ejemplo en el caso de la empresa de salud el orden de prioridades es diferente a la de electrónica, en la de salud el seria: **Confidencialidad-Integridad-Disponibilidad** y en la de electrónico seria: **Disponibilidad-Integridad-Confidencialidad.**

Defina y Ejemplo

Virus: Es un programa malicioso que se adjunta a archivos legítimos y se propaga cuando el archivo infectado se ejecuta. Necesita intervención del usuario para activarse.

Ejemplo: Un archivo PDF que al ejecutarse se comiencen a borrar archivos del sistema.

Gusano: Un gusano es un tipo de malware autónomo que se propaga automáticamente a través de redes, aprovechando vulnerabilidades en sistemas sin necesidad de intervención del usuario ni de adjuntarse a otros programas.

Ejemplo: El gusano Blaster (2003) explotaba una vulnerabilidad en Windows XP y se propagaba por Internet causando reinicios automáticos en los equipos infectados, afectando miles de empresas.

Troyano: Es un malware que se oculta dentro de un programa aparentemente legítimo para ejecutar acciones maliciosas sin que el usuario lo note.

Ejemplo: Un programa que aparenta ser un juego gratuito, pero al instalarlo abre una puerta trasera para que un atacante controle tu PC.

Ransomware: Es un software malicioso que cifra los archivos del sistema y exige un rescate para restaurarlos.

Ejemplo: Recibes un correo con un archivo PDF, lo abres y en segundos todos tus archivos están cifrados. Aparece una nota pidiendo $300 en bitcoin para recuperarlos.

Spyware: Es un software que se instala sin permiso para espiar la actividad del usuario y robar información como contraseñas, correos o historial de navegación.

Ejemplo: Un programa gratuito que monitorea las teclas que pulsas para robar tus contraseñas y enviarlas al atacante.

CURSO CISCO