

CIBERSEGURIDAD – BASICO

ALUMNO: NEIDER ANDRES MEJIA GARISABALO

SESIÓN #2 DIFERENCIAR ENTRE CONFIDENCIALIDAD,

INTEGRIDAD Y DISPONIBILIDAD

UNIVERSIDAD POPULAR DEL CESAR

SEDE – SABANAS

VALLEDUPAR

HORARIO – NOCTURNO

2025

DEFINIR Y EJEMPLOS

Comprender los principios de Confidencialidad, Integridad y Disponibilidad.

Respuesta:

Confidencialidad

Esto trata de proteger la información para que solo las personas autorizadas puedan verla o acceder a ella.

Ejemplo cotidiano:

Piensa en tus mensajes privados de WhatsApp. La confidencialidad es que nadie más (ni tus amigos, ni tu jefe, ni un hacker) pueda leer esos mensajes, excepto tú y la persona con la que hablas.

Cómo se logra:

- Contraseñas
- Cifrado
- Control de acceso

Integridad

Significa que la información se mantiene exacta y completa, sin alteraciones no autorizadas.

Ejemplo cotidiano:

Imagina que haces una transferencia de dinero desde tu app del banco por \$1,000. La integridad garantiza que ese monto no cambie a \$10,000 por error o manipulación en el camino.

Cómo se protege:

- Firmas digitales
- Suma de verificación (hash)
- Control de versiones

Disponibilidad

Esto significa que la información y los sistemas están accesibles cuando los necesitas.

Ejemplo cotidiano:

Si un día entras a tu correo electrónico y está caído justo cuando más lo necesitas, ahí falla la disponibilidad. Este pilar busca que eso no pase.

Cómo se mantiene:

- Copias de seguridad
- Servidores redundantes
- Protección contra ataques (como DDoS)

Pregunta 1. ¿Qué concepto consideras más crítico en una empresa de salud?

Respuesta:

En una empresa de salud, la Confidencialidad suele ser el concepto más crítico. Porque los sistemas de salud manejan información altamente sensible y privada: diagnósticos, tratamientos, historiales médicos, datos personales, etc. Si esa información cae en manos equivocadas, se puede dañar gravemente la privacidad de los pacientes y hasta enfrentar demandas legales muy serias.

¿Y en una empresa de correo electrónico?

Respuesta:

En este caso, el pilar más crítico suele ser la Disponibilidad. Porque el principal servicio que ofrece una empresa de correo es el acceso constante a los mensajes. Si no puedes enviar o recibir correos, o el sistema está caído, el servicio pierde su razón de ser. En muchos casos, negocios enteros dependen del correo para funcionar día a día.

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

Respuesta:

En una empresa con recursos limitados, la seguridad debe priorizarse estratégicamente. Lo primero es identificar qué tipo de información y procesos son más críticos para el negocio. Luego, clasificar los datos por su nivel de sensibilidad para proteger primero lo más valioso.

Se recomienda implementar la seguridad en etapas. Comienza con lo básico: contraseñas fuertes, acceso restringido, respaldos y control de cambios. Después, refuerza con medidas como cifrado, antivirus y firewalls. Finalmente, promueve una cultura de seguridad en el equipo y mejora continuamente los procesos.

El enfoque ideal es proteger lo más importante desde el principio y avanzar paso a paso según los recursos disponibles.

SEGUNDA PARTE

Defina y Ejemplo:

Virus, Gusano, Troyano, Ransomware, spyware.

Respuesta:

1. Virus

Definición:

Un virus es un programa malicioso que se adhiere a otros archivos o programas legítimos y se activa cuando ese archivo es ejecutado. Se replica e intenta propagarse a otros archivos o dispositivos.

Ejemplo:

Descargas un archivo adjunto en un correo que parece ser una factura. Cuando lo abres, se ejecuta un virus que infecta otros documentos de tu computadora y daña el sistema.

2. Gusano**Definición:**

Un gusano es similar a un virus, pero no necesita que el usuario lo ejecute ni que se adjunte a otro programa. Se propaga automáticamente por redes, copiándose a sí mismo.

Ejemplo:

Un gusano se propaga por la red de una empresa, copiándose de un equipo a otro sin que nadie lo abra. Puede ralentizar toda la red y consumir recursos del sistema.

3. Troyano**Definición:**

Un troyano es un malware que se disfraza de programa legítimo o inofensivo, pero al ejecutarse, permite que un atacante tome el control del equipo o robe datos.

Ejemplo:

Instalas lo que parece ser un juego gratuito, pero en realidad es un troyano. Mientras juegas, en segundo plano alguien está accediendo a tu información o instalando otros programas maliciosos.

4. Ransomware**Definición:**

El ransomware es un tipo de malware que bloquea el acceso a los archivos o al sistema y pide un rescate económico para liberarlos.

Ejemplo:

Un empleado abre un correo con un archivo malicioso. En minutos, todos los archivos de la empresa son cifrados y aparece un mensaje pidiendo dinero para desbloquearlos.

5. Spyware**Definición:**


El spyware es un software que espía al usuario sin su conocimiento, recolectando datos como contraseñas, historial de navegación o información personal.

Ejemplo:

Instalas una aplicación gratuita de edición de fotos y, sin saberlo, viene con spyware que registra todo lo que tecleas, incluyendo tus contraseñas.

TERCERA PARTE

Curso de Cisco

 **Introducción a la Ciberseguridad**

Esquema del curso

Recursos

Prueba de mi conocimiento (beta)

Tutorial de Navegación del Curso

Módulo 1: Introducción a la Ciberseguridad

Módulo 2: Ataques, conceptos y técnicas

Módulo 3: Protegiendo sus datos y su privacidad

Módulo 4: Protegiendo a la organización

Módulo 5: ¿Su futuro estará relacionado con la ciberseguridad?

Introducción a la ciberseguridad: examen final del curso

Prueba de mi conocimiento

Felicitades

Ha completado con éxito la actividad Prueba De Mi Conocimiento.

Puede ver el Historial de Prueba De Mi Conocimiento haciendo clic en el botón [Historial de Prueba De Mi Conocimiento](#).

Si lo desea, puede retomar la [Prueba De Mi Conocimiento](#).