SEGURIDAD INFORMATICA

GLOSARIO

ANGEL ANTONIO LOZA FLORES-22624

Seguridad informática: Conjunto de prácticas para proteger la información y los sistemas contra accesos no autorizados, daños o pérdidas.

Confidencialidad: Garantizar que solo las personas autorizadas puedan ver cierta información.

Integridad: Asegurar que la información no sea alterada o modificada sin permiso.

Disponibilidad: Mantener los sistemas y la información accesibles cuando se necesiten.

Autenticidad: Verificar que los datos o usuarios sean realmente quienes dicen ser.

No repudio: Evitar que alguien niegue haber realizado una acción, como enviar un mensaje o una transacción.

Amenaza: Posible situación o acción que puede dañar la información o los sistemas.

Vulnerabilidad: Debilidad o falla en un sistema que puede ser aprovechada por un atacante.

Riesgo: Probabilidad de que una amenaza aproveche una vulnerabilidad y cause un daño.

Ataque informático: Acción malintencionada para afectar la seguridad de un sistema o información.

Malware: Programa dañino que busca alterar, robar o dañar información.

Phishing: Engaño en el que alguien se hace pasar por una entidad confiable para robar datos, como contraseñas.

Spyware: Programa que espía y recopila información del usuario sin que este lo sepa.

Ransomware: Tipo de malware que bloquea archivos o sistemas y pide un pago para liberarlos.

Firewall: Sistema que filtra y controla el tráfico de red para proteger contra accesos no deseados.

Antivirus: Programa que detecta y elimina malware en una computadora o dispositivo.

Backup: Copia de seguridad de la información para recuperarla en caso de pérdida.

Política de seguridad: Conjunto de reglas y prácticas que definen cómo proteger la información en una organización.

Cifrado: Técnica para transformar datos en un formato ilegible para quien no tenga la clave.

Criptografía: Ciencia que estudia cómo proteger la información mediante técnicas como el cifrado.