# ***Actividad 02. Principios de la seguridad informática***

1. Describe con tus propias palabras estos tres conceptos y pon algún ejemplo de cada uno de ellos.

## *1. Describe con tus propias palabras estos tres conceptos y pon algún ejemplo de cada uno de ellos.*

La seguridad informática se basa en una serie de principios fundamentales que buscan, no sólo proteger la información, sino también proteger los sistemas de diversos riesgos y amenazas. Dichos principios son los siguientes:

***CONFIDENCIALIDAD***

Garantizar que la información sólo sea accesible por las personas autorizadas. Su objetivo es evitar que los datos sean revelados a personas no autorizadas.

EJEMPLO: Sistema de banca que utiliza encriptación para asegurar que el cliente y el banco sean los únicos que puedan leer la información de las transacciones que se han realizado.

***INTEGRIDAD***

Asegurar que la información no sea alterada de manera no autorizada y que cualquier cambio sea detectado. Incluye la protección contra la modificación, destrucción o pérdida de los datos.

EJEMPLO: Empresa que implementa controles de hash en sus bases de datos para asegurar que los archivos no hayan sido alterados por hackers o errores del sistema.

***DISPONIBILIDAD***

Garantizar que los sistemas y la información estén disponibles para los usuarios autorizados cuando necesiten. Implica proteger los sistemas contra fallos y ataques que puedan causar interrupciones.

EJEMPLO: Servicio de atención médica utiliza servidores redundantes y copias de seguridad para asegurar que sus sistemas de información estén accesibles, incluso en caso de fallos técnicos o ciberataques.

# ADICIONAL

### *AUTENTICACIÓN*

Verifica la identidad de los usuarios que intentan acceder a los sistemas de información para asegurarse de que dicen ser quiénes son.

EJEMPLO: Sitio web que utiliza autenticación de dos factores (2FA), en donde el usuario debe ingresar con su contraseña y un código enviado a su teléfono móvil, para garantizar que el acceso sea legítimo.

### *AUTORIZACIÓN*

Controla qué recursos y datos puede acceder un usuario una vez autenticado. Determina los permisos y niveles de acceso dentro del sistema.

EJEMPLO: En una empresa, los empleados tienen diferentes niveles de acceso según su rol en la misma. Un empleado del departamento de finanzas por ejemplo puede acceder a datos financieros, pero no a la información de recursos humanos.

### *NO REPUDIO*

Asegura que una vez realizada una transacción o comunicación, el autor no pueda negar haberla realizado. Esto es crucial para las transacciones financieras y comunicaciones legales.

EJEMPLO: Un banco que utiliza firmas digitales para las transacciones en línea, lo que garantiza que el cliente no pueda negar haber realizado una transferencia de dinero.

### *AUDITORÍA*

Implica registrar y monitorear las actividades dentro del sistema para identificar y responder a los posibles incidentes de seguridad. Esto ayuda a

rastrear la fuente de problemas y asegurar el cumplimiento de las políticas de seguridad.

EJEMPLO: Una empresa de tecnología registra todas las actividades de los usuarios en sus servidores para poder revisar y analizar cualquier actividad sospechosa o no autorizada.