Ejercicios UD1. SAD

PRINCIPIOS DE LA SEGURIDAD INFORMATICA

1. Confidencialidad: Imagina que tienes un diario personal. ¿Qué medidas tomarías para asegurarte de que nadie más pueda leerlo? Escribe al menos tres.

2. Integridad: Piensa en un archivo importante en tu computadora. ¿Qué pasos seguirías para asegurarte de que no se modifique sin tu permiso? Enumera al menos dos.

3. Autenticación: Describe un método que usarías para verificar la identidad de alguien que dice ser tu amigo en línea. ¿Qué preguntas o pruebas podrías usar?

4. Disponibilidad: Si tu sitio web se cae y no está disponible para los usuarios, ¿qué acciones tomarías para restaurar el servicio? Escribe al menos dos.

5. No repudio: Imagina que envías un correo electrónico importante. ¿Qué medidas podrías tomar para asegurarte de que la otra persona no pueda negar haberlo recibido? Menciona al menos dos.

6. Confidencialidad: ¿Qué tipo de información personal crees que debería ser protegida y por qué? Haz una lista de tres tipos de información.

7. Integridad: Piensa en un documento colaborativo en línea. ¿Qué herramientas o funciones podrías usar para asegurarte de que todos los cambios sean rastreados y que no haya modificaciones no autorizadas?

8. Autenticación: ¿Qué opinas sobre el uso de la autenticación de dos factores? ¿Cómo crees que mejora la seguridad?

9. Disponibilidad: Reflexiona sobre un servicio en línea que utilizas a menudo. ¿Qué impacto tendría en tu vida diaria si ese servicio no estuviera disponible por un tiempo prolongado?

10. No repudio: Si participas en una transacción en línea, ¿qué tipo de recibo o confirmación te gustaría recibir para asegurarte de que ambas partes están de acuerdo con la transacción?

1. Confidencialidad: Para proteger mi diario personal, tomaría las siguientes medidas:
- Mantenerlo en un lugar seguro: Guardarlo en un cajón con llave o en una caja fuerte.
- Usar un código o contraseña: Si es digital, aseguraría el acceso con una contraseña fuerte.
- Escribir en un lenguaje encriptado: Utilizar un código personal o símbolos que solo yo entienda.

2. Integridad: Para proteger un archivo importante en mi computadora, haría lo siguiente:
- Hacer copias de seguridad regularmente: Utilizar un disco duro externo o un servicio en la nube.
- Configurar permisos de acceso: Asegurarme de que solo yo o personas autorizadas puedan modificar el archivo.

3. Autenticación: Para verificar la identidad de un amigo en línea, podría hacer preguntas específicas que solo él o ella sabría, como:
- Preguntar sobre un recuerdo compartido o una anécdota que solo nosotros conocemos.
- Pedir que me envíe una foto o un mensaje de voz que confirme su identidad.

4. Disponibilidad: Si mi sitio web se cae, tomaría las siguientes acciones:
- Contactar al proveedor de hosting: Para averiguar la causa del problema y solicitar asistencia.
- Revisar los registros de errores: Para identificar y solucionar cualquier problema técnico que haya causado la caída.

5. No repudio: Para asegurarme de que la otra persona no pueda negar haber recibido un correo electrónico importante, podría:
- Solicitar una confirmación de lectura: Para que me notifiquen cuando abran el correo.
- Usar un servicio de correo electrónico que ofrezca seguimiento: Que registre cuándo se envió y se recibió el mensaje.

6. Confidencialidad: Creo que debería protegerse la siguiente información personal:
- Números de identificación personal (como el DNI): Para evitar el robo de identidad.
- Información financiera (como números de cuentas bancarias): Para prevenir fraudes y robos.
- Datos de salud: Para proteger la privacidad y la confidencialidad de la información médica.

7. Integridad: Para asegurarte de que todos los cambios en un documento colaborativo en línea sean rastreados y que no haya modificaciones no autorizadas, podrías utilizar herramientas como el historial de versiones, que te permite ver quién hizo qué cambios y cuándo. También es útil implementar permisos de edición, donde solo ciertas personas pueden hacer modificaciones, y funciones de comentarios para discutir cambios sin alterar el contenido original. Además, algunas plataformas ofrecen la opción de bloquear el documento para evitar cambios temporales.

8. Autenticación: La autenticación de dos factores (2FA) es una excelente medida de seguridad. Al requerir un segundo método de verificación, como un código enviado a tu teléfono, se añade una capa extra de protección. Esto significa que incluso si alguien logra obtener tu contraseña, necesitaría también acceso a tu segundo factor para entrar a tu cuenta. Esto reduce significativamente el riesgo de accesos no autorizados.

9. Disponibilidad: Si un servicio en línea que utilizo a menudo, como un correo electrónico o una plataforma de mensajería, no estuviera disponible por un tiempo prolongado, podría afectar bastante mi vida diaria. Podría perder la comunicación con amigos y familiares, no podría acceder a información importante o incluso afectar mi trabajo si dependo de esa herramienta para colaborar con otros. La falta de acceso podría generar frustración y complicaciones en la organización de mis tareas diarias.

10. No repudio: Al participar en una transacción en línea, me gustaría recibir un recibo detallado que incluya la fecha, la hora, el monto, una descripción del producto o servicio, y la información de ambas partes involucradas. Esto no solo sirve como prueba de la transacción, sino que también asegura que ambas partes están de acuerdo con los términos. Un correo electrónico de confirmación con esta información sería ideal.