Caso práctico UNIDAD 2

1. Análisis de la situación de SecureTech:
   a. SecureTech se enfrenta a diversos tipos de riesgos de seguridad en sus servicios de almacenamiento en la nube, tales como el acceso no autorizado, la pérdida de datos debido a fallos técnicos, desastres naturales o errores humanos, ataques de denegación de servicio (DDoS), la interceptación de comunicaciones y la explotación de vulnerabilidades en el software y los sistemas utilizados.
   b. Probablemente SecureTech utilice TLS para proteger los datos durante la transmisión entre usuarios y servidores y AES con claves de 256 bits para proteger los datos almacenados en los servidores, ya que estas son las prácticas más comunes y recomendadas en la industria del almacenamiento en la nube.
2. Criptografía:
   a. Fundamentos de la criptografía:
      La criptografía es la ciencia que se encarga de la seguridad de la información, y sus cuatro principios básicos son:
      - ***Confidencialidad:*** Garantiza que solo las partes autorizadas puedan acceder a la información.
      - ***Integridad:*** Asegura que los datos no han sido alterados.
      - ***Autenticación:*** Verifica la identidad de los usuarios.
      - ***No repudio:*** Garantiza que las partes no puedan negar la autenticidad de sus comunicaciones.

      Estos principios son vitales para la protección de la información ya que aseguran que los datos estén protegidos contra accesos no autorizados, alteraciones no deseadas, confirman la identidad del usuario y que las comunicaciones son auténticas y verificables.
   b. Los algoritmos de cifrado pueden ser simétricos, utilizando la misma clave para cifrar y descifrar datos, estos son rápidos y eficientes, pero presentan desafíos en la gestión de claves; mientras que los asimétricos, utilizan un par de claves (pública y privada), facilitando el intercambio de claves, pero siendo más lentos y consumiendo más recursos.
      Para SecureTech recomendaría una combinación de ambos, cifrado simétrico para datos en reposo, y asimétrico para el intercambio seguro de claves.
3. Políticas y estándares de seguridad:
   a. Las principales normas y regulaciones relevantes para SecureTech serian la ISO 27001 ya que es el estándar para la gestión de la seguridad de la información; la GDPR sería también importante para manejar los datos personales en posesión de SecureTech de manera legal y segura.

b. Frameworks de seguridad aplicables:
   SecureTech debería aplicar el NIST para mejorar la gestión de riesgos de ciberseguridad, y tratar de conseguir la certificación CSA STAR que es específica para proveedores de servicios en la nube.

c. El cumplimiento de estándares de seguridad ayuda a SecureTech a establecer buenas prácticas, mitigar riesgos y generar confianza entre sus clientes ya que demuestra un compromiso con la seguridad y la privacidad de los datos.

4. Recomendaciones para SecureTech:
   Para mejorar las prácticas de cifrado, recomendaría a la empresa a migrar a AES-256 para cifrado simétrico y ECC para cifrado asimétrico, así como implementar políticas de rotación de claves periódicas. En cuanto apolíticas y procedimientos de seguridad, SecureTech debería utilizar módulos de seguridad de Hardware para el almacenamiento y manejo seguro de claves, implementar controles de acceso estrictos basados en roles y responsabilidades reforzando la autenticación para acceder a los sistemas críticos. También deberían realizar auditorías de seguridad internas y externas periódicas para identificar y corregir vulnerabilidades, y contratar auditores externos para obtener una visión imparcial del estado de la seguridad.