Nadia Arellano G.
Ingeniera en Informática

Actividad – Sesión 6: Evaluación del Modelo de Responsabilidad Compartida en la Nube

1. **Responsabilidades del Proveedor y del Cliente:** Describe dos responsabilidades clave del proveedor y dos del cliente en el modelo de responsabilidad compartida. Explica por qué cada una es importante.

   (R). Responsabilidades del Proveedor (CSP):

   - Seguridad Física: Es responsable de proteger los centros de datos mediante vigilancia, acceso controlado y monitoreo constante. Esto es clave para evitar intrusiones físicas que comprometan la infraestructura que sustenta los servicios en la nube.
   - Seguridad de Datos en Tránsito: Debe asegurar que los datos que viajan entre el cliente y la nube estén cifrados y protegidos mediante protocolos. Esta medida previene el robo o manipulación de información sensible durante la transmisión.

   Responsabilidades del Cliente:

   - Protección de Datos: El cliente debe aplicar cifrado y políticas de seguridad a los datos almacenados. Esta responsabilidad es esencial para cumplir con normativas como GDPR y prevenir accesos no autorizados a información confidencial.
   - Gestión de Accesos: El cliente debe configurar adecuadamente los permisos, usuarios y autenticaciones. Una mala gestión de accesos puede facilitar filtraciones internas o ataques externos, afectando directamente la confidencialidad y reputación de la empresa.

2. **Escenarios por Tipo de Servicio:** Explica un ejemplo de incidente para IaaS, PaaS y SaaS debido a la falta de cumplimiento de responsabilidades del cliente. ¿Cómo podría haberse evitado cada uno?

   (R). IaaS: Atacantes acceden con credenciales robadas, comprometiendo los recursos críticos. Se podría haber evitado implementando autenticación multifactor (MFA). PaaS: Usuarios externos acceden a datos confidenciales. Se podría haber evitado estableciendo reglas de acceso seguras y segmentación de usuarios en la base de datos. SaaS: Empleados acceden a documentos sensibles sin justificación. Se podría haber evitado revisando y ajustando la configuración de accesos desde el inicio.

3. **Evaluación de Riesgos:** ¿Qué riesgos pueden surgir si el cliente no comprende el modelo de responsabilidad compartida? Menciona dos medidas de mitigación para evitar estos riesgos.

   (R). Riesgos: Robo de información por accesos no seguros y pérdida de datos críticos debido a la falta de respaldo.

   Medidas de mitigación: Capacitación, el personal debe entender bien su rol en el modelo compartido y auditorías continuas, para detectar errores en configuraciones o accesos.

4. **Reflexión Final:** Reflexiona sobre cómo una organización puede fortalecer su seguridad aplicando correctamente el modelo de responsabilidad compartida.

   (R). Aplicar correctamente el modelo de responsabilidad compartida permite a una organización definir con claridad qué tareas debe asumir el proveedor y cuáles le corresponden como cliente. Esta claridad evita errores comunes como asumir que la seguridad es completamente responsabilidad del proveedor. Teniendo claro lo anterior, se minimizan riesgos como fugas de información, pérdida de datos o incumplimientos normativos.