Nadia Arellano G.
Ingeniera en Informática

Actividad – Sesión 5: Relación entre los Principios CIA y los Modelos de Despliegue

1. **Características y Riesgos de los Modelos de Despliegue:** Describe dos características de cada modelo (nube pública, privada e híbrida) y menciona un riesgo específico asociado a cada uno.
   (R). Nube Pública: Es de bajo costo de inversión y alta escalabilidad. Uno de sus riesgos es mayor disposición a fugas de datos por el menor control directo sobre la seguridad.
   Nube Privada: Ofrece un mayor control sobre la infraestructura y una alta confidencialidad. Uno de sus riesgos es que tiene una gestión de seguridad más compleja porque responsabiliza completamente a la organización, por lo que requiere especialistas.
   Nube Híbrida: Entrega flexibilidad y eficiencia por la combinación de recursos públicos y privados. Uno de sus riesgos es la posibilidad de transferencias inseguras de datos entre entornos cuando no se implementan controles adecuados.

2. **Análisis de la Confidencialidad en los Modelos de Despliegue:** Explica cómo se garantiza la confidencialidad en cada modelo de despliegue. ¿Cuál crees que es el modelo más seguro en términos de confidencialidad y por qué?
   (R). Nube Pública: Se garantiza la confidencialidad mediante el cifrado de datos en tránsito y en reposo junto con el uso de la autenticación multifactor (MFA). Pero, el control directo sobre la seguridad depende del proveedor.
   Nube Privada: Se garantiza la confidencialidad principalmente a través de controles de acceso personalizados y seguridad a medida de la organización.
   Nube Híbrida: Se garantiza la confidencialidad principalmente a través de segmentación lógica de los datos y cifrado durante las transferencias entre entornos para evitar fugas.

   De acuerdo con la información anterior y con relación a la confidencialidad, creo que el modelo más seguro es la nube privada, porque la organización tiene un control completo sobre la infraestructura y no depende de terceros para aplicar políticas de seguridad estrictas.

3. **Estrategias de Mitigación:** Propón una estrategia de mitigación para cada uno de los modelos que ayude a reducir el riesgo de interrupciones o accesos no autorizados.
   (R). Nube Pública: Realizar cifrado de datos en tránsito y en reposo junto con autenticación multifactor (MFA).

   Nube Privada: Realizar auditorías de seguridad, implementar políticas de acceso mínimo y tener mecanismos de seguridad ante fallos.

   Nube Híbrida: Establecer monitoreo en tiempo real, utilizar cifrado en las transferencias de datos entre entornos y planificar la continuidad operacional para ambos entornos.

Nadia Arellano G.
Ingeniera en Informática

4. **Reflexión Final - Ventajas y Desventajas de los Modelos de Despliegue:** Reflexiona sobre la importancia de seleccionar el modelo adecuado de despliegue en función de las necesidades de seguridad de una organización. ¿Cómo influye esta decisión en la gestión de la confidencialidad, integridad y disponibilidad de los datos?

   (R). Tener claro cuál es el modelo adecuado es muy importante para asegurar una gestión efectiva de la confidencialidad, integridad y disponibilidad de los datos en la nube. Cada modelo presenta ventajas específicas, pero también presenta riesgos que deben ser evaluados de acuerdo con las necesidades de cada empresa.

   Una decisión bien fundamentada influirá en el costo, el control y la seguridad. Elegir el modelo correcto mejorará la eficiencia operativa pero también fortalecerá la resistencia y la confianza de estos sistemas.