Buenas prácticas para gestionar la seguridad de la información

Fase 1: Investigación Guiada (Componente teórico)

1. Modelo de Responsabilidad Compartida:

- ¿Qué es el "Modelo de Responsabilidad Compartida" en la nube?

Es un enfoque en el que tanto el proveedor de servicios en la nube como el cliente comparten responsabilidades sobre la seguridad y operación del entorno. El proveedor asegura la infraestructura y los servicios base, mientras que el cliente es responsable de la configuración, el uso seguro y la protección de los datos.

- ¿Cómo se aplica a un escenario donde ustedes desarrollan una aplicación bancaria (su responsabilidad) y la alojan en un proveedor de nube (su responsabilidad)? Den ejemplos concretos de quién es responsable de qué.

  En una aplicación bancaria en la nube, el equipo de desarrollo es responsable del código, los datos, la configuración y la seguridad lógica. El proveedor de nube gestiona la infraestructura física y los servicios fundamentales que soportan la aplicación.

  Cifrado de Datos en la Nube:

- ¿Por qué es crucial cifrar los datos en una aplicación bancaria?

  El cifrado es fundamental para proteger la información sensible en aplicaciones bancarias, evitando el almacenamiento en texto plano y reduciendo riesgos como el robo de datos y ataques de suplantación.

- ¿Qué tipos de herramientas o servicios de cifrado (en reposo y en tránsito) ofrece un proveedor de nube (como AWS, Azure o Google Cloud) que podrían usar para proteger la información sensible de su app bancaria (ej. saldos, historial de transacciones, datos personales)? Mencionen al menos dos ejemplos de servicios o enfoques.

Cifrado en reposo (data at rest)

Se refiere a proteger los datos almacenados en discos, bases de datos, backups

AWS:

- AWS Key Management Service (KMS) para gestionar claves y cifrar datos en S3, EBS, RDS y DynamoDB..

Google Cloud:

- Cloud KMS, que permite la gestión centralizada de claves para cifrar datos en Cloud Storage, BigQuery y Cloud SQL.

Cifrado en tránsito (data in transit)

Protege los datos mientras se transfieren entre usuarios, servicios o sistemas.

AWS:

- TLS/SSL para comunicaciones: AWS ofrece soporte para TLS en servicios como API Gateway, ELB (Elastic Load Balancer), CloudFront para cifrar conexiones HTTP (HTTPS).

Google Cloud:

- Google Cloud Load Balancing con HTTPS: Termina TLS para tráfico seguro entre cliente y servic 3.

Gestión de Identidades y Accesos (IAM):

- ¿Qué es IAM y cuál es su objetivo principal en un entorno de nube?¿Quién puede acceder (identidades: usuarios, grupos, roles, servicios)?¿Qué pueden hacer (permisos y privilegios)?¿En qué recursos (servicios, bases de datos, APIs, almacenamiento)?

Objetivo principal:

Garantizar accesos seguros mediante permisos mínimos necesarios, reduciendo riesgos de accesos no autorizados o fugas de información.

- ¿Cómo usarían IAM para controlar quién puede acceder a los recursos de su aplicación bancaria en la nube (ej. los desarrolladores al código, los administradores a la base de datos, la aplicación a otros servicios de la nube)? Den un ejemplo de una política de acceso básica que implementarían.

¿Cómo usarían IAM para controlar accesos en su app bancaria en la nube?

Ejemplos de control de acceso con IAM:

- Desarrolladores:

  Acceso a repositorios y entornos de desarrollo, sin permisos sobre bases de datos de producción o servicios críticos. Se asignan roles con permisos mínimos necesarios.

- Administradores de bases de datos:

  Acceso exclusivo a bases de datos de producción para tareas específicas (mantenimiento, backups, monitoreo), sin acceso a código o servicios externos.

- La aplicación (servicio):
  Utiliza roles o identidades gestionadas que limitan su acceso solo a los recursos necesarios. por ejemplo: lectura en base de datos, acceso a servicios de mensajería, sin permisos administrativos.

Ejemplo de una política básica de acceso (AWS IAM Policy)

Supongamos que queremos crear una política para un desarrollador que solo pueda leer el código almacenado en un repositorio de AWS CodeCommit, pero sin acceso a otros recursos.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "codecommit:GitPull",
 "codecommit:ListRepositories",
 "codecommit:GetRepository"
 ],
 "Resource": "*"
 }
 ]
}
```

¿Qué hace?

Permite al usuario listar repositorios, obtener detalles y clonar código, sin permisos para modificar repositorios ni acceder a otros servicios.

. Continuidad del Negocio y Recuperación ante Desastres (BCDR):

- ¿Por qué es VITAL tener un plan de Continuidad del Negocio y Recuperación ante Desastres para una aplicación bancaria?

- Garantizar disponibilidad 24/7, asegurando acceso ininterrumpido a servicios.
- Proteger datos sensibles frente a pérdidas o corrupción.
- Cumplir con normativas regulatorias.
- Mantener la confianza y reputación del banco.
- Minimizar pérdidas económicas y sanciones por interrupciones o fallos.

- ¿Qué estrategias o servicios ofrece la nube para garantizar que su app siga funcionando incluso si ocurre un desastre (ej. fallas de hardware, ataques)? Mencionen al menos dos ejemplos (ej. backups automáticos, replicación de datos, zonas de disponibilidad).

Zonas de Disponibilidad (Availability Zones) y Regiones

Despliegue replicado en múltiples zonas físicas para asegurar alta disponibilidad y failover automático mediante balanceadores de carga.

Backups y restauración automatizada

Copias de seguridad automáticas y restauración a puntos en el tiempo, almacenadas en ubicaciones separadas para protección contra pérdidas o corrupciones.

Replicación síncrona o asíncrona entre bases de datos en diferentes regiones o zonas.

Ejemplo: Amazon Aurora Global Database o Azure Geo-Replication permiten tener una copia casi en tiempo real para recuperación rápida.

5. Evaluación de Proveedores de Servicios Cloud (CSP):

Cumplimiento normativo y certificaciones de seguridad

Es esencial que el proveedor cuente con certificaciones internacionales y del sector financiero, como ISO 27001, PCI DSS, SOC 2, FedRAMP o HIPAA, que aseguran el cumplimiento de estándares rigurosos en protección de datos y controles de seguridad.

2. Seguridad física y lógica de la infraestructura

- ¿Cómo protege el proveedor sus centros de datos? (Control de acceso físico, vigilancia, redundancia eléctrica y climatización).

  Todo lo protege por medio de algoritmos que encriptan la información para que los mal intencionados no hagan daños o falsos positivos en la nube

- ¿Qué mecanismos de seguridad lógica ofrecen? (Firewalls, detección y mitigación de ataques DDoS, monitoreo 24/7, gestión de vulnerabilidades).

Mecanismo	Función principal	Ejemplos en nube
Firewalls	Controlar tráfico y filtrar accesos	Security Groups, WAF
Anti-DDoS	Detectar y mitigar ataques de denegación de servicio	AWS Shield, Azure DDoS, Cloud Armor
Monitoreo 24/7	Supervisar salud, detectar anomalías y alertar	CloudWatch, Azure Monitor, Stackdriver
Gestión de vulnerabilidades	Detectar, analizar y corregir fallos de seguridad	Amazon Inspector, Azure Security Center

- ¿Tienen controles para aislamiento multi-tenant y protección de datos en entornos compartidos?

Sí, existen controles que garantizan el aislamiento entre clientes en entornos compartidos. Los administradores únicamente pueden monitorear las actividades realizadas, sin acceso directo a los datos sensibles.

3. Gestión y control de acceso (IAM) y auditorías

- ¿Qué herramientas ofrece el CSP para la gestión granular de identidades y permisos?

  Servicios IAM (Identity and Access Management) para definir roles, políticas y permisos

precisos. ● ¿Permite la integración con sistemas de autenticación propios (SAML, LDAP, MFA)?

Sí, el proveedor soporta integración con SAML, LDAP y autenticación multifactor (MFA).

- ¿Ofrece capacidades de registro y auditoría detallada (logs de acceso, cambios en configuración) para seguimiento y cumplimiento?

Sí, el proveedor ofrece registros detallados de accesos y cambios de configuración para garantizar monitoreo y cumplimiento normativo.

Fase 2: Aplicación teórica (Modelo Básico de Arquitectura Segura)

Solo el administrador tiene acceso completo al sistema, mientras que los usuarios están limitados al acceso a la interfaz frontend.

Origen	Destino	Propósito / Tipo de Comunicación
Cliente-Usuario	Servidor-Frontend	Interacción con la interfaz de usuario (web/app). Acceso público desde internet.
PC-Admin	Servidor-Backend y Servidor-BD	Administración, mantenimiento, monitoreo y gestión. Acceso restringido y seguro.
Servidor-Frontend	Servidor-Backend	Peticiones de negocio, procesamiento de lógica y reglas. Comunicación interna privada.
Servidor-Backend	Servidor-BD	Acceso a datos, lectura y escritura de información sensible. Comunicación interna privada y segura.
Switch-Core	Todos los dispositivos	Switch conectar físicamente y permitir la comunicación interna en la red.
Switch-Core	Todos los dispositivos	Switch conectar físicamente y permitir la comunicación interna en la red.
Switch-Core	Router-Gateway	Salida hacia internet o redes externas. Tráfico de entrada/salida controlado por firewall.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name PUBLICA
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name PRIVADA
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name MGMT
Switch(config-vlan)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#whire memory
```

- Define las VLANs en el switch con nombres (PÚBLICA, PRIVADA, MGMT), para separar lógicamente el tráfico en diferentes dominios de difusión y mejorar seguridad y organización.

```
Switch#config t
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range Fa0/1 - 2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range Fa0/3 - 4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#interface Fa0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 99
Switch(config-if)#exit
Switch(config)#interface Gi0/1
Switch(config-if)#switchport trunk encapsulation dot1q
                                  ^
% Invalid input detected at '^' marker.

Switch(config-if)#
```

Eligiendo en qué puertos vamos a trabajar

```
Port              Link   VLAN   IP Address         MAC Address
FastEthernet0/1   Up     10     --                 0001.C7C2.8301
FastEthernet0/2   Up     10     --                 0001.C7C2.8302
FastEthernet0/3   Up     20     --                 0001.C7C2.8303
FastEthernet0/4   Up     20     --                 0001.C7C2.8304
FastEthernet0/5   Up     99     --                 0001.C7C2.8305
FastEthernet0/6   Down   1      --                 0001.C7C2.8306
FastEthernet0/7   Down   1      --                 0001.C7C2.8307
FastEthernet0/8   Down   1      --                 0001.C7C2.8308
FastEthernet0/9   Down   1      --                 0001.C7C2.8309
FastEthernet0/10  Down   1      --                 0001.C7C2.830A
FastEthernet0/11  Down   1      --                 0001.C7C2.830B
FastEthernet0/12  Down   1      --                 0001.C7C2.830C
FastEthernet0/13  Down   1      --                 0001.C7C2.830D
FastEthernet0/14  Down   1      --                 0001.C7C2.830E
FastEthernet0/15  Down   1      --                 0001.C7C2.830F
FastEthernet0/16  Down   1      --                 0001.C7C2.8310
FastEthernet0/17  Down   1      --                 0001.C7C2.8311
FastEthernet0/18  Down   1      --                 0001.C7C2.8312
FastEthernet0/19  Down   1      --                 0001.C7C2.8313
FastEthernet0/20  Down   1      --                 0001.C7C2.8314
FastEthernet0/21  Down   1      --                 0001.C7C2.8315
FastEthernet0/22  Down   1      --                 0001.C7C2.8316
FastEthernet0/23  Down   1      --                 0001.C7C2.8317
FastEthernet0/24  Down   1      --                 0001.C7C2.8318
GigabitEthernet0/1 Down  --     --                 0001.C7C2.8319
GigabitEthernet0/2 Down  1      --                 0001.C7C2.831A
Vlan1             Down   1      <not set>          0090.2173.D30C
```

Revisión final del estado y asignación de puertos a VLANs para asegurar que la configuración está correcta y lista para operar.

```
Router>
Router>
Router>enable
Router#config t
Router#config t
Router#config t |
Router#config t |
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0/0.99
Router(config-subif)#encapsulation dot1Q 99 native
Router(config-subif)#ip address 192.168.99.1 255.255.255.0
Router(config-subif)#exit
Router(config)#ip routing
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Hacemos el cli en el otro router

Integrantes:

- SAMUEL ALZATE ECHEVERRI
- JUAN JOSE RIVERA VERGARA
- MARIA CAMILA ROJAS OSPINA