M1877 - Seguridad en Cloud Computing.

José Enrique Rodríguez González.

PEC1: Fundamentos y seguridad en cloud computing.

Indice

Pregunta 1.

El cloud computing es una propuesta tecnológica actualmente muy extendida y aceptada por una gran variedad de empresas de todos los ámbitos. Esta tecnología está basada en diferentes tipos de cloud compuestos de múltiples herramientas y protocolos. En este ejercicio repasaremos algunos de los componentes que integran estas tecnologías y cómo afectan a la seguridad.
Responde a las siguientes preguntas:
a) (1 punto) Comenta cuáles son las principales diferencias entre virtualización completa (virtualbox, kvm, VMware…) y virtualización a escala de sistema operativo (LXC/LXD, Docker, OpenVZ…). Explica las ventajas e inconvenientes de cada una.
b) (1 punto) Analiza los diferentes tipos de hipervisores (bare-metal, hosted) comentados en el primer módulo y extrae conclusiones sobre las ventajas de cada uno.

Respuesta a la pregunta 1.a.

La virtualización es una técnica que permite ejecutar múltiples sistemas operativos o aplicaciones en un mismo servidor físico, utilizando recursos de hardware de manera más eficiente. Existen dos tipos principales de virtualización: la virtualización completa y la virtualización a escala de sistema operativo. Ambos tienen sus propias ventajas e inconvenientes.

1. Virtualización completa (VirtualBox, KVM, VMware, etc.):

- En la virtualización completa, se emula el hardware de una máquina completa, permitiendo que múltiples sistemas operativos diferentes se ejecuten en un mismo servidor físico sin modificaciones. El hipervisor es la capa que media entre el hardware y los sistemas operativos invitados, asignando y administrando los recursos de hardware.

- Ventajas:

    - Permite ejecutar diferentes sistemas operativos en una misma máquina, lo que es útil para la consolidación de servidores y la compatibilidad de aplicaciones.
    - Aísla completamente los entornos de las máquinas virtuales, lo que mejora la seguridad y facilita la gestión de cada máquina virtual de manera independiente.

- Inconvenientes:

    - La emulación del hardware puede generar cierta sobrecarga y reducir el rendimiento en comparación con el hardware nativo.
    - Requiere más recursos de hardware para ejecutar múltiples sistemas operativos, lo que puede aumentar los costos.

2. Virtualización a escala de sistema operativo (LXC/LXD, Docker, OpenVZ, etc.):

- En la virtualización a escala de sistema operativo, se crea un entorno aislado y seguro para ejecutar aplicaciones o procesos dentro de un único sistema operativo. Estos entornos aislados, llamados contenedores, comparten el mismo kernel del sistema operativo y algunos recursos, pero funcionan como entidades separadas.

- Ventajas:

    - Menor sobrecarga en comparación con la virtualización completa, ya que los contenedores comparten el mismo kernel del sistema operativo y no requieren emular el hardware.
    - Mayor densidad de contenedores en un mismo servidor, lo que permite un mejor aprovechamiento de los recursos y reduce los costos.
    - Facilita la portabilidad de las aplicaciones, ya que los contenedores pueden ejecutarse en diferentes plataformas con poco o ningún cambio.

- Inconvenientes:

    - Menor aislamiento entre los contenedores en comparación con la virtualización completa, lo que puede suponer un riesgo de seguridad si un contenedor se ve comprometido.
    - Los contenedores deben ser compatibles con el mismo kernel del sistema operativo, lo que limita la diversidad de sistemas operativos y aplicaciones que se pueden ejecutar en un mismo servidor.

3. Conclusión:
   En resumen, la virtualización completa ofrece un mayor aislamiento y diversidad de sistemas operativos, pero puede tener un mayor impacto en el rendimiento y los recursos. La virtualización a escala de sistema operativo ofrece una mayor eficiencia y portabilidad, pero con un menor aislamiento y diversidad de sistemas operativos compatibles. La elección entre ambas dependerá de los requisitos específicos de la empresa y las aplicaciones que se deseen ejecutar.

Respuesta a la pregunta 1.b.

El cloud computing ha revolucionado la forma en que las empresas almacenan, procesan y gestionan sus datos. Una de las tecnologías fundamentales que respaldan la computación en la nube son los hipervisores, que son programas que permiten la creación y administración de máquinas virtuales en un sistema físico. Existen dos tipos principales de hipervisores: bare-metal y hosted.

1. Bare-metal (Tipo 1):

- Los hipervisores bare-metal, también conocidos como hipervisores de tipo 1, se ejecutan directamente en el hardware del sistema, sin necesidad de un sistema operativo subyacente. Estos hipervisores interactúan directamente con el hardware y proporcionan una capa de abstracción para que las máquinas virtuales puedan funcionar de manera eficiente y segura.

- Ventajas de los hipervisores bare-metal:

    - Mayor rendimiento: Dado que se ejecutan directamente en el hardware, los hipervisores bare-metal ofrecen un mejor rendimiento en comparación con los hipervisores hosted.
    - Mayor seguridad: La ausencia de un sistema operativo subyacente reduce la superficie de ataque y las vulnerabilidades, lo que mejora la seguridad general del sistema.
    - Aislamiento entre máquinas virtuales: Los hipervisores bare-metal proporcionan un mejor aislamiento entre las máquinas virtuales, lo que limita el impacto de problemas o ataques en una máquina virtual sobre las demás.

2. Hosted (Tipo 2):

- Los hipervisores hosted, también llamados hipervisores de tipo 2, se ejecutan como una aplicación dentro de un sistema operativo existente. Estos hipervisores crean y gestionan máquinas virtuales en el mismo sistema operativo en el que se ejecutan, lo que significa que el rendimiento y la seguridad pueden verse afectados por el sistema operativo anfitrión.

- Ventajas de los hipervisores hosted:

    - Facilidad de instalación y uso: Los hipervisores hosted son más fáciles de instalar y utilizar, ya que se ejecutan como una aplicación en un sistema operativo existente. Esto los hace más accesibles para usuarios no expertos.
    - Mayor flexibilidad: Al funcionar como una aplicación en un sistema operativo, los hipervisores hosted ofrecen una mayor flexibilidad en términos de compatibilidad con hardware y software.
    - Menores costos iniciales: Los hipervisores hosted suelen tener costos iniciales más bajos, ya que no requieren hardware dedicado ni sistemas operativos especializados.

3. Conclusión:
   En resumen, los hipervisores bare-metal son una opción más segura y con mejor rendimiento, mientras que los hipervisores hosted ofrecen mayor flexibilidad y facilidad de uso. La elección entre uno u otro dependerá de las necesidades específicas de una empresa, el presupuesto y los requisitos de seguridad y rendimiento.

Pregunta 2.

Explica cuáles son las diferentes opciones del cloud por el nivel de servicio que prestan, con sus ventajas y desventajas, y propón un modelo de negocio basado en una de ellas, teniendo en cuenta los condicionantes, el modelo de monetización, la infraestructura, el nicho y todos los elementos que consideres necesarios y que pueden condicionar un negocio basado en esta tecnología.

Respuesta a Pregunta 2.

Las opciones de servicios en la nube se pueden clasificar en tres niveles principales: Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS). Cada nivel tiene sus propias ventajas y desventajas.

- Infraestructura como Servicio (IaaS):
    - Ventajas:
        - Flexibilidad: Los usuarios pueden escalar fácilmente los recursos según sus necesidades.
        - Costo-eficiencia: Solo se paga por los recursos que se utilizan.
        - Control: Los usuarios mantienen un mayor control sobre la configuración del sistema.
    - Desventajas:
        - Mayor responsabilidad en la gestión: El cliente debe encargarse de la administración y mantenimiento del sistema.
        - Seguridad: Los usuarios son responsables de garantizar la seguridad de su propia infraestructura.
- Plataforma como Servicio (PaaS):
    - Ventajas:
        - Reducción de costos de infraestructura: Los usuarios no necesitan invertir en hardware y software.
        - Facilita el desarrollo: Las herramientas y servicios de desarrollo están integrados en la plataforma.
    - Desventajas:
        - Menos control: Los usuarios tienen menos control sobre la infraestructura y la configuración del sistema.
        - Dependencia del proveedor: La plataforma puede limitar las opciones de tecnologías y herramientas.
- Software como Servicio (SaaS): Ventajas:
    - Accesibilidad: Los usuarios pueden acceder al software desde cualquier dispositivo con conexión a internet.
    - Actualizaciones y mantenimiento: El proveedor se encarga de las actualizaciones y el mantenimiento del software. Desventajas:
    - Personalización limitada: Las opciones de personalización suelen ser limitadas en comparación con soluciones locales.
    - Dependencia del proveedor: La continuidad del negocio depende de la estabilidad y disponibilidad del proveedor del SaaS.

Modelo de negocio propuesto: ***Desarrollo de una plataforma SaaS para gestión de proyectos y colaboración en equipo.***

1. Condicionantes:

- Competencia en el mercado.
- Necesidad de garantizar la seguridad y privacidad de los datos de los clientes.
- Ofrecer una experiencia de usuario satisfactoria y fácil de usar.

2. Modelo de monetización:

- Suscripción mensual o anual basada en el número de usuarios y las funcionalidades requeridas.
- Ofrecer una versión gratuita con funcionalidades limitadas para atraer a nuevos usuarios.
- Servicios adicionales, como soporte premium y capacitación.

3. Infraestructura:

- Utilizar una plataforma PaaS para el desarrollo y despliegue del software, lo que reduce costos y facilita el mantenimiento.
- Implementar medidas de seguridad para proteger la plataforma y los datos de los clientes.

4. Nicho:

- Pequeñas y medianas empresas que buscan una solución de gestión de proyectos y colaboración en equipo accesible y fácil de usar.

5. Elementos adicionales a considerar:

- Integraciones con otras herramientas y servicios populares (CRM, servicios de almacenamiento en la nube, etc.).
- Desarrollar una estrategia de marketing y promoción para llegar al nicho de mercado objetivo.
- Ofrecer soporte al cliente en varios idiomas y adaptar la plataforma a diferentes regiones geográficas.
- Personalización y marca blanca: Permitir a los clientes personalizar la apariencia de la plataforma con su propia marca, lo que puede aumentar la adopción y satisfacción del usuario.
- API abierta: Ofrecer una API abierta para que los desarrolladores externos puedan crear integraciones y complementos adicionales, lo que aumenta la versatilidad de la plataforma y la hace más atractiva para diferentes tipos de usuarios.
- Enfoque en la movilidad: Desarrollar aplicaciones móviles para dispositivos iOS y Android, lo que permitirá a los usuarios acceder y colaborar en la plataforma desde cualquier lugar y en cualquier momento.
- Análisis de datos e informes: Integrar funcionalidades de análisis de datos e informes para ayudar a los usuarios a tomar decisiones basadas en datos y mejorar la eficiencia y la productividad de sus proyectos.
- Establecer alianzas estratégicas: Colaborar con otras empresas y proveedores de servicios en la nube para ampliar la oferta de productos y aumentar la visibilidad y el alcance en el mercado.
- Programa de afiliados y referidos: Implementar un programa de afiliados y referidos para incentivar a los clientes actuales a recomendar la plataforma a otros, generando un crecimiento orgánico y reduciendo los costos de adquisición de nuevos clientes.

- Cumplimiento con regulaciones y estándares: Asegurar que la plataforma cumpla con las regulaciones y estándares locales e internacionales en términos de privacidad y protección de datos, como el GDPR, para generar confianza en los clientes y evitar posibles sanciones.
- Programa de pruebas beta: Antes del lanzamiento, realizar un programa de pruebas beta con un grupo de usuarios seleccionados, lo que permitirá obtener comentarios y realizar mejoras en la plataforma antes de su lanzamiento oficial.
- Escuchar a los usuarios: Establecer canales de comunicación efectivos con los usuarios para recibir retroalimentación y sugerencias, lo que permitirá mejorar continuamente la plataforma y adaptarse a las necesidades cambiantes del mercado.
- Estrategia de precios flexible: Ofrecer diferentes planes de precios y opciones de suscripción para adaptarse a las necesidades y presupuestos de diversos tipos de usuarios y empresas. También se pueden ofrecer descuentos para usuarios que se comprometan a suscripciones anuales o para organizaciones sin fines de lucro y educativas.

Pregunta 3.

a) (1 punto) Realiza un cuadro comparativo explicando de quien depende la responsabilidad de la seguridad en los distintos modelos de servicios cloud (IaaS/PaaS/SaaS).

b) (1 punto) Analiza las principales amenazas de seguridad relacionadas a servicios en el cloud y comenta qué mecanismos podemos introducir para minimizar todos estos riesgos. Detalla qué nos aporta tener nuestros servicios en cloud.

Respuesta a Pregunta 3.a.

Modelo de Servicio Cloud	**Responsabilidad de seguridad**
IaaS (Infrastructure as a Service)	Compartida entre el proveedor y el usuario. El proveedor se encarga de asegurar la infraestructura básica, como la seguridad física de los servidores y la protección contra ataques externos. El usuario es responsable de la configuración y la gestión de la seguridad de la aplicación y de los datos alojados en la infraestructura.
PaaS (Platform as a Service)	Principalmente del proveedor. El proveedor se encarga de asegurar la plataforma y proporcionar herramientas para la gestión de la seguridad de la aplicación y de los datos. Sin embargo, el usuario también tiene cierta responsabilidad en la configuración y uso adecuado de estas herramientas.
SaaS (Software as a Service)	Totalmente del proveedor. El proveedor es responsable de la seguridad de la aplicación y de los datos alojados en su plataforma, así como de garantizar la disponibilidad y el acceso a los servicios. El usuario no tiene control sobre la infraestructura ni sobre la gestión de la seguridad.

En resumen, la responsabilidad de la seguridad en los distintos modelos de servicios cloud varía según el nivel de control y gestión que tenga el usuario sobre la infraestructura y la plataforma. En IaaS, la responsabilidad es compartida, mientras que en PaaS y SaaS es principalmente del proveedor.

Respuesta a Pregunta 3.b.

Las principales amenazas de seguridad relacionadas con los servicios en el cloud incluyen:

1. Ataques externos: Una de las mayores preocupaciones es la exposición de los datos a ataques externos, como virus, malware, ataques DDoS (Denegación de Servicio Distribuido) y hacking.
2. Pérdida de datos: La pérdida de datos puede ser causada por fallos en el hardware, desconexiones de la red, errores humanos, etc.
3. Acceso no autorizado: El acceso no autorizado a los datos almacenados en la nube puede ser una amenaza importante para la privacidad y la seguridad de los datos.

Para minimizar estos riesgos, es importante implementar medidas de seguridad efectivas, como:

1. Cifrado de datos: El cifrado de datos ayuda a proteger los datos contra accesos no autorizados y pérdida de datos.
2. Autenticación de usuarios: La autenticación de usuarios es una medida importante para garantizar que solo personas autorizadas tengan acceso a los datos almacenados en la nube.
3. Copias de seguridad regulares: Las copias de seguridad regulares ayudan a proteger los datos contra la pérdida de datos.
4. Control de acceso: El control de acceso es una medida importante para garantizar que solo personas autorizadas tengan acceso a los datos almacenados en la nube.

Tener nuestros servicios en el cloud nos aporta muchas ventajas, como:

1. Flexibilidad: Los servicios en el cloud permiten acceder a los datos y aplicaciones desde cualquier lugar y dispositivo con conexión a Internet.
2. Escalabilidad: Los servicios en el cloud permiten ajustar la capacidad de almacenamiento y procesamiento de acuerdo con las necesidades de negocio.
3. Costos: Los servicios en el cloud suelen ser más económicos que los servicios tradicionales de TI, ya que no requieren una inversión en hardware y software costoso.
4. Fiabilidad: Los servicios en el cloud están respaldados por proveedores de confianza, que ofrecen garantías de disponibilidad y continuidad del servicio.

En resumen, es importante tener en cuenta las amenazas de seguridad relacionadas con los servicios en el cloud y adoptar medidas de seguridad efectivas para minimizar estos riesgos. Al mismo tiempo, los servicios en el cloud ofrecen muchas ventajas, como flexibilidad, escalabilidad, costes y fiabilidad.

Pregunta 4.

El Cloud Control Matrix (CCM) es una herramienta (en formato Excel) para el control de la seguridad en cloud computing alineada con el conjunto de buenas prácticas que nos ofrece el Cloud Security Alliance (CSA). El objetivo de este conjunto de controles es el poder disponer de una hoja de ruta práctica y ejecutable para ayudar a las organizaciones a evaluar el riesgo asociado de contratar servicios en proveedores basados en el cloud.

Como podréis comprobar esta herramienta está compuesta por 17 dominios de control donde se engloban los diferentes campos relacionados con arquitecturas cloud:

1. Audit & Assurance - A&A
2. Application & Interface Security - AIS
3. Business Continuity Management and Operational Resilience - BCR
4. Change Control and Configuration Management - CCC
5. Cryptography, Encryption & Key Management - CEK
6. Datacenter Security - DCS
7. Data Security and Privacy Lifecycle Management - DSP
8. Governance, Risk and Compliance - GRC
9. Human Resources - HRS
10. Identity & Access Management - IAM
11. Interoperability & Portability - IPY
12. Infrastructure & Virtualization Security - IVS
13. Logging and Monitoring - LOG
14. Security Incident Management, E-Discovery, & Cloud Forensics - SEF
15. Supply Chain Management, Transparency, and Accountability - STA
16. Threat & Vulnerability Management - TVM
17. Universal Endpoint Management - UEM

Para la realización de este ejercicio primero deberás descargarte la herramienta (https://cloudsecurityalliance.org/research/cloud-controls-matrix/ también está en el excel adjunto) y responder a las siguientes preguntas:

a) (1,5 puntos) Selecciona uno de los 17 dominios de control definidos en la Cloud Controls Matrix (CCM) y revisa de forma detallada los controles de seguridad que incluye, a continuación elige 5 controles y describe alguna de las medidas para cumplir con el control seleccionado. Puedes ayudarte de la CCM de alguno de los proveedores públicos más conocidos como AWS, Azure o Google Cloud.
b) (1,5 puntos) Si tuvieras que desplegar un servicio en la nube (web corporativa) qué dominios de seguridad definidos en la CCM darías prioridad y en base al cumplimiento de qué controles basarías tu elección. Justifica tu respuesta.

Respuesta a Pregunta 4.a.

Para elaborar esta pregunta me voy a apoyar en el CCM de Google Cloud para tratar todos los controles relativos al apartado `10. Identity & Access Management - IAM`.

El dominio Identity & Access Management (IAM) se refiere a la gestión de identidades y accesos dentro de una arquitectura cloud.

IAM-01: Política y procedimientos de gestión de identidades y accesos

- IAM-01 se refiere a la política y procedimientos de gestión de identidades y accesos, que deben ser definidos para garantizar que los usuarios tengan acceso solo a los recursos que necesitan para realizar sus tareas.
- Para cumplir con este control en Google Cloud, se pueden utilizar las siguientes medidas:
    - Crear reglas de acceso basadas en roles para controlar los permisos de los usuarios.
    - Configurar la autenticación de dos factores para fortalecer la seguridad de las cuentas de usuario.
    - Crear políticas de seguridad que establezcan los requisitos mínimos para las contraseñas, como la longitud y la complejidad.

IAM-02: Política y procedimientos de contraseñas seguras

- IAM-02 se refiere a la política y procedimientos de contraseñas seguras. Esto incluye la implementación de medidas de seguridad para proteger las contraseñas y prevenir su uso no autorizado.
- Para cumplir con este control en Google Cloud, se pueden utilizar las siguientes medidas:
    - Implementar la autenticación de dos factores para fortalecer la seguridad de las contraseñas.
    - Configurar el tiempo de caducidad de las contraseñas y requerir que los usuarios cambien sus contraseñas periódicamente.
    - Prohibir la reutilización de contraseñas antiguas y implementar la verificación de contraseñas débiles.

IAM-03: Inventario de identidades

- Este control requiere que las organizaciones mantengan un registro completo y actualizado de todas las identidades y sus permisos de acceso a los recursos en la nube.
- Para cumplir con este control en Google Cloud, se pueden utilizar los siguientes recursos:
    - Google Cloud Identity: Es un sistema de gestión de identidades que permite a las organizaciones administrar y controlar los permisos de acceso de los usuarios a los recursos en la nube de Google.
    - IAM: El sistema de Identity and Access Management de Google Cloud permite a las organizaciones asignar roles y permisos específicos a usuarios y grupos, lo que ayuda a mantener un control sobre quién tiene acceso a qué recursos.
    - Registro de auditoría: Google Cloud ofrece un registro de auditoría detallado que permite a las organizaciones monitorear y auditar los accesos y permisos de los usuarios en la nube.

IAM-04: Separación de funciones

- Este control requiere que las organizaciones implementen medidas de seguridad para evitar conflictos de intereses y garantizar que los usuarios no tengan acceso a recursos o información a los que no estén autorizados.
- Para cumplir con este control en Google Cloud, se pueden utilizar los siguientes recursos:
    - Roles: Google Cloud permite a las organizaciones crear roles personalizados y asignarlos a los usuarios, lo que ayuda a mantener una separación de funciones y a evitar conflictos de intereses.
    - Permisos: Google Cloud ofrece una gran variedad de permisos que se pueden asignar a los usuarios, lo que ayuda a controlar y limitar el acceso a los recursos en la nube.
    - Políticas de acceso: Google Cloud permite a las organizaciones crear políticas de acceso que definen los permisos y restricciones de acceso de los usuarios a los recursos en la nube.

IAM-05:Privilegio mínimo

- Este control se refiere a la práctica de asignar el nivel mínimo de privilegios necesarios para realizar una tarea específica. De esta manera, se minimiza el riesgo de acceso no autorizado o daños causados por errores humanos.
- Para cumplir con este control en Google Cloud, se pueden utilizar los siguientes recursos:
    - Utilizar roles predefinidos que proporcionen el nivel mínimo de acceso necesario para realizar una tarea específica.
    - Utilizar reglas de seguridad de acceso condicional para limitar el acceso a recursos específicos basándose en las necesidades del usuario.

IAM-06:Aprovisionamiento de acceso de usuarios

- Este control se refiere a la gestión de los procesos de aprovisionamiento de acceso para los usuarios, incluyendo la asignación y revocación de permisos. Es importante asegurarse de que los usuarios tengan acceso solo a los recursos que necesitan para realizar sus tareas y que los permisos se revoquen cuando ya no sean necesarios.
- Para cumplir con este control en Google Cloud, se pueden utilizar los siguientes recursos:
    - Utilizar el panel de control de IAM de Google Cloud para gestionar los permisos de acceso de los usuarios.
    - Utilizar scripts o herramientas de automatización para aprovisionar y revocar permisos de acceso de manera eficiente.

IAM-07:Cambios y revocación de acceso de usuarios

- Google Cloud IAM permite a los administradores de seguridad revocar o modificar los permisos de acceso de los usuarios en tiempo real.
    - Para cumplir con este control en Google Cloud, puede hacerse mediante la eliminación o modificación de roles asignados a los usuarios.

IAM-08:Revisión de acceso de usuarios

- Este control es esencial para mantener la seguridad de la información y los recursos en el cloud.
- Para cumplir con este control en Google Cloud, se pueden utilizar los siguientes recursos:
    - Asignación de roles basados en el acceso: Google Cloud permite asignar roles a los usuarios que definen los permisos y privilegios de acceso a los recursos y datos en el cloud.
    - Revisión periódica de permisos de acceso: Google Cloud permite realizar revisiones periódicas de los permisos de acceso de los usuarios para asegurarse de que solo los usuarios autorizados tengan acceso a los recursos y datos sensibles.
    - Eliminación de cuentas inactivas: Google Cloud permite eliminar automáticamente las cuentas de usuario inactivas para evitar que los usuarios que ya no necesitan acceso tengan acceso a los recursos y datos sensibles.
    - Monitoreo de actividades de acceso: Google Cloud permite monitorear las actividades de acceso de los usuarios para detectar cualquier actividad sospechosa o no autorizada.

IAM-09:Segregación de roles de acceso privilegiado

- Es la función de asignar diferentes niveles de acceso y privilegios a los usuarios y sistemas en una organización. Esto significa que cada usuario o sistema solo tiene acceso a los recursos y servicios que necesita para realizar su trabajo, y no tiene acceso a otros recursos o servicios que no son relevantes o que podrían poner en riesgo la seguridad de la organización.
- Para cumplir con este control en Google Cloud, se pueden utilizar los siguientes recursos:
    - Asignación de roles: Google Cloud permite asignar roles a los usuarios y grupos en función de sus necesidades y responsabilidades, lo que permite una separación clara de los roles y privilegios de acceso.
    - Control de acceso basado en roles: Los roles en Google Cloud se pueden definir con un conjunto de permisos y políticas, lo que permite controlar y limitar el acceso a los recursos y servicios en la plataforma.
    - Uso de cuentas de servicio: Google Cloud permite crear cuentas de servicio para automatizar tareas y limitar el acceso a los recursos y servicios a través de roles específicos.
    - Monitoreo y registro de actividades: Google Cloud ofrece herramientas de monitoreo y registro de actividades para rastrear y auditar el acceso y la actividad de los usuarios en la plataforma.

IAM-10:Gestión de roles de acceso privilegiado

- Este control se enfoca en asegurar que se tenga una gestión adecuada de los roles de acceso privilegiado en la nube, lo que incluye la asignación, revocación y monitoreo de permisos a usuarios con acceso administrativo.
- Google Cloud ofrece una solución integrada de IAM que permite a los usuarios asignar y gestionar roles a usuarios y equipos específicos. Los roles se pueden asignar a nivel de proyecto o de recurso, y los permisos se pueden personalizar para limitar el acceso a los recursos apropiados.

IAM-11:Aprobación de CSC para roles de acceso privilegiado acordados

- Se refiere a la aprobación de roles de acceso privilegiado por parte de los responsables de seguridad de la información (CSC, por sus siglas en inglés). Esto significa que antes de que un usuario tenga acceso a cualquier recurso con privilegios elevados, debe ser aprobado por el CSC.
- Para cumplir con este control en Google Cloud, se pueden tomar las siguientes medidas:
    - Creación de roles de acceso privilegiado: Se pueden crear roles de acceso privilegiado en Google Cloud que tengan acceso a los recursos y acciones esenciales para el trabajo.
    - Aprobación por parte del CSC: Antes de que un usuario tenga acceso a estos roles, el CSC debe revisar y aprobar el acceso.
    - Monitoreo y revocación: Una vez que se ha aprobado el acceso, es importante monitorear de cerca el uso de los roles y revocarlos si se detecta un uso inapropiado.

IAM-12:Proteja la integridad de los registros

- Este control específico se enfoca en proteger la integridad de los registros de acceso y usuarios en la nube.
- Para cumplir con este control en Google Cloud, se pueden tomar las siguientes medidas:
    - Uso de autenticación de dos factores: para proteger la integridad de los registros de acceso, es importante habilitar la autenticación de dos factores para todos los usuarios que tengan acceso a los recursos en la nube.
    - Monitoreo y supervisión de actividades: Google Cloud ofrece la capacidad de monitorear y supervisar las actividades de los usuarios en tiempo real, lo que permite detectar y mitigar cualquier intento de acceso no autorizado o actividad sospechosa.
    - Registro de auditoría: Google Cloud también proporciona un registro de auditoría detallado para todas las acciones realizadas por los usuarios, lo que permite una revisión exhaustiva de las actividades y una mejor protección de la integridad de los registros de acceso.
    - Políticas de contraseñas seguras: se recomienda establecer políticas de contraseñas seguras que requieran la creación de contraseñas fuertes y la rotación periódica de las mismas para proteger los registros de acceso.

IAM-13:Usuarios identificables de forma única

- Este control es importante para garantizar la seguridad y controlar quién tiene acceso a qué recursos y a qué nivel.
- Para cumplir con este control en Google Cloud, se pueden tomar las siguientes medidas:
    - Utilizar cuentas de usuario únicas: Cada usuario debe tener una cuenta única con información de inicio de sesión y contraseña segura.
    - Configurar autenticación de dos factores (2FA): La autenticación de dos factores proporciona una capa adicional de seguridad, ya que requiere que el usuario proporcione dos formas de identificación.
    - Monitoreo y auditoría de actividades: Es importante monitorear y auditar las actividades de los usuarios para detectar cualquier actividad sospechosa o no autorizada.
    - Políticas de contraseñas seguras: Las políticas de contraseñas seguras, como la longitud de la contraseña y la frecuencia de cambios de contraseña, deben establecerse para garantizar la seguridad de la información.

IAM-14:Autenticación reforzada

- Este control se refiere a la necesidad de implementar medidas adicionales para verificar la identidad de un usuario antes de otorgarle acceso a los recursos en el cloud.
- En Google Cloud, existen varias medidas que se pueden implementar para cumplir con este control:
    - Uso de contraseñas seguras: Google Cloud permite exigir a los usuarios que utilicen contraseñas seguras y complejas para proteger sus cuentas.
    - Verificación de dos factores (2FA): Google Cloud permite habilitar la verificación de dos factores para mejorar la seguridad de las cuentas de los usuarios.
    - Uso de certificados SSL: Google Cloud permite utilizar certificados SSL para cifrar la información y garantizar la privacidad de los datos.
    - Monitoreo de accesos: Google Cloud ofrece herramientas de monitoreo de accesos para detectar y prevenir accesos no autorizados a los recursos en el cloud.

IAM-15:Gestión de contraseñas

- Este control es importante para garantizar que los usuarios utilicen contraseñas seguras y únicas para acceder a los recursos en la nube.
- Algunas medidas para cumplir con el control IAM-15 en Google Cloud incluyen:
    - Política de contraseñas: Establecer una política de contraseñas que incluya requisitos como la longitud, la complejidad y la frecuencia de cambio de las contraseñas.
    - Autenticación de dos factores: Habilitar la autenticación de dos factores para reforzar la seguridad de las cuentas de usuario.
    - Monitoreo de inicios de sesión: Monitorear los inicios de sesión para detectar posibles intentos de acceso no autorizados.
    - Gestión de contraseñas débiles: Impedir que los usuarios utilicen contraseñas débiles o comunes.
    - Almacenamiento seguro de contraseñas: Almacenar las contraseñas de los usuarios de manera segura, utilizando cifrado y otras medidas de seguridad.

IAM-16:Mecanismos de autorización

- Este control hace hincapié en la importancia de tener mecanismos de autorización sólidos en place para garantizar que solo los usuarios autorizados tengan acceso a los recursos y datos en la nube.
- En Google Cloud, existen varias medidas que se pueden implementar para cumplir con los controles de IAM-16:
    - Asignación de roles: Google Cloud permite asignar roles a los usuarios y grupos que controlan qué acciones pueden realizar en la nube. Esto permite una gran flexibilidad en la asignación de permisos y facilita la gestión de los mismos.
    - Autenticación de dos factores: La autenticación de dos factores (2FA) es una medida adicional de seguridad que requiere que los usuarios proporcionen dos formas de identificación antes de acceder a los recursos. Esto reduce el riesgo de accesos no autorizados.
    - Uso de credenciales seguras: Google Cloud permite la creación y gestión de credenciales seguras para los usuarios y servicios. Esto garantiza que solo los usuarios autorizados tengan acceso a los recursos y a los datos.
    - Monitoreo y registro de actividades: Google Cloud proporciona un sistema de monitoreo y registro de actividades que permite a los administradores de seguridad ver qué acciones están realizando los usuarios y detectar cualquier actividad sospechosa.

Respuesta a Pregunta 4.b.

Si tuviera que desplegar un servicio en la nube, como una web corporativa, daría prioridad a los siguientes dominios de seguridad definidos en la CCM:

1. Data Security and Privacy Lifecycle Management (DSP):

La protección de datos es crucial en cualquier servicio en la nube, y es especialmente importante para una web corporativa. Asegurarse de que los datos del cliente están seguros y protegidos es esencial para construir confianza y credibilidad.

Para cumplir con este dominio de seguridad, se debe asegurar la protección de los datos a través de su ciclo de vida completo, incluyendo la recolección, almacenamiento, procesamiento y eliminación segura de los mismos.

2. Identity & Access Management (IAM):

La gestión de identidades y accesos es un aspecto clave de la seguridad en la nube. Es necesario garantizar que solo los usuarios autorizados tengan acceso a los datos y sistemas relevantes.

Para cumplir con este dominio de seguridad, se deben implementar políticas y procedimientos para la gestión de identidades y accesos, tales como autenticación, autorización y administración de cuentas de usuario.

3. Infrastructure & Virtualization Security (IVS):

La infraestructura y la virtualización son fundamentales en la nube, y es importante garantizar que se apliquen controles adecuados para protegerlas.

Para cumplir con este dominio de seguridad, se deben implementar medidas de seguridad para la infraestructura de la nube y la virtualización, incluyendo la segmentación de redes, la protección contra malware y la autenticación para el acceso a las consolas de administración.

4. Logging and Monitoring (LOG):

La supervisión y registro de eventos es un aspecto importante de la seguridad en la nube. Es necesario recopilar y analizar los registros de eventos para identificar actividades sospechosas o malintencionadas.

Para cumplir con este dominio de seguridad, se deben implementar mecanismos de registro y supervisión, incluyendo la configuración de alertas y la implementación de mecanismos de auditoría.

En estos dominios de seguridad anteriormente indicados se basaría mi elección para desplegar un servicio en la nube. En particular, me aseguraría de que se cumplan los controles relacionados con la protección de datos, la gestión de identidades y accesos, la seguridad de la infraestructura y la virtualización, y la supervisión y registro de eventos. Estos controles son fundamentales para garantizar la seguridad y protección de un servicio en la nube basándonos en los pilares de la seguridad de la información (disponibilidad, integridad, confidencialidad, trazabilidad y no repudio). Estos dominios son fundamentales para la implementación de cualquier organización que desee desplegar un servicio en la nube, debiendo de ser concretamente tratadas y asesoradas durante el ERS del sistema con el cliente para un desarrollo idóneo, eficiente y seguro del mismo.