Instituto Tecnológico y de Estudios Superiores de Monterrey

Inteligencia Artificial Avanzada para la Ciencia de Datos II

Grupo 101

31 de octubre de 2024

Evidencia Portafolio - Módulo cloud computing

Autor:

Catherine Johanna Rojas Mendoza - A01798149

Profesor:

Félix Ricardo Botello Urrutia

Resumen

Se realiza un análisis de las prácticas de seguridad en el almacenamiento y procesamiento en la nube de tres proveedores principales: AWS, Google Cloud y Azure. Se discute el contexto normativo y se evalúan sus características de seguridad, como el cifrado de datos en reposo y en tránsito, políticas de acceso y autenticación multifactorial. A través de una matriz comparativa con cada proveedor. Se concluye que implementar una combinación de cifrado avanzado, control de acceso estricto y auditorías periódicas es esencial para garantizar la protección de datos en entornos de nube.

Abstract

An analysis of the security practices in cloud storage and processing is conducted for three main providers: *AWS, Google Cloud, and Azure. The regulatory context is discussed, and their security features, such as data encryption at rest and in transit, access policies, and multifactor authentication, are evaluated. This is done through a comparative matrix with each provider. It is concluded that implementing a combination of advanced encryption, strict access control, and regular audits is essential to ensure data protection in cloud environments.*

Palabras clave: seguridad en la nube, almacenamiento de datos, cifrado de datos, control de acceso, autenticación multifactorial, proveedores de nube (AWS, Google Cloud, Azure), protección de datos.

Keywords: *cloud security, data storage, data encryption, access control, multifactor authentication, cloud providers* (*AWS, Google Cloud, Azure*), *data protection.*

Índice

1. Introducción

La creciente dependencia de los servicios en la nube por parte de empresas y organizaciones ha incrementado la necesidad de asegurar la protección de los datos almacenados y procesados en estos entornos. En este contexto, la seguridad en la nube se ha convertido en un tema de gran relevancia, particularmente cuando se consideran los aspectos normativos y de cumplimiento que regulan el uso de tecnologías de la información.

Este trabajo se enfoca en analizar las prácticas de seguridad implementadas por tres de los proveedores de servicios en la nube más importantes: AWS, Google Cloud y Azure. Específicamente, se abordan aspectos clave como el cifrado de datos en reposo y en tránsito, las políticas de control de acceso, y la autenticación multifactorial, comparándolos mediante una matriz que permite identificar fortalezas y debilidades.

A través de este análisis, se busca establecer las mejores prácticas que deben seguirse para garantizar un alto nivel de seguridad en entornos de nube, promoviendo así la confianza de los usuarios y el cumplimiento de los estándares regulatorios vigentes.

2. Evaluación de Prácticas de Almacenamiento y Procesamiento en la Nube

2.1. Contexto Normativo

El artículo 32 del Reglamento General de Protección de Datos (RGPD) establece que las organizaciones deben implementar “medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado para el riesgo”, incluyendo estrategias como la seudonimización y el cifrado de datos personales. La implementación de cifrado de datos es una medida esencial para mitigar los riesgos de acceso no autorizado y para cumplir con las normativas de seguridad en la protección de datos personales. El cifrado efectivo de datos minimiza el riesgo de exposición de datos y asegura que solo aquellos con acceso autorizado puedan acceder a la información.[17]

Características de Seguridad

2.2. AWS - Características de Seguridad

AWS ofrece una arquitectura de seguridad en la nube que incorpora medidas tanto para el cifrado de datos en reposo como en tránsito. La seguridad es una responsabilidad compartida entre AWS y el cliente: gestiona la “seguridad de la nube” (infraestructura, red y centros de datos), mientras que el cliente es responsable de la “seguridad

en la nube" (configuración y acceso a los datos y recursos).[7]

2.2.1. Cifrado de Datos en Reposo

AWS proporciona múltiples opciones para cifrar datos almacenados, que se adaptan a distintos tipos de almacenamiento y cumplen con requisitos de cumplimiento normativo. Los clientes pueden utilizar el AWS Key Management Service (KMS) para administrar claves y cifrar datos con AES-256. Además, servicios como Amazon S3, Amazon EBS y Amazon RDS admiten cifrado en reposo, permitiendo la protección de datos almacenados sin intervención del usuario.[11]

Opciones de Cifrado:

- **Cifrado en el Nivel del Disco:** Utiliza XTS-AES-256 para proteger el almacenamiento de instancias de Amazon EC2, con claves únicas generadas y destruidas al detener la instancia, evitando la recuperación de datos.
- **Cifrado en el Nivel del Sistema de Archivos:** Permite cifrar archivos y directorios de forma independiente, compatible con varios sistemas operativos, como EFS en NTFS.

2.2.2. Cifrado de Datos en Tránsito

AWS promueve el cifrado de datos en tránsito mediante conexiones seguras (TLS) en todas las interacciones entre los sistemas y los recursos de AWS. Las opciones incluyen la Virtual Private Cloud (VPC) y la AWS Client VPN para establecer conexiones privadas seguras entre entornos corporativos y recursos en la nube.[12]

Opciones de Conectividad Segura:

- **Amazon VPC:** Proporciona una red virtual aislada para el despliegue de recursos, permitiendo gestionar direcciones IP, subredes y tablas de enrutamiento.
- **AWS Direct Connect y Site-to-Site VPN:** Facilitan conexiones privadas con seguridad física e IPsec, asegurando el transporte de datos entre redes corporativas y Amazon VPC.
- **AWS Certificate Manager (ACM):** Simplifica la gestión de certificados SSL/TLS para cifrar la comunicación entre aplicaciones, soportando el cifrado HTTPS con Elastic Load Balancing y Amazon CloudFront.

2.3. Google Cloud - Características de Seguridad

Google Cloud emplea un enfoque integral de encriptación para proteger los datos en reposo, en tránsito y en uso, garantizando altos niveles de seguridad y cumpliendo con normativas como el RGPD. Estas medidas incluyen la autenticación, integridad y privacidad de datos en diferentes capas de la red.[27]

2.3.1. Cifrado de Datos en Reposo

Google Cloud cifra los datos almacenados en discos duros, SSD y copias de seguridad mediante algoritmos de Encriptación Avanzada (AES), usando AES-256 como estándar predeterminado. Los datos son fragmentados en subarchivos, cada uno con una clave de encriptación de datos (DEK) única, proporcionando seguridad adicional mediante la encriptación redundante de capas.

- **Capas de Encriptación:** Google aplica múltiples capas de encriptación desde los sistemas de archivos hasta los dispositivos de almacenamiento, utilizando una DEK específica para cada fragmento de datos, lo que dificulta el acceso no autorizado.[22]
- **Cloud Key Management Service (KMS):** Permite a los clientes gestionar sus propias claves de encriptación, incluyendo su creación, rotación y auditoría, proporcionando control y transparencia.
- **Encriptación de Copias de Seguridad:** Google cifra cada copia de seguridad de forma individual con DEKs únicas, asegurando que los archivos de respaldo no se expongan como texto plano.

2.3.2. Cifrado de Datos en Tránsito

Google Cloud protege los datos en tránsito con medidas de encriptación que buscan mantener la autenticidad, integridad y privacidad de los datos durante su transferencia, tanto dentro de su infraestructura como hacia ubicaciones externas.[25]

- **Protocolos de Seguridad:** Google utiliza TLS para asegurar las comunicaciones con sus servicios y ofrece túneles IPSec y certificados SSL para conexiones WAN seguras.
- **Encriptación de Red Privada Virtual (VPC):** El tráfico entre máquinas virtuales dentro de la misma VPC se encripta automáticamente, protegiendo los datos durante su transferencia entre servicios de Google o redes corporativas.

- **Confidential Computing:** Google Cloud utiliza máquinas virtuales confidenciales que encriptan los datos en uso, además del cifrado de datos en tránsito y reposo, asegurando que no puedan ser accedidos sin la autenticación adecuada.

Con estas características, Google Cloud garantiza una estrategia de seguridad robusta que permite a los clientes mantener el control sobre sus datos y protegerlos contra accesos no autorizados o exposiciones de información.

2.4. Azure - Características de Seguridad

Azure implementa una sólida estrategia de cifrado de datos en reposo y en tránsito, garantizando que los clientes mantengan el control de sus datos en todo momento y asegurando la protección contra accesos no autorizados.[51]

2.4.1. Cifrado de Datos en Reposo

Para la protección de los datos almacenados, Azure utiliza cifrado avanzado AES-256, conforme a la norma FIPS 140-2, que aplica a múltiples servicios como Azure Storage, Azure SQL Database y Azure Data Lake. Azure ofrece diferentes modelos de cifrado de datos en reposo, que incluyen: [46]

- **Cifrado del Servidor:** Utiliza claves administradas por el servicio o por el cliente en Azure Key Vault, permitiendo flexibilidad en la gestión de claves, que pueden almacenarse en entornos locales o hardware controlado.
- **Cifrado de Datos Transparente (TDE) en Azure SQL Database:** Cifra en tiempo real archivos de datos y registros en SQL Database con AES o 3DES, incluyendo la opción de cifrar columnas específicas para mayor granularidad.
- **Cifrado de Azure Data Lake Store:** Los datos se cifran automáticamente en reposo durante la creación de cuentas con MEK, DEK y BEK. Las empresas pueden optar por gestionar sus propias claves para mayor control.
- **Azure Key Vault:** Facilita la gestión y control de acceso a claves de cifrado mediante permisos configurados con Microsoft Entra, sin necesidad de módulos de seguridad de hardware.

2.4.2. Cifrado de Datos en Tránsito

Para la protección de datos en tránsito, Azure implementa medidas robustas que incluyen protocolos de seguridad estándar como TLS y IPsec, asegurando la integridad y confidencialidad de los datos mientras se transfieren entre clientes y centros de datos de Microsoft o dentro de la infraestructura de Azure. [46]

- **Cifrado TLS:** Azure utiliza TLS por defecto en todas las conexiones, con claves de 2048 bits o más para asegurar la confidencialidad de los datos en movimiento.
- **Cifrado de Capa de Enlace de Datos (MACsec):** Emplea MACsec en hardware de red para el tráfico entre centros de datos, protegiendo contra ataques "Man in the Middle"sin agregar latencia.
- **VPN de Azure:** Ofrece VPN de sitio a sitio y punto a sitio con IPsec/IKE para conexiones cifradas entre redes virtuales y locales, así como para dispositivos individuales.
- **Cifrado SMB y SSH en VM:** Admite cifrado SMB 3.0 y SSH en máquinas virtuales para proteger transferencias de datos en entornos Windows y Linux.
- **Azure Storage y Firma de Acceso Compartido (SAS):** Todas las interacciones se realizan mediante HTTPS, con uso de firmas de acceso compartido para garantizar la transmisión segura.

Azure ofrece herramientas avanzadas como Azure Policy para personalizar y aplicar políticas de seguridad, reforzando la confidencialidad, integridad y disponibilidad de los datos.

Prácticas de confidencialidad

2.5. AWS - Políticas de acceso basadas en permisos

AWS utiliza un sistema de control de acceso basado en políticas para gestionar los permisos de los usuarios y recursos. Estas políticas definen qué acciones puede realizar una entidad en los recursos de AWS, y se asocian tanto a identidades de IAM (usuarios, grupos y roles) como a recursos específicos. Cada política, en formato JSON, se evalúa en cada solicitud para decidir si se permite o deniega la acción solicitada [14].

Políticas Basadas en Identidad

Estas políticas se asocian directamente a usuarios, grupos o roles de IAM y controlan los permisos en función de la identidad que las recibe. Las políticas basadas en identidad incluyen: [14]

- **Políticas administradas por AWS:** Creada y administrada por AWS, estas políticas están diseñadas para facilitar la asignación de permisos comunes sin necesidad de configuración adicional.

- **Políticas administradas por el cliente:** Estas son políticas personalizadas que los clientes pueden crear y administrar en su cuenta para proporcionar un control más detallado y específico sobre los permisos.
- **Políticas Insertadas:** Se asocian directamente a una identidad (usuario, grupo o rol) y crean una relación estricta uno a uno. Estas políticas se eliminan si se elimina la identidad, permitiendo un control preciso sobre un usuario o rol específico.

Políticas Basadas en Recursos

Las políticas basadas en recursos controlan el acceso a nivel de recurso, asociándose a recursos específicos como buckets de S3. Pueden definir permisos para usuarios internos y entidades de IAM en otras cuentas, permitiendo el acceso entre cuentas con condiciones, como la autenticación multifactor (MFA).[14]

Límites de Permisos

Los límites de permisos establecen el máximo de permisos que una política basada en identidad puede otorgar a un usuario o rol, asegurando que no se otorguen permisos más allá de los especificados en el límite.[14]

Políticas de Control de Servicios (SCP)

Las SCP, exclusivas de AWS Organizations, se aplican a cuentas y unidades organizativas para limitar los permisos máximos. No otorgan permisos directamente, sino que restringen los permisos otorgados por otras políticas.[14]

Listas de Control de Acceso (ACL)

Las ACL controlan el acceso a recursos en escenarios de múltiples cuentas, permitiendo definir permisos básicos para entidades de otras cuentas en servicios como Amazon S3 y AWS WAF.[14]

Políticas de Sesión

Las políticas de sesión son temporales y limitan los permisos durante una sesión de usuario o rol federado, sin modificar la política principal de la entidad de IAM, útiles para accesos temporales o con condiciones específicas.[14]

Buenas Prácticas para la Gestión de Permisos

Para garantizar la seguridad en AWS, es fundamental implementar el principio de *privilegios mínimos*, proporcionando a cada usuario solo los permisos necesarios para realizar sus tareas. AWS ofrece herramientas adicionales para ayudar a refinar y validar estos permisos, como:

- **Analizador de acceso de IAM:** Esta herramienta analiza políticas y detecta permisos excesivos, proporcionando recomendaciones para ajustarlas a un nivel mínimo de privilegios.
- **Generación de Políticas Basadas en la Actividad de Acceso:** Permite generar políticas específicas basadas en las acciones realizadas por una entidad, basándose en los registros de AWS CloudTrail para crear permisos más precisos.
- **Información de Acceso Reciente:** AWS muestra las acciones realizadas recientemente, ayudando a identificar permisos innecesarios y ajustando las políticas en función de las actividades reales de los usuarios.

Estas prácticas permiten asegurar el acceso adecuado, minimizando riesgos y mejorando la gestión de permisos en AWS.

2.6. AWS - Auditorías de acceso

Las políticas de auditoría de acceso en AWS son fundamentales para garantizar la seguridad y el cumplimiento normativo de los recursos en la nube. Estas políticas definen quién puede acceder a qué recursos y bajo qué condiciones, permitiendo un control granular sobre las operaciones en su entorno de AWS. A continuación, se detallan los aspectos más relevantes:

Políticas Basadas en Identidad

Estas políticas se asocian a identidades de AWS IAM (usuarios, grupos o roles) y especifican los permisos que una identidad tiene. Se recomienda otorgar los permisos mínimos necesarios para reducir riesgos.[14]

Políticas Basadas en Recursos

Se adjuntan directamente a recursos específicos, definiendo quién puede interactuar con el recurso y qué acciones están permitidas, esenciales para controlar recursos compartidos o sensibles.[9]

Límites de Permisos

Restringen los permisos máximos que una identidad puede tener, proporcionando control adicional sobre las políticas basadas en identidad.

Políticas de Control de Servicios (SCP)

Utilizadas en AWS Organizations, las SCP limitan los permisos máximos de las cuentas miembro. No otorgan permisos directamente, sino que restringen los otorgados por otras políticas.

Listas de Control de Acceso (ACL)

Controlan el acceso a ciertos recursos, como buckets de S3, especificando qué entidades tienen acceso y qué operaciones pueden realizar.

Políticas de Sesión

Aplicadas a credenciales temporales, permiten restringir permisos durante una sesión específica, útiles para operaciones temporales o delegadas.

Prácticas Recomendadas

- **Revisión Periódica:** Auditar regularmente políticas y permisos para garantizar el principio de privilegios mínimos.
- **Uso de Herramientas de Análisis:** Utilizar el Analizador de Acceso de IAM para ajustar permisos excesivos o no utilizados.
- **Autenticación Multifactor (MFA):** Habilitar MFA para usuarios con permisos sensibles, añadiendo una capa adicional de seguridad.

Implementar y gestionar adecuadamente estas políticas permite establecer un control de acceso robusto y garantizar el cumplimiento de normativas de seguridad en AWS.

2.7. AWS - Autenticación multifactor (MFA)

La autenticación multifactor (MFA) proporciona una protección adicional, ya que, incluso si una contraseña es comprometida, previene el acceso no autorizado al requerir un segundo factor de autenticación. AWS recomienda habilitar MFA tanto para el usuario raíz de la cuenta como para todos los usuarios de IAM con acceso interactivo, siguiendo las mejores prácticas de seguridad [16]. Además, implementar MFA

contribuye al cumplimiento de estándares y regulaciones de seguridad que demandan medidas de autenticación sólidas y confiables.

Métodos de MFA disponibles en AWS

- **Aplicaciones de autenticación virtual:** Aplicaciones como Google Authenticator, Microsoft Authenticator o Authy generan códigos temporales de un solo uso (TOTP) en dispositivos móviles.
- **Dispositivos de hardware:** Tokens físicos que generan códigos TOTP, disponibles a través de proveedores como Gemalto o Yubico [10].
- **Claves de seguridad FIDO:** Dispositivos físicos que utilizan estándares FIDO para proporcionar una autenticación sólida y resistente a la suplantación de identidad [8].

Implementación de MFA en AWS

- **Usuario raíz de la cuenta:** Es fundamental habilitar MFA para el usuario raíz, ya que posee acceso completo a todos los recursos de la cuenta.
- **Usuarios de IAM:** Configure MFA para cada usuario de IAM que tenga acceso a la consola de administración de AWS o a la AWS CLI.
- **Políticas de seguridad:** Puede crear políticas que requieran MFA antes de permitir que un usuario acceda a recursos específicos o realice acciones determinadas [15].

Implementar MFA es una medida sencilla pero poderosa para proteger sus recursos en AWS, alineándose con las mejores prácticas de seguridad y reduciendo significativamente el riesgo de accesos no autorizados.

2.8. Google Cloud - Políticas de acceso basadas en permisos

En Google Cloud, la gestión de acceso a los recursos se realiza mediante **Identity and Access Management (IAM)**, que permite definir políticas de acceso basadas en permisos específicos. Estas políticas determinan quién (principal) tiene qué tipo de acceso (rol) a qué recurso.[24]

Componentes clave de IAM

1. **Principales (principals):** Identidades que pueden acceder a los recursos, como cuentas de usuario, cuentas de servicio, grupos de Google y dominios de Google Workspace o Cloud Identity.

2. **Permisos:** Acciones específicas que se pueden realizar en los recursos de Google Cloud, como `compute.instances.list` para listar instancias de Compute Engine.

3. **Roles:** Conjuntos de permisos agrupados que se asignan a los principales. Existen tres tipos de roles:[23]

   - **Roles básicos:** Incluyen `Viewer`, `Editor` y `Owner`, que otorgan permisos amplios y no se recomiendan en entornos de producción debido a su alcance extenso.
   - **Roles predefinidos:** Diseñados para tareas específicas, ofrecen un control más granular y son administrados por Google Cloud.
   - **Roles personalizados:** Definidos por el usuario, permiten agrupar permisos según necesidades específicas de la organización.

Mejores prácticas

- **Principio de privilegio mínimo:** Asigne a cada principal solo los permisos necesarios para realizar sus tareas, evitando otorgar permisos excesivos.
- **Uso de roles predefinidos o personalizados:** Evite utilizar roles básicos en entornos de producción. En su lugar, utilice roles predefinidos o cree roles personalizados que se ajusten a las necesidades específicas.
- **Revisión periódica de políticas:** Realice auditorías regulares de las políticas de IAM para garantizar que los permisos otorgados sigan siendo adecuados y seguros.

2.9. Google Cloud - Auditorías de acceso

En Google Cloud, las **políticas de auditoría de acceso** se implementan mediante **Cloud Audit Logs**, un servicio que registra las actividades administrativas y los accesos a los datos dentro de tus recursos de Google Cloud. Estos registros te permiten responder a preguntas como "¿quién hizo qué, cuándo y dónde?.[en] relación con tus recursos, proporcionando transparencia y facilitando el cumplimiento de normativas de seguridad [20].

Tipos de registros de auditoría

- **Registros de actividad administrativa (Admin Activity):** Documentan las operaciones que modifican la configuración o los metadatos de los recursos, como la creación de instancias de VM o cambios en las políticas de IAM. Estos registros se generan automáticamente y no se pueden deshabilitar.
- **Registros de acceso a los datos (Data Access):** Registran las operaciones que leen o modifican datos proporcionados por el usuario. Excepto para BigQuery, estos registros están deshabilitados por defecto y deben habilitarse explícitamente [21].
- **Registros de eventos del sistema (System Event):** Contienen entradas para acciones que modifican la configuración de los recursos y son generadas por los sistemas de Google, no por acciones directas de los usuarios. Estos registros se generan automáticamente y no se pueden deshabilitar.
- **Registros de políticas denegadas (Policy Denied):** Se registran cuando un servicio de Google Cloud deniega el acceso a un usuario o cuenta de servicio debido a una violación de políticas de seguridad. Estos registros se generan por defecto y no se pueden deshabilitar, aunque es posible excluirlos de su almacenamiento en Cloud Logging si es necesario.

Implementación y gestión de políticas de auditoría

- **Habilitación de Registros:** Para servicios distintos de BigQuery, los registros de acceso deben habilitarse manualmente mediante la consola de Google Cloud o comandos `gcloud`.
- **Control de Acceso:** Asignar roles adecuados, como `roles/logging.viewer` y `roles/logging.privateLogViewer`, es esencial para gestionar y visualizar los registros de auditoría.
- **Almacenamiento y Retención:** Los registros se almacenan en Cloud Logging, donde se pueden configurar políticas de retención y exportación según los requisitos organizacionales.

2.10. Google Cloud - Autenticación multifactor (MFA)

En Google Cloud, la **autenticación multifactor (MFA)** es una medida de seguridad esencial que añade una capa adicional de protección al requerir múltiples formas de verificación para acceder a los recursos. Implementar MFA ayuda a prevenir accesos no autorizados, incluso si las credenciales principales han sido comprometidas.

Implementación de MFA en Google Cloud

Google Cloud ofrece varias opciones para implementar MFA, adaptándose a las necesidades específicas de las organizaciones:

1. **Cloud Identity:**
   - **MFA para usuarios y administradores:** Cloud Identity permite configurar MFA para usuarios y administradores, asegurando que solo personas autorizadas accedan a los recursos.
   - **Métodos de verificación:** Se pueden utilizar diversos métodos de verificación, como notificaciones push, aplicaciones de autenticación (por ejemplo, Google Authenticator) y claves de seguridad resistentes al phishing, como las Titan Security Keys [19].
2. **Identity Platform:**
   - **MFA para aplicaciones:** Identity Platform facilita la integración de MFA en aplicaciones web y móviles, mejorando la seguridad de los usuarios finales.
   - **Soporte para múltiples factores:** Permite la implementación de factores como SMS, aplicaciones de autenticación y métodos biométricos [31].

Mejores prácticas para la implementación de MFA

- **Verificación de Correos Electrónicos:** Asegúrese de verificar los correos de los usuarios antes de habilitar MFA para evitar registros malintencionados.[35]
- **Selección de Métodos de Autenticación:** Ofrezca múltiples opciones de autenticación para adaptarse a las preferencias de los usuarios.
- **Educación y Soporte al Usuario:** Proporcione información clara sobre la configuración de MFA y ofrezca soporte para resolver dudas o problemas.

La implementación de MFA en Google Cloud fortalece la seguridad y protege los datos sensibles de la organización.

2.11. Azure - Políticas de acceso basadas en permisos

En Azure, la gestión de acceso basada en permisos se implementa mediante el **Control de Acceso Basado en Roles (RBAC)** y **Azure Policy**. Estas herramientas permiten definir y aplicar políticas que controlan quién puede realizar acciones específicas en los recursos de Azure, garantizando una administración segura y eficiente.

Control de Acceso Basado en Roles (RBAC)

RBAC es un sistema que proporciona un control detallado sobre el acceso a los recursos de Azure. Permite asignar permisos a usuarios, grupos y aplicaciones en función de roles específicos. Los componentes clave de RBAC son: [45]

- **Roles:** Conjuntos de permisos para acciones como leer, escribir o eliminar recursos. Azure ofrece roles integrados (p. ej., "Lector", Çolaborador", "Propietario") y permite crear roles personalizados.
- **Asignaciones de Roles:** Vinculan un rol a un principal (usuario, grupo o aplicación) en un ámbito específico (suscripción, grupo de recursos o recurso).

Por ejemplo, para otorgar permisos de lectura a un usuario en un grupo de recursos específico, se asigna el rol de "Lector.ª ese usuario en el ámbito del grupo de recursos correspondiente.

Azure Policy

Azure Policy es un servicio para crear, asignar y gestionar políticas que aplican reglas sobre los recursos de Azure, garantizando el cumplimiento de estándares corporativos. A diferencia de RBAC, Azure Policy se enfoca en el cumplimiento de recursos, no en las acciones de los usuarios.[48]

Con Azure Policy, se puede:

- **Definir Políticas:** Establecer reglas para que los recursos cumplan ciertas condiciones, como el uso de discos administrados o la implementación en regiones específicas.
- **Asignar Políticas:** Aplicar estas reglas a suscripciones, grupos de recursos o recursos individuales.
- **Evaluar el Cumplimiento:** Supervisar los recursos para garantizar que cumplen con las políticas y tomar medidas correctivas cuando sea necesario.

Por ejemplo, se puede requerir el cifrado en todas las cuentas de almacenamiento para garantizar el cumplimiento de estándares de seguridad.

Integración de RBAC y Azure Policy

Aunque RBAC y Azure Policy tienen objetivos diferentes, se complementan para proporcionar un control integral sobre los recursos de Azure. RBAC gestiona quién

puede realizar acciones específicas, mientras que Azure Policy garantiza que los recursos cumplan con las políticas corporativas.[48, 45]

El uso conjunto de ambas herramientas permite establecer un marco sólido de gobernanza y seguridad, asegurando que solo personas autorizadas realicen acciones permitidas y que los recursos cumplan con los estándares establecidos.

2.12. Azure - Auditorías de acceso

En Azure, las **políticas de auditoría de acceso** se implementan mediante servicios como **Azure Monitor**, **Azure Active Directory (Azure AD)** y **Azure Policy**. Estos servicios permiten supervisar, registrar y controlar las actividades de acceso a los recursos, garantizando el cumplimiento de las directrices de seguridad y facilitando la detección de actividades sospechosas.

Azure Monitor

Azure Monitor proporciona capacidades de supervisión y diagnóstico para los recursos de Azure. A través de estas, es posible habilitar el registro de actividades y eventos relacionados con el acceso a los recursos. Estos registros se pueden enviar a Log Analytics, Event Hubs o cuentas de almacenamiento para su análisis y retención. Por ejemplo, los registros de auditoría de consultas en Azure Monitor ofrecen datos sobre la ejecución de consultas, incluyendo información sobre quién las ejecutó y cuándo [42].

Azure Active Directory (Azure AD)

Azure AD es el servicio de administración de identidades y acceso de Azure. Proporciona registros de auditoría que documentan todas las actividades relacionadas con la autenticación y la autorización, como inicios de sesión, cambios de contraseña y modificaciones en las directivas de acceso. Estos registros son esenciales para supervisar y analizar los intentos de acceso, y están disponibles para su revisión en Azure Portal [52].

Azure Policy

Azure Policy permite crear, asignar y gestionar políticas que aplican reglas y efectos sobre los recursos de Azure. Aunque su enfoque principal es garantizar que los recursos cumplan con los estándares corporativos, también puede utilizarse para auditar configuraciones y prácticas de seguridad. Por ejemplo, se pueden definir políticas que requieran la habilitación de diagnósticos en ciertos recursos, asegurando que las actividades de acceso se registren adecuadamente.

Mejores Prácticas para la Auditoría de Acceso en Azure

- **Habilitar Registros de Auditoría:** Active los registros en todos los servicios críticos para capturar actividades relevantes.
- **Configurar Alertas:** Utilice Azure Monitor para alertar sobre actividades sospechosas, permitiendo respuestas rápidas.
- **Revisar Registros Periódicamente:** Revise y analice los registros de auditoría para identificar patrones inusuales o comportamientos anómalos.
- **Implementar Políticas RBAC:** Asigne permisos de manera granular para garantizar acceso adecuado según las funciones del usuario.[43]

2.13. Azure - Autenticación multifactor (MFA)

La **autenticación multifactor (MFA)** en Azure es una medida de seguridad que requiere que los usuarios proporcionen más de una forma de verificación al iniciar sesión, añadiendo una capa adicional de protección contra accesos no autorizados.

Azure ofrece varias formas de implementar MFA:

- **Valores predeterminados de seguridad:** Una configuración básica que habilita MFA para todos los usuarios de forma predeterminada.
- **Acceso condicional:** Permite crear directivas que exigen MFA en situaciones específicas, como cuando se accede desde ubicaciones no confiables o dispositivos no compatibles.
- **MFA por usuario:** Habilita MFA para usuarios individuales, aunque Microsoft recomienda utilizar el acceso condicional para una gestión más granular.

Directivas de Acceso Condicional

Las directivas de acceso condicional son herramientas que permiten controlar el acceso a los recursos de Azure en función de condiciones específicas. Por ejemplo, se puede requerir MFA para:

- Usuarios con roles administrativos que acceden a portales de administración de Microsoft.
- Inicios de sesión desde ubicaciones geográficas inusuales.
- Dispositivos que no cumplen con los estándares de seguridad de la organización.

Estas directivas ayudan a equilibrar la seguridad con la facilidad de uso, aplicando MFA solo cuando es necesario.

Próximos Cambios en MFA

A partir de 2024, Microsoft implementará la autenticación multifactor obligatoria para todos los intentos de inicio de sesión en Azure. Esta medida busca reforzar la seguridad de las cuentas y proteger contra ataques de compromiso de cuentas. Se recomienda a las organizaciones planificar y preparar la implementación de MFA para cumplir con este requisito [47].

Mejores Prácticas

- **Habilitar MFA:** Active la autenticación multifactor para todos los usuarios, ya que bloquea más del 99.2 % de los ataques de compromiso de cuentas.
- **Métodos de Autenticación Seguros:** Use métodos resistentes al phishing, como claves de seguridad FIDO2 o aplicaciones de autenticación con códigos de un solo uso.
- **Revisión Regular de Directivas:** Revise y ajuste las directivas de acceso condicional y MFA para adaptarse a cambios organizacionales y amenazas emergentes.

3. Matriz Comparativa

Prácticas y Herramientas de Seguridad y Confidencialidad

Proveedor	Confidencialidad	Integridad	Disponibilidad
AWS	Encriptación de datos en tránsito y reposo. Control de acceso granular mediante IAM. Reducción de acceso a datos personales mediante arquitecturas seguras.	Auditoría de registros de acceso y actividades. Validación de integridad de datos mediante AWS Config. Protección de aplicaciones y servicios con herramientas como AWS Shield.	Redundancia de datos en distintas zonas de disponibilidad (AZs). Escalabilidad automática para mantener servicios activos.
Google Cloud	Encriptación en tránsito y reposo con TLS y AES. Autenticación multifactorial y acceso con privilegios mínimos. Data Loss Prevention (DLP) para evitar exfiltración de datos.	Auditoría de cambios y actividades mediante Cloud Audit Logs. Integridad de datos garantizada mediante controles de cambios.	Replicación en zonas geográficas y tolerancia a fallos. Infraestructura escalable para alta disponibilidad. Recuperación rápida ante desastres.
Azure	Encriptación de datos en reposo (AES-256) y tránsito. Administración de identidad y accesos (Azure AD). Políticas de protección de datos personales.	Validación de integridad a través de Azure Policy. Control de auditorías y cambios de configuración. Seguridad ante amenazas con Azure Security Center.	Alta disponibilidad mediante replicación en múltiples regiones. Planes de recuperación ante desastres y continuidad de negocios. Escalabilidad y redundancia.

Proveedor	ISO/IEC 27001	NIST	GDPR
AWS	Certificación ISO 27001 para centros de datos. Prácticas alineadas con controles de seguridad y protección de datos.	Implementación de prácticas basadas en los marcos NIST 800-53 y NIST CSF. Seguridad en red y controles de acceso.	Servicios y políticas de privacidad y gestión de datos personales alineadas con el GDPR. Notificación rápida en caso de brechas de seguridad.
Google Cloud	Certificación ISO 27001 y revisiones constantes de auditoría. Estándares de seguridad y mejores prácticas para cumplir con normativas.	Cumple con NIST SP 800-53 y NIST CSF, con medidas de ciberseguridad implementadas en cada capa de seguridad.	Prácticas de gestión de datos alineadas con GDPR, como el derecho de acceso y eliminación. Información y control del procesamiento de datos.
Azure	Certificación ISO 27001 para centros de datos y servicios. Auditoría y cumplimiento de normativas de seguridad de la información.	Compatibilidad con NIST SP 800-53, con medidas de control de seguridad para entornos de ciberseguridad. Protocolo de respuesta a incidentes.	Conformidad con GDPR, incluyendo acceso y supresión de datos personales. Notificación y respuesta rápida ante incidentes de seguridad.

4. Selección de Prácticas, Herramientas de Seguridad y Confidencialidad para Proteger los Datos en la Nube

Para proteger los datos en la nube, se destacan las siguientes prácticas y herramientas de seguridad aplicadas por los principales proveedores (AWS, Google Cloud, y Azure). Estas prácticas abarcan el cifrado avanzado, el control de acceso, y los registros de auditoría.

4.1. Cifrado avanzado de datos sensibles

- **AWS**: Implementa cifrado en tránsito y en reposo mediante AES-256 y TLS. Proporciona el servicio **AWS Key Management Service (KMS)**, que permite administrar claves de cifrado de forma segura, junto con **AWS CloudHSM** para proteger claves criptográficas en hardware especializado. [3]
- **Google Cloud**: Utiliza cifrado en tránsito y en reposo mediante TLS y AES-256. Ofrece **Cloud Key Management** para administrar y proteger claves de cifrado, además de **Cloud HSM** para el almacenamiento seguro de claves en hardware.[30]
- **Azure**: Aplica cifrado en reposo y en tránsito, utilizando AES-256. Su servicio **Azure Key Vault** permite la administración segura de claves, certificados y secretos de cifrado, además de opciones de hardware seguro con **Azure Dedicated HSM**.[40]

4.2. Control de acceso basado en permisos y principio de mínimo privilegio

- **AWS**: Utiliza **AWS Identity and Access Management (IAM)** para controlar el acceso a recursos, aplicando permisos detallados y autenticación multifactorial. IAM permite la configuración de políticas de acceso basadas en roles, cumpliendo el principio de mínimo privilegio.[2]
- **Google Cloud**: Emplea **Cloud Identity and Access Management (IAM)** para administrar permisos y definir roles específicos en función de cada usuario. También permite la autenticación multifactorial y el uso de **Context-Aware Access** para configurar condiciones de acceso adicionales.[29]
- **Azure**: **Azure Active Directory (AAD)** gestiona la identidad y el acceso, permitiendo políticas basadas en roles, autenticación multifactorial y el uso de **Conditional Access** para imponer políticas de acceso adaptadas al contexto.[38]

4.3. Registros de auditoría para monitorear y revisar accesos a los datos

- **AWS**: **AWS CloudTrail** ofrece registros detallados de acceso y actividades realizadas en los servicios, lo cual facilita el monitoreo y auditoría de eventos. También permite el almacenamiento seguro de registros para auditorías y el monitoreo de amenazas.[1]

- **Google Cloud**: **Cloud Audit Logs** proporciona registros detallados de actividades y acceso a recursos, con capacidades de monitoreo y auditoría. Estos registros pueden integrarse con **Cloud Monitoring** para una vigilancia continua y rápida detección de incidentes.[26]
- **Azure**: **Azure Monitor** y **Azure Security Center** recopilan y gestionan registros de actividades y accesos a los datos. **Azure Activity Log** y **Azure Diagnostic Logs** brindan visibilidad completa y ayudan a la detección y mitigación de amenazas.[41]

Resumen de herramientas y prácticas

Proveedor	Cifrado avanzado	Control de acceso	Registros de auditoría
AWS	KMS, CloudHSM	IAM, permisos detallados	CloudTrail
Google Cloud	Cloud Key Management, Cloud HSM	Cloud IAM, Context-Aware Access	Cloud Audit Logs, Cloud Monitoring
Azure	Key Vault, Dedicated HSM	AAD, Conditional Access	Azure Monitor, Security Center, Activity Logs

Cuadro 3: Resumen de herramientas y prácticas de seguridad en la nube

4.4. Mejores prácticas comunes

- **Cifrado robusto**: Usar cifrado de datos en reposo y en tránsito, junto con el almacenamiento de claves en hardware seguro (HSM).
- **Políticas de mínimo privilegio**: Configurar roles y permisos específicos y revisarlos regularmente.
- **Monitoreo y auditoría continua**: Implementar registros de auditoría y monitoreo continuo para la detección de amenazas y el cumplimiento de normativas.

Estas herramientas y prácticas permiten una protección integral de los datos en la nube, abordando las necesidades de seguridad de manera eficaz y conforme a los estándares internacionales de privacidad y protección de datos.

4.5. Herramientas y Componentes de los Proveedores de Nube

Se presentan cinco herramientas clave de los principales proveedores de servicios en la nube, junto con una breve explicación de sus ventajas y funcionamiento:

1. **AWS Identity and Access Management (IAM):**
   - **Ventajas:** Permite gestionar de forma segura el acceso a los servicios y recursos de AWS mediante políticas detalladas y control de permisos.
   - **Funcionamiento:** IAM facilita la creación y administración de usuarios y grupos, asignando permisos específicos para controlar quién puede acceder a qué recursos y en qué condiciones [2].
2. **Google Cloud Identity and Access Management (IAM):**
   - **Ventajas:** Ofrece un control unificado de acceso a los recursos de Google Cloud, permitiendo definir roles y permisos precisos para usuarios y servicios.
   - **Funcionamiento:** Mediante IAM, se asignan roles predefinidos o personalizados a los usuarios, determinando sus niveles de acceso y garantizando el principio de mínimo privilegio [29].
3. **Azure Active Directory (Azure AD):**
   - **Ventajas:** Proporciona servicios de gestión de identidades y acceso, incluyendo autenticación multifactor y políticas de acceso condicional, mejorando la seguridad y el control.
   - **Funcionamiento:** Azure AD permite integrar identidades locales y en la nube, gestionar accesos a aplicaciones y recursos, y aplicar políticas de seguridad adaptativas basadas en el contexto del usuario [39].
4. **AWS Key Management Service (KMS):**
   - **Ventajas:** Facilita la creación y control de claves criptográficas para cifrar datos, integrándose con otros servicios de AWS para proteger la información de manera eficiente.
   - **Funcionamiento:** AWS KMS permite generar, almacenar y administrar claves de cifrado, ofreciendo opciones de rotación automática y control de acceso detallado para garantizar la confidencialidad de los datos [3].
5. **Google Cloud Key Management Service (KMS):**

- **Ventajas:** Ofrece una gestión centralizada de claves criptográficas, permitiendo cifrar datos en reposo y en tránsito, con opciones de integración en múltiples servicios de Google Cloud.
- **Funcionamiento:** Cloud KMS permite crear, rotar y destruir claves criptográficas, además de establecer políticas de acceso y auditoría para asegurar el uso adecuado de las claves en las aplicaciones y servicios [30].

Estas herramientas son fundamentales para implementar prácticas de seguridad robustas en entornos de nube, garantizando la protección de datos y el control de acceso adecuado.

5. Establecimiento de un Proceso o Estándar de Validación

La gestión ética y segura de los datos dentro de cualquier organización requiere un proceso de validación riguroso que asegure el cumplimiento de las normativas legales y la protección de la privacidad de los individuos involucrados. El establecimiento de un estándar de validación, que contemple una evaluación periódica de permisos y accesos, el monitoreo continuo de la seguridad y la actualización constante de políticas de acceso, resulta esencial para garantizar un manejo responsable de los datos. A continuación, se detallan los componentes clave para establecer un proceso de validación que cumpla con estos requisitos éticos y de seguridad.

5.1. Evaluación Periódica de Permisos y Accesos

Uno de los principios fundamentales en el manejo seguro de datos es la limitación de accesos y permisos, también conocida como *Principio de Privilegio Mínimo* [56]. Este principio sugiere que cada usuario dentro de una organización debe tener únicamente los permisos necesarios para realizar sus funciones específicas. Para asegurar la aplicación de este principio, es necesario implementar una evaluación periódica de todos los permisos y accesos. Este proceso de evaluación debería incluir los siguientes pasos:

1. **Identificación de Roles y Permisos:** Establecer y documentar claramente los roles dentro de la organización, junto con los permisos y accesos necesarios para cada uno. Estos permisos deben estar alineados con las responsabilidades laborales, evitando accesos innecesarios a datos sensibles. La identificación y documentación deben actualizarse en respuesta a cambios organizacionales [37].

2. **Revisión Trimestral de Permisos:** Con una frecuencia mínima trimestral, realizar revisiones exhaustivas de todos los accesos concedidos a los empleados, contratistas y colaboradores externos. La revisión debe confirmar que los accesos siguen siendo necesarios para las tareas específicas asignadas y debe documentarse en un informe formal.

3. **Revocación de Accesos No Necesarios:** Identificar y revocar accesos no necesarios o excesivos. Este paso incluye la eliminación de permisos que se otorgaron para tareas temporales o proyectos específicos ya finalizados. Para asegurar la objetividad, el proceso debería realizarse con la participación del equipo de seguridad y el departamento de recursos humanos.

Según un estudio reciente, la evaluación periódica de permisos y accesos reduce en un 45 % las probabilidades de accesos no autorizados [36]. Asimismo, asegura el cumplimiento de normativas como el Reglamento General de Protección de Datos (GDPR) en Europa y la Ley de Privacidad del Consumidor de California (CCPA) en Estados Unidos, que exigen la protección de datos personales mediante controles de acceso rigurosos [53].

5.2. Monitoreo Continuo de la Seguridad con Auditorías y Reportes de Acceso

Para mantener la seguridad de los datos, es fundamental un monitoreo continuo de todos los accesos y actividades dentro de los sistemas de información. El monitoreo permite detectar y responder a incidentes de seguridad en tiempo real y está conformado por las siguientes actividades:

1. **Auditorías de Seguridad Periódicas:** Realizar auditorías regulares en los sistemas de almacenamiento y procesamiento de datos, con una frecuencia mínima anual. Estas auditorías deben evaluar la integridad de los datos, la efectividad de las políticas de acceso y el cumplimiento de las normativas de seguridad vigentes. La implementación de auditorías también debe incluir la revisión de configuraciones y el análisis de cualquier modificación a los permisos [57].

2. **Generación y Revisión de Reportes de Acceso:** Implementar sistemas de generación automática de reportes que registren todas las actividades de acceso a los datos. Estos reportes deben revisarse regularmente para identificar posibles patrones de uso anómalo que indiquen accesos no autorizados o intentos de manipulación de los datos.

3. **Alertas en Tiempo Real y Respuesta a Incidentes:** Configurar alertas en tiempo real para actividades sospechosas, tales como accesos desde ubicaciones inusuales o intentos de acceso repetidos y fallidos. Estas alertas deben integrarse con un plan de respuesta a incidentes que permita la detección y mitigación rápida de posibles violaciones de seguridad [18].

El monitoreo continuo, reforzado con auditorías y reportes de acceso, ha demostrado ser una medida eficaz para reducir las amenazas internas y externas en los sistemas de información [55]. Este enfoque garantiza una detección rápida de actividades anómalas y fortalece la respuesta ante incidentes, reduciendo la probabilidad de un impacto negativo.

5.3. Revisión y Actualización de Políticas de Acceso y Uso de Datos

Las políticas de acceso y uso de datos deben ser documentos vivos que evolucionen conforme a los avances en tecnología y cambios en el entorno regulatorio. Estas políticas no solo deben definir los procedimientos de acceso, sino también los roles y responsabilidades de todos los actores involucrados en el manejo de datos. A continuación se describen los pasos necesarios para una revisión y actualización efectivas:

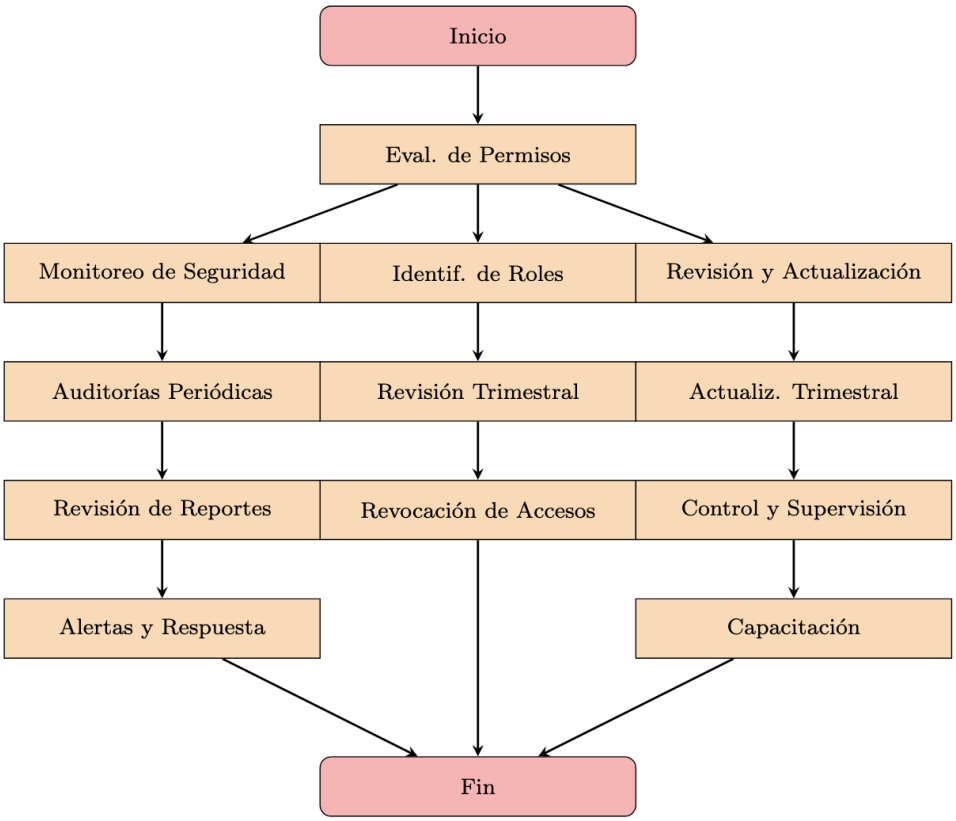
1. **Actualización Trimestral de Políticas de Acceso:** Las políticas de acceso deben revisarse y actualizarse trimestralmente para reflejar cambios organizacionales, actualizaciones tecnológicas y nuevas normativas de privacidad y seguridad de datos. Esta actualización debe considerar los roles críticos que requieren acceso privilegiado y limitar los permisos según la relevancia actual de cada rol.

2. **Establecimiento de Mecanismos de Control y Supervisión:** Implementar controles de supervisión, como auditorías independientes, para verificar que las políticas de acceso sean seguidas adecuadamente. Los mecanismos de control deben incluir revisiones de cumplimiento de políticas por terceros, asegurando que los estándares éticos y legales se mantengan [58].

3. **Capacitación Continua para el Cumplimiento:** Ofrecer programas de capacitación para todos los empleados en temas de privacidad, manejo ético de datos y cumplimiento de políticas. Esto ayuda a crear una cultura de seguridad y privacidad dentro de la organización, garantizando que el personal esté al tanto de sus responsabilidades en la gestión segura de datos.

La revisión y actualización de políticas de acceso permite que la organización se mantenga en cumplimiento con las leyes actuales, como el GDPR y la CCPA, además de mejorar la seguridad general de la información [54].

5.4. Diagrama: Establecimiento de un Proceso o Estándar de Validación



6. Conclusión

La presente investigación nos permite evaluar y comparar las prácticas de seguridad y herramientas de protección de datos implementadas por los principales proveedores de servicios en la nube: AWS, Google Cloud y Azure. A través de la revisión de sus características de seguridad, se ha destacado la importancia de aplicar medidas avanzadas de cifrado, control de acceso basado en permisos, y auditorías constantes para garantizar la integridad, confidencialidad y disponibilidad de los datos. La adopción de buenas prácticas como el principio de privilegio mínimo y la autenticación multifactor, así como el monitoreo continuo de actividades, resulta esencial para mitigar riesgos y cumplir con las normativas vigentes. Así, se concluye que la implementación de estas medidas robustas no solo protege la infraestructura, sino que también refuerza la confianza de los usuarios y asegura un manejo ético y seguro de la información.

Bibliografía

[1] Amazon Web Services. *AWS CloudTrail*. Disponible en `https://aws.amazon.com/cloudtrail`. n.d.

[2] Amazon Web Services. *AWS Identity and Access Management (IAM)*. Disponible en `https://aws.amazon.com/iam`. n.d.

[3] Amazon Web Services. *AWS Key Management Service (KMS)*. Disponible en `https://aws.amazon.com/kms`. n.d.

[4] Amazon Web Services. *Conformidad con la norma ISO/IEC 27001:2022: Amazon Web Services (AWS)*. Disponible en `https://aws.amazon.com/es/compliance/iso-27001-faqs/`. n.d.

[5] Amazon Web Services. *Programas de conformidad - Amazon Web Services (AWS)*. Disponible en `https://aws.amazon.com/compliance/programs/`. n.d.

[6] Amazon Web Services. *RGPD – Amazon Web Services (AWS)*. Disponible en `https://aws.amazon.com/es/compliance/gdpr-center/`. n.d.

[7] AWS. *AWS Security Learning*. Disponible en `https://aws.amazon.com/es/security/security-learning/?cards-top.sort-by=item.additionalFields.sortDate&cards-top.sort-order=desc&awsf.Types=*all`. n.d.

[8] AWS. *Claves de seguridad FIDO para MFA en AWS*. Disponible en `https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/id_credentials_mfa_fido.html`. n.d.

[9] AWS. *Control de acceso en IAM*. Disponible en `https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/access_controlling.html`. n.d.

[10] AWS. *Dispositivos de hardware para MFA en AWS*. Disponible en `https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/id_credentials_mfa_enable_physical.html`. n.d.

[11] AWS. *Encrypt data at rest*. Disponible en `https://docs.aws.amazon.com/es_es/whitepapers/latest/navigating-gdpr-compliance/encrypt-data-at-rest.html`. n.d.

[12] AWS. *Encrypt data in transit*. Disponible en `https://docs.aws.amazon.com/es_es/whitepapers/latest/navigating-gdpr-compliance/encrypt-data-in-transit.html`. n.d.

[13] AWS. *Información general sobre el cumplimiento del reglamento GDPR en AWS*. Inf. téc. Disponible en `https://docs.aws.amazon.com/es_es/whitepapers/latest/navigating-gdpr-compliance/navigating-gdpr-compliance.pdf#encrypt-data-in-transit`. AWS, 2020.

[14] AWS. *Políticas de acceso de IAM*. Disponible en `https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/access_policies.html`. n.d.

[15] AWS. *Políticas de seguridad que requieren MFA en AWS*. Disponible en `https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/access_policies.html`. n.d.

[16] AWS. *Prácticas de seguridad para MFA en AWS*. Disponible en `https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/id_credentials_mfa.html`. n.d.

[17] AWS. *Protecting your data on AWS*. Disponible en `https://docs.aws.amazon.com/es_es/whitepapers/latest/navigating-gdpr-compliance/protecting-your-data-on-aws.html`. n.d.

[18] M. Bishop. *Computer Security: Art and Science*. Addison-Wesley, 2003.

[19] Google Cloud. *Autenticación multifactor en Google Cloud Identity*. Disponible en `https://cloud.google.com/identity/docs/concepts/mfa`. n.d.

[20] Google Cloud. *Cloud Audit Logs en Google Cloud*. Disponible en `https://cloud.google.com/logging/docs/audit/`. n.d.

[21] Google Cloud. *Data Access Logs en Google Cloud*. Disponible en `https://cloud.google.com/logging/docs/audit/configure-data-access`. n.d.

[22] Google Cloud. *Default Encryption in Google Cloud*. Disponible en `https://cloud.google.com/docs/security/encryption/default-encryption?hl=es_419`. n.d.

[23] Google Cloud. *Descripción general de roles y permisos en Google Cloud IAM*. Disponible en `https://cloud.google.com/iam/docs/understanding-roles`. n.d.

[24] Google Cloud. *Documentación oficial de IAM en Google Cloud*. Disponible en `https://cloud.google.com/iam/docs/`. n.d.

[25] Google Cloud. *Encryption in Transit in Google Cloud*. Disponible en `https://cloud.google.com/docs/security/encryption-in-transit?hl=es_419`. n.d.

[26] Google Cloud. *Google Cloud Audit Logs*. Disponible en `https://cloud.google.com/logging/docs/audit`. n.d.

[27] Google Cloud. *Google Cloud Encryption*. Disponible en `https://cloud.google.com/security/encryption?hl=es-419&sjid=11067362784077954658-NC`. n.d.

[28] Google Cloud. *Google Cloud Identity*. Disponible en `https://cloud.google.com/identity/docs`. n.d.

[29] Google Cloud. *Google Cloud Identity and Access Management (IAM)*. Disponible en `https://cloud.google.com/iam`. n.d.

[30] Google Cloud. *Google Cloud Key Management Service (KMS)*. Disponible en `https://cloud.google.com/kms`. n.d.

[31] Google Cloud. *Implementación de MFA en Identity Platform*. Disponible en `https://cloud.google.com/identity-platform/docs/mfa`. n.d.

[32] Google Cloud. *ISO/IEC 27001 - Conformidad | Google Cloud*. Disponible en `https://cloud.google.com/security/compliance/iso-27001/`. n.d.

[33] Google Cloud. *NIST SP 800-53 - Google Cloud*. Disponible en `https://cloud.google.com/security/compliance/nist800-53/`. n.d.

[34] Google Cloud. *RGPD y Google Cloud | Google Cloud*. Disponible en `https://cloud.google.com/privacy/gdpr`. n.d.

[35] Google Cloud. *Verificación de correos electrónicos antes de habilitar MFA en Google Cloud*. Disponible en `https://cloud.google.com/identity/docs/email-verification`. n.d.

[36] S. Jones y M. Allen. «Periodic Access Reviews as a Data Security Measure in Corporate Environments». En: *Journal of Data Security and Privacy* 12.3 (2021), págs. 204-220.

[37] L. Lamport. *LaTeX: A Document Preparation System*. 2nd. Addison-Wesley, 1995.

[38] Microsoft Azure. *Azure Active Directory (AAD)*. Disponible en `https://azure.microsoft.com/en-us/services/active-directory`. n.d.

[39] Microsoft Azure. *Azure Active Directory (Azure AD)*. Disponible en `https://azure.microsoft.com/en-us/services/active-directory`. n.d.

[40] Microsoft Azure. *Azure Key Vault*. Disponible en `https://azure.microsoft.com/en-us/services/key-vault`. n.d.

[41] Microsoft Azure. *Azure Monitor*. Disponible en `https://azure.microsoft.com/en-us/services/monitor`. n.d.

[42] Microsoft Azure. *Azure Monitor y registros de auditoría*. Disponible en `https://learn.microsoft.com/es-es/azure/azure-monitor/overview`. n.d.

[43] Microsoft Azure. *Control de Acceso Basado en Roles (RBAC) en Azure*. Disponible en `https://learn.microsoft.com/es-es/azure/role-based-access-control/overview`. n.d.

[44] Microsoft Azure. *Cumplimiento del RGPD de Microsoft Azure*. Disponible en `https://learn.microsoft.com/es-es/compliance/regulatory/gdpr`. n.d.

[45] Microsoft Azure. *Descripción general de Control de Acceso Basado en Roles (RBAC) en Azure*. Disponible en `https://learn.microsoft.com/es-es/azure/role-based-access-control/overview`. n.d.

[46] Microsoft Azure. *Descripción general de la encriptación en Azure*. Disponible en `https://learn.microsoft.com/es-es/azure/security/fundamentals/encryption-overview`. n.d.

[47] Microsoft Azure. *Enable multifactor authentication for your tenant by 15 October 2024*. Disponible en `https://azure.microsoft.com/en-us/updates/v2/Enable-multifactor-authentication-for-your-tenant-by-15-October-2024`. 2024.

[48] Microsoft Azure. *Introducción a Azure Policy*. Disponible en `https://learn.microsoft.com/es-es/azure/governance/policy/overview`. n.d.

[49] Microsoft Azure. *Microsoft Azure obtiene la certificación ISO/IEC 27001:2013*. Disponible en `https://learn.microsoft.com/es-es/compliance/regulatory/offering-iso-27001`. n.d.

[50] Microsoft Azure. *Microsoft Azure y el cumplimiento de NIST SP 800-53*. Disponible en `https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-nist-800-53`. n.d.

[51] Microsoft Azure. *Privacidad en la nube de confianza de Azure*. Disponible en `https://azure.microsoft.com/es-es/explore/trusted-cloud/privacy/`. n.d.

[52] Microsoft Azure. *Registros de auditoría en Azure Active Directory*. Disponible en `https://learn.microsoft.com/es-es/azure/active-directory/reports-monitoring/reference-audit-logs`. n.d.

[53] *Reglamento General de Protección de Datos (GDPR)*. 2020. URL: `https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679`.

[54] R. Ross, M. McEvilley y J. Oren. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. Inf. téc. National Institute of Standards y Technology, 2019. URL: `https://doi.org/10.6028/NIST.SP.800-160v1`.

[55] S. Schneider. «Auditing and Continuous Monitoring in IT Security». En: *Cybersecurity Journal* 8.2 (2018), págs. 95-110.

[56] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley, 2020.

[57] W. Stallings y L. Brown. *Computer Security: Principles and Practice*. 4th. Pearson, 2018.

[58] M. E. Whitman y H. J. Mattord. *Principles of Information Security*. 6th. Cengage Learning, 2017.