Instituto Tecnológico y de Estudios Superiores de Monterrey

Inteligencia Artificial Avanzada para la Ciencia de Datos II

Módulo 4: Cómputo en la nube

Evidencia Módulo 4 Cloud

Autor: Rodolfo Jesús Cruz Rebollar

Matrícula: A01368326

Grupo: 101

Profesor: Félix Ricardo Botello Urrutia

Fecha: 10 de Noviembre de 2024

1. Evaluación de prácticas de almacenamiento y procesamiento en la nube

Principios/Normas	Proveedor de Servicios en la Nube		
	AWS	**Google Cloud**	**Azure**
Confidencialidad	Los datos se cifran estando en tránsito mediante TLS y estando en reposo con diversas metodologías tales como AES-256 [1]. El servicio IAM (Gestión de identidad y acceso) de AWS posibilita establecer permisos específicos para acceder a recursos y servicios, de forma que solamente aquellos usuarios con autorización tengan posibilidad de acceder a información sensible [1]. Los centros de datos pertenecientes a AWS cuentan con un sistema avanzado de seguridad física, mismo que involucra funciones como la vigilancia continua, además de acceso controlado [2].	Google Cloud lleva a cabo la encriptación de datos tanto en reposo como en tránsito mediante el empleo de estándares avanzados, tales como AES (Advanced Encription Standard) de claves conformadas por 256 bits, además de TLS (Transport Layer Security) [3]. Además, Google Cloud también posee el servicio IAM para gestionar los accesos a los recursos, esto a través de funciones como políticas de permisos y autenticación de varios factores (MLA) [3]. Adicionalmente, Google firma diversos acuerdos de procesamiento de datos tales como el DPA, además de otros acuerdos de confidencialidad, los cuales garantizan que los datos de su clientela no sean divulgados a terceras personas sin el debido consentimiento de los clientes [3].	Azure utiliza encriptación de tipo TLS (Transport Layer Security) para datos en tránsito, además de la encriptación del almacenamiento mediante la utilización de AES-256 en el caso de los datos en reposo [4]. Además, Azure también emplea el servicio Azure AD (Azure Active Direcvtory) para tener el control de los accesos por medio de la autenticación multifactor (MLA), el Single Sign On (SSO) y la gestión de mínimos privilegios con el propósito de erradicar en la medida de los posible todos los posibles riesgos [4]. Por otro lado, también se emplea el servicio de Azure Key Vault para la protección de claves de encriptación, secretos, además de certificaciones con hardware de seguridad dedicado (HSM) [4].

Continúa en la siguiente página

Principios/Normas	Proveedor de Servicios en la Nube		
	AWS	**Google Cloud**	**Azure**
Integridad	Validación de datos por medio de firmas digitales y los servicios de auditoría son asegurados por medio del servicio AWS CloudTrail cuya función es registrar todas las operaciones ejecutadas sobre los recursos [1]. La función de versionado ofrecida por Amazon S3 posibilita guardar múltiples versiones de los objetos, lo que sirve para protegerlos de eliminaciones no intencionadas, o de la corrupción de datos. Servicios de AWS como AWS Key Management Service y AWS Config contribuyen a identificar y reportar modificaciones no autorizadas realizadas sobre los datos y recursos, al permitir respuestas automatizadas, además de diferentes tipos de alertas [1].	En cuanto al principio de integridad, Google Cloud se encarga de verificar la integridad de los datos de sus clientes por medio de diferentes controles de autenticidad, entre los que se encuentran el hashing, además de auditorías automatizadas para el reconocimiento de modificaciones no autorizadas en los datos, además de que los sistemas que posee Google Cloud realizan constante rastreo de modificaciones tanto en los datos como en las configuraciones de los sistemas, además dichos sistemas también se encargan del mantenimiento de registros de auditorías, los cuales permiten comprobar si los datos han sufrido alguna alteración no autorizada [3].	Para que los datos no sean alterados sin autorización, Azure Security Center en conjunto con Log Analytics se encargan de supervisar las modificaciones en la configuración y acceso a los recursos, además las alertas son generadas cuando se identifica cualquier clase de actividad sospechosa [4]. Por otro lado, las soluciones en materia de seguridad implementadas por Azure, tales como Defender for Cloud, llevan a cabo escaneos periódicos buscando detectar malware y otras vulnerabilidades, garantizando de esa manera la integridas de los datos [4]. Además, Azure Blob Storage usa sumas de verificación, además de paridad de datos con el objetivo llevar a cabo una detección y corrección eficientes en el amcenamiento de los datos [4].

Continúa en la siguiente página

Principios/Normas	Proveedor de Servicios en la Nube		
	AWS	**Google Cloud**	**Azure**
Disponibilidad	AWS ofrece diversos servicios para replicar datos entre múltiples regiones de disponibilidad, garantizando así que sus servicios continúen funcionando en caso de presentarse fallas en hardware, o intermitencia en la zona geográfica. Además, AWS cuenta con tecnologías como Elastic Load Balancing y Auto Scaling para permitir automáticamente la distribución del tráfico por medio de varias instancias, además del ajuste de carácter dinámico de los recursos dependiendo de la demanda. Por otro lado, AWS también posee centros de datos ubicados en distintas zonas a nivel internacional [1], lo que proporciona acceso y rápida recuperación de la infraestructura en caso de algún desastre o falla de magnitud mayor.	En relación a temas de disponibilidad, Google Cloud se encarga de la distribución de los datos en numerosos centros de datos, lo cual garantiza la disponibilidad de los mismos, al igual que la resistencia frente a fallas del hardware, problemáticas de red, o eventos naturales adversos, además de ofrecer también diversas opciones de recuperación avanzadas ante dichos sucesos desfavorables [3]. Adicionalmente, los servicios ofrecidos por Google Cloud también se encuentran diseñados con el propósito de realizar escalamientos automáticos con el propósito de poder manejar incrementos considerables en la demanda de los servicios, garantizando de esa manera una continua disponibilidad de los mismos, además de que también Google Cloud ofrece SLAs (Service Level Agreements) para garantizar niveles de disponibilidad de los servicios hasta de un 99.999 % [3].	Por medio de diversas acciones tales como replicación geográfica, backups automatizados, y otras soluciones como Azure Site Recovery, se garantiza una continua disponibilidad de los datos, además de que Azure también implementa una arquitectura altamente escalable y distribuible, misma que asegura que las aplicaciones puedan mantenerse en funcionamiento, incluso frente a la ocurrencia de fallos de hardware o interrupciones [4]. Por otra parte, Azure también implementa SLA (Service Level Agreements) para cada uno de sus servicios, lo cual garantiza niveles específicos en cuanto a tiempo de actividad [4].

Continúa en la siguiente página

Principios/Normas	Proveedor de Servicios en la Nube		
	AWS	**Google Cloud**	**Azure**
ISO/IEC 27001	AWS cuenta con la certificación ISO/IEC 27001, dado que AWS lleva a cabo la implementación de un enfoque sistemático para una gestión efectiva de riesgos asociados con los principios éticos de confidencialidad, integridad y disponibilidad de información [5]. Además, AWS posee controles y políticas que son auditados con regularidad para garantizar el cumplimiento de los estándares establecidos por ISO 27001, además de la aplicación de controles de acceso, gestión de amenazas y mejora continua [5].	Con respecto a la norma ISO/IEC 27001, el proveedor de Google Cloud se encuentra certificado en este aspecto, dado que posee un sistema de gestión de seguridad de la información (ISMS) que cumple con los diferentes requisitos establecidos por dicha normativa, lo cual engloba el hecho de establecer reglamentos de seguridad, evaluación de riesgos de seguridad, además de implementar controles que aseguran un alto grado de seguridad de la información, además dichos controles contemplan diferentes funcionalidades, tales como el control de acceso, evaluación de riesgos de seguridad, encriptación, gestión de activos y respuesta oportuna frente a brechas de seguridad [6].	Azure mantiene un ISMS (Sistema de Gestión de Seguridad de la Información), mismo que abarca la totalidad de las actividades y otros servicios que importancia crítica para asegurar el continuo cumplimiento de los requisitos de la normativa ISO 27001 [7]. Por otro lado, Azure también implementa controles de acceso, cifrado y gestión de riesgos de seguridadque se encuentran alineados con las políticas establecidas por la norma ISO 27001 [7].

Continúa en la siguiente página

Principios/Normas	Proveedor de Servicios en la Nube		
	AWS	**Google Cloud**	**Azure**
NIST	AWS cumple con diversos marcos de seguridad de la norma NIST, tales como: **NIST SP 800-53:** AWS se apega a las sugerencias establecidas por el marco **NIST SP 800-53** para la implementación de controles de privacidad y seguridad, tales como la protección de perímetro y cifrado, además de la MFA (multi-factor authentication) [8]. **NIST CSF (Cybersecurity Framework):** AWS también ofrece guías y servicios para auxiliar a los clientes para que cumplan los estándares de seguridad establecidos por el marco CSF que contempla detección, protección, respuesta y recuperación frente a ataques cibernéticos [8]. **Control de acceso en base a esquema Zero Trust:** AWS incentiva la utilización del esquema Zero Trust al exigir constantes comprobaciones de acceso e identidad [8].	Google Cloud también se apega al marco establecido por el NIST Cybersecurity Framework (CSF), debido a que Google Cloud implementa diversas acciones tales como la realización periódica de evaluaciones de riesgos y activos de importancia crítica, implementación de distintos controles de acceso encriptación y gestión de identidad, la utilización de sistemas avanzados para la identificación de amenazas cibernéticas y otras posibles irregularidades, además del establecimiento de diversos protocolos para el manejo efectivo de problemas de seguridad y la rápida restauración de aquellos sistemas vulnerados [9].	En cuanto al cumplimiento de la norma NIST, Azure emplea los controles y guías establecidos por el NIST SP 800-53 para la gestión efectiva de riesgos de seguridad cibernética, abordando los principios de seguridad de la siguiente forma: **Ciberseguridad basada en NIST:** Azure utiliza un marco de seguridad basado en el NIST (National Institute of Standards and technology), mismos que abarca aspectos como la gestión de amenazas cibernéticas, supervisión, respuesta, protección y recuperación de posibles ataques que puedan ocurrir [10]. **Evaluaciones periódica de riesgos:** Supervisión activa de vulnerabilidades y riesgos de acuerdo al marco establecido por el NIST [10]. Además de lo anterior, Azure también implementa la seguridad de sus servicios en varias capas, que van desde la infraestructura física hasta la virtualización y el software [10].

Continúa en la siguiente página

Principios/Normas	Proveedor de Servicios en la Nube		
	AWS	**Google Cloud**	**Azure**
GDPR	AWS realiza prácticas para cumplir con los requisitos establecidos por la norma GDPR, entre los que se encuentran: herramientas para que la clientela pueda implementar prácticas de seguridad altamente robustas tales como el control de acceso granular, además de la encriptación de información personal. Además, AWS posibilita la eliminación de datos de acuerdo con los requerimientos de la norma GDPR, de forma que los clientes poseen el control sobre sus datos, pudiendo eliminarlos de los sistemas cuando consideren pertinente [11]. Por otro lado, AWS realiza procesos debidamente documentados para notificar a la brevedad posible cualquier amenaza de seguridad que se presente, cumpliendo así con el requisito de GDPR acerca de informar sobre brechas de seguridad en un lapso de 3 días posteriores al surgimiento de las mismas. Finalmente, AWS posee diferentes acuerdos relacionados con el procesamiento de datos, tales como el DPA (Data Processing Addendum), mismos que toman en cuenta diversas claúsulas contractuales estándar con el objetivo de asegurar que las transferencias internacionales de datos personales cumplan con las normativas legales vigentes [11].	Por otra parte, Google Cloud también cumple con el estándar GDPR, dado que este proveedor se asegura que los procesamientos de datos llevados a cabo por su personal se apegue a los diferentes principios de protección de datos establecidos en la norma GDPR, lo cual incluye el explícito consentimiento de los usuarios, además del derecho al olvido de datos por parte de los mismos usuarios, junto con la portabilidad de los mismos, además de que los clientes también pueden escoger la ubicación para almacenar sus datos personales, cumpliendo así con los requerimientos de residencia de los datos, estipulados por la norma GDPR [12].	Con el objetivo de cumplir con los requisitos establecidos por la norma GDPR, Azure implementa una serie de medidas concretas para la protección de datos personales y para agrantizar la privacidad de sus usuarios, entre las que se encuentran: **Derechos de titulares de los datos:** Azure ofrece una variedad de herramientas para simplificar la utilización, rectificación, portabilidad y eliminación de datos personales, garantizando de esa manera que los clientes puedan ejercer sus derechos bajo el marco establecido por el GDPR [13]. **Evaluaciones de impacto sobre privacidad (DPIA):** Axure ofrece apoyo a sus clientes para realizar evaluaciones de impacto en la privacidad, con el propósito de cumplir con los requerimientos establecidos en el artículo 35 de la norma GDPR [13]. **Notifcación de brechas o incidentes de seguridad:** Azure pone en marcha varios procedimientos que tienen el objetivo principal de notificar a la brevedad posible, cualquier violación a la seguridad de los datos de los clientes y si la situación lo amerita, también se emite un aviso a las autoridades encargadas de regular dicha situación [13].

2. Selección de Prácticas y Herramientas de Seguridad y Confidencialidad

A continuación se describe el funcionamiento de algunas de las prácticas y herramientas de seguridad empleadas por los proveedores de nube de AWS, Google Cloud y Azure para proteger los datos en la nube:

2.1. Autenticación multifactor (MLA)

La autenticación multifactor (MLA) hace referencia a un mecanismo de seguridad que necesita que los usuarios proporcionen más de 2 maneras de verificación de su identidad para poder acceder a sistemas, cuentas, o redes, además, éstos factores por lo general son algo conocido por los usuarios (por ejemplo un password), algo que los usuarios poseen (por ejemplo un teléfono celular o token de autenticación), o algo que los usuarios son (por ejemplo reconocimiento facial o huella digital) [14].

Además de lo anterior, la autenticación multifactor también posee la principal ventaja de que incrementa de forma significativa el nivel de seguridad al dificultar que los atacantes puedan acceder a recursos simplemente mediante la obtención de un password o contraseña [14].

2.2. Esquema Zero Trust

El esquema Zero trust consiste principalmente en un enfoque de seguridad que se encuentra basado en la premisa principal de "no tener confianza en nadie y comprobar todo", motivo por el cual, en este esquema se asume que las posibles amenazas puedan encontrase tanto en el interior como en el exterior de la red, por lo cual, se necesita de autenticación continua, supervisión y validación de todos los usuarios y dispositivos que tienen acceso a los recursos de una empresa u organización, independientemente de si se encuentran en el interior de la red interna o en el exterior de la misma [15].

Adicionalmente, la ventaja que posee el esquema de Zero Trust radica principalmente en que minimiza en la medida de lo posible, el riesgo de que ocurran brechas o incidentes de seguridad al reducir la superficie donde se lleva a cabo el ataque cibernético, debido a que no se otorga confianza intrínseca a nadie [15].

2.3. Cifrado AES-256

el AES-256 (Advanced Encryption Standard con clave de 256 bits) consiste en un algoritmo de cifrado simétrico que emplea una clave conformada por 256 bits para la encriptación y decodificación de los datos, además es ampliamente empleada en entornos de importancia crítica debido a que es un algoritmo altamente robusto y muy complicado de romper [16].

Además, la ventaja que ofrece el algoritmo AES-256 radica principalmente en el hecho de que dicho algoritmo proporciona un grado muy elevado de seguridad, puesto que una clave de 256 bits resulta extremadamente complicada de romper mediante fuerza bruta (prueba y error) empleando la tecnología actual [16].

2.4. Cifrado TLS (Transport Layer Security)

El TLS hace alusión a un protocolo de cifrado que asegura que las comunicaciones a través de las redes tengan el máximo grado de seguridad posible, tales como el internet, además éste protocolo de encriptación tiene la función principal de garantizar la protección de la integridad, autenticación y confidencialidad de aquellos datos que son transmitidos entre los clientes y los servidores, además de que el TLS también resulta ser ampliamente usado en páginas web con el objetivo de garantizar la seguridad en las conexiones HTTP, generando lo que generalmente se conoce con el nombre de HTTPS [17].

De forma adicional, la ventaja que proporciona el cifrado TLS radica en que provee seguridad de extremo a extremo en las conexiones, con lo cual se protegen los datos en tránsito de posibles

ataques cibernéticos, tales como la interceptación de datos y el ataque conocido como "man-in-the-middle"("hombre en el medio") [17].

2.5. Defender for Cloud

Microsoft Defender for Cloud hace referencia a una plataforma de seguridad en la nube que posibilita a las empresas el hecho de proteger sus ambientes híbridos y de múltiples nubes, además de que ofrece varias características muy útiles como lo son la supervisión continua, evaluaciones de seguridad, además de alertas frente a posibles amenazas cibernéticas o vulnerabilidades, además de que también, Defender for Cloud ofrece sugerencias automatizadas con el objetivo de mejorar la postura de seguridad de las empresas [18].

Adicionalmente, también es relevante mencionar que la principal ventaja que proporciona Defender for Cloud radica principalmente en el hecho de que simplifica notablemente la protección y monitoreo integral de las infraestructuras en la nube, apoyando de esa manera a las empresas a detectar y erradicar los posibles riesgos con la mayor rapidez posible [18].

3. Establecimiento de un Proceso o Estándar de Validación

Nombre del procedimiento: Validación y Control Ético de Acceso y Seguridad de los Datos

3.1. Validación y Control Ético de Acceso y Seguridad de los Datos

3.1.1. Alcance

El presente procedimiento es aplicable a todas las áreas y departamentos encargados del manejo de datos confidenciales o sensibles dentro de una empresa, con el propósito de asegurar que el acceso, utilización y protección de dichos datos cumplan con los estándares de seguridad, éticos y reglamentarios, además éste proceso también abarca sistemas internos al igual que plataformas externas para el almacenamiento o procesamiento de los datos.

Además, el alcance de éste procedimiento también contempla que se garantice el manejo seguro, ético y en conformidad con la normativa con las normativas en vigor de los datos de la empresa, por medio de evaluaciones realizadas periódicamente, además de auditorías y revisiones de políticas de acceso y utilización de los datos.

3.1.2. Diagrama del procedimiento

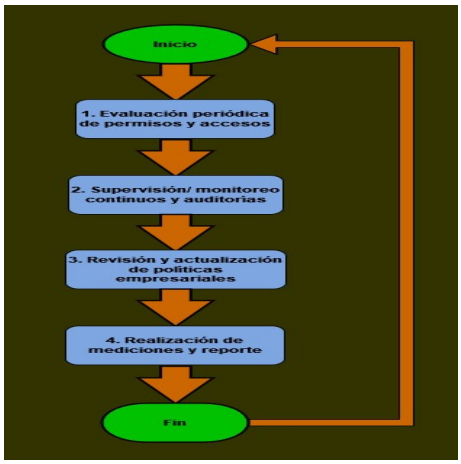

Figura 1: Diagrama del proceso o estándar de validación para el manejo seguro de los datos en una empresa. Fuente: elaboración propia.

3.1.3. Explicación de cada paso

Éste proceso está conformado por 4 pasos principales que se describen a continuación:

Paso 1. Evaluación periódica de permisos y accesos:

El propósito de éste paso consiste principalmente en garantizar que solamente el personal autorizado tenga acceso a los datos confidenciales y sensibles, motivo por el cual, la evaluación de los accesos debe ser realizada de forma trimestral o en cada ocasión que se produzca una modificación en el equipo o en los roles de trabajo de los empleados de la empresa, para lo cual se llevarán a cabo las acciones mencionadas a continuación:

1. Llevar a cabo una revisión del listado de usuarios con acceso a los distintos sistemas computacionales/digitales y bases de datos de la organización.

2. Comprobar si los permisos otorgados a los empleados de la empresa continúan siendo necesarios para la correcta realización de sus funciones actuales.

3. Eliminación de permisos o accesos expirados o innecesarios.

4. Registro y reporte de las modificaciones en una base de datos de auditoría.

Además de lo anterior, como resultado de las medidas antes mencionadas, se espera que únicamente los empleados que se encuentren actualmente activos en la empresa y que además tengan roles que requieran del acceso a datos sensibles, conserven sus permisos correspondientes, por lo que la evaluación realizada garantizará que no existan más accesos de los necesarios para cada empleado de la empresa y además que tampoco existan accesos no autorizados dentro de la empresa.

Paso 2. Continua supervisión de seguridad mediante auditorías y reportes de acceso:

En éste paso del procedimiento, el objetivo radica principalmente en poder identificar y prevenir aquellos accesos no autorizados, o bien, que sean potencialmente riesgosos para los datos de la empresa, por lo que se realizará un diario monitoreo de los accesos con auditorías en materia de seguridad llevadas a cabo de forma mensual, para lo cual, se llevarán a cabo las acciones a continuación:

1. Implementación de herramientas de vigilancia/monitoreo encargadas de registrar todos los accesos a aquellos datos confidenciales o sensibles.

2. Generación de reportes de acceso, en los cuales se detallen:
   - Cuáles usuarios tuvieron acceso a los datos sensibles o confidenciales.
   - Fecha y hora de ocurrencia de la situación.
   - Desde cuál dispositivo o ubicación se accedió a los datos.
   - Cuáles datos fueron consultados o alterados.

3. Revisión de éstos reportes para buscar actividades que levanten sospechas o que sean claramente atípicas.

4. Realización de auditorías de seguridad cada mes para comprobar el debido cumplimiento de las normas de seguridad en vigor e identificar oportunamente posibles vulnerablidades en los procesos de seguridad de la empresa.

Además de lo anterior, como resultado de la implementación de las acciones antes mencionadas, se espera que sea posible lograr una detección temprana de accesos no autorizados, junto con conductas anormales de parte de los usuarios que accedan a los datos, además también se espera que se genere un informe de auditoría en el cual se demuestre que el acceso a los datos de la empresa está altamente monitoreado y controlado de una manera segura.

Paso 3. Revisión y actualización de reglamentos de acceso y utilización de datos

En éste paso del procedimiento, el propósito principal consiste en que se garantice que los reglamentos o políticas de la empresa se encuentren alineadas con las modificaciones tecnológicas, legales y empresariales, y que únicamente el personal autorizado tenga el acceso a los datos de la empresa de acuerdo con las normativas actuales en vigor, motivo por el cual, se realizarán revisiones de las políticas de acceso y uso de datos de forma semestral, o cuando surjan modificaciones en las normativas legales o en los procesos empresariales internos, para lo cual, se llevarán a cabo las siguientes acciones:

1. Lleva a cabo una reunión de un equipo interdisciplinario que incluya a personal de los departamentos de TI (tecnologías de la información), seguridad y legal, con el objetivo principal de revisar los reglamentos o políticas de acceso a los datos de la empresa.

2. Realizar una actualización de los reglamentos de acceso tomando en consideración los aspectos a continuación:
   - Nuevas normas legales tales como GDPR y la Ley de Protección de Datos.
   - Modificaciones en la estructura empresarial o en los roles del personal de la empresa.
   - Nuevos avances tecnológicos en materia de seguridad de los datos.

3. Informar de las actualizaciones a las normas a todos los empleados de la empresa implicados y asegurar que éstos poseen una plena comprensión de las nuevas normas.

4. Llevar a cabo la implementación de controles adicionales en caso de que se requieran para cumplir con las nuevas políticas, tales como autenticación de doble factor o restringir accesos a los datos desde dispositivos que no sean aprobados o permitidos.

Adicionalmente, como resultado de implementar las acciones previamente descritas, se espera que las políticas de la empresa en materia de seguridad y utilización de los datos estén debidamente actualizadas y alineadas con los requerimientos establecidos por las normativas de seguridad vigentes, además de que todo el personal de la empresa estará debidamente informado y capacitado para garantizar el cumplimiento de las nuevas normas de acceso y utilización de los datos.

Paso 4. Medición y elaboración de reporte

Ésta última etapa del procedimiento se encuentra conformada por las siguientes actividades o acciones:

1. **Informe de cada trimestre:** el personal responsable de las áreas de tecnologías de la información (TI) y seguridad deberán entregar un informe en el que se resuman las actividades de validación de accesos realizadas por la empresa, además de los hallazgos de las auditorías de seguridad y las actualizaciones de los reglamentos de acceso y uso de datos, llevados a cabo por la empresa en el último periodo trimestral.

2. Además, el informe entregado por los responsables de seguridad y del departamento de TI de la empresa deberán tener en cuenta los siguientes aspectos o indicadores clave al momento de elaborar el informe de seguridad trimestral:

    - Cantidad de accesos eliminados o modificados.

    - Registro de aquellos accesos no autorizados detectados por el sistema de seguridad de la empresa.

    - Cumplimiento de la empresa con las normas legales en vigor.

4. Conclusiones

En conclusión, después de realizar todo el análisis anterior, es posible concluir que actualmente el hecho de establecer un procedimiento para validar y controlar los accesos a los datos de parte de todos los miembros de una organización resulta fundamental para prevenir en la medida de lo posible, una amplia variedad de riesgos relacionados con la seguridad de los datos, tales como el robo de los mismos, alteración no autorizada de ellos, entre otros incidentes de seguridad, por lo que el hecho de implementar medidas se seguridad altamente robustas para proteger los datos como lo son las distintas técnicas de cifrado de los datos tanto en reposo como en tránsito, autenticación de múltiples factores, entre otras, ayudarán a que a los atacantes se les complique significativamente el acceder a los datos de las empresas y manipularlos de forma maliciosa, puesto que las medidas de seguridad que es posible implementar hoy en día para garantizar la seguridad de los datos, son en realidad muy complicadas de violar mediante los ciberataques conocidos hasta el momento, otorgando así la oportunidad de robustecer aún más las medidas de contención de amenazas cibernéticas ante la posibilidad de futuros ataques.

No obstante, también es importante enfatizar que las empresas actualmente también deben asegurarse de estar debidamente informadas acerca de los nuevos métodos que vayan surgiendo en materia de seguridad de los datos e infraestructuras virtuales, así como los beneficios o ventajas que ofrecen, junto con sus posibles desventajas, esto con el propósito de que las organizaciones puedan evaluar si su esquema actual de seguridad de la información aún continúa siendo funcional para erradicar los ciberataques más comúnmente utilizados por los atacantes y en caso necesario, modificarlos para adaptarlos a nuevos tipos de ciberamenazas que también surjan en un futuro cuando la tecnología avance aún más, por lo cual también habrá que estar preparados para aquellos otros ataques que aunque no sean demasiado frecuentes o habituales, también es posible que se presenten en un momento dado, por lo que en esos casos, será necesario llevar a cabo auditorías de seguridad de forma más frecuente para que las empresas se enteren de las vulnerabilidades que puedan tener sus procedimientos de seguridad actuales frente a nuevas amenazas y corregir dichas vulnerabilidades de forma oportuna antes de que los sistemas de la empresa sufran un ataque para el que no estén preparados y eso repercuta de forma bastante negativa en el rendimiento y operaciones empresariales.

Referencias

[1] *AWS Compliance Programs*. https://aws.amazon.com/compliance/programs/. Accessed: 2024-11-10.

[2] *AWS Security Documentation*. https://aws.amazon.com/security/. Accessed: 2024-11-10.

[3] *Google Cloud Security Overview*. https://cloud.google.com/security/overview. Accessed: 2024-11-11.

[4] Microsoft. *Azure Security Overview*. Accessed: 2024-11-23. 2023. URL: https://azure.microsoft.com/en-us/explore/security/.

[5] *ISO/IEC 27001 on AWS*. https://aws.amazon.com/compliance/iso-27001-faqs/. Accessed: 2024-11-10.

[6] *Google Cloud Compliance: ISO/IEC 27001*. https://cloud.google.com/security/compliance/iso-27001. Accessed: 2024-11-11.

[7] Microsoft. *ISO/IEC 27001:2013 Overview*. Accessed: 2024-11-23. 2023. URL: https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-iso-27001.

[8] Amazon Web Services. *NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud*. https://aws.amazon.com. Updated October 12, 2021. First published January 2019. Oct. de 2021.

[9] *Google Cloud Compliance: NIST SP 800-53*. https://cloud.google.com/security/compliance/nist800-53?hl=es-419. Accessed: 2024-11-11.

[10] Microsoft. *NIST Cybersecurity Framework (CSF) Compliance Offering*. Accessed: 2024-11-23. 2023. URL: https://learn.microsoft.com/en-us/azure/compliance/offerings/nist-csf.

[11] *AWS and GDPR*. https://aws.amazon.com/compliance/gdpr-center/. Accessed: 2024-11-10.

[12] *Google Cloud GDPR Compliance*. https://cloud.google.com/security/gdpr. Accessed: 2024-11-11.

[13] Microsoft. *General Data Protection Regulation (GDPR)*. Accessed: 2024-11-23. 2023. URL: https://learn.microsoft.com/en-us/microsoft-365/compliance/gdpr?view=o365-worldwide.

[14] National Institute of Standards y Technology. *Digital Identity Guidelines: Multi-Factor Authentication*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf. 2020.

[15] John Kindervag. *Building a Zero Trust Network: A Roadmap to Build Security in the Cloud*. Wiley, 2021. ISBN: 9781119689050.

[16] National Institute of Standards y Technology. *Announcing the Advanced Encryption Standard (AES)*. https://csrc.nist.gov/publications/detail/fips/197/final. Available at: https://csrc.nist.gov/publications/detail/fips/197/final. 2001.

[17] T. Dierks y E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.2*. RFC 5246, https://tools.ietf.org/html/rfc5246. Available at: https://tools.ietf.org/html/rfc5246. 2008.

[18] Microsoft Corporation. *Microsoft Defender for Cloud Documentation*. https://learn.microsoft.com/en-us/azure/defender-for-cloud/. Available at: https://learn.microsoft.com/en-us/azure/defender-for-cloud/. 2023.