

APRENDE
.CLOUD



Google Cloud Digital Leader

Confianza y Seguridad con Google Cloud

[1.01.008]





Google Cloud Cloud Digital Leader

[Confianza y Seguridad con Google Cloud]

[Sesión #8]



<https://www.linkedin.com/in/nicolepainem/>

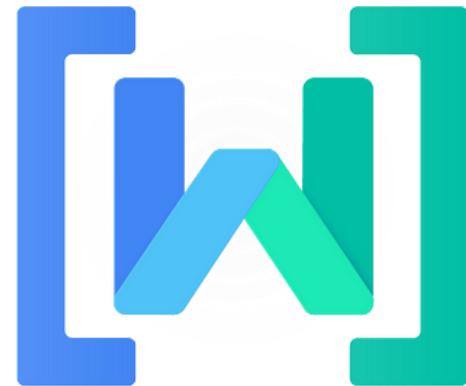


Nicole Paine Mansilla · 1st

Abogada | Tecnología y Regulación | LegalTech | Google WTM

Ambassador | Datos Personales | Ciberseguridad.

Santiago, Santiago Metropolitan Region, Chile



Women
Techmakers

translated by Google
Se usó la [API de Cloud Translation](#) para traducir esta página.

[Switch to English](#)

Estamos construyendo un mundo en el que **todas las mujeres** puedan prosperar en el campo de la tecnología.

El programa Women Techmakers de Google brinda visibilidad,
una comunidad y recursos para las mujeres que se dedican a la
tecnología.



<https://developers.google.com/womentechmakers>

[Síguenos en LinkedIn]



 /company/aprende-cloud
 @aprendecloud
 @aprende.cloud

<https://www.linkedin.com/company/aprende-cloud/>



APRENDE.CLOUD

Education · Santiago de Chile · 528 followers · 2-10 employees



[Síguenos en Instagram]



aprende.cloud Sigiendo ▾ Enviar mensaje +8 ...

10 publicaciones

169 seguidores

88 seguidos

APRENDE.CLOUD

Súbete a la Nube y aprende cloud en Español.

🔗 www.aprende.cloud

abogadasentech, culturadatos y 17 más siguen este perfil

■ PUBLICACIONES

etag ETIQUETAS

<https://www.instagram.com/aprende.cloud/>



[Suscríbete en YouTube]



[/company/aprende-cloud](#)
[@aprendecloud](#)
[@aprende.cloud](#)

aprendecloud



@aprendecloud · 1.29 K suscriptores · 7 videos

[https://aprende.cloud/ ...más](https://aprende.cloud/)

[aprende.cloud](#) y 1 vínculo más

Personalizar canal

Administrar videos

Principal Videos En vivo Playlists Comunidad



[1.01.001] Google Cloud Digital Leader - Cómo Convertirse en ...

1,053 vistas · hace 1 mes

[1.01.001] Google Cloud Digital Leader - Cómo Convertirse en un Cloud Digital Leader

Anfitriona: Nicole Paine Mansilla

<https://www.linkedin.com/in/nicolepai...>

MÁS INFORMACIÓN

Playlists creadas



(Resumen) [1.01.000] Google Cloud Digital Leader - Lista de...

Se actualizó hoy

[Ver playlist completa](#)

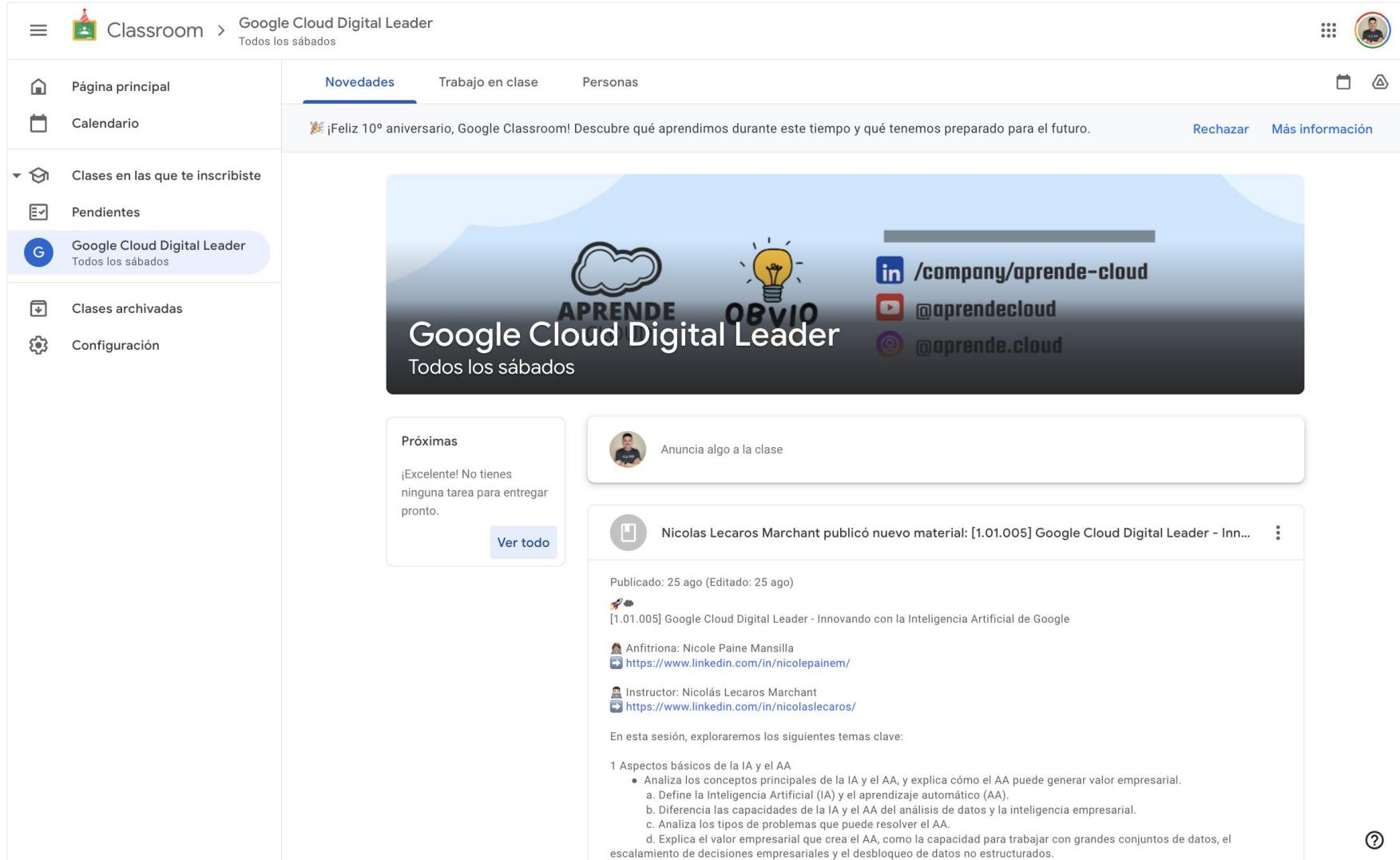
[1.01.000] Google Cloud Digital Leader - Lista de Reproducción

Se actualizó hoy

[Ver playlist completa](#)

<https://www.youtube.com/@aprendecloud>

Google Classroom:



The screenshot shows the Google Classroom interface for the 'Google Cloud Digital Leader' class. The left sidebar shows navigation options like 'Página principal', 'Calendario', and 'Clases en las que te inscribiste'. The 'Google Cloud Digital Leader' class is selected. The main content area displays a banner for the 10th anniversary of Google Classroom, followed by a large image featuring the APRENDE and OBVIO logos, along with social media links for LinkedIn, YouTube, and Instagram. Below the banner, there's a 'Próximas' section indicating no tasks are due soon, and a feed showing a post from Nicolas Lecaros Marchant.

Classroom > Google Cloud Digital Leader
Todos los sábados

Página principal Calendario Clases en las que te inscribiste Pendientes Google Cloud Digital Leader Todos los sábados Clases archivadas Configuración

Novedades Trabajo en clase Personas

¡Feliz 10º aniversario, Google Classroom! Descubre qué aprendimos durante este tiempo y qué tenemos preparado para el futuro.

Rechazar Más información

APRENDE OBVIO

Google Cloud Digital Leader

Todos los sábados

Próximas

Anuncia algo a la clase

Nicolas Lecaros Marchant publicó nuevo material: [1.01.005] Google Cloud Digital Leader - Innovando con la Inteligencia Artificial de Google

Publicado: 25 ago (Editado: 25 ago)

[1.01.005] Google Cloud Digital Leader - Innovando con la Inteligencia Artificial de Google

Anfitriona: Nicole Paine Mansilla

Instructor: Nicolás Lecaros Marchant

En esta sesión, exploraremos los siguientes temas clave:

1 Aspectos básicos de la IA y el AA

- Analiza los conceptos principales de la IA y el AA, y explica cómo el AA puede generar valor empresarial.
- Define la Inteligencia Artificial (IA) y el aprendizaje automático (AA).
- Diferencia las capacidades de la IA y el AA del análisis de datos y la inteligencia empresarial.
- Analiza los tipos de problemas que puede resolver el AA.
- Explica el valor empresarial que crea el AA, como la capacidad para trabajar con grandes conjuntos de datos, el escalamiento de decisiones empresariales y el desbloqueo de datos no estructurados.



Cloud Digital Leader

Un Cloud Digital Leader puede expresar con claridad las capacidades de los productos y servicios principales de Google Cloud y cómo se benefician las organizaciones. También pueden describir casos de uso empresariales habituales y cómo las soluciones de la nube respaldan a una empresa.

Esta certificación está destinada a cualquier persona que desee demostrar sus conocimientos de los conceptos básicos de la computación en la nube y cómo los productos y servicios de Google Cloud se pueden usar para lograr los objetivos de una organización.

El examen Cloud Digital Leader evalúa sus conocimientos en estas áreas:

- ✓ Transformación digital con Google Cloud
- ✓ Innova con la Inteligencia Artificial de Google Cloud
- ✓ Seguridad y confianza con Google Cloud
- ✓ Explora la transformación de datos con Google Cloud
- ✓ Moderniza la infraestructura y las aplicaciones con Google Cloud
- ✓ Escalamiento con Google Cloud Operations

Material del programa:

- Información General del Examen (Español):**

<https://cloud.google.com/learn/certification/cloud-digital-leader>

- Guía de temas para preparar el Examen (Español):**

<https://cloud.google.com/learn/certification/guides/cloud-digital-leader?hl=es-419>

- Curso de Preparación desde CloudSkillsBoost.Google (English):**

<https://www.cloudskillsboost.google/parts/9?hl=es-419>

- Curso de Preparación desde APRENDE.CLOUD (Español):**

Acceso al curso en Google Classroom + Clases En Vivo: Sábados y Miércoles

<https://classroom.google.com/c/NzAxMDAxNTgwMzA0?cjc=abknrmt>

- Examen de Ejemplo (English):**

<https://docs.google.com/forms/d/e/1FAIpQLSc4Emr0lwIEEE5kliPif9O9JctGwnYvPNUPoqViZDm9wH72ug/viewform>

- Examen de Practica (Español):**

Se liberará el acceso en la última sesión.



Google I/O



<https://www.linkedin.com/in/nicolaslecaros/>



Nicolás Lecaros Marchant

   Principal Data Architect | Cloud Solution Architect | Professor
| Entrepreneur | AI/ML/GenAI | AWS Community Builder | Google
Cloud Champion Innovator | GDG Organizer | Certified in AWS, Azure,
GCP and FinOps

Santiago, Santiago Metropolitan Region, Chile



Pontificia Universidad
Católica de Chile

Cloud Digital Leader

Ruta Aprendizaje Oficial

Google Cloud

Digital Transformation
with Google Cloud



COMPLETION BADGE

Google Cloud

Exploring Data
Transformation with
Google Cloud



COMPLETION BADGE

Google Cloud

Innovating with
Google Cloud
Artificial Intelligence



COMPLETION BADGE

Google Cloud

Modernize Infrastructure
and Applications with
Google Cloud



COMPLETION BADGE

Google Cloud

Trust and Security
with Google Cloud



COMPLETION BADGE

Google Cloud

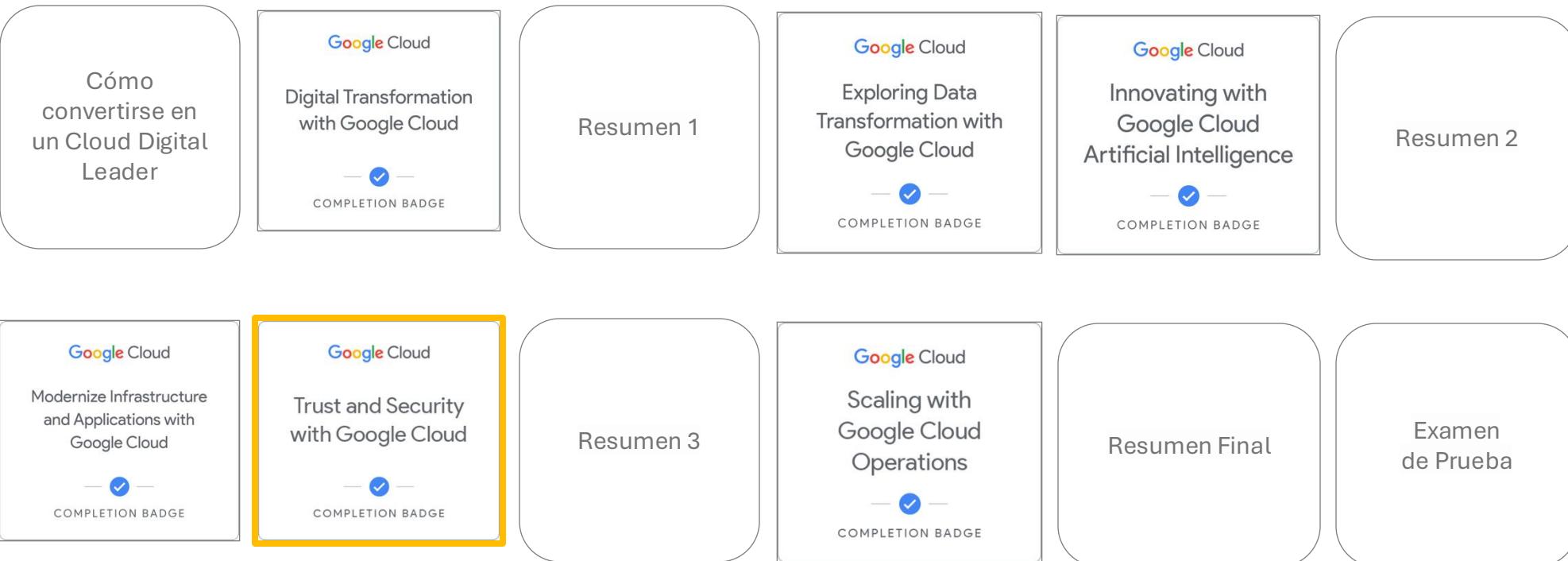
Scaling with
Google Cloud
Operations



COMPLETION BADGE

Cloud Digital Leader

Ruta Aprendizaje Propuesta APRENDE.CLOUD



[Confianza y Seguridad con Google Cloud]

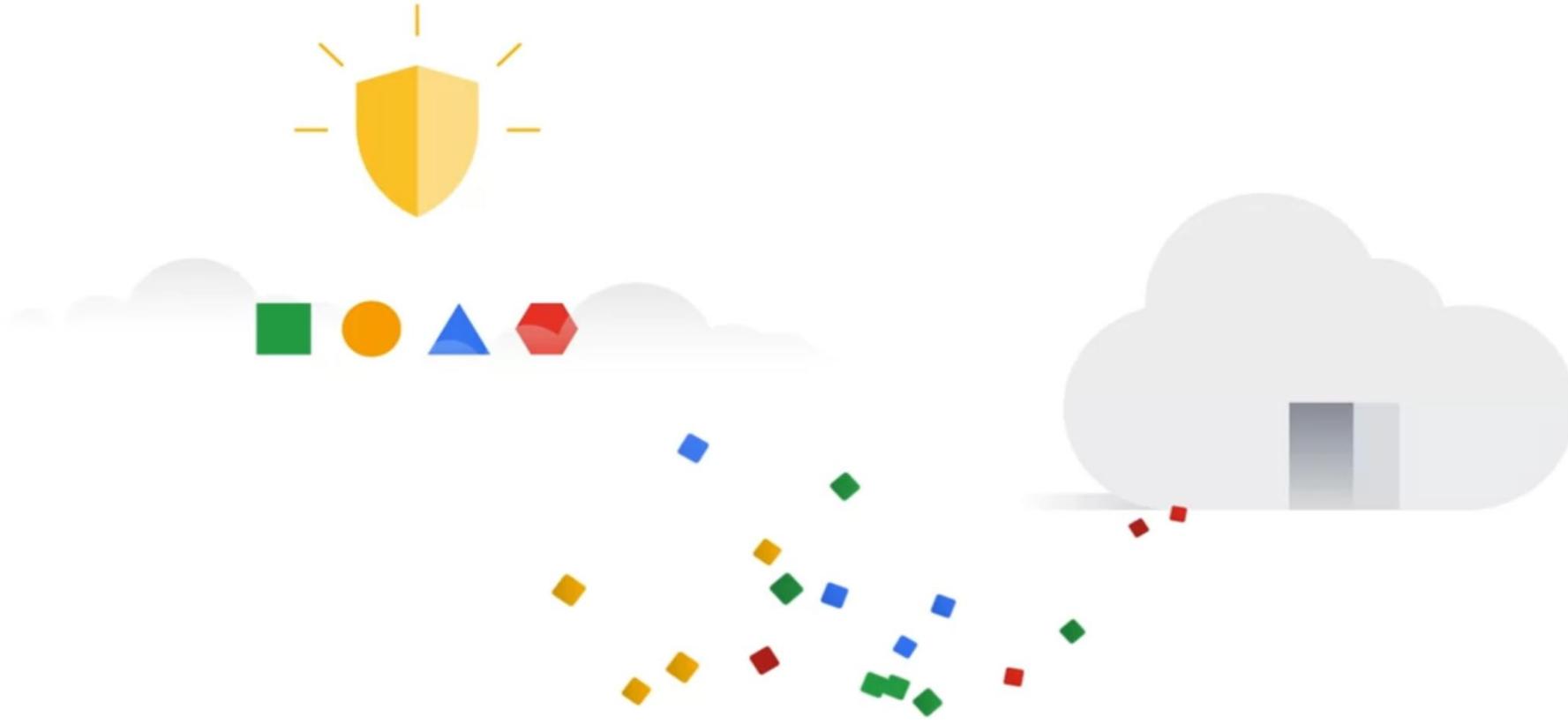




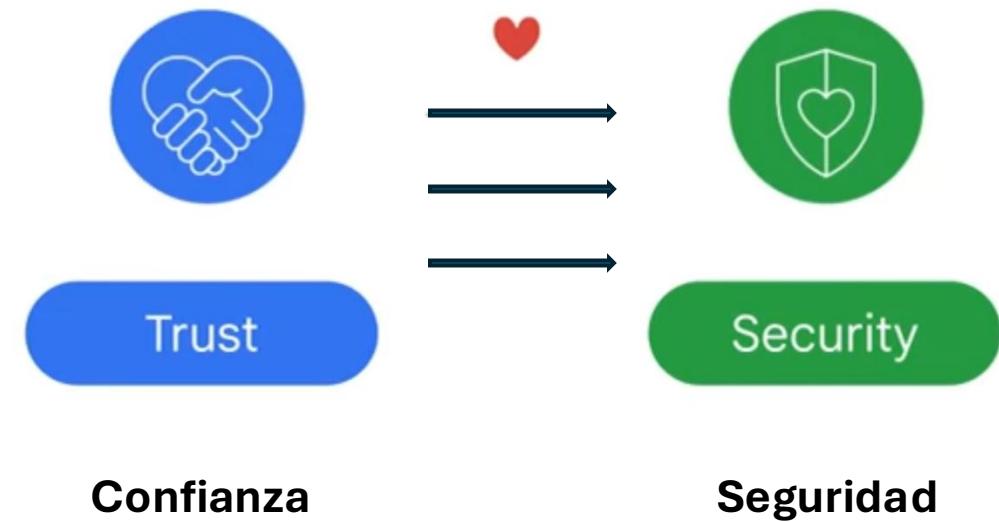
Analizar los conceptos fundamentales de seguridad en la nube.

Explicar el valor comercial del enfoque multicapa de Google para la seguridad de la infraestructura.

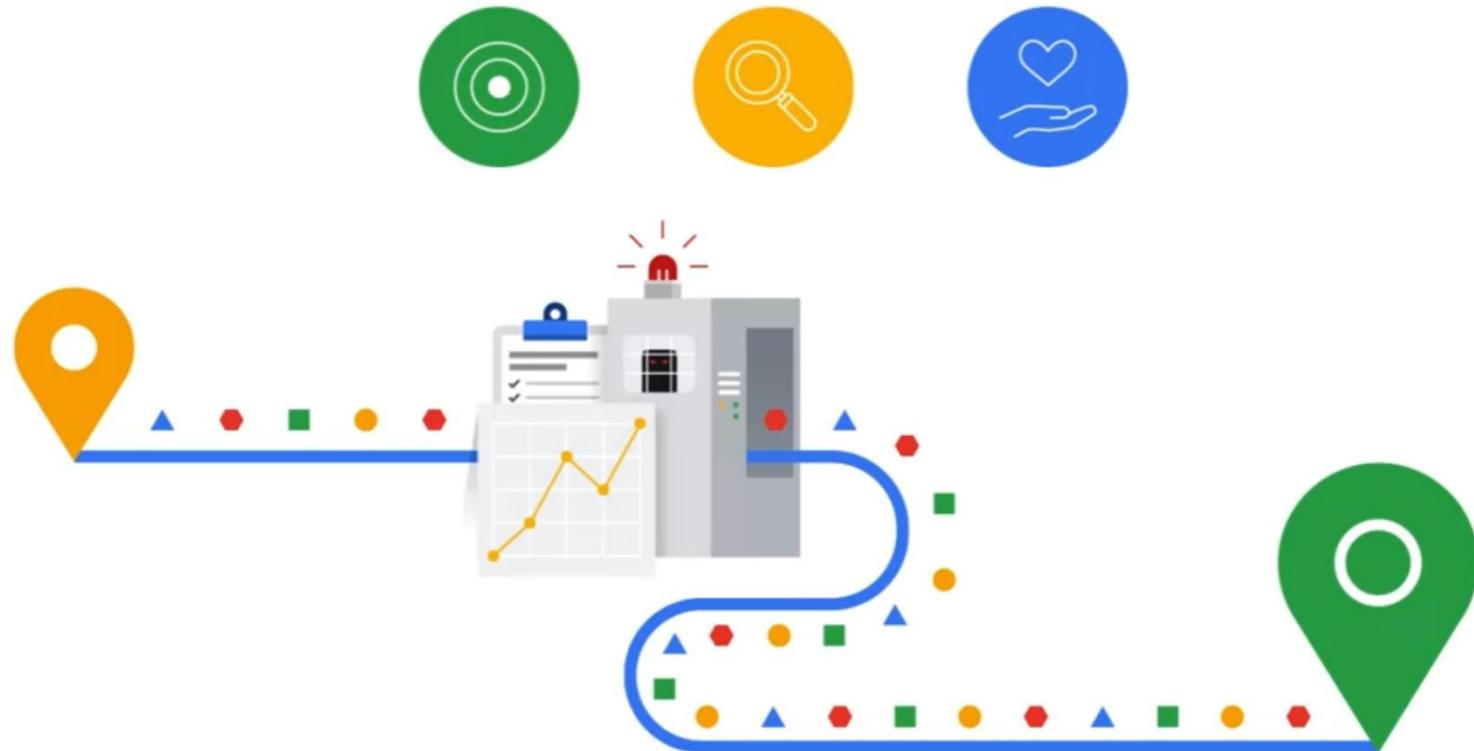
Describir cómo Google Cloud gana y mantiene la confianza de los clientes en la nube.



“A medida que las organizaciones migran cada vez más sus datos y aplicaciones a la nube, se vuelve crucial abordar los desafíos de seguridad.”



Confianza y Seguridad



Conceptos

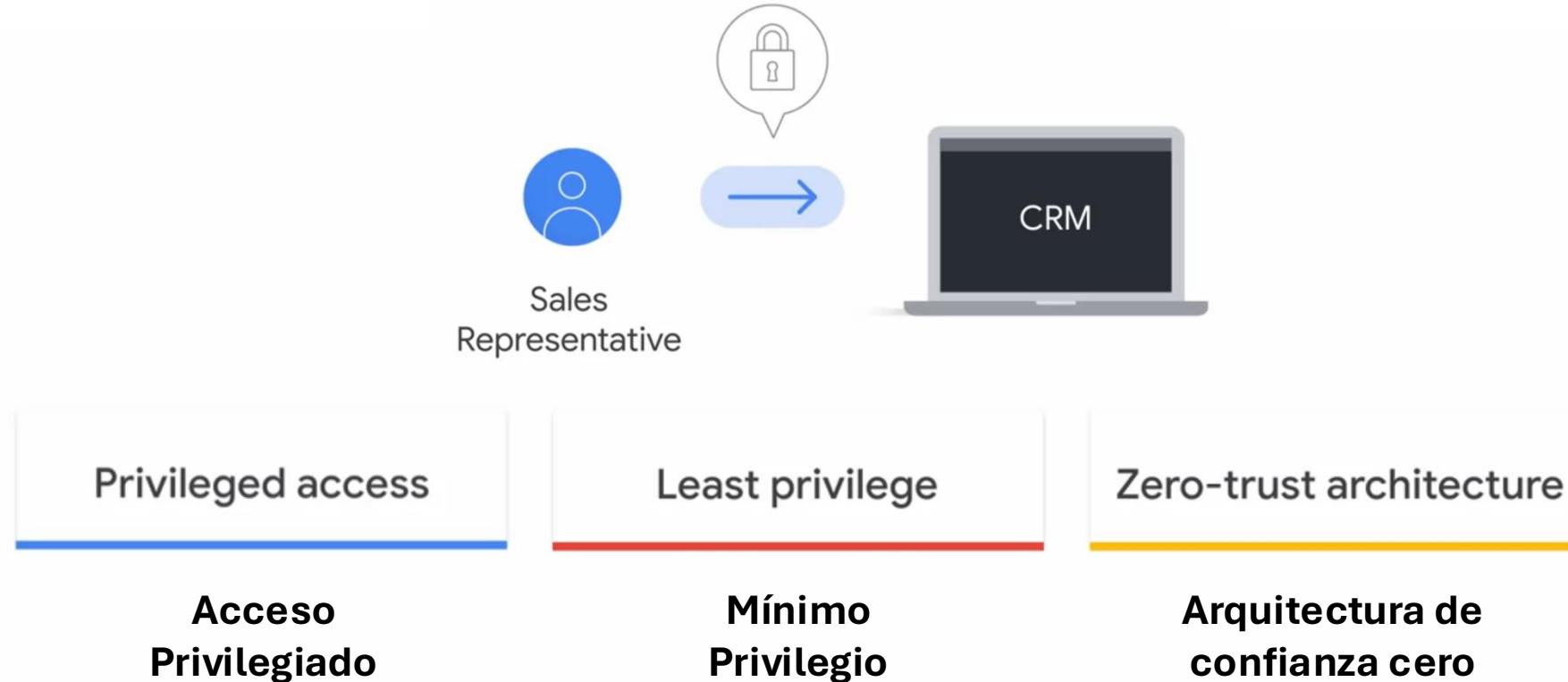
Los primeros tres conceptos están enfocados en reducir el riesgo de acceso no autorizado a datos sensibles.

El **modelo de acceso con privilegios** otorga a ciertos usuarios acceso a un conjunto más amplio de recursos que el de los usuarios normales. Por ejemplo, un administrador del sistema puede tener privilegios especiales para realizar tareas como la solución de problemas o el restablecimiento de datos. Sin embargo, el mal uso de estos privilegios puede generar riesgos significativos, por lo que es esencial gestionar y supervisar este acceso con cuidado.

El **principio de privilegio mínimo** busca otorgar a cada usuario solo el acceso necesario para realizar sus tareas laborales. Al restringir los permisos a lo estrictamente necesario, las organizaciones reducen el riesgo de accesos no autorizados. Por ejemplo, un representante de ventas solo requeriría acceso al sistema CRM, sin necesidad de acceso a sistemas como nóminas o finanzas.

El **modelo de seguridad de confianza cero**, parte de la premisa de que ningún usuario ni dispositivo es de confianza por defecto. Cada usuario y dispositivo debe autenticarse y autorizarse antes de acceder a los recursos, lo que garantiza una seguridad robusta mediante la verificación continua de identidades y controles de acceso estrictos.

Conceptos



Conceptos



Privileged access

Acceso
Privilegiado

Least privilege

Mínimo
Privilegio

Zero-trust architecture

Arquitectura de
confianza cero

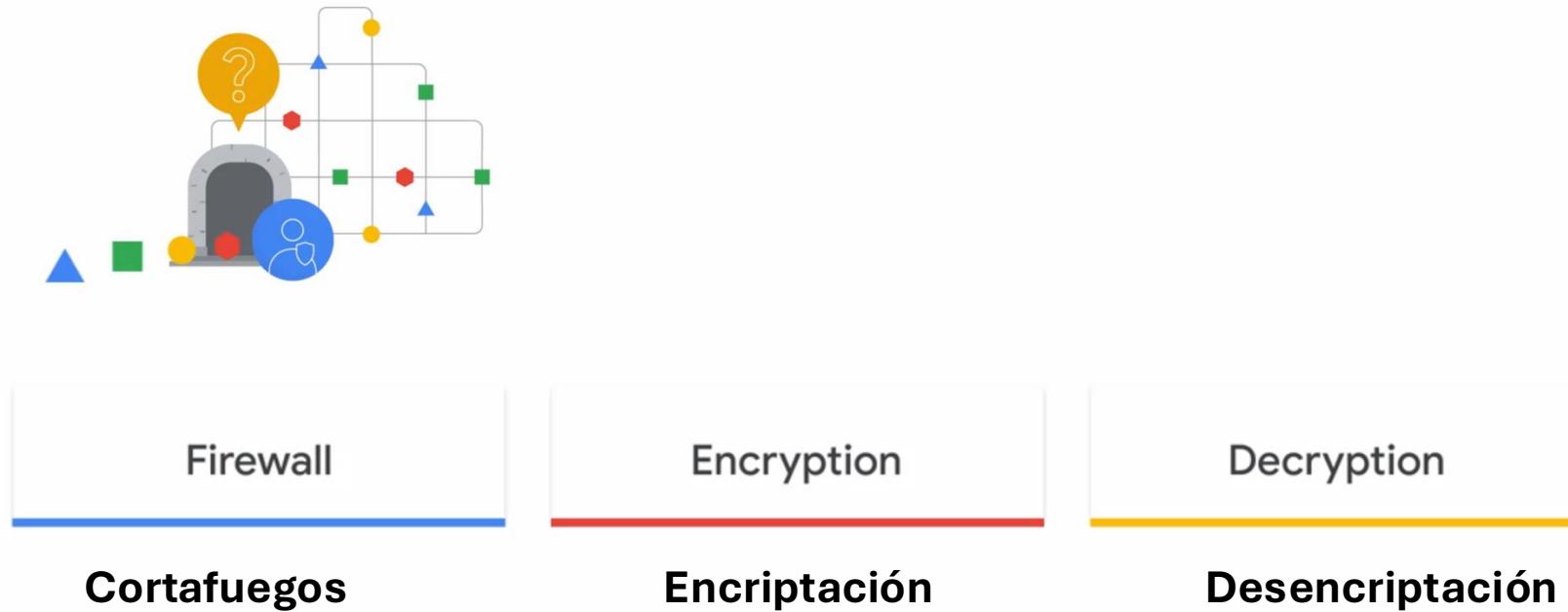
Conceptos

Un **firewall** es un dispositivo de red que regula el tráfico en función de reglas de seguridad predefinidas.

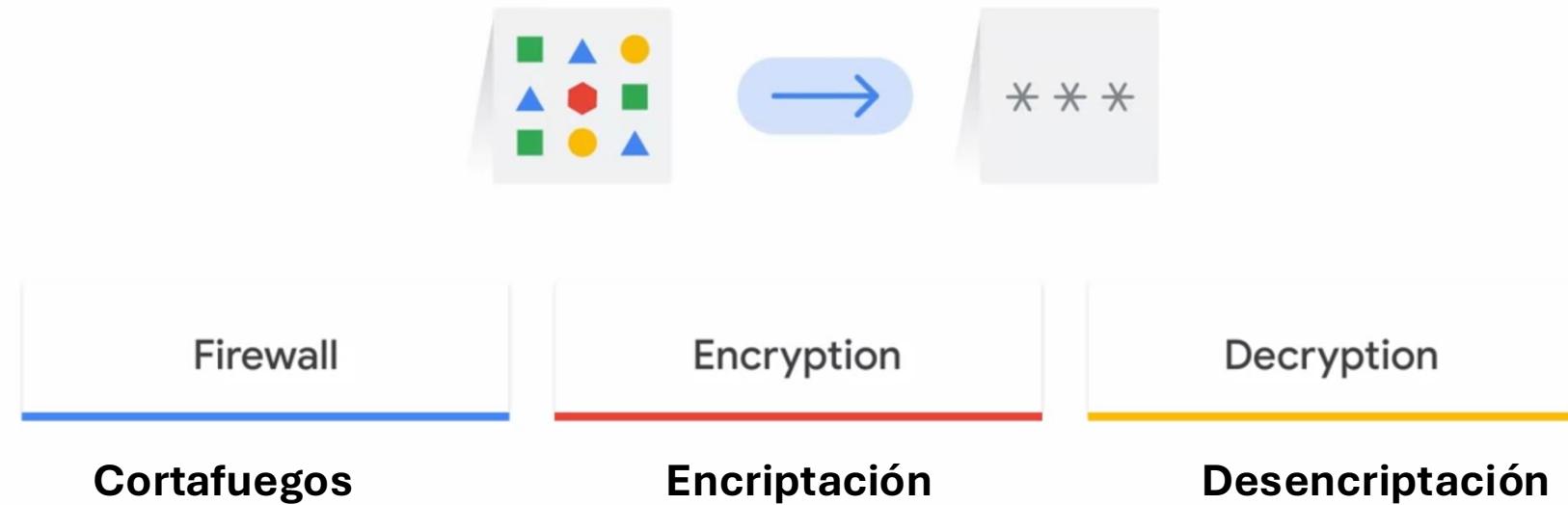
Puedes imaginar un firewall como un guardia de seguridad de la red: revisa el tráfico que ingresa o sale y solo permite aquel que cumpla con los criterios establecidos, protegiendo recursos clave como servidores, bases de datos y aplicaciones. De forma similar a un guardia, que solo deja entrar a quienes tienen autorización, el firewall permite solo el tráfico seguro y autorizado.

La **encriptación** es el proceso de convertir datos en un formato ilegible mediante un algoritmo. Por otro lado, la **desencriptación** convierte esos datos nuevamente a su formato original usando una clave secreta. Proteger esta clave es crucial, ya que es el elemento que permite revertir el cifrado. Puedes pensar en la encriptación como escribir un mensaje en un lenguaje secreto que solo tú y el destinatario pueden entender. Si alguien intercepta el mensaje, no podrá leerlo sin conocer el "lenguaje secreto".

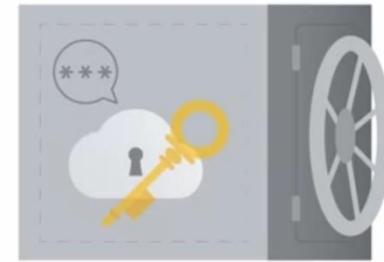
Conceptos



Conceptos



Conceptos



Firewall

Cortafuegos

Encryption

Encriptación

Decryption

Desencriptación

Conceptos



Conceptos

- 1. Confidencialidad:** Se refiere a la protección de la información sensible, asegurando que solo las personas autorizadas tengan acceso a ella, independientemente de su ubicación o medio de transmisión. En el entorno de la nube, la confidencialidad es crítica, ya que los datos sensibles pueden estar expuestos a mayores riesgos. La encriptación desempeña un papel clave.
- 2. Integridad:** La integridad asegura que los datos se mantengan precisos y confiables, evitando modificaciones no autorizadas. Esto es comparable a asegurarse de que un mensaje llegue a su destinatario sin cambios. En la nube, mantener la integridad de los datos implica aplicar controles como sumas de comprobación o firmas digitales, que permiten verificar la autenticidad y exactitud de los datos a lo largo de su ciclo de vida.
- 3. Disponibilidad:** Garantiza que los sistemas y servicios en la nube estén siempre accesibles cuando los usuarios autorizados los necesiten. Es como contar con un suministro eléctrico confiable que nunca se interrumpe. Para maximizar la disponibilidad y reducir el tiempo de inactividad, los entornos de nube deben incorporar mecanismos de conmutación por error, redundancia y planes de recuperación ante desastres.



Confidentiality

Confidencialidad



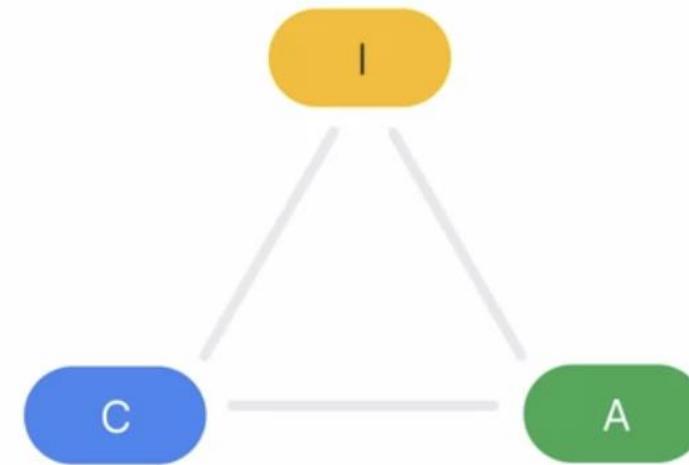
Integrity

Integridad



Availability

Disponibilidad

**Confidencialidad****Integridad****Disponibilidad**

4. Control: Se refiere a las medidas implementadas para gestionar y mitigar los riesgos de seguridad. Incluye la creación de políticas, procedimientos y salvaguardas técnicas que previenen accesos no autorizados y usos indebidos. Los controles de acceso sólidos, las restricciones de permisos y la formación en seguridad son fundamentales para reducir las amenazas. Al garantizar que solo los usuarios autorizados puedan acceder a los datos sensibles, las organizaciones disminuyen considerablemente el riesgo de violaciones de seguridad.

5. Cumplimiento: Implica la adhesión a las regulaciones del sector, normativas legales y políticas internas. El cumplimiento de estas normativas no solo refuerza la seguridad de los datos, sino que también demuestra el compromiso de una organización con la privacidad y seguridad, fomentando la confianza entre las partes interesadas. Los proveedores de servicios en la nube ofrecen marcos y certificaciones que ayudan a las organizaciones a cumplir con sus obligaciones regulatorias, minimizando riesgos legales y financieros.

Ubicación:

En la seguridad en la nube, los datos y aplicaciones se alojan y gestionan en centros de datos externos operados por proveedores de servicios en la nube. La protección de la infraestructura y el hardware subyacente recae en dichos proveedores. Por otro lado, la seguridad local tradicional implica que la organización aloje y gestione sus datos y aplicaciones en su propia infraestructura, lo que le otorga control directo y responsabilidad total sobre el entorno físico y virtual.

Responsabilidad:

En un modelo de seguridad en la nube, la protección de la infraestructura, las redes y las instalaciones físicas es responsabilidad del proveedor de servicios. El cliente, por su parte, es responsable de proteger los datos, las aplicaciones, el acceso de usuarios y la configuración de los sistemas. En contraste, en un entorno local, la organización asume toda la responsabilidad, desde la protección del hardware y la red hasta la gestión de sistemas operativos, aplicaciones y datos.

Escalabilidad:

La seguridad en la nube ofrece escalabilidad y elasticidad, permitiendo a las organizaciones aumentar o reducir recursos según la demanda de manera eficiente y sin complicaciones. Esto es ideal para cargas de trabajo dinámicas y el crecimiento acelerado. En cambio, en un entorno local, las empresas deben aprovisionar y mantener su propia infraestructura, lo que puede ser más lento y costoso al escalar o reducir la capacidad.

Mantenimiento y Actualizaciones:

Los proveedores de servicios en la nube se encargan de la gestión de la infraestructura, incluyendo las actualizaciones de seguridad, parches y mejoras de software. Esto permite a las organizaciones centrarse en sus aplicaciones y datos sin preocuparse por el mantenimiento de la infraestructura subyacente. En contraste, en un entorno local, las organizaciones deben gestionar y actualizar su propia infraestructura, lo que implica tareas regulares como aplicar parches y actualizar tanto software como hardware.

Gastos de Capital:

La seguridad en la nube sigue un modelo basado en gastos operativos (OpEx), donde las organizaciones pagan solo por los servicios que utilizan a través de suscripciones, eliminando la necesidad de grandes inversiones iniciales en infraestructura física. Por el contrario, la seguridad local tradicional requiere un gasto de capital (CapEx) considerable, ya que las empresas deben adquirir y mantener su propia infraestructura de seguridad.



El panorama de los ciberataques evoluciona rápidamente, y estas amenazas pueden venir de fuentes inesperadas, incluso entidades gubernamentales. ¿Cuáles son algunas de las amenazas más comunes para las organizaciones?

1. Ingeniería Social Engañosa

La primera amenaza es la ingeniería social, una técnica manipuladora que explota la confianza de los usuarios para extraer información confidencial. Los cibercriminales utilizan ataques de phishing para recopilar datos personales de empleados, estudiantes o cualquier persona vinculada a la organización. A través de correos electrónicos cuidadosamente diseñados que parecen auténticos, los atacantes engañan a sus víctimas, llevándolas a descargar archivos adjuntos maliciosos, divulgar contraseñas o comprometer información sensible. Ningún miembro de tu organización está exento de ser un blanco potencial.

2. Daño Físico

Además de las amenazas digitales, las organizaciones también enfrentan daños físicos que comprometen sus datos. Esto puede incluir daños a componentes de hardware, interrupciones eléctricas o desastres naturales como inundaciones, incendios o terremotos. Aun en medio de estos eventos, la responsabilidad de proteger la información recae en la organización, que debe garantizar la seguridad de los datos frente a adversidades físicas. Es como asegurar un tesoro valioso incluso cuando la naturaleza desata su furia.

3. Software Malicioso, Virus y Ransomware

Otra amenaza importante son los malwares y virus, que son como "villanos digitales" diseñados para interrumpir operaciones, dañar sistemas o permitir accesos no autorizados. El ransomware es quizás el más siniestro de todos, secuestrando archivos críticos y exigiendo un rescate para liberarlos, en un esquema de extorsión digital premeditado. Estos programas maliciosos pueden paralizar una organización y causar pérdidas financieras y operativas significativas.

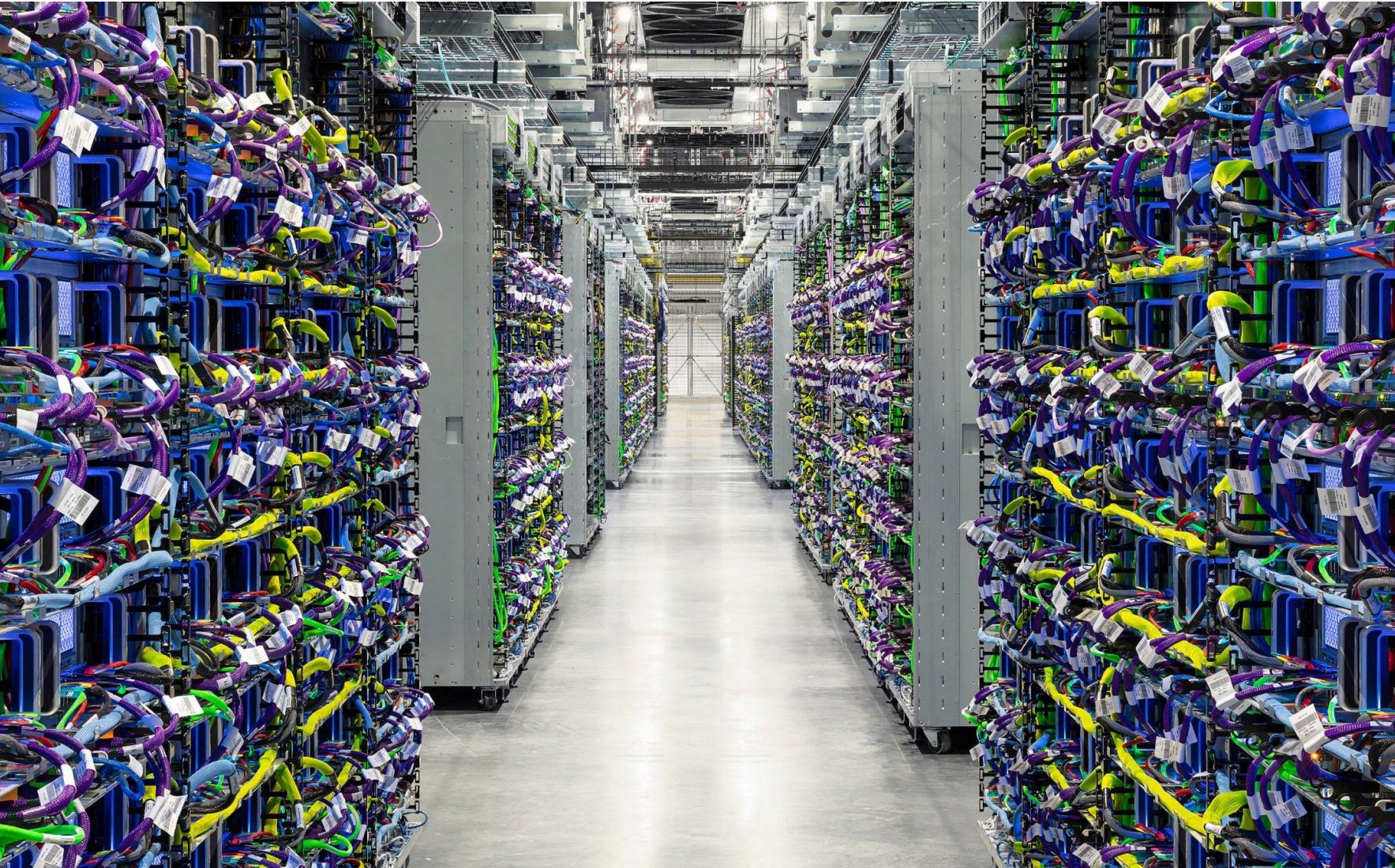
4. Sistemas Externos Vulnerables

Las organizaciones suelen depender de sistemas externos para funciones esenciales como la gestión de inventarios, finanzas o contabilidad. Aunque estos aliados son fundamentales para el funcionamiento del negocio, si no cuentan con las medidas de seguridad adecuadas o no son sometidos a evaluaciones periódicas, pueden convertirse en una amenaza. Un sistema externo comprometido puede poner en riesgo la seguridad de toda la organización, como si una herramienta valiosa se convirtiera accidentalmente en un peligro para tus activos.

5. Errores de Configuración

Incluso los expertos pueden cometer errores. Los errores de configuración son una de las principales amenazas a la seguridad en la nube. Surgen cuando los recursos se configuran incorrectamente, exponiendo involuntariamente sistemas y datos sensibles a accesos no autorizados. Adoptar principios de privilegio mínimo y acceso con privilegios es fundamental para minimizar estos riesgos, asegurando que solo personas autorizadas accedan a recursos específicos cuando sea necesario. Es como dar las llaves solo a quienes realmente confías.

[Infraestructura de Confianza de Google]



1. Centros de Datos

Los centros de datos de Google no son simplemente instalaciones llenas de computadoras; son el pilar fundamental que sustenta la operación continua de servicios clave como Búsqueda, Gmail y YouTube. Además, juegan un rol crucial en el almacenamiento y procesamiento de los datos que impulsan Google Cloud.

2. Eficiencia Energética y Sostenibilidad

La eficiencia es otro pilar del diseño de los centros de datos de Google. Los servidores personalizados están optimizados para realizar tareas específicas de manera más rápida y eficiente, lo que se traduce en un menor consumo de energía, reducción de costos operativos y beneficios ambientales significativos.

3. Escalabilidad y Flexibilidad

La escalabilidad es otro aspecto crucial de los centros de datos de Google. Estas instalaciones están diseñadas para adaptarse rápidamente a nuevas demandas, permitiendo agregar hardware y servidores a medida que crece el tráfico o se requieren más recursos de procesamiento. Esta flexibilidad es clave para manejar el inmenso volumen de datos y el tráfico sin interrupciones, asegurando que los servicios de Google funcionen sin problemas, incluso bajo una alta demanda.

Cumplimiento



The screenshot shows the Google Cloud Compliance Center page. At the top, there's a navigation bar with links for Google Cloud, Descripción General, Soluciones, Productos, Precios, Recursos, Comunicarse Con Nosotros, Documentación, Asistencia, a language dropdown set to Español, a Consola link, and user profile icons.

Centro de recursos de cumplimiento

Certificaciones, documentación y auditorías externas líderes de la industria de Google Cloud para respaldar tu cumplimiento.

[Comunícate con nosotros](#) [Ver las ofertas de cumplimiento](#)

Cumplimiento en Google Cloud

Como parte de la migración a la nube, es posible que debas validar nuestra documentación de cumplimiento, las certificaciones y los controles. Google Cloud crea y comparte asignaciones de nuestros controles de cumplimiento, seguridad y privacidad líderes de la industria para estándares de todo el mundo. También realizamos verificaciones independientes con regularidad, lo que nos permite obtener informes de auditoría y certificaciones para ayudar a demostrar el cumplimiento.

[Descargar informes directamente mediante el Administrador de informes de cumplimiento](#)

Informe sobre la confianza de la IA

Los clientes interesados en el enfoque de Google Cloud para la IA pueden consultar el [Enfoque de confianza en la Inteligencia Artificial de Google Cloud](#) para conocer nuestra postura de seguridad, privacidad, IA responsable y administración.

cloud.google.com/security/compliance

Los principios de confianza y los informes de transparencia de Google Cloud

Tú eres el dueño de tus datos, no Google.

En Google Cloud, priorizamos tu control. Tienes acceso total para gestionar, exportar, eliminar y administrar los permisos de tus datos en nuestra plataforma.

Google no vende los datos de los clientes a terceros.

Tus datos están protegidos, y garantizamos que no se utilizarán con fines publicitarios o de marketing por parte de Google.

Google Cloud no usa los datos de los clientes para publicidad.

Tus datos permanecen confidenciales, y Google Cloud asegura que nunca se utilicen para la segmentación de anuncios.

Los principios de confianza y los informes de transparencia de Google Cloud

Todos los datos de los clientes están encriptados por defecto.

La protección de tus datos es nuestra prioridad. Aplicamos encriptación robusta para mantenerlos seguros, incluso en el caso improbable de un acceso no autorizado.

Protección contra el acceso de usuarios internos no autorizados.

Implementamos medidas de seguridad estrictas para evitar que cualquier personal interno acceda a tus datos sin autorización.

No permitimos accesos no autorizados a gobiernos.

Tus datos están seguros, y ninguna entidad gubernamental puede acceder a ellos sin los procesos legales correspondientes y la debida autorización.

[Preguntas y respuestas]





[¡Muchas
gracias!]