Ficha técnica de licencia de software de ofimática

Indique Nombre Comercial completo del software de Ofimática (si hay más de una licencia lístela)	**Google Education Teaching and Learning**
Capacidad Unidad de almacenamiento de archivos (GB)	100.000 de almacenamiento en la nube compartido entre todos los recursos
Capacidad Unidad de almacenamiento de correos (GB)	100.000 de almacenamiento en la nube compartido entre todos los recursos
¿Requiere licencia CAL? (*)	No require CAL
Límite de Usuarios	Usuarios ilimitados
Informes y Auditoria Web	SI
Antiphishing y Antispam	SI

(*) Si es necesario una licencia adicional (CAL) esta debe estar incluida en el precio

1) Herramientas de Ofimática incluidas

Google Gmail

Google Gmail es un servicio de correo electrónico que permite enviar y recibir correos electrónicos. Correo electrónico empresarial seguro. Con un correo electrónico seguro y sin publicidad como base, también es posible chatear, hacer llamadas de voz o video y estar al tanto del trabajo del proyecto con archivos y tareas compartidos, todo directamente en Gmail.

Más información: https://workspace.google.com/intl/es-419/products/gmail/

Google Docs

Google Docs es un procesador de textos que permite crear, editar y colaborar en documentos con otros usuarios. Es una herramienta muy versátil que se puede utilizar para una gran variedad de tareas, como escribir informes, crear presentaciones, o incluso diseñar folletos.

Más información:https://workspace.google.com/intl/es-419/products/docs/

Google Sheets

Google Sheets es una hoja de cálculo que permite crear, editar y colaborar en hojas de cálculo con otros usuarios. Es una herramienta muy útil para realizar cálculos, crear gráficos, o incluso gestionar datos.

Más información: https://workspace.google.com/intl/es-419/products/sheets/

Google Slides

Google Slides es una aplicación de presentación que permite crear, editar y colaborar en presentaciones con otros usuarios. Es una herramienta muy eficaz para transmitir información a una audiencia.

Más información:https://workspace.google.com/intl/es-419/products/slides/

Google Forms

Google Forms es una herramienta para crear encuestas y cuestionarios. Es una herramienta muy útil para recopilar información de los usuarios, como sus opiniones o preferencias.

Más información: https://workspace.google.com/intl/es-419/products/forms/

Google Sites

Google Sites es una herramienta para crear sitios web. Es una herramienta muy útil para crear sitios web sencillos y funcionales.

Más información:https://workspace.google.com/intl/es-419/products/sites/

Google Chat

Google Chat es un servicio de mensajería instantánea que permite chatear con otros usuarios en tiempo real. Es una herramienta muy útil para comunicarse con otros usuarios de forma rápida y sencilla.

Más información: https://workspace.google.com/intl/es-419/products/chat/

Google Meet

Google Meet es una aplicación de videoconferencia que permite realizar reuniones y conferencias con otros usuarios. Es una herramienta muy útil para colaborar con otros usuarios en tiempo real.

Más información:https://workspace.google.com/intl/es-419/products/meet/

Grabación de Meet:

- **Grabación de clases:** Permite grabar las videollamadas de Meet y guardarlas en Google Drive.
- **Acceso flexible:** Los alumnos pueden acceder a las grabaciones para repasar el contenido o para ponerse al día si faltaron a la clase.
- **Almacenamiento:** Las grabaciones se almacenan en Drive, lo que facilita su organización y acceso.

Classroom:

- **Gestión de clases:** Crea y gestiona clases virtuales, añade alumnos y organiza materiales.
- **Comunicación:** Facilita la comunicación entre profesores y alumnos a través de anuncios, debates y mensajería.
- **Asignación de tareas:** Crea y asigna tareas, proporciona retroalimentación y califica el trabajo de los alumnos.
- **Integración con Meet:** Programa y realiza videollamadas de Meet directamente desde Classroom.

- **Herramientas de originalidad:** Ayuda a los profesores a verificar la originalidad del trabajo de los alumnos.

Beneficios adicionales:

- **Mayor capacidad en Meet:** Permite realizar videollamadas con hasta 250 participantes.

Google Calendar

Google Calendar es una aplicación de calendario que permite programar reuniones y eventos. Es una herramienta muy útil para organizar el tiempo y las tareas.

Más información:https://workspace.google.com/intl/es-419/products/calendar/

Google Drive

Google Drive es un servicio de almacenamiento en la nube que permite almacenar y compartir archivos. Es una herramienta muy útil para compartir archivos con otros usuarios o para acceder a ellos desde cualquier lugar.

Más información: https://workspace.google.com/intl/es-419/products/drive/

Preguntas frecuentes: https://workspace.google.com/intl/es-419_ar/faq/

2) Seguridad Estándar y herramientas de administración Estándar

Google Workspace for Education Teaching and Learning Upgrade incluye un conjunto sólido de características de seguridad estándar para proteger los datos y las cuentas de los usuarios. Estas características son similares a las que se encuentran en otras ediciones de Google Workspace for Education, como Education Fundamentals y Education Plus.

Autenticación:

- **Verificación en dos pasos (2SV):** Añade una capa adicional de seguridad al inicio de sesión, requiriendo un segundo factor de autenticación, como un código enviado al teléfono o una clave de seguridad.
- **Gestión de contraseñas:** Permite a los administradores definir políticas de contraseñas seguras, como la longitud mínima, la complejidad y la frecuencia de cambio.
- **Inicio de sesión único (SSO):** Permite a los usuarios acceder a múltiples aplicaciones y servicios con un solo conjunto de credenciales.

Protección contra amenazas:

- **Protección contra phishing y malware:** Filtros avanzados para detectar y bloquear correos electrónicos y archivos maliciosos.

- **Navegación segura:** Protege a los usuarios de sitios web peligrosos y descargas de archivos maliciosos.
- **Prevención de pérdida de datos (DLP) para Gmail y Drive:** Identifica y protege información confidencial, como números de tarjetas de crédito o datos de identificación personal.

Control de acceso:

- **Gestión de usuarios y grupos:** Crea, gestiona y elimina cuentas de usuario y grupos. Define roles y permisos para controlar el acceso a los datos y las aplicaciones.
- **Control de dispositivos:** Gestiona los dispositivos que acceden a Google Workspace, incluyendo la posibilidad de bloquear o borrar dispositivos de forma remota.

Herramientas de administración:

- **Consola de administración:** Una interfaz centralizada para gestionar todos los aspectos de Google Workspace, incluyendo usuarios, dispositivos, aplicaciones y seguridad.
- **Informes de auditoría:** Accede a registros detallados de la actividad de los usuarios, como inicios de sesión, acceso a archivos y uso de aplicaciones.
- **Gestión de dispositivos móviles:** Configura y gestiona dispositivos móviles, incluyendo la aplicación de políticas de seguridad.
- **Alertas de seguridad:** Recibe notificaciones sobre eventos de seguridad importantes, como intentos de inicio de sesión sospechosos o detección de malware.

Beneficios:

- **Protección de datos:** Protege los datos confidenciales de estudiantes, profesores y personal administrativo.
- **Cumplimiento normativo:** Ayuda a cumplir con las leyes y regulaciones de protección de datos, como FERPA y COPPA.
- **Gestión eficiente:** Facilita la administración de usuarios, dispositivos y aplicaciones.
- **Entorno de aprendizaje seguro:** Crea un entorno de aprendizaje online seguro y protegido

<u>3) Seguridad Avanzada y herramientas de administración móviles</u>

Seguridad Avanzada:

- **Prevención de pérdida de datos (DLP) para Drive, Gmail y Chat:** Teaching and Learning Upgrade incluye DLP para Drive, Gmail y Chat, lo que permite a los administradores identificar y proteger información confidencial en estos servicios. Puedes configurar reglas para detectar contenido sensible, como números de tarjetas de crédito, información de identificación personal, y tomar medidas como bloquear el envío de correos electrónicos o la descarga de archivos.
- **Vault para retención y búsqueda de datos:** Vault está incluido en Teaching and Learning Upgrade. Permite a los administradores retener, buscar y exportar datos de Gmail, Drive (incluyendo Mi unidad, unidades compartidas y carpetas compartidas), Grupos de Google y Chat. Esto es crucial para cumplir con las regulaciones, gestionar registros y realizar investigaciones.
- **Informes de seguridad:** Teaching and Learning Upgrade proporciona informes de seguridad que permiten a los administradores monitorear la actividad de los usuarios y detectar posibles amenazas. Estos informes pueden ayudar a identificar intentos de inicio de sesión sospechosos, el

uso de aplicaciones no autorizadas y otras actividades que podrían poner en riesgo la seguridad de los datos.

Herramientas de administración móvil:

- **Administración básica de dispositivos móviles:** Esta función está incluida en Teaching and Learning Upgrade y permite a los administradores gestionar dispositivos móviles Android e iOS. Puedes requerir contraseñas en los dispositivos, borrar datos de forma remota en caso de pérdida o robo, y aprobar o bloquear aplicaciones.
- **Aplicaciones móviles de Google Workspace:** Los usuarios pueden acceder a las aplicaciones móviles de Google Workspace, como Gmail, Drive, Docs, Meet y Chat, para trabajar y colaborar desde cualquier lugar.

Limitaciones:

Es importante tener en cuenta que Teaching and Learning Upgrade **no incluye todas las funciones de seguridad avanzada** que ofrece Education Plus. Por ejemplo, puede que no tenga el Centro de seguridad, DLP avanzada, análisis de seguridad y gestión de puntos finales. Si la seguridad es una prioridad principal, Education Plus ofrece una solución más completa.

En resumen, Google Workspace for Education Teaching and Learning Upgrade incluye algunas características de seguridad avanzada y herramientas de administración móvil para ayudar a proteger los datos y gestionar los dispositivos. Sin embargo, es importante evaluar las necesidades de seguridad de tu institución para determinar si esta edición ofrece la protección adecuada o si se requiere una edición con más funciones de seguridad, como Education Plus.

4) DLP

Sí, Google Workspace for Education Teaching and Learning Upgrade incluye Prevención de pérdida de datos (DLP).

Aunque no es tan completa como la DLP avanzada que se encuentra en Education Plus, la DLP en Teaching and Learning Upgrade te permite:

- **Proteger información confidencial en Drive, Gmail y Chat:** Puedes crear reglas para detectar contenido sensible, como números de tarjetas de crédito, información de identificación personal, y tomar medidas para evitar que se comparta fuera de la organización.
- **Escanear archivos en Drive:** DLP escanea los archivos almacenados en Drive, incluyendo Mi unidad, unidades compartidas y carpetas compartidas, para detectar información confidencial.
- **Analizar correos electrónicos en Gmail:** DLP analiza los correos electrónicos, tanto el cuerpo del mensaje como los archivos adjuntos, en busca de información confidencial.
- **Monitorear mensajes en Chat:** DLP analiza los mensajes de chat y los archivos compartidos en Google Chat para detectar información confidencial.

Acciones que puedes tomar con DLP:

- **Alertas:** Recibir notificaciones cuando se detecta información confidencial.
- **Bloqueo:** Impedir que se comparta o se descargue el contenido que contiene información confidencial.

- **Cuarentena:** Mover el contenido que contiene información confidencial a una ubicación segura para su revisión.
- **Modificación:** Redactar o enmascarar la información confidencial en el contenido.

5) Aplicación de políticas de retención

Google Workspace for Education Teaching and Learning Upgrade incluye la aplicación de políticas de retención a través de Google Vault.

Esto significa que los administradores pueden usar Vault para:

- **Crear políticas de retención**: Puedes establecer políticas que retengan datos de Gmail, Drive (incluyendo Mi unidad, unidades compartidas y carpetas compartidas), Grupos de Google y Chat durante un período de tiempo específico. Esto ayuda a cumplir con las regulaciones y a preservar información importante.
- **Aplicar retenciones legales**: Puedes colocar retenciones legales en cuentas de usuario específicas para conservar datos relevantes para litigios o investigaciones. Esto garantiza que los datos se conserven, incluso si un usuario los elimina de su cuenta.
- **Buscar y exportar datos**: Vault permite buscar datos retenidos utilizando diferentes criterios y exportarlos en varios formatos. Esto es útil para fines de auditoría, cumplimiento o litigios.

Beneficios de las políticas de retención en Teaching and Learning Upgrade:

- **Cumplimiento normativo:** Ayuda a las instituciones educativas a cumplir con las leyes y regulaciones que requieren la retención de datos, como FERPA.
- **Gestión de registros:** Permite a las instituciones gestionar el ciclo de vida de la información, conservando los datos importantes y eliminando los que ya no son necesarios.
- **Descubrimiento electrónico:** Facilita el proceso de descubrimiento electrónico en caso de litigios o investigaciones.
- **Protección de datos:** Ayuda a prevenir la pérdida accidental o intencional de datos importantes.

6) Identidad Avanzada

Autenticación:

- **Verificación en dos pasos (2SV):** Añade una capa adicional de seguridad al inicio de sesión, requiriendo un segundo factor de autenticación, como un código enviado al teléfono o una clave de seguridad.
- **Gestión de contraseñas:** Permite a los administradores definir políticas de contraseñas seguras, como la longitud mínima y la complejidad, y obliga a los usuarios a cambiar sus contraseñas periódicamente.
- **Inicio de sesión único (SSO):** Permite a los usuarios acceder a múltiples aplicaciones y servicios con un solo conjunto de credenciales, lo que simplifica el acceso y mejora la seguridad.

Autorización:

- **Control de acceso basado en roles (RBAC):** Permite a los administradores asignar roles a los usuarios con permisos específicos, lo que garantiza que solo las personas autorizadas puedan acceder a la información y realizar ciertas acciones.
- **Grupos de usuarios:** Facilita la gestión de permisos al permitir a los administradores asignar permisos a grupos de usuarios en lugar de a usuarios individuales.

Protección de la identidad:

- **Prevención de phishing y malware:** Filtros avanzados para detectar y bloquear correos electrónicos y archivos maliciosos que podrían comprometer las cuentas de los usuarios.
- **Alertas de seguridad:** Notifica a los administradores sobre eventos de seguridad importantes, como intentos de inicio de sesión sospechosos o cambios en la configuración de la cuenta.

6) Informes y Auditoria Móvil

Sí, Google Workspace for Education Teaching and Learning Upgrade incluye informes de auditoría móvil.

Estos informes te permiten rastrear y analizar la actividad de los usuarios en los servicios de Google Workspace desde sus dispositivos móviles.

Información que puedes obtener de los informes de auditoría móvil:

- **Dispositivos:** Tipo de dispositivo (teléfono, tablet), sistema operativo, modelo, ID del dispositivo.
- **Usuarios:** Nombre del usuario, dirección de correo electrónico, grupos a los que pertenece.
- **Aplicaciones:** Aplicaciones de Google Workspace utilizadas en el dispositivo móvil (Gmail, Drive, Meet, Chat, etc.).
- **Acciones:** Acciones realizadas en las aplicaciones, como enviar correos electrónicos, editar documentos, iniciar sesión en Meet, etc.
- **Fechas y horas:** Registro con marca de tiempo de cada acción.
- **Ubicación (en algunos casos):** Ubicación aproximada del dispositivo al realizar la acción.

Acceso a los informes:

Puedes acceder a los informes de auditoría móvil a través de la consola de administración de Google Workspace. Puedes filtrar los informes por diferentes criterios, como fecha, usuario, dispositivo y tipo de acción.

Beneficios de los informes de auditoría móvil:

- **Monitorear el uso de dispositivos móviles:** Te permite comprender cómo se están utilizando los dispositivos móviles para acceder a los servicios de Google Workspace.
- **Identificar posibles problemas de seguridad:** Puedes detectar actividades sospechosas o accesos no autorizados desde dispositivos móviles.
- **Cumplir con las normativas:** Proporciona registros de auditoría para cumplir con las regulaciones de privacidad y seguridad de datos.
- **Mejorar la gestión de dispositivos:** Te ayuda a tomar decisiones informadas sobre la gestión de dispositivos móviles en tu institución educativa.

7) Requisitos de instalación y/o uso

Para licenciamiento nuevo:
La entidad se debe registrar dentro del partner sales console de Noventiq. Una vez esta registrado el cliente debe validar la propiedad de su dominio gubernamental por medio de verificación de DNS publica utilizando registros de tipo TXT. Una vez verificado el dominio de propiedad Noventiq hace el provisionamiento del licenciamiento adquirido en la consola del cliente previamente registrado.
Las suscripciones del licenciamiento google Workspace provisionadas quedan sujetas a ser aprobadas por el cliente mediante la aceptación de términos y condiciones. Esto en un periodo no mayor a 24 horas en el cual el administrador de consola verá en el momento en que inicia sesión, deberá aceptar los términos y condiciones de licenciamiento. Este es mediante consola en un mensaje emergente.
Es responsabilidad del cliente asignar las licencias en la consola admin.google.com a los usuarios que el cliente estime pertinente, esto se realiza a través del sitio admin.google.com por el administrador que la institución gubernamental haya decidido asignar internamente.
[1] La primera vez que el administrador ingrese al sitio admin.google.com con Noventiq como proveedor debe aceptar los términos y condiciones del sitio de administración.
[2] La activación de las licencias debe realizarla directamente el cliente pues en el sitio se maneja información sensible, adicionalmente sí es la primera vez que el cliente compra servicios.
[3] Cabe destacar que el periodo de entrega de licencias comienza a regir desde la aceptación de los términos y condiciones del sitio de administración con Noventiq como su proveedor.

*****Todas las consolas están registradas como Noventiq international**
Suscripciones no suspendidas
Cuentas heredadas gsuite o antiguas de licenciamiento
No tenga ciertas suscripciones que no permiten una transferencia de consola: ejemplo si un cliente tiene Enterprise starter no es autorizado transferir consola con ese licenciamiento.
El cliente no debe tener deudas con Google o con su Partner actual.
Si el cliente tiene suscripciones anualizadas y quiere agregar a ese contrato mediante convenio marco, no es factible salvo que Noventiq sea el Partner incumbente.

Requisitos técnicos servicios Google Workspace

Servicio	Enlaces a requisitos y recomendaciones
Tareas	• **Navegador:** navegadores compatibles con Google Workspace
Directorio	• *Sin requisitos específicos*
Gmail	• **Navegador:** navegadores compatibles con Google Workspace • **Red:** configuración del cortafuegos de Gmail
Google Calendar	• **Navegador:** empezar a utilizar Google Calendar
Google Chat	• **Navegador y hardware:** requisitos de Chat
Contactos de Google	• **Navegador:** navegadores compatibles con Google Workspace
Documentos de Google	• **Navegador y sistema operativo:** requisitos del sistema y navegadores
Google Drive	• **Navegador y sistema operativo:** requisitos del sistema y navegadores • **Red:** configuración del cortafuegos y del proxy de Drive
Google Drive para ordenadores	• **Navegador:** requisitos del sistema y navegadores • **Sistema operativo:** revisa los requisitos del sistema en el artículo Utilizar Google Drive para ordenadores en casa, en el trabajo o en clase.
Formularios de Google	• **Navegador y sistema operativo:** requisitos del sistema y navegadores
Grupos de Google y Grupos para empresas	• **Navegador:** navegadores compatibles con Google Workspace
Google Keep	• *Sin requisitos específicos*
Google Meet	• **Navegador y sistema operativo:** requisitos de uso de Google Meet • **Red:** preparar tu red para videollamadas de Meet **Nota:** Estos requisitos también se aplican a la emisión en directo de Meet.
Hojas de cálculo de Google	• **Navegador y sistema operativo:** requisitos del sistema y navegadores
Google Sites	• **Navegador:** requisitos para usar Google Sites • **Red:** requisitos de Google Sites
Presentaciones de Google	• **Navegador y sistema operativo:** requisitos del sistema y navegadores
Google Tasks	• *Sin requisitos específicos*

Servicio	Enlaces a requisitos y recomendaciones
Google Vault	• *N/A*
Gestión de identidades	• **Navegador:** navegadores compatibles con Google Workspace

8) Consola

Desde la consola se pueden generar políticas de conservación local y retención por juicio, al colocar un buzón en Conservación local o retención por juicio, la conservación o retención se aplica al buzón principal y al buzón de archivo.

Estas funcionalidades se administran desde el portal de cumplimiento Microsoft Purview para habilitar buzones de archivo en pos de admitir los requisitos de retención de mensajes, exhibición de documentos electrónicos y retención de mensajes de la organización, adicionalmente puede crear una directiva de archivado y eliminación en Microsoft 365 que mueva automáticamente los elementos al buzón de archivo de un usuario.

Sobre el cifrado de la información en el correo electrónico, Microsoft usa seguridad de la capa de transporte (TLS) y secreto de reenvío (FS) para proteger las comunicaciones.

TLS (Seguridad de la capa de transporte) y SSL (antecesor de TLS) son protocolos criptográficos que protegen la comunicación por red con certificados de seguridad que cifran una conexión entre equipos. TLS reemplaza a Capa de sockets seguros (SSL) y a menudo se conoce como SSL 3.1. Exchange Online usa TLS para cifrar las conexiones entre los servidores de Exchange y las conexiones entre los servidores de Exchange y otros servidores, como los servidores de Exchange locales o los servidores de correo de los destinatarios. Una vez cifrada la conexión, todos los datos enviados a través de esa conexión se envían a través del canal cifrado. Sin embargo, si reenvía un mensaje que se envió a través de una conexión cifrada con TLS a una organización de destinatarios que no admite el cifrado TLS, ese mensaje no se cifra necesariamente.

Use TLS en situaciones en las que quiera configurar un canal seguro de correspondencia entre Microsoft y su organización local u otra organización, como un asociado. Exchange Online siempre intenta usar TLS primero para proteger el correo electrónico, pero no puede hacerlo si la otra parte no ofrece seguridad TLS.

En cuanto al cifrado de la información confidencial en sus centros de datos, Microsoft utiliza una tecnología denominada Distributed Key Manager, esta es una funcionalidad del lado cliente que usa un conjunto de claves secretas para cifrar y descifrar información. Solo los miembros de un grupo de seguridad específico de los Servicios de dominio de Active Directory pueden tener acceso a dichas claves para descifrar los datos cifrados por el DKM. En Exchange Online, solo determinadas cuentas de servicio bajo las cuales se ejecutan procesos de Exchange forman parte del grupo de seguridad. Como parte del procedimiento operativo estándar en el centro de datos, ningún humano tiene credenciales que forman parte de este grupo de seguridad y, por lo tanto, nadie tiene acceso a las claves que pueden descifrar la información confidencial.

Para depuración, solución de problemas o fines de auditoría, un administrador del centro de datos debe solicitar acceso con privilegios elevados para obtener credenciales temporales que forman parte del grupo de seguridad. Este proceso requiere varios niveles de aprobación legal. Si se concede acceso, toda la actividad se registra y se audita. Además, solo se otorga acceso durante un determinado intervalo de tiempo, que caduca automáticamente una vez concluido.

Para brindar protección adicional, la tecnología del DKM incluye sustitución de claves y archivado automático. Esto también garantiza el acceso al contenido anterior sin tener que recurrir a la misma clave de forma indefinida.

En cuanto a la gestión de políticas de Grupo y políticas en la nube, la consola en el centro de administración de Aplicaciones Microsoft 365 permite aplicar la configuración de directivas para Aplicaciones Microsoft 365 para empresas en el dispositivo de un usuario, incluso si el dispositivo no está unido a un dominio o

administrado de otro modo. Cuando un usuario inicia sesión en las Aplicaciones de Microsoft 365 para empresas en un dispositivo, la configuración de la Directiva se desplaza a ese dispositivo. La configuración de directivas está disponible para dispositivos con Windows, macOS, iOS y Android, aunque no todas las opciones de configuración de directiva están disponibles para todos los sistemas operativos. También puede aplicar algunas configuraciones de directiva para Office para la Web, tanto para los usuarios que han iniciado sesión como para los usuarios que tienen acceso a documentos de forma anónima.
La directiva de nube admite grupos de seguridad y grupos de seguridad habilitados para correo creados o sincronizados con Azure AD.
Al crear configuraciones de directiva, puede revisar y aplicar las directivas recomendadas por Microsoft como directivas de línea base de seguridad. Estas recomendaciones se marcan como "Línea base de seguridad" al seleccionar directivas.
Más información sobre Archiving en este link, en cuanto al cifrado de la información en la capa de transporte en este link, sobre la protección de los datos en almacenamiento en este link y sobre políticas de directivas en este link.
*Para crear una configuración de directiva, debe tener asignado el rol adecuado dentro del portal de administración, el cual se gestiona a nivel interno en la organización.

9) Otra información relevante del producto

Diferencias entre Google Workspace Education Plus y Teching and Learning.

Característica	Education Plus	Teaching and Learning Upgrade
Enfoque	Seguridad avanzada, herramientas completas, amplio almacenamiento	Herramientas de enseñanza y aprendizaje mejoradas, mayor almacenamiento
Seguridad	Estándar + Avanzada	Estándar (algunas funciones avanzadas)
Herramientas de enseñanza y aprendizaje	Completas	Completas
Almacenamiento	100 TB + 20 GB/usuario	100 TB + 100 GB/usuario
Precio	Más caro	Intermedio