Ficha técnica de licencia de software para ofimática

Indique Nombre Comercial completo del software de Ofimática (si hay más de una licencia lístela)	Microsoft Teams Enterprise, Office 365 E3 (no Teams), Microsoft Defender for Office 365 (Plan 1)
Capacidad mínima de Unidad de almacenamiento de archivos (GB)	5000 GB, expandible hasta 25.000 GB (sin costo)
Capacidad mínima de Unidad de almacenamiento de correos (GB)	100 GB (hasta 1.500 GB de archivado)
¿Requiere licencia CAL? (*)	No
Límite de Usuarios	Sin límite de usuarios
Informes y Auditoría Web	Incluido
Antiphishing y Antispam	Incluido

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

1. **Herramientas de Ofimática incluidas** (sujetas a disponibilidad de la marca):

- ✓ Correo electrónico: incluye Exchange Online Plan 2 que contiene Buzón de 100 GB y mensajes de hasta 150 MB, además proteger la información mediante funcionalidades avanzadas. Los filtros antimalware y contra correo no deseado protegen los buzones.
- ✓ OneDrive: obtén acceso a una capacidad de entre 1 y 5 TB o más de almacenamiento en la nube personal desde cualquier lugar o dispositivo (expandible). Comparte documentos fácilmente con otros usuarios de tu organización o ajenos a ella y controla quién puede ver y editar cada archivo.
- ✓ SharePoint: Comparte y administra contenido, información y aplicaciones con el almacenamiento de SharePoint. Impulsa el trabajo en equipo, encuentra información rápidamente y colabora con todos los miembros de la organización sin problemas.
- ✓ Cumplimiento de normas: Aumenta tus capacidades de cumplimiento con Microsoft Purview eDiscovery y Auditoría de Microsoft Purview (Estándar).
- ✓ Protección de información: Ayuda a proteger la información con el cifrado básico de mensajes y la prevención de pérdida de datos de Microsoft 365 (para correo electrónico y archivos).
- ✓ Apps de Microsoft 365: Instala las aplicaciones de Microsoft 365, como Word, Excel, PowerPoint, OneNote (solo para PC) y Microsoft Access (solo para PC), en hasta cinco equipos PC o Mac, cinco tabletas y cinco teléfonos por usuario.
- ✓ Microsoft 365 en la web: Crea, comparte y colabora dondequiera que estés.
- ✓ Sway: Crea boletines, presentaciones y documentaciones visualmente atractivos en cuestión de minutos.
- ✓ Microsoft Graph: Usa este modelo de programación unificado para acceder a datos para crear aplicaciones para organizaciones y consumidores que interactúen con millones de usuarios.
- ✓ Planner: Organiza el trabajo en equipo, crea planes, asigna tareas, comparte archivos, chatea y recibe actualizaciones sobre el progreso.
- ✓ Forms: Crea encuestas, cuestionarios y sondeos fácilmente.
- ✓ Microsoft Teams Enterprise: plataforma de colaboración y comunicación empresarial que ayuda a los equipos a mantenerse enfocados, colaborar eficientemente e impulsar el negocio

Más información en: Office 365 E3 (sin Teams)

2. **Seguridad Estándar y herramienta de administración estándar:** El Centro de administración de Microsoft 365 permite gestionar los usuarios y aplicaciones de forma rápida y simple, en este portal se pueden agregar o eliminar a los usuarios y asignarle/desasignarle las licencias correspondientes, este portal tiene dos vistas: la vista simplificada ayuda a las organizaciones más pequeñas a administrar sus tareas más comunes. La vista panel incluye tareas y configuraciones más complejas. Puede cambiar entre ellos desde un botón en la parte superior del centro de administración.

En el Centro de administración de Microsoft 365, puede restablecer contraseñas, ver la factura, agregar o quitar usuarios y mucho más en un solo lugar.

Las áreas de trabajo especializadas, como seguridad o administración de dispositivos, permiten un control más pormenorizado y pueden descargar reportes de uso u obtener recomendaciones de seguridad presentes en la plataforma a través de una puntuación en el panel Secure Score.

Seguir las recomendaciones de la puntuación de seguridad puede proteger a su organización de amenazas

La puntuación de seguridad ayuda a las organizaciones a:

- ✓ Informar sobre el estado actual de la situación en materia de seguridad de la organización.
- ✓ Mejorar la situación de seguridad proporcionando capacidad de descubrimiento, visibilidad, orientación y control.
- ✓ Comparar con puntos de referencia y establecer indicadores clave de rendimiento (KPI).

De forma predeterminada, la persona que se registra y compra una suscripción de Microsoft 365 para empresas obtiene permisos de administrador. Esa persona puede asignar permisos de administrador a otras personas para ayudarles a administrar Microsoft 365 para su organización.

**Para poder descargar estos reportes se requiere el rol adecuado dentro del portal de administración, el cual se gestiona a nivel interno en la organización.* Más información en este link.

Del lado de Teams Enterprise:

- ✓ Cifrado: Las comunicaciones en Teams están cifradas por defecto. Teams utiliza certificados, OAUTH, Transport Layer Security (TLS) y Secure Real-Time Transport Protocol (SRTP) para proteger todos los datos en la red
- ✓ Modelo de seguridad Zero Trust: Teams sigue el modelo de seguridad Zero Trust, que incluye la autenticación y autorización en función de todos los puntos, como la identidad del usuario, la ubicación, el estado del dispositivo, el servicio o la carga de trabajo, la clasificación de datos y las anomalías
- ✓ Protección contra amenazas comunes: Teams maneja amenazas comunes como ataques de denegación de servicio distribuido (DDoS) y ataques de clave comprometida mediante el uso de características de PKI en el sistema operativo Windows Server para proteger los datos clave utilizados para el cifrado de las conexiones TLS
- ✓ Más información: Security and Microsoft Teams

3. **Seguridad Avanzada y herramientas de administración móviles:** las etiquetas de confidencialidad de Microsoft Purview Information Protection le permiten clasificar y proteger

los datos de su organización, a la vez que se asegura de que la productividad de los usuarios y su capacidad de colaboración no se vean obstaculizadas (fuente).

Defender for Office 365 Plan 1 detecta y bloquea intentos de phishing, protegiendo a los usuarios de correos electrónicos fraudulentos que buscan robar información sensible. También, filtra correos no deseados para mantener las bandejas de entrada libres de spam.

4. **DLP:** incluido (fuente)

5. **Identidad Avanzada:** Entra ID for O365 admite autenticación multifactor, SSO ilimitado en cualquier aplicación SaaS, informes básicos y cambio de contraseña de autoservicio para usuarios de la nube. Administrar usuarios y grupos en la nube. Sincroniza el directorio local con MIcrosoft Entra ID (fuente).

6. **Informes y Auditoría móvil**

Microsoft Purview Compliance Manager ayuda desde realizar un inventario de los riesgos de protección de datos hasta administrar las complejidades de la implementación de controles, para que puedan realizar auditoría web interna (fuente).

Microsoft Teams permite buscar eventos en el registro de auditoría, lo que te ayuda a investigar actividades específicas en los servicios de Microsoft 365. Algunas de las actividades auditadas en Teams incluyen la creación y eliminación de equipos, la adición y eliminación de canales, y cambios en la configuración de los canales1. Para recuperar los registros de auditoría de las actividades de Teams, puedes ir al portal de cumplimiento de Microsoft Purview y seleccionar la opción de auditoría (fuente).

Defender for Office 365 Plan 1 ofrece informes de auditoría que permiten a los administradores de seguridad, equipos de TI, equipos de riesgo internos e investigadores legales y de cumplimiento buscar registros de auditoría para diversos eventos.

7. **Requisitos de instalación y/o uso:** Office 365 E3 permite instalar las aplicaciones de Microsoft 365, como Word, Excel, PowerPoint, OneNote (solo para PC) y Microsoft Access (solo para PC), en hasta cinco equipos PC o Mac, cinco tabletas y cinco teléfonos por usuario. Para instalar Microsoft 365 u Office, es necesario asociar la cuenta a una cuenta de Microsoft o a una cuenta profesional o educativa. En el caso de Teams Enterprise:

➔ Para equipos de escritorio de Windows:
- Ordenador y procesador: Mínimo 1,1 GHz o más rápido, dos núcleos.
- Memoria: 4,0 GB de RAM.
- Disco duro: 3,0 GB de espacio disponible en disco.
- Pantalla: Resolución de 1024 x 768 o superior.
- Hardware de gráficos: DirectX 9 o posterior, con WDDM 2.0 o posterior para Windows 10.
- Sistema operativo: Windows 10 versión 10.0.19041 o posterior (excepto las versiones LTSC de Windows para la aplicación de escritorio de Teams).
- Webview2: Actualizar a la versión más reciente.
- Vídeo: Cámara de vídeo USB 2.0.

- Dispositivos: Cámara estándar de portátil, micrófono y altavoces.

➔ Para macOS Desktop:
- Ordenador y procesador: Procesador de doble núcleo.
- Memoria: 4,0 GB de RAM.
- Disco duro: 1,5 GB de espacio disponible en disco.
- Pantalla: Resolución de 1200 x 800 o superior.
- Sistema operativo: Una de las tres versiones más recientes de macOS.
- Webview2: Actualizar a la versión más reciente.
- Vídeo: Cámara web compatible.
- Voz: Micrófono y altavoces compatibles, auriculares con micrófono o dispositivo equivalente.

➔ Para la Web:
- Exploradores compatibles: Microsoft Edge (últimas tres versiones), Chrome (últimas tres versiones).
- Sistemas operativos: Windows, macOS, Linux.

- Más información: Nuevos requisitos del sistema de Teams

Sobre Defender for Office 365 P1:

- Configuración de la autenticación de correo electrónico: Es necesario configurar la autenticación de correo electrónico para los dominios de Microsoft 365, lo que incluye la habilitación de DKIM, DMARC y SPF
- Configuración de directivas de protección: Debes configurar las directivas de protección en Exchange Online Protection (EOP) y Defender para Office 365 para maximizar las capacidades de protección
- Asignación de permisos a administradores: Es necesario asignar roles y permisos adecuados a los administradores para configurar y gestionar las características de EOP y Defender para Office 365 (Introducción a Microsoft Defender para Office 365

Para poder ejecutar la carga de licenciasen el tenant necesario y usar estas licencias es necesario lo siguiente:

1. **Provisión de Información del Tenant**: La institución gubernamental debe proporcionar la información del tenant. Con esta información, Noventiq enviará un enlace al administrador del tenant para vincularnos como administradores delegados. Este paso es crucial técnicamente, ya que sin esta vinculación, Noventiq no podrá cargar las licencias en el tenant.
2. **Aceptación de Términos de Uso**: La institución gubernamental debe aceptar los términos de uso de las licencias Microsoft.

8. Otra información relevante del producto:

Office 365 E3 se integra completamente con otras herramientas de Microsoft, tiene enfoque en la seguridad y cumplimiento, y su capacidad para facilitar la colaboración y comunicación en entornos educativos y empresariales. Microsoft Teams Enterprise permite una colaboración eficiente al conectar

a las personas adecuadas con la información correcta y ofrece seguridad avanzada con cifrado y un **modelo de seguridad Zero Trust.** Además, se integra perfectamente con otras herramientas de Microsoft 365, lo que facilita el flujo de trabajo. Incluye características impulsadas por inteligencia artificial que simplifican la colaboración y permite personalizar la experiencia con características de accesibilidad. Microsoft Defender for Office 365 Plan 1 ofrece protección avanzada contra ciberataques como phishing, malware, spam y compromisos de correo electrónico empresarial.