Apuntes — Módulo 1: Fundamentos: qué es Copilot, cómo funciona y bajo qué reglas

Copilot para las herramientas básicas de Microsoft 365

Aprendizaje esperado. Identificar los componentes, alcances y restricciones de Microsoft 365 Copilot, conforme a condiciones de licenciamiento y reglas de seguridad y privacidad de la organización.

1. Bienvenido a tu nuevo asistente de IA

Microsoft 365 Copilot es un asistente con inteligencia artificial que se integra directamente en las aplicaciones de productividad que ya usas: Word, Excel, PowerPoint, Outlook, Teams, Forms y OneDrive. No es un software aparte ni una ventana flotante; aparece *dentro* de cada herramienta cuando lo necesitas.

Funciona a partir de **indicaciones (prompts)**: tú escribes lo que necesitas y Copilot responde en tiempo real, combinando tres elementos clave:

- **Los modelos de lenguaje grandes (LLM)**, que procesan el lenguaje natural.
- **Microsoft Graph**, que reúne tus correos, chats, documentos, calendario, reuniones y contactos.
- **Las aplicaciones de Microsoft 365**, donde trabajas cada día.

Lo importante: Copilot **solo accede a la información que tú ya tienes permiso de ver**. Si no puedes abrir un archivo, Copilot tampoco. Este principio se llama **permisos heredados** y es la base de su funcionamiento seguro.

Copilot no adivina ni inventa: usa **indexación semántica** para entender el significado de tus datos y responder con precisión, siempre dentro del límite de acceso basado en tu identidad.

2. Copilot vs. Copilot Chat: no es lo mismo

Existen dos experiencias que parecen iguales pero no lo son:

	Microsoft 365 Copilot	Microsoft 365 Copilot Chat
Licencia	Requiere licencia de complemento	No requiere licencia adicional
Datos que usa	Datos de la organización *y* la web	La web; el usuario puede aportar datos manualmente
Dónde aparece	Integrado en Word, Excel, PowerPoint, Outlook, Teams, etc.	Chat independiente, sin integración profunda en apps
Etiqueta en producto	M365 Copilot (Premium)	Chat de Copilot (Básico)

Si tu organización te asignó la **licencia de complemento**, verás la etiqueta *M365 Copilot (Premium)* y tendrás acceso prioritario. Sin ella, verás *Chat de Copilot (Básico)* o *M365 Copilot (Básico)*, con acceso estándar y sin las funciones integradas en Excel, Word, PowerPoint y OneNote.

Importante: También existe Microsoft Copilot gratuito para consumidores (uso personal), que es otra cosa completamente distinta y no tiene acceso a datos corporativos.

3. Qué hace Copilot en cada aplicación

Copilot actúa de forma distinta según dónde lo uses. Aquí tienes un resumen práctico:

- **Word:** Redacta borradores en documentos nuevos o existentes, resume, responde preguntas sobre el texto y ejecuta comandos ligeros de edición.
- **Excel:** Sugiere fórmulas, crea gráficos y tablas dinámicas, identifica tendencias, ordena, filtra y resalta datos. Trabaja en modo edición directa, Plan (propone pasos antes de ejecutar) o Chat (analiza sin modificar).
- **PowerPoint:** Crea presentaciones desde cero o desde un archivo de Word, agrega diapositivas, imágenes y aplica formato a toda la presentación usando las plantillas de tu organización.
- **Outlook:** Resume hilos de correo, redacta mensajes extrayendo información de otros correos o archivos de Microsoft 365, y ofrece sugerencias de tono, claridad y sentimiento.
- **Teams:** En *chat*, resume hasta 30 días del hilo actual (solo ese chat, no otros hilos ni correos). En *reuniones*, usa la transcripción en tiempo real, captura puntos clave, responsables y pasos siguientes.
- **Forms:** Redacta preguntas y opciones para encuestas y formularios.
- **OneDrive:** Facilita la recuperación de archivos mediante búsqueda en lenguaje natural.

Atención: Las interfaces pueden cambiar; lo importante es entender *el criterio*: Copilot accede solo a los datos que ya puedes ver y responde dentro del contexto de cada aplicación.

4. Seguridad, privacidad y cumplimiento normativo

Las solicitudes, respuestas y datos que Copilot consulta en Microsoft Graph NO se usan para entrenar los modelos de lenguaje base, incluidos los que usa Copilot. Tus indicaciones y las respuestas quedan en tu **historial de actividad de Copilot**, cifrado en reposo (BitLocker, cifrado por archivo) y en tránsito (TLS, IPsec). Puedes eliminar tu historial desde el portal Mi cuenta.

Cumplimiento normativo:

- **RGPD** (Reglamento General de Protección de Datos de la Unión Europea).
- **ISO 27001** (gestión de seguridad de la información).
- **ISO 42001** (sistemas de gestión de inteligencia artificial).
- **HIPAA** (datos de salud en EE.UU.).
- **Límite de datos de la Unión Europea:** el tráfico de la UE permanece dentro de ese límite (desde el 1 de marzo de 2024).

Protecciones integradas: Copilot bloquea contenido dañino (odio, violencia, sexual, autolesión), detecta material protegido por copyright o licencias de código, y bloquea inyecciones de instrucciones (jailbreak) mediante clasificadores XPIA.

Importante: Los administradores pueden ver y gestionar el historial con Búsqueda de contenido o Microsoft Purview, y aplicar directivas de retención. Si la organización desactiva las experiencias conectadas que analizan contenido, Copilot deja de funcionar en Excel, OneNote, Outlook, PowerPoint y Word.

5. Expectativas realistas: qué hace y qué NO garantiza

El resultado de Copilot NO está garantizado como 100 % exacto. Copilot genera borradores, resúmenes y sugerencias basándose en datos y patrones, pero puede cometer errores de interpretación, omitir detalles o inventar información que parezca coherente (*alucinaciones*).

Tu responsabilidad:

- Revisar críticamente cada respuesta antes de compartirla.
- Verificar datos, cifras, nombres y fechas contra las fuentes originales.
- Confirmar que el tono y el mensaje sean apropiados para el destinatario.
- No delegar tu criterio profesional a la herramienta.

Propiedad del resultado: Microsoft no reclama derechos sobre lo que generas con Copilot. Además, existe el **Compromiso de derechos de autor de Copilot**: si un tercero demanda a tu organización por infracción de copyright derivada del uso de Copilot (con los filtros activos), Microsoft asume la defensa legal y los costos.

Límites técnicos: Copilot no puede inferir, juzgar ni evaluar el rendimiento, actitud o estado emocional de empleados a partir de sus comunicaciones (restricción de *daños en el lugar de trabajo*). Tampoco crea nuevos permisos: si no puedes

ver un archivo, Copilot tampoco.

Copilot **hace visible** lo que ya existe en tus datos; no crea filtraciones, pero sí las expone si los permisos están mal configurados.

6. Cómo escribir una buena indicación y qué NO entregar a la IA

Anatomía de una buena indicación (prompt):

- **Objetivo:** ¿Qué necesitas? (resumir, redactar, analizar, crear gráfico).
- **Contexto:** ¿Para quién? ¿Con qué propósito? ¿Qué tono?
- **Fuente:** ¿De dónde debe sacar la información? (este documento, los correos de esta semana, la hoja Ventas).
- **Formato esperado:** tabla, lista con viñetas, párrafo formal, presentación de 5 diapositivas.

Ejemplo: *«Resume los puntos clave de la reunión de ayer en Teams, identifica los responsables de cada tarea y preséntalo como una tabla con tres columnas: Tarea, Responsable, Plazo.»*

Qué información NO debes entregar a Copilot (ni a ninguna IA):

- **Datos personales de terceros** sin base legal (Ley N° 21.719 de protección de datos personales de Chile): RUT, domicilios, correos personales, antecedentes de salud, etc.
- **Información confidencial** que la política interna de tu organización prohíba procesar externamente.
- **Material de terceros con restricciones de licencia o copyright** que no tengas autorización de usar.

Regla de oro: La política interna de tu organización manda sobre lo que técnicamente sea posible hacer. Antes de entregar cualquier dato a Copilot, pregúntate: ¿tengo autorización legal y organizacional para tratarlo así?

Recuerda: aunque Copilot cumpla RGPD e ISO 42001, **la responsabilidad de uso correcto es tuya y de tu organización**, no de la herramienta.