MATERIAL DEL WEBINAR

Tu equipo ya está usando IA. ¿Sabes qué información está compartiendo?

8 de octubre de 2026 · 10:00, hora de la Ciudad de México · Webinar organizado por NetBIT

Kit de gobernanza de IA en 30 días

Lista de verificación (checklist) de implementación inmediata para pasar del uso de IA sin control a un uso con visibilidad, reglas y evidencia. Aplica a cualquier herramienta de IA y a cualquier plataforma; incluye un anexo para Microsoft 365 y Google Workspace.

Qué incluye	Para qué sirve
Parte 1 · Autodiagnóstico (12 preguntas)	Saber en 10 minutos dónde está tu organización.
Parte 2 · Lista de verificación por fases (30 días)	Qué hacer cada semana, cómo comprobar que quedó hecho y quién suele resolverlo.
Parte 3 · De la demo a tu entorno	Conectar lo que viste en el webinar con tus propios controles.
Anexos · Microsoft 365 y Google Workspace	Dónde vive cada capacidad en tu suite, qué suele requerir y los errores más comunes.
Complemento · Plantilla de política de uso de IA	Documento editable para adaptar y publicar en la semana 2.
Glosario, aviso legal y condiciones de uso	Las siglas del kit explicadas y las reglas para usar este material.

Panel del webinar

- **David Farías**, CEO, F2M
- **Adrián Martínez**, Arquitecto de soluciones, F2M
- **Quauhtli Martínez**, Director de TI y estrategia digital, ENI Networks
- **Francisco Bravo**, Director comercial, NetBIT

Preparado por F2M®, integración de tecnología para el negocio.

© 2026 F2M, S.A. de C.V. · Material del webinar organizado por NetBIT

Si solo haces esto en 30 días

Es la meta del kit en una página. Si cierras estos puntos, ya puedes contestar las tres preguntas que importan: qué se usa, con qué reglas y quién se entera.

1. Nombra a un responsable, envía el comunicado inicial y publica el aviso de privacidad para colaboradores (2.1, 2.2 y 2.6).
2. Activa el segundo factor de autenticación (MFA) y revisa qué apps de terceros están conectadas a tus cuentas corporativas (5.1 y 1.3).
3. Haz el inventario de herramientas de IA en uso y de agentes, automatizaciones, conectores, asistentes de notas en reuniones y llaves de API (1.1, 1.2 y 1.4).
4. Revisa los términos de cada herramienta y firma el anexo de tratamiento de datos con el proveedor oficial (9.1 a 9.3).
5. Aprueba y publica la política con sus niveles de clasificación, la lista de herramientas y la fecha de próxima revisión; obtén la aceptación de cada colaborador (2.3, 2.4, 3.1, 4.3 y 12.2).
6. Revisa lo que está compartido de más y después habilita una herramienta oficial con cuenta corporativa (4.1 y 4.2).
7. Capacita al equipo, publica la guía de una página y abre el canal para reportar incidentes (10.1, 10.2 y 11.1).
8. Prueba una alerta y comprueba que los registros de uso funcionan (7.2 y 8.1).

© 2026 F2M, S.A. de C.V. · Material del webinar organizado por NetBIT

Cómo usar este kit

Si tu equipo ya usa IA, la pregunta no es si se usa, sino si alguien sabe con qué datos, en qué herramientas y con qué reglas. Este kit te lleva de esa pregunta a un primer nivel de control en 30 días.

1. Contesta el autodiagnóstico (Parte 1). Te dice por dónde empezar.
2. Nombra a un responsable y arma un equipo con Dirección, TI y seguridad, Legal, Procesos y procedimientos, y Recursos humanos, más un representante de las áreas de negocio.
3. Sigue la lista de verificación por semanas (Parte 2). Empieza por los controles de nivel Básico; los de nivel Intermedio y Avanzado pueden esperar a una segunda vuelta.
4. Usa la plantilla de política en la semana 2. Adáptala, apruébala y publícala.
5. Revisa el anexo de tu suite para identificar qué capacidades quizá ya tienes en tus licencias actuales.

Quién participa. Un solo responsable coordina; estas áreas encabezan los controles:

Área	Papel	Controles que encabeza
Dirección	Patrocina, nombra al responsable, aprueba la política y el presupuesto	2.1, 2.3, 12.1
TI y seguridad de la información	Inventario técnico, identidad, prevención de fuga, alertas y bitácoras	1.1, 1.3, 1.4, 4, 5, 6, 7 y 8
Legal y cumplimiento	Proveedores, aviso de privacidad, retención y notificaciones	2.6, 8.2, 9, 11.2
Procesos y procedimientos	Documenta los flujos: solicitudes, incidentes y revisión periódica	2.5, 11.2, 12.2, 12.3
Recursos humanos	Aceptación de la política, capacitación, bajas y medidas disciplinarias	2.4, 5.3, 10
Áreas de negocio	Dueñas de la información: encuesta, clasificación y casos de uso	1.2, 3.1, 3.2

¿Necesitas comprar algo para llegar a la meta?

La meta del día 30 (todos los controles Básicos, la alerta probada y los registros comprobados) sí se alcanza con Microsoft 365 E3 o Business Premium: MFA y acceso condicional, Cloud Discovery, alertas de prevención de pérdida de datos (DLP) en Exchange, SharePoint y OneDrive, y Audit (Standard).

Lo que por lo general requiere compra es bloquear lo que se pega o se sube a una IA (controles 6.2 y 6.3): en Microsoft, E5 o un complemento (E5 Compliance o Purview Suite); en Google, Chrome Enterprise Premium o una edición Enterprise de Workspace.

Cloud Discovery solo da visibilidad (no bloquea) y necesita un cortafuegos o un proxy que exporte sus bitácoras. En Google Workspace, las ediciones Business no incluyen DLP, acceso adaptado al contexto ni el Centro de seguridad; revisa el Anexo B.

Antes de empezar

Lo que este kit da por sentado

Este kit se enfoca en el uso de la IA y parte de que tu organización ya tiene una base de seguridad operando, por ejemplo:

- **Seguridad de red:** cortafuegos, filtrado web o de DNS y bitácoras que se puedan consultar.
- **Protección de equipos:** antivirus o EDR, actualizaciones al día e inventario de equipos.
- **Cuentas corporativas nominales** (una por persona), con altas y bajas controladas.
- **Respaldos** y un **plan básico de respuesta a incidentes de seguridad**.
- Una persona, área o proveedor a cargo de la **ciberseguridad**.

Si alguno de estos puntos no está resuelto, atiéndelo primero o en paralelo. Varios controles del kit se apoyan en ellos: el inventario (1.1) usa las bitácoras del cortafuegos y el procedimiento de incidentes (11.2) se integra al plan que ya existe. ***El kit no los sustituye ni los evalúa***.

Por dónde se escapa la información

- **Cuentas personales y versiones de consumo.** Alguien pega o sube un documento a una IA gratuita o a un plan individual pagado (por ejemplo, Plus, Pro o Max), que también es de consumo. Controles 1.1, 6.1 y 9.2.
- **Extensiones y navegadores con IA.** Pueden leer la página o el documento abierto. Controles 1.1 y 1.3.
- **Apps conectadas a tus cuentas.** Una autorización OAuth da acceso a correo, archivos o calendario. Controles 1.3 y 5.2.
- **Asistentes de notas en reuniones.** Graban, transcriben y guardan lo que se dice. Control 1.4.
- **Agentes, automatizaciones y llaves de API.** Mueven datos entre sistemas sin que nadie los vea. Control 1.4.
- **IA integrada en la suite.** Ve todo lo que el usuario puede ver, incluido lo que está compartido de más. Control 4.1.
- **Celulares.** Copiar y pegar de una app corporativa a una app personal de IA. Control 5.4.

Los datos de mayor riesgo

- Estados financieros no publicados, estrategia, contratos y propuestas comerciales.
- Datos personales de clientes y colaboradores, incluidos identificadores mexicanos: CURP, RFC, número de seguridad social (NSS) y cuenta CLABE.
- Datos personales sensibles, información de salud y nómina individual.
- Código fuente, contraseñas, llaves de API y otras credenciales.
- Secretos industriales. La ley solo los protege si la empresa adoptó medios suficientes para preservar su confidencialidad (art. 163 de la LFPPI); compartirlos sin control con una IA de consumo debilita ese argumento.

Si tu empresa es financiera, aseguradora o de salud, la regulación de tu sector puede imponer reglas adicionales sobre la información de clientes y la contratación de servicios de tecnología; revísalas con tu área de cumplimiento.

Las 12 capacidades de la gobernanza de IA

Todo el kit se organiza alrededor de 12 capacidades. Son agnósticas: se pueden resolver con distintas herramientas, y muchas no requieren tecnología, sino decisiones.

#	Capacidad	Pregunta que responde
1	Visibilidad (uso de IA no autorizada)	¿Qué herramientas de IA se usan hoy y quién las usa?
2	Política	¿Cuáles son las reglas y quién las aprobó?
3	Clasificación de datos	¿Qué información es confidencial y está marcada como tal?
4	Herramienta oficial	¿Qué opción segura y aprobada le damos al equipo?
5	Identidad y acceso	¿Quién entra, con qué cuenta y desde dónde?
6	Prevención de fuga	¿Qué impide que un dato confidencial llegue a una IA no autorizada?
7	Monitoreo y alertas	¿Quién se entera, y en cuánto tiempo, cuando algo pasa?
8	Evidencia (bitácoras)	¿Podemos demostrar qué pasó, cuándo y quién lo hizo?
9	Proveedores	¿Qué hace cada proveedor con nuestros datos?
10	Capacitación	¿El equipo sabe qué sí y qué no compartir?
11	Respuesta a incidentes	¿Qué hacemos cuando alguien comparte lo que no debía?
12	Revisión periódica	¿Cómo se mantiene vigente todo lo anterior?

> **Una idea para todo el kit**
>
> La meta de los primeros 30 días no es bloquear la IA, sino dar una opción segura, poner reglas claras y enterarte cuando algo pasa. Bloquear todo suele empujar a la gente a usar su celular o su cuenta personal, y entonces pierdes la visibilidad.

Parte 1 · Autodiagnóstico

Marca Sí solo si puedes demostrarlo hoy (un documento, una pantalla, un reporte). «Creo que sí» o «está en proceso» cuenta como No.

#	Capacidad	Afirmación	Sí	No
1	Visibilidad	Tenemos una lista de las herramientas de IA que se usaron en la organización en los últimos 30 días.	☐	☐
2	Política	Existe una política de uso de IA aprobada, publicada y aceptada por los colaboradores.	☐	☐
3	Clasificación	Los documentos confidenciales (finanzas, RH, legal) están marcados o etiquetados de forma consistente.	☐	☐
4	Herramienta oficial	El equipo tiene al menos una herramienta de IA empresarial aprobada, con cuenta corporativa.	☐	☐
5	Identidad	El acceso a la herramienta oficial es con la cuenta corporativa (SSO) y con segundo factor (MFA).	☐	☐
6	Prevención de fuga	Existe algún control técnico que advierte o bloquea cuando se intenta subir información confidencial a una IA no autorizada.	☐	☐
7	Monitoreo y alertas	Si alguien sube información confidencial a una IA, una persona con nombre se entera en menos de un día.	☐	☐
8	Evidencia	Podemos responder en menos de una hora: «¿quién usó IA con este archivo y cuándo?».	☐	☐
9	Proveedores	Revisamos los términos de cada herramienta aprobada: si entrena con nuestros datos, cuánto los retiene y dónde.	☐	☐
10	Capacitación	Más del 80 % del equipo recibió capacitación sobre qué sí y qué no compartir con la IA.	☐	☐
11	Respuesta a incidentes	Hay un canal y un procedimiento definido para reportar y atender un incidente de IA.	☐	☐
12	Revisión periódica	La política y la lista de herramientas se revisan al menos cada trimestre.	☐	☐

La pregunta 7 dice «menos de un día» porque mide madurez: que alguien se entere el mismo día. La meta técnica de la prueba de alerta (control 7.2) es más exigente: 15 minutos.

© 2026 F2M, S.A. de C.V. · Material del webinar organizado por NetBIT

Tu resultado

Respuestas «Sí»	Semáforo	Qué significa	Por dónde empezar
0 a 4	**ROJO**	La IA se usa sin visibilidad ni reglas. Es el escenario A de la demo: si un dato sale, nadie se entera.	Semana 1 completa: responsable, inventario, MFA y comunicado inicial.
5 a 8	**AMARILLO**	Hay piezas sueltas (por ejemplo, una herramienta oficial o una política) pero no se conectan entre sí.	Cierra los «No» de nivel Básico de la Parte 2, empezando por clasificación y alertas.
9 a 12	**VERDE**	Tienes una base. El reto es sostenerla y medirla.	Controles Intermedios y Avanzados, y la revisión periódica.

El semáforo es una referencia interna para ordenar el trabajo, no una evaluación de cumplimiento.

Las tres preguntas que más pesan

Si contestaste No a la 1 (visibilidad), la 7 (alertas) o la 8 (evidencia), trátalas como prioridad aunque tu semáforo salga amarillo o verde: sin ellas no sabrías si el resto de los controles funciona.

Parte 2 · Lista de verificación en 30 días

Cada control tiene una pregunta de verificación de sí o no: si no la puedes contestar con evidencia, el control no está terminado. La columna «Dónde suele resolverse» es genérica a propósito; en los anexos está el equivalente para Microsoft 365 y Google Workspace.

Fase	Objetivo	Al terminar tendrás
Semana 1 · Descubrir	Saber qué está pasando hoy y cerrar las puertas más obvias.	Responsable nombrado, aviso de privacidad para colaboradores, inventario de herramientas, apps conectadas y agentes, MFA activo y revisión de proveedores.
Semana 2 · Decidir	Poner reglas y dar una opción segura.	Política publicada, niveles de clasificación, permisos revisados y herramienta oficial habilitada.
Semanas 3 y 4 · Proteger	Que controles técnicos respalden las reglas.	Acceso con cuenta corporativa, controles contra fuga, celulares protegidos y equipo capacitado.
Semana 4 y continuo · Vigilar	Enterarte a tiempo y poder demostrarlo.	Alertas probadas, bitácoras con retención, procedimiento de incidentes y revisión mensual.

Semana 1 · Descubrir

2. Política (arranque)

	Control	Cómo verificarlo	Nivel	Dónde suele resolverse
☐	2.1 Nombrar un responsable de gobernanza de IA y armar un equipo con Dirección, TI y seguridad, Legal, Procesos y procedimientos, Recursos humanos y un representante de las áreas de negocio.	¿Hay un nombre y una fecha de primera reunión?	Básico	Dirección general; comité existente de seguridad o riesgos.
☐	2.2 Enviar un comunicado inicial: «estamos ordenando el uso de IA; mientras tanto, no compartas información confidencial».	¿Se envió y quedó registro?	Básico	Comunicación interna; correo o intranet.
☐	2.6 Poner a disposición de los colaboradores un aviso de privacidad que cubra el inventario por usuario, las alertas y las bitácoras, antes de activarlos (en México, arts. 14 a 16 de la LFPDPPP).	¿El aviso existe, menciona este tratamiento y se comunicó antes de activar el monitoreo?	Básico	Legal y recursos humanos; intranet o expediente laboral.

© 2026 F2M, S.A. de C.V. · Material del webinar organizado por NetBIT

1. Visibilidad (uso de IA no autorizada)

	Control	Cómo verificarlo	Nivel	Dónde suele resolverse
☐	1.1 Inventariar las herramientas de IA en uso, aprobadas o no, con número de usuarios y volumen. Incluye cuentas personales de consumo, planes individuales pagados (Plus, Pro, Max) y navegadores con IA.	¿Tienes una lista de los últimos 30 días con herramienta, usuarios y área? Si identifica personas, ¿ya está el aviso 2.6?	Básico	Registros de cortafuegos, proxy o DNS; consola del navegador corporativo; CASB o SSE.
☐	1.2 Levantar una encuesta breve por área: para qué usan IA y con qué tipo de datos.	¿Respondió al menos un representante de cada área?	Básico	Formulario interno; entrevistas con líderes de área.
☐	1.3 Identificar extensiones de navegador y aplicaciones de IA conectadas a cuentas corporativas (permisos OAuth).	¿Sabes qué apps de terceros tienen acceso a correo, archivos o calendario?	Básico	Consola de identidad o de la suite (apps de terceros); administración del navegador.
☐	1.4 Inventariar agentes, automatizaciones, conectores, asistentes de notas en reuniones y llaves de API que usan IA o tocan datos corporativos.	¿Cada uno tiene un dueño con nombre y sabes a qué datos accede?	Básico	Consola de la suite (apps y conectores); plataformas de automatización; consola de la nube; aplicaciones de reuniones.

5. Identidad y acceso (arranque)

	Control	Cómo verificarlo	Nivel	Dónde suele resolverse
☐	5.1 Acceso a la herramienta oficial y a la suite solo con cuenta corporativa (SSO) y segundo factor (MFA).	¿Se puede entrar con una cuenta personal o sin segundo factor? (debe ser No)	Básico	Proveedor de identidad (IdP).
☐	5.2 Restringir que los usuarios autoricen por su cuenta apps de IA de terceros sobre datos corporativos: activar el flujo de aprobación del administrador, avisando al equipo, en lugar de un bloqueo total sin aviso.	¿Una app nueva que pide acceso a datos corporativos queda en espera de aprobación de TI?	Intermedio	Proveedor de identidad; consola de la suite.

© 2026 F2M, S.A. de C.V. · Material del webinar organizado por NetBIT

9. Proveedores

	Control	Cómo verificarlo	Nivel	Dónde suele resolverse
☐	9.1 Revisar los términos de cada herramienta detectada: si entrena con tus datos, retención, ubicación y subprocesadores.	¿Cada herramienta del inventario tiene una ficha con esas cuatro respuestas?	Básico	Términos de servicio y centro de privacidad del proveedor; área legal.
☐	9.2 Distinguir versión gratuita o de consumo y versión empresarial de la misma herramienta. Los planes individuales pagados (Plus, Pro, Max) también son de consumo.	¿Está documentado qué versión es aceptable y cuál no?	Básico	Área legal y TI; contrato o licenciamiento.
☐	9.3 Firmar o confirmar el anexo de tratamiento de datos con el proveedor oficial antes de usarlo con datos de clientes o colaboradores. Precisar si actúa como encargado y si hay transferencias (en México, art. 2 fr. XII y XX y arts. 35 y 36 de la LFPDPPP).	¿Existe un anexo de tratamiento de datos vigente y revisado por legal?	Básico	Legal y compras; portal de confianza del proveedor.

Semana 2 · Decidir

2. Política

	Control	Cómo verificarlo	Nivel	Dónde suele resolverse
☐	2.3 Adaptar, aprobar y publicar la política de uso de IA (usa la plantilla incluida).	¿Está publicada en un lugar conocido y tiene fecha de aprobación?	Básico	Intranet o portal de políticas; dirección y legal.
☐	2.4 Obtener la aceptación formal de cada colaborador.	¿Qué porcentaje la aceptó? (meta: 100 % en 30 días)	Básico	Firma electrónica, formulario o términos de uso en el inicio de sesión.
☐	2.5 Definir cómo se solicita una herramienta o un caso de uso nuevo y quién lo aprueba.	¿Existe el formulario y un tiempo de respuesta comprometido?	Intermedio	Mesa de servicio de TI; comité de IA.

© 2026 F2M, S.A. de C.V. · Material del webinar organizado por NetBIT

3. Clasificación de datos

	Control	Cómo verificarlo	Nivel	Dónde suele resolverse
☐	3.1 Definir 3 o 4 niveles (por ejemplo: Público, Interno, Confidencial, Restringido) y qué puede ir a la IA en cada uno. Ubicar en ellos los identificadores mexicanos: CURP, RFC, NSS y CLABE.	¿Cualquier colaborador puede explicar qué nivel tiene un estado financiero no publicado o una lista de clientes con RFC?	Básico	Política de clasificación; seguridad de la información.
☐	3.2 Marcar los documentos sensibles empezando por finanzas, RH y legal con una etiqueta de sensibilidad (una leyenda escrita en el encabezado es fácil de quitar).	¿Las plantillas de esas áreas ya incluyen la etiqueta?	Intermedio	Plantillas de documentos; etiquetas de la suite de productividad.
☐	3.3 Aplicar etiquetas por defecto o automáticas según contenido (CURP, RFC, NSS, CLABE, cuentas, cifras). De fábrica, Microsoft Purview detecta la CURP y Google Workspace la CURP y el pasaporte (en ediciones Enterprise); RFC, NSS y CLABE requieren un detector personalizado.	¿Un documento nuevo con datos sensibles se etiqueta sin intervención? ¿Probaste cada identificador?	Avanzado	Herramienta de protección de información o DLP.

4. Herramienta oficial

	Control	Cómo verificarlo	Nivel	Dónde suele resolverse
☐	4.1 Antes de habilitar IA integrada en la suite, revisar permisos de carpetas y sitios compartidos de más.	¿Se revisaron los sitios con «cualquier persona con el enlace» o «toda la organización»?	Básico	Administración de la suite; informes de uso compartido.
☐	4.2 Habilitar al menos una herramienta de IA empresarial aprobada, con cuenta corporativa.	¿El equipo sabe cuál es y cómo entrar?	Básico	IA integrada en la suite; plataforma de IA empresarial; nube.
☐	4.3 Publicar la lista de herramientas aprobadas, condicionadas y no permitidas.	¿La lista está en la política o junto a ella?	Básico	Intranet; anexo de la política.

© 2026 F2M, S.A. de C.V. · Material del webinar organizado por NetBIT

Semanas 3 y 4 · Proteger

5. Identidad y acceso

	Control	Cómo verificarlo	Nivel	Dónde suele resolverse
☐	5.3 Revocar accesos en las bajas y restringir el acceso desde dispositivos no administrados.	¿Una baja pierde acceso a la IA el mismo día?	Avanzado	IdP con acceso condicional; administración de dispositivos (MDM).
☐	5.4 Proteger los datos corporativos en celulares y tabletas: bloqueo de pantalla, impedir copiar y pegar de apps corporativas a apps personales (incluidas las de IA) y poder borrar a distancia los datos corporativos.	En un celular de prueba, ¿puedes copiar texto de un correo corporativo a una app personal de IA? (debe ser No)	Intermedio	Administración de aplicaciones o dispositivos móviles (MAM o MDM).

6. Prevención de fuga

	Control	Cómo verificarlo	Nivel	Dónde suele resolverse
☐	6.1 Advertir o bloquear el acceso a herramientas de IA no aprobadas, empezando en modo «advertir».	¿Al entrar a una IA no aprobada aparece un aviso que remite a la herramienta oficial?	Intermedio	Filtro web, SSE o CASB; navegador corporativo.
☐	6.2 Reglas que impidan pegar o subir información etiquetada como Confidencial a sitios de IA.	¿Una prueba con un documento etiquetado se bloquea y queda registrada?	Avanzado	DLP de endpoint o de navegador.
☐	6.3 Excluir el contenido Restringido de lo que la IA integrada puede leer o resumir.	¿La IA de la suite se niega a resumir un documento Restringido?	Avanzado	DLP de la suite; etiquetas con cifrado.

10. Capacitación

	Control	Cómo verificarlo	Nivel	Dónde suele resolverse
☐	10.1 Sesión de 30 a 45 minutos: la política, qué no compartir y ejemplos concretos (como el ejercicio de los estados financieros de la demo).	¿Qué porcentaje asistió o vio la grabación? (meta: más del 80 %)	Básico	RH o capacitación; plataforma de aprendizaje.
☐	10.2 Guía de una página para el escritorio: qué sí, qué no, a quién preguntar.	¿Está publicada junto a la herramienta oficial?	Básico	Intranet; anexo de la política.
☐	10.3 Usar los avisos de los controles («este contenido es confidencial») como capacitación en el momento, y capacitar aparte a quien construye agentes o automatizaciones.	¿Los avisos explican qué hacer en lugar de solo bloquear?	Intermedio	DLP o navegador corporativo; equipos de desarrollo.

© 2026 F2M, S.A. de C.V. · Material del webinar organizado por NetBIT

Semana 4 y continuo · Vigilar

7. Monitoreo y alertas

	Control	Cómo verificarlo	Nivel	Dónde suele resolverse
☐	7.1 Definir qué eventos generan alerta (por ejemplo: bloqueo de un dato confidencial, una IA nueva con muchos usuarios) y a quién le llegan. Confirmar que el aviso 2.6 cubre este registro.	¿Cada alerta tiene un destinatario con nombre, no un buzón genérico?	Intermedio	Consola de seguridad o de la suite; SIEM.
☐	7.2 Probar la alerta: provocar un evento de prueba y medir cuánto tarda en llegar.	¿Llegó en menos de 15 minutos a la persona correcta?	Intermedio	Las mismas consolas; ejercicio controlado.
☐	7.3 Revisar las alertas al menos cada semana y ajustar las que generan ruido.	¿Hay una revisión agendada y un registro de ajustes?	Intermedio	Responsable de seguridad; SIEM o SOC.

8. Evidencia (bitácoras)

	Control	Cómo verificarlo	Nivel	Dónde suele resolverse
☐	8.1 Activar y comprobar los registros de uso de IA: quién, cuándo, qué herramienta y qué resultado. Restringir quién puede consultarlos.	¿Puedes ver hoy un registro de ayer? ¿Solo lo ven las personas autorizadas?	Intermedio	Auditoría de la suite; registros de la plataforma de IA o del navegador.
☐	8.2 Definir el tiempo de retención con legal (por ejemplo, 180 días o un año).	¿La retención configurada coincide con la acordada?	Intermedio	Configuración de auditoría; SIEM o almacenamiento de registros.
☐	8.3 Prueba de auditoría: responder «¿quién usó IA con este archivo y cuándo?».	¿Lo respondiste en menos de una hora?	Avanzado	Herramientas de investigación o eDiscovery.

© 2026 F2M, S.A. de C.V. · Material del webinar organizado por NetBIT

11. Respuesta a incidentes

	Control	Cómo verificarlo	Nivel	Dónde suele resolverse
☐	11.1 Definir qué es un incidente de IA y abrir un canal para reportarlo sin miedo a represalias.	¿El equipo sabe a dónde escribir si compartió algo por error?	Básico	Política; mesa de servicio; seguridad.
☐	11.2 Escribir un procedimiento corto: reportar; contener (conservar evidencia; si se compartieron credenciales, revocarlas y rotarlas de inmediato; después borrar la conversación y solicitar su eliminación al proveedor, porque borrarla en la herramienta no elimina el dato en el proveedor); evaluar qué datos salieron; notificar (a los titulares de forma inmediata cuando la vulneración afecte de forma significativa sus derechos patrimoniales o morales, art. 19 de la LFPDPPP; la evaluación no retrasa ese aviso), y aprender.	¿Está escrito, con responsables y tiempos?	Intermedio	Plan de respuesta a incidentes existente; legal.
☐	11.3 Hacer un simulacro con un caso como el de la demo (estados financieros subidos a una IA).	¿Se hizo y se documentaron las mejoras?	Avanzado	Equipo de seguridad y legal.

12. Revisión periódica

	Control	Cómo verificarlo	Nivel	Dónde suele resolverse
☐	12.1 Revisar cada mes cinco indicadores: herramientas detectadas, uso de la oficial, bloqueos, alertas e incidentes.	¿Existe el tablero y se presentó al menos una vez?	Intermedio	Reportes de las consolas; hoja de cálculo o tablero.
☐	12.2 Revisar cada trimestre la política y la lista de herramientas.	¿La política tiene fecha de próxima revisión?	Básico	Comité de IA.
☐	12.3 Evaluar cada capacidad nueva (agentes, IA integrada, conectores) antes de habilitarla.	¿Hay una evaluación escrita antes de cada activación?	Avanzado	Comité de IA; arquitectura y seguridad.

Tu meta al día 30

Todos los controles de nivel Básico marcados, más 7.2 (alerta probada) y 8.1 (registros comprobados). Con eso ya puedes contestar las tres preguntas que importan: qué se usa, con qué reglas y quién se entera.

Parte 3 · De la demo a tu entorno

> **Nota sobre la demostración**
>
> La demostración se preparó en un ambiente de prueba, con datos ficticios y una configuración hecha para el ejercicio. No es un caso de un cliente ni una configuración lista para producción; los tiempos y resultados pueden variar en tu entorno.
>
> La alerta, la bitácora y las cuentas con vigencia que viste son componentes construidos a la medida sobre un ambiente de F2M Guardrails para la demostración.

Dos capas distintas

1. **Lo que la gente usa.** Cuando alguien pega o sube información a un chat de IA público o de consumo, el control vive en tu suite, tu navegador, tu red y tu proveedor de identidad (capacidades 1, 5 y 6). Con una plataforma Empresarial de IA con Guardrails no actúa en esta capa.
2. **Lo que tu empresa construye.** Cuando tu empresa crea aplicaciones, agentes o automatizaciones sobre un modelo de IA, controles como los mostrados en el ambiente de F2M Guardrails revisan lo que entra y sale de esas aplicaciones. Sus filtros de información sensible evalúan solo texto y no incluyen de fábrica identificadores mexicanos como CURP, RFC, NSS o CLABE; hay que agregarlos como patrones a la medida.

La demo muestra la segunda capa. En el webinar viste el mismo documento pasar por dos escenarios; cada momento corresponde a una capacidad del kit. Usa esta tabla para preguntarte si en tu organización ocurriría lo mismo.

Lo que viste en la demo	Capacidad	Pregúntate
Escenario A: el analista sube los estados financieros, el modelo responde y nadie se entera.	1 Visibilidad / 7 Monitoreo	Si hoy alguien sube un documento confidencial a una IA, ¿quién se enteraría y cuándo?
La palabra CONFIDENCIAL en el encabezado del documento es lo que detona el bloqueo.	3 Clasificación	¿Tus documentos sensibles llevan una etiqueta de sensibilidad que un control pueda reconocer? Una palabra escrita es fácil de quitar.
El control del ambiente de F2M Guardrails bloquea en la entrada: el documento nunca llega al modelo.	6 Prevención de fuga	¿Tus controles actúan antes de que el dato salga, o solo te enteras después?
El comunicado público sí pasa, con el mismo control encendido.	2 Política / 3 Clasificación	¿Tu control distingue lo público de lo confidencial, o bloquea todo y empuja a la gente a buscar otra vía?
El administrador recibe la alerta en segundos, con usuario, archivo y política (componente a la medida).	7 Monitoreo y alertas	¿Tu alerta llega a una persona con nombre, con el contexto suficiente para actuar?
La bitácora guarda nombre del archivo, resultado y huella SHA-256, sin guardar el contenido (componente a la medida).	8 Evidencia	¿Puedes demostrar qué pasó sin crear una copia más del dato sensible?

Lo que viste en la demo	Capacidad	Pregúntate
Cada persona entra con su propia cuenta, con fecha de vigencia (componente a la medida).	5 Identidad	¿Sabes quién hizo cada acción, o hay cuentas compartidas?
Todo ocurre dentro de una plataforma empresarial aprobada. Según la documentación pública de algunos proveedores de plataformas empresariales de IA, el servicio no usa tus entradas ni tus resultados para entrenar modelos.	4 Herramienta oficial / 9 Proveedores	¿Tu equipo tiene una opción así, o usa versiones gratuitas de consumo?

Lo importante no es la herramienta de la demo

En la demo se usó el ambiente de F2M Guardrails, pero la lógica es la misma en cualquier plataforma: clasificar, aplicar la política antes de que el dato salga, avisar a una persona y dejar evidencia. Los anexos muestran dónde vive cada pieza en Microsoft 365 y en Google Workspace.

Anexo A · Microsoft 365

Dónde vive cada una de las 12 capacidades en Microsoft 365 (y Microsoft Entra, Defender y Purview).

Capacidad	Dónde se resuelve	Qué suele requerir	Errores comunes
1 Visibilidad	Microsoft Defender for Cloud Apps (Cloud Discovery y catálogo de apps, categoría de IA generativa). Microsoft Purview DSPM (experiencia unificada) para la actividad de IA.	Cloud Discovery básico con Entra ID P1 (incluido en E3 y Business Premium). Defender for Cloud Apps completo en E5, E5 Security o como licencia independiente. Necesita bitácoras de cortafuegos o proxy, o Defender for Endpoint. Solo da visibilidad.	Mirar solo Copilot e ignorar las IA de terceros. No conectar la fuente de registros, y el informe sale vacío.
2 Política	Fuera de la herramienta: SharePoint o la intranet para publicar. Aceptación con Términos de uso de Microsoft Entra.	Términos de uso con acceso condicional requiere Entra ID P1 (incluido en Business Premium y E3).	Publicar la política sin aceptación formal ni fecha de revisión.
3 Clasificación	Microsoft Purview Information Protection: etiquetas de confidencialidad manuales, por defecto o automáticas.	Etiquetado manual en varios planes (Business Premium, E3). Etiquetado automático y funciones avanzadas, por lo general en E5 o complementos. De fábrica detecta la CURP; RFC, NSS y CLABE requieren un tipo de información confidencial personalizado.	Crear demasiadas etiquetas. Etiquetas solo visuales, sin cifrado ni política asociada.
4 Herramienta oficial	Microsoft 365 Copilot Chat con cuenta de Entra (protección de datos empresarial). Microsoft 365 Copilot. Microsoft Foundry (antes Azure AI Foundry) para desarrollos propios.	Copilot Chat se incluye con cuentas de Entra; Microsoft 365 Copilot es una licencia por usuario.	Habilitar Copilot sin revisar permisos de SharePoint y OneDrive: Copilot ve todo lo que el usuario puede ver.
5 Identidad	Microsoft Entra ID: SSO, MFA, acceso condicional, flujo de aprobación del administrador para el consentimiento de aplicaciones. Intune para celulares (MAM o MDM).	Acceso condicional requiere Entra ID P1. Funciones basadas en riesgo, P2. Intune incluido en E3 y Business Premium.	Permitir que cualquier usuario autorice apps OAuth de IA. Excepciones de MFA que se vuelven permanentes.
6 Prevención de fuga	Purview DLP en endpoint (pegar o subir a sitios de IA). Protección de datos en Edge for Business. Apps no autorizadas en Defender for Cloud Apps. DLP para Copilot (contenido etiquetado).	Por lo general E5, E5 Compliance o Purview Suite; dispositivos incorporados a Purview. Microsoft anunció que desde mediados de octubre de 2026 retira el pago por uso del DLP de Edge for Business para apps no administradas (aviso MC1470881); confirma cómo queda en tu contrato.	Activar en modo bloqueo sin probar antes en modo auditoría. Olvidar otros navegadores y equipos no administrados.
7 Monitoreo y alertas	Alertas de DLP en Purview. Microsoft Defender XDR. Insider Risk Management (uso riesgoso de IA). Informes de Microsoft Purview DSPM (experiencia unificada).	Alertas de DLP de Exchange, SharePoint y OneDrive desde E3 y Business Premium. Insider Risk Management y DSPM, por lo general E5 o complementos. La versión clásica de DSPM for AI se retira a fines de 2026 (aviso MC1481315).	Alertas que llegan a un buzón que nadie revisa. No ajustar el ruido las primeras semanas.
8 Evidencia	Microsoft Purview Audit (incluye interacciones con Copilot y otras IA). eDiscovery.	Audit (Standard) incluido, con retención de 180 días. Retención mayor con Audit (Premium) o complementos.	Suponer que la auditoría está activa sin comprobarlo. Retención menor a la que pide legal.
9 Proveedores	Anexo de protección de datos de productos y servicios de Microsoft (Microsoft Products and Services Data Protection Addendum) y Service Trust Portal. Para terceros: puntuación de riesgo en el catálogo de Defender for Cloud Apps.	Revisión legal; sin licencia adicional para la documentación.	Suponer que una versión de consumo tiene las mismas garantías que la empresarial.
10 Capacitación	Avisos de directiva de DLP como capacitación en el momento. Contenidos de Microsoft Learn y Viva Learning.	Avisos incluidos con DLP; contenidos de aprendizaje sin costo o con Viva.	Capacitar solo en «cómo usar Copilot» y no en «qué no compartir».
11 Respuesta a incidentes	Incidentes en Defender XDR. Investigación con Purview Audit y eDiscovery. Revocar sesiones en Entra ID.	Mismo licenciamiento que monitoreo y evidencia.	Nadie sabe cómo revocar una sesión o investigar fuera de horario.
12 Revisión periódica	Recomendaciones e informes de Microsoft Purview DSPM (experiencia unificada). Compliance Manager. Microsoft Secure Score.	Según plan; Secure Score incluido.	Mirar los tableros solo durante la implementación.

Los nombres de producto y el licenciamiento cambian con frecuencia; esta tabla refleja la información pública disponible en octubre de 2026 y es orientativa. Verifica con tu proveedor o socio qué incluye tu contrato.

Anexo B · Google Workspace

Dónde vive cada una de las 12 capacidades en Google Workspace (y Chrome Enterprise). Importante: las ediciones Business no incluyen DLP, acceso adaptado al contexto ni el Centro de seguridad.

Capacidad	Dónde se resuelve	Qué suele requerir	Errores comunes
1 Visibilidad	Chrome Enterprise Core (inventario de extensiones e informes del navegador). Controles de API de la consola de administración (apps de terceros con acceso OAuth).	Chrome Enterprise Core sin costo, con navegadores inscritos. Más detalle de eventos con Chrome Enterprise Premium.	Navegadores no inscritos o perfiles personales. Mirar solo Gemini e ignorar las IA de terceros.
2 Política	Fuera de la herramienta: Google Sites o Drive para publicar. Aceptación con Formularios.	Sin licencia adicional.	Publicar la política sin aceptación formal ni fecha de revisión.
3 Clasificación	Etiquetas de Drive (clasificación), manuales, por defecto o aplicadas por reglas de DLP.	Disponibilidad según edición; etiquetado automático, por lo general en ediciones Enterprise. Detectores de fábrica para CURP y pasaporte mexicanos (ediciones Enterprise); RFC, NSS y CLABE requieren un detector personalizado.	Etiquetas que nadie aplica. No conectar las etiquetas con reglas de DLP.
4 Herramienta oficial	Gemini en Google Workspace y la app Gemini con cuenta corporativa (protección de datos empresarial). Vertex AI para desarrollos propios.	Incluido en las ediciones Business y Enterprise actuales; verifica funciones según edición.	Habilitar Gemini sin revisar el uso compartido de Drive: Gemini ve lo que el usuario puede ver.
5 Identidad	Cloud Identity y Workspace: SSO, verificación en dos pasos obligatoria, acceso adaptado al contexto, control de apps OAuth. Administración de dispositivos móviles.	Acceso adaptado al contexto, en ediciones Enterprise o con Chrome Enterprise Premium; no se incluye en ediciones Business.	Permitir que cualquier usuario autorice apps OAuth. No forzar la verificación en dos pasos.
6 Prevención de fuga	Filtrado y bloqueo de URL en Chrome Enterprise Core. Chrome Enterprise Premium: DLP al pegar, subir, descargar o imprimir (bloquear, advertir o auditar). DLP para Drive, Gmail y Chat. DLP para Gemini (datos de Drive).	Filtrado de URL sin costo. Chrome Enterprise Premium es un complemento por usuario. DLP de Workspace y de Gemini, en ediciones Enterprise y algunas Frontline y Education; no en ediciones Business.	Bloquear solo direcciones URL: la gente cambia de navegador o usa el celular. Activar el bloqueo sin un periodo de auditoría.
7 Monitoreo y alertas	Centro de alertas. Reglas de informes. Eventos de seguridad de Chrome. Exportación a SIEM o Google Security Operations.	Algunas reglas e integraciones, solo en ediciones Enterprise.	Alertas que llegan a un superadministrador que no las revisa.
8 Evidencia	Registros de auditoría (Gemini, Drive, Chrome). Herramienta de investigación. Google Vault donde aplique.	Herramienta de investigación y exportación a BigQuery, en ediciones Enterprise o Education. La retención varía por edición.	Suponer que los registros se guardan para siempre. No exportar lo que legal necesita conservar.
9 Proveedores	Cloud Data Processing Addendum (anexo de tratamiento de datos). Centro de privacidad de IA generativa de Google Workspace.	Revisión legal; sin licencia adicional.	Confundir la app Gemini personal con la de cuenta corporativa.
10 Capacitación	Avisos de «advertir» de Chrome Enterprise Premium y de DLP como capacitación en el momento. Contenidos del Google Workspace Learning Center.	Avisos con Chrome Enterprise Premium o DLP; contenidos sin costo.	Bloquear sin explicar qué hacer en su lugar.
11 Respuesta a incidentes	Herramienta de investigación (acciones sobre archivos y usuarios). Centro de alertas. Cerrar sesiones desde la consola.	Herramienta de investigación, en ediciones Enterprise o Education.	Sin procedimiento para quitar un archivo compartido o revocar el acceso de una app.
12 Revisión periódica	Panel de seguridad y Centro de seguridad. Informes de uso de Gemini.	Centro de seguridad, en ediciones Enterprise; no se incluye en ediciones Business.	Revisar los tableros solo durante la implementación.

Los nombres de producto y el licenciamiento cambian con frecuencia; esta tabla refleja la información pública disponible en octubre de 2026 y es orientativa. Verifica con tu proveedor o socio qué incluye tu contrato.

© 2026 F2M, S.A. de C.V. · Material del webinar organizado por NetBIT · Página 18

Siguiente paso

Conversación de 30 minutos sobre tu resultado

Con F2M, sin costo. Partimos de tu resultado del autodiagnóstico y de lo que tu empresa construye o va a construir con IA: agentes, automatizaciones e integraciones. Revisamos contigo:

- Tu resultado y las tres capacidades que más riesgo representan hoy.
- Cómo gobernar lo que tu empresa construye o va a construir con IA, y qué de esto probablemente ya cubre tu suite.
- Un orden recomendado para tus siguientes 30 días.

Solicítala en el siguiente enlace:

https://a.dix.mx/jh7s

Al solicitarla, F2M, S.A. de C.V. tratará tus datos de contacto para coordinar la conversación. Aviso de privacidad: https://www.f2m.com.mx/AvisoPrivacidad. Lo que compartas en la conversación se trata como confidencial.

Glosario de siglas y términos

Sigla o término	Significado
API	Interfaz de programación de aplicaciones. Una «llave de API» permite que un sistema use un servicio en nombre de la empresa.
CASB	Agente de seguridad de acceso a la nube: controla el uso de aplicaciones en la nube.
CLABE	Clave Bancaria Estandarizada.
Cortafuegos	Equipo o servicio que filtra el tráfico de red (en inglés, firewall).
CURP	Clave Única de Registro de Población.
DLP	Prevención de pérdida de datos: reglas que advierten o bloquean cuando un dato sensible sale por un canal no permitido.
DNS	Sistema de nombres de dominio; sus registros muestran a qué sitios se conectan los equipos.
DSPM	Gestión de la postura de seguridad de los datos.
eDiscovery	Búsqueda y conservación de información para investigaciones o asuntos legales.
IA	Inteligencia artificial.
IdP	Proveedor de identidad: el servicio con el que la empresa autentica a sus usuarios.
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
LFPPI	Ley Federal de Protección a la Propiedad Industrial.
MAM / MDM	Administración de aplicaciones móviles / administración de dispositivos móviles.
MFA	Autenticación multifactor: además de la contraseña, un segundo factor (aplicación, llave física o código).
NSS	Número de Seguridad Social.
OAuth	Estándar con el que una aplicación obtiene permiso para acceder a datos de una cuenta sin conocer su contraseña.
Proxy	Servidor intermediario por el que pasa la navegación de la red de la empresa.
RFC	Registro Federal de Contribuyentes.
SHA-256	Función que genera una huella única de un archivo, útil como evidencia sin guardar su contenido.
SIEM	Sistema de gestión de información y eventos de seguridad.
SOC	Centro de operaciones de seguridad.
SSE	Borde de servicio de seguridad: servicios de seguridad de red entregados desde la nube.
SSO	Inicio de sesión único con la cuenta corporativa.
XDR	Detección y respuesta extendidas.

Aviso legal y condiciones de uso

Aviso legal y condiciones de uso. © 2026 F2M, S.A. de C.V. Material preparado para el webinar del 8 de octubre de 2026 organizado por NetBIT y entregado sin costo. Puedes copiarlo, adaptarlo y usarlo dentro de tu organización; no puedes venderlo ni distribuirlo como producto o servicio propio. Es información general y orientativa: no constituye asesoría legal, laboral, de seguridad ni de licenciamiento, no es una auditoría y no certifica el cumplimiento de ninguna ley. Antes de adoptarlo, revísalo con tus áreas legal, de recursos humanos y de seguridad. Se entrega en el estado en que se encuentra, sin garantía de resultados, de vigencia ni de adecuación a tu organización. La información técnica y de licenciamiento refleja fuentes públicas a octubre de 2026 y puede cambiar. Los nombres de productos mencionados son marcas de sus respectivos titulares; se citan solo como referencia y no implican patrocinio ni aval.

© 2026 F2M, S.A. de C.V. · Material del webinar organizado por NetBIT