POSSUMUS

T: 0810 345 0562
E: info@possumus.tech
A: Agustín Álvarez 25, San Rafael, Mendoza, Argentina

We Love Tech

Ciberseguridad Inteligente: Cómo Microsoft Protege el Futuro del Trabajo

Oct 2025

Sumario

¿De qué vamos a hablar hoy?

Quiénes somos

Somos una compañía enfocada en crear valor,
que impulsa a las empresas a lograr su transformación
digital con estrategia, conocimiento e innovación.

AI First

- Digital Product Engineering
- Data & Analytics
- Cloud Services and DevOps
- AI/ML Engineering

Somos un equipo movido por:

- **Experiencia positiva de las personas**
- **En equipo siempre sucede**
- **Somos protagonistas**
- **Nos desafiamos**

Clientes: CHUBB, bind, Grupo Petersen G·P, HSBC

Speaker

Matias Aguilera

Tech Leader

Microsoft
Solutions Partner

- AZ-104 Azure Administrator Associate
- MS-102 Administrator Expert
- SC-100 CCybersecurity Architect Expert
- AZ-500 Azure Security Engineer
- SC-300 Seguridad: Identidad y Accesos.
- SC-200 Seguridad: Analista de operaciones.
- MS-203 Administrador de servicios Mensajería
- AI-102 Azure AI Engineer
- AZ-305 Azure Solutions Architect Expert
- AZ-700 Azure Network Engineer Associate

Somos Microsoft Solution Partners

Contamos con certificaciones en todas las verticales del ecosistema Microsoft Cloud.

Estamos en el 99.9% superior de las empresas socias de negocios de Microsoft globalmente.

Nuestra especialización en Adoption and Change Management en la categoría Modern Work, demuestra que no solo instalamos: acompañamos hasta que funcione.

Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Business Applications

Microsoft Solutions Partner
Digital & App Innovation
Azure

Specialist
Accelerate Developer Productivity with Microsoft Azure

Microsoft Solutions Partner
Modern Work

Specialist
Teamwork Deployment Adoption and Change Management

Microsoft Solutions Partner
Security

Specialist
Identity and Access Management
Threat Protection

Microsoft Solutions Partner
Microsoft Cloud

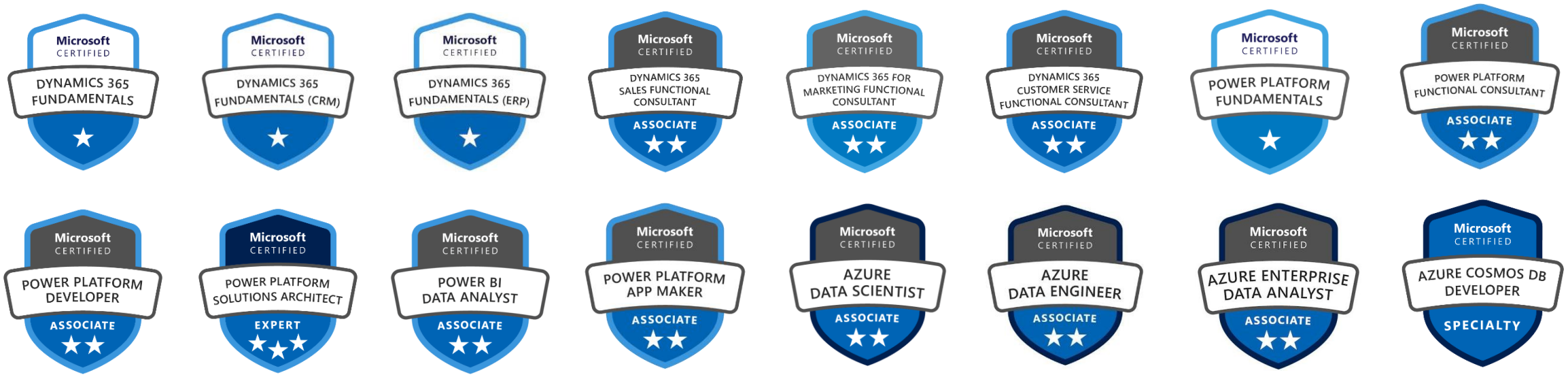
120 Certificaciones avalan a nuestro equipo técnico para implementar y evolucionar soluciones de productividad, seguridad colaboración en todo el ecosistema Microsoft 365.

Team Certifications

Microsoft Ecosystem

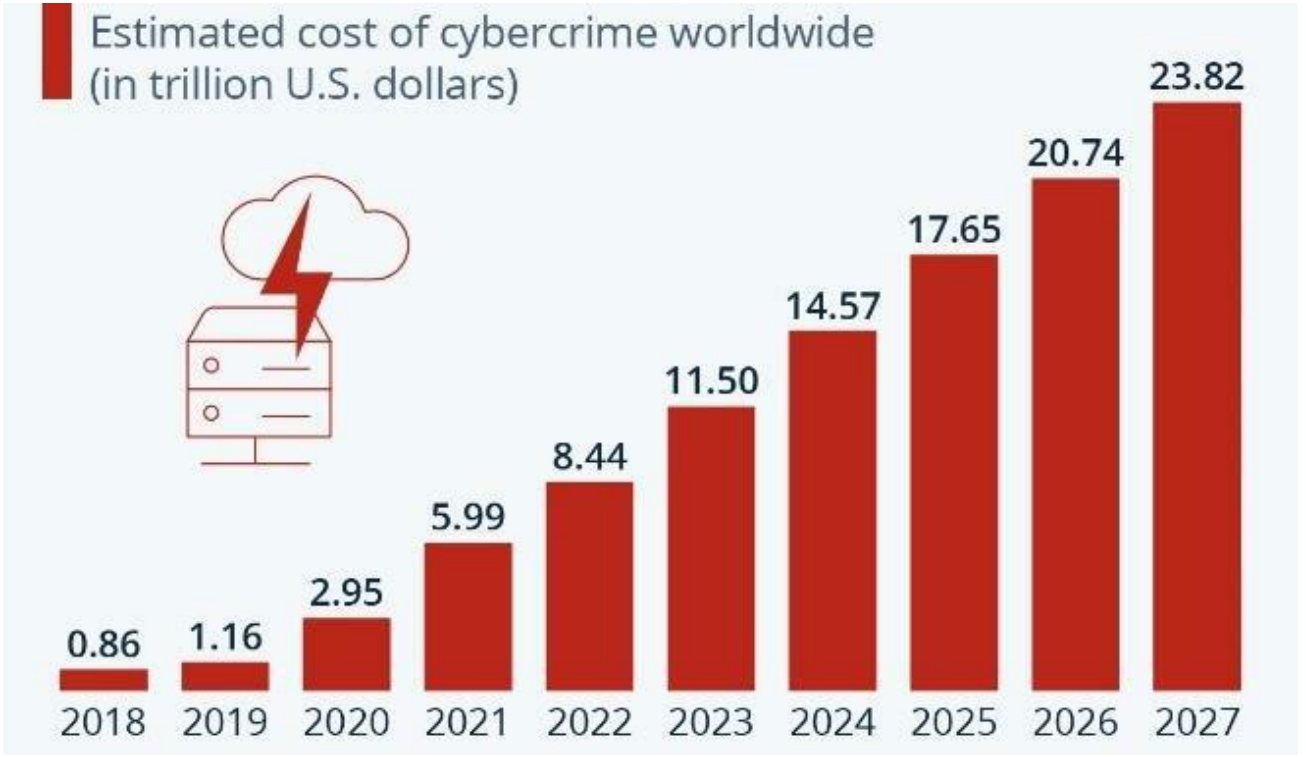
120

Certificaciones obtenidas por
nuestro equipo técnico, entre
las cuales se encuentran las siguientes:



Algunos Datos

- Se estima que el costo mundial anual del delito cibernético superará los U$S 20 trillones en 2026
- En 2025 se incrementaron en promedio un 44% los ataques semanales
- La AI permite que los ataques sean mas sofisticados y escalables.
- El uso indebido de las herramientas de IA por parte de colaboradores exponen a las organizaciones.



Casos Ciberataques

Caso Ciberataque: Extracción de fondos

Contexto: Una empresa del sector alimenticio ubicada en Mendoza sufrió un ataque informático que dejó su cuenta bancaria sin fondos. El incidente se originó desde el equipo de un empleado administrativo, que contaba con una baja protección de seguridad.

Infección inicial:

El empleado administrativo recibió un correo de phishing con un archivo malicioso. Al abrirlo, se instaló un troyano bancario en su PC.

Control remoto del equipo:

Los atacantes tomaron el control del dispositivo sin ser detectados, monitoreando sus acciones.

Pantalla falsa de actualización:

Al ingresar al sitio del banco, se mostró una pantalla simulando una "actualización de Windows", bloqueando el teclado y distrayendo al usuario.

Fraude bancario:

En segundo plano, los atacantes accedieron a la cuenta bancaria de la empresa, interceptaron el código de doble autenticación (2FA) y realizaron transferencias a cuentas externas.

Eliminación de rastros:

El malware se autoeliminó, y el empleado retomó el uso del equipo sin notar el fraude hasta que la empresa detectó la pérdida de fondos.

Perdidas

USD 380K perdida bancaria
USD 50K remediación

Caso Ciberataque: Cadena de artículos para el hogar perdió $15.000 USD en Azure

Contexto: Una empresa del rubro retail, con varias sucursales en Buenos Aires, sufrió un ataque informático que comprometió su cuenta de Azure.

Acceso inicial:

Los atacantes robaron credenciales y lograron interceptar el código MFA enviado por SMS.

Ingreso a Azure:

Los atacantes accedieron al portal como administradores y evadieron controles gracias a la debilidad del MFA por SMS.

Persistencia oculta:

Luego crearon usuarios y apps maliciosas para mantener el acceso sin ser detectados.

Consumo masivo:

Los atacantes desplegaron máquinas virtuales para minar criptomonedas, generando más de 15.000 USD en gastos.

Descubrimiento tardío:

La empresa detectó el fraude al recibir la factura; no había alertas ni límites configurados.

Caso Ciberataque: Ransomware Empresa de Logística

Contexto: Una empresa del rubro logístico en Buenos Aires, sufrió un ataque informático que comprometió su operación mediante un ransomware.

Infección inicial:

Un empleado abrió un archivo malicioso recibido por correo, activando el ransomware.

Propagación rápida:

El malware cifró los servidores, sistemas de gestión y terminales operativos en toda la red.

Sin respaldo ni segmentación:

La empresa no contaba con copias de seguridad offline ni redes separadas, lo que agravó el impacto.

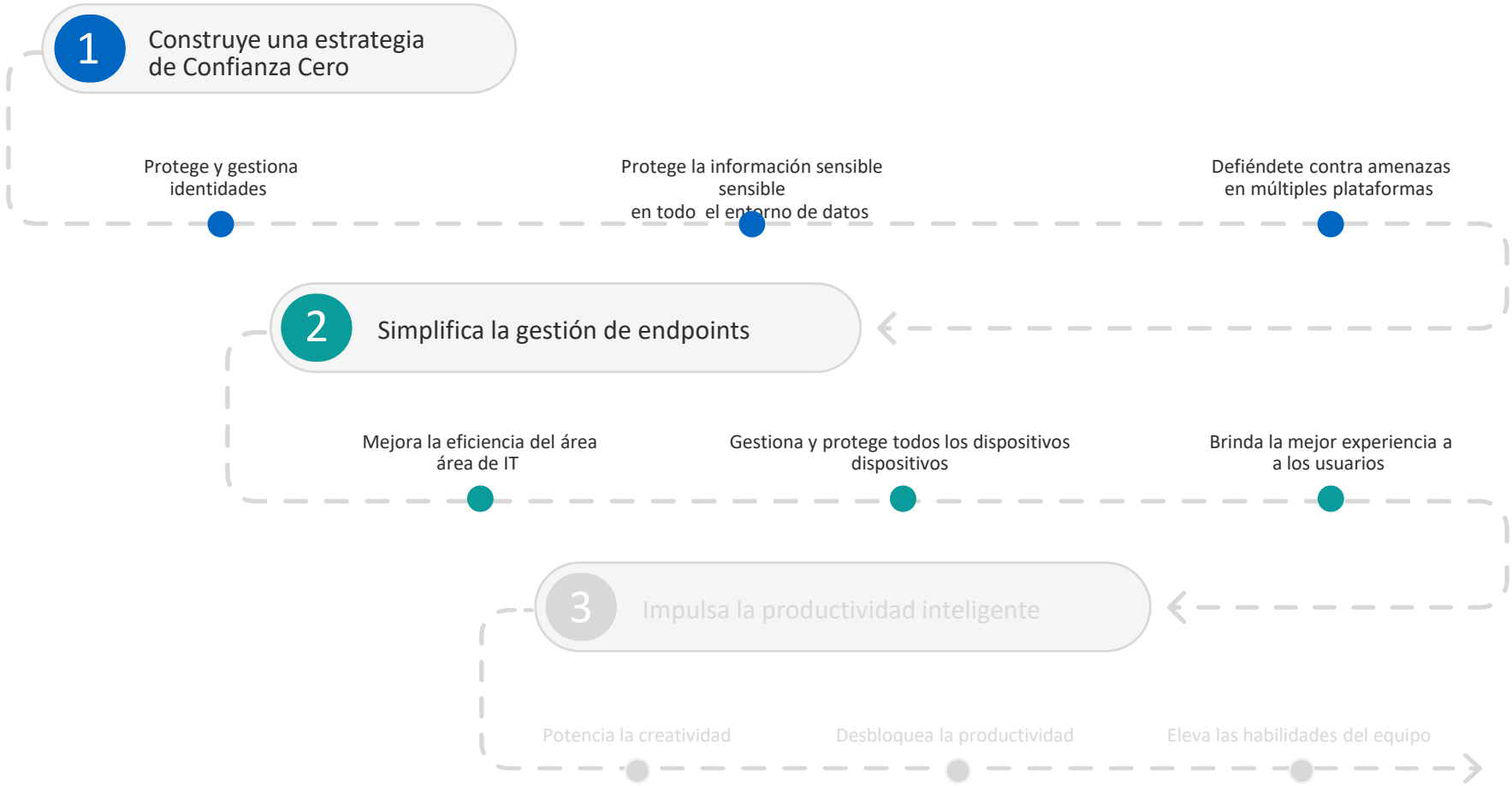
Parálisis total:

Durante una semana la empresa no pudo coordinar envíos, gestionar almacenes ni operar sus sistemas logísticos.

Impacto masivo:

Se ocasionaron pérdidas por interrupción de servicios, penalizaciones contractuales y daño a la confianza de clientes. USD 30.000 servicios IT para volver a estar operativos.

¿Qué camino debemos seguir?



POSSUMUS

Construye una estrategia de Confianza Cero

Mantén tus datos protegidos, defiéndete de amenazas cibernéticas avanzadas y reduce los tiempos objetivos de recuperación (RTO)

¿Qué desafíos encontramos?

Acceso no autorizado a los datos de trabajo

Empleados remotos acceden a información crítica desde múltiples múltiples ubicaciones. Sin las medidas medidas adecuadas, pueden sufrir sufrir intentos de intrusión mediante mediante el robo de credenciales. credenciales.

Ataques de Phishing

Un usuario ingresa sus datos en un un sitio falso tras recibir un correo correo fraudulento. La amenaza pasa pasa desapercibida y compromete la compromete la seguridad de la organización.

Datos de trabajo en dispositivos personales

Información confidencial se almacena accidentalmente en secciones no seguras de dispositivos personales, exponiendo datos sensibles fuera del entorno corporativo.

Pérdida accidental o intencional de datos

Documentos sensibles se comparten comparten sin cifrado, se almacenan almacenan en USB sin protección o se o se protegen de forma inconsistente, inconsistente, aumentando el riesgo riesgo de pérdida o filtración.

Ransomware

Archivos esenciales quedan cifrados por malware. Se exige un pago para recuperarlos, generando interrupciones operativas, pérdida de datos y altos costos.

Primer paso: protege tu identidad y tus datos desde el origen

1 Construye una estrategia de Confianza Cero

Protege y gestiona identidades

Protege la información sensible en todo el entorno de datos

Defiéndete contra amenazas en múltiples plataformas

- MFA previene el 99.9% de los ataques de identidad.
- Intune garantiza que solo apps autorizadas accedan a los datos.
- Defender analiza amenazas en tiempo real.
- Azure Information Protection extiende la seguridad a todo el ecosistema.

Microsoft Defender

Microsoft Intune

Azure Information Protection

Azure AD Premium P1

Control total sobre identidad, dispositivos, datos y aplicaciones

Security

Identidad y controles de acceso

Microsoft Entra ID Plan 1

- Autenticación multifactor para proteger contra la pérdida de contraseña.
- Restablecimiento de contraseña de autoservicio.
- Acceso condicional para proporcionar controles de acceso a los datos de trabajo.
- Descubrimiento de aplicaciones en la nube para descubrir Shadow IT.

Administración de dispositivos

Microsoft Intune

- Gestión centralizada de dispositivos dispositivos móviles y de escritorio, escritorio, Mac.
- Exigir que solo se acceda a los datos de datos de trabajo a través de aplicaciones autorizadas.
- Borrado remoto de datos de dispositivos perdidos y robados.
- Cifrado de BitLocker.
- Aplique los requisitos de Pin seguro seguro junto con los perfiles de Wi-Fi y Wi-Fi y VPN.

Seguridad del dispositivo

Microsoft Defender for Business

- Protección contra ransomware con EDR EDR impulsado por IA con interrupción interrupción automática de ataques.
- Protección AV de última generación.
- Protección en Android, iOS, Max, Windows y Linux.
- Gestión de amenazas y vulnerabilidades. vulnerabilidades.

Seguridad email y aplicaciones

Microsoft Defender for Office 365

- Defensa contra phishing y malware en el correo electrónico.
- Microsoft Teams, OneDrive y SharePoint.
- SafeLinks con filtrado de URL a la hora del clic.
- Archivos adjuntos seguros con escaneo de archivos adjuntos en tiempo real en sandbox.

Seguridad de los datos

Microsoft Purview

- Prevención de pérdida de datos para proteger datos confidenciales, como números de tarjetas de crédito o de la seguridad social.
- Clasifique y etiquete los datos confidenciales.
- Aplique protección como "No reenviar" o "Cifrar correo electrónico“
- Auditoría, búsqueda y retención legal.

Simplifica la gestión de endpoints

Centraliza la administración y aplica configuraciones de seguridad desde desde cualquier lugar y ahorra hasta 1.700 horas al año* automatizando automatizando tareas repetitivas de IT (300 endpoints)

¿Qué desafíos encontramos?

> El equipo de TI se enfrenta al desafío diario de aprovisionar manualmente todos los equipos de trabajo, incluyendo PC, notebooks y celulares. Cada dispositivo debe configurarse individualmente, instalarse el software necesario y asegurarse de que todas las políticas de seguridad estén en su lugar.
>
> Este proceso no solo es tedioso y consume mucho tiempo, sino que también es propenso a errores humanos. Los colaboradores esperan días o incluso semanas para recibir sus dispositivos, lo que retrasa la productividad y aumenta los costos operativos.

- **Aprovisionamiento manual:** TI configura cada dispositivo uno por uno.
- **Demora en entrega:** Nuevos ingresos esperan días para operar.
- **Errores humanos:** Falta de estandarización en seguridad y aplicaciones.
- **Costos altos:** Más horas dedicadas por equipo técnico.

Segundo paso: centraliza la gestión y protección de tus dispositivos

2 Simplifica la gestión de endpoints

Mejora la eficiencia del área de IT

Gestiona y protege todos los dispositivos

Brinda la mejor experiencia a los usuarios

- Intune permite gestión unificada multiplataforma
  Windows Autopilot automatiza la configuración de equipos
  Ayuda remota y control de privilegios de usuario.
- Seguridad integrada sin depender de soluciones de terceros
  IA para detectar, corregir y prevenir incidentes de forma proactiva.

Microsoft Defender

Microsoft Intune

Azure Information Protection

Azure AD Premium P1

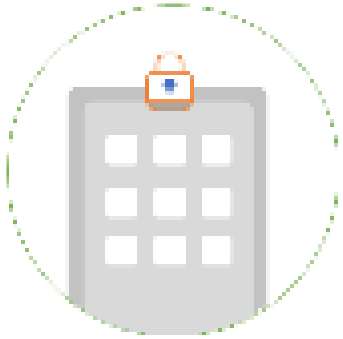
Simplifica la gestión de endpoints

Administra los datos laborales en móviles, con o sin provisión, vía Intune.

Mobile Device Management (MDM)

Administración de Dispositivos Móviles

Gestiona el acceso a dispositivos propiedad de propiedad de la empresa.



Registrar dispositivos para su gestión.

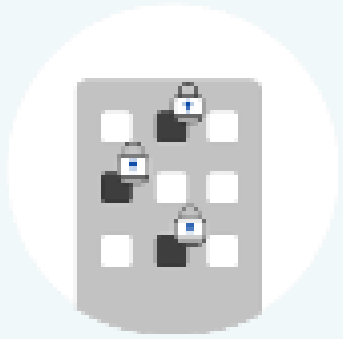
Configurar ajustes, certificados y perfiles.

Generar reportes y medir el compliance.

Eliminar datos corporativos de los dispositivos de forma remota.

Mobile Application Management (MAM)

Administración de Aplicaciones Móviles Móviles
Controla qué aplicaciones pueden usarse para acceder al correo electrónico o archivos laborales desde dispositivos personales.



Publicar aplicaciones móviles para los usuarios.

Configurar y actualizar aplicaciones.

Evitar que los datos laborales se guarden en aplicaciones personales.

Proteger y eliminar datos corporativos dentro de aplicaciones móviles.

Gestión de endpoints con Intune y sus aplicaciones

Panel único para la administración

Valor integrado en toda la cartera de productos de Microsoft

Gestión de última generación con con IA

Incluidos macOS, Linux y trabajadores de primera línea.

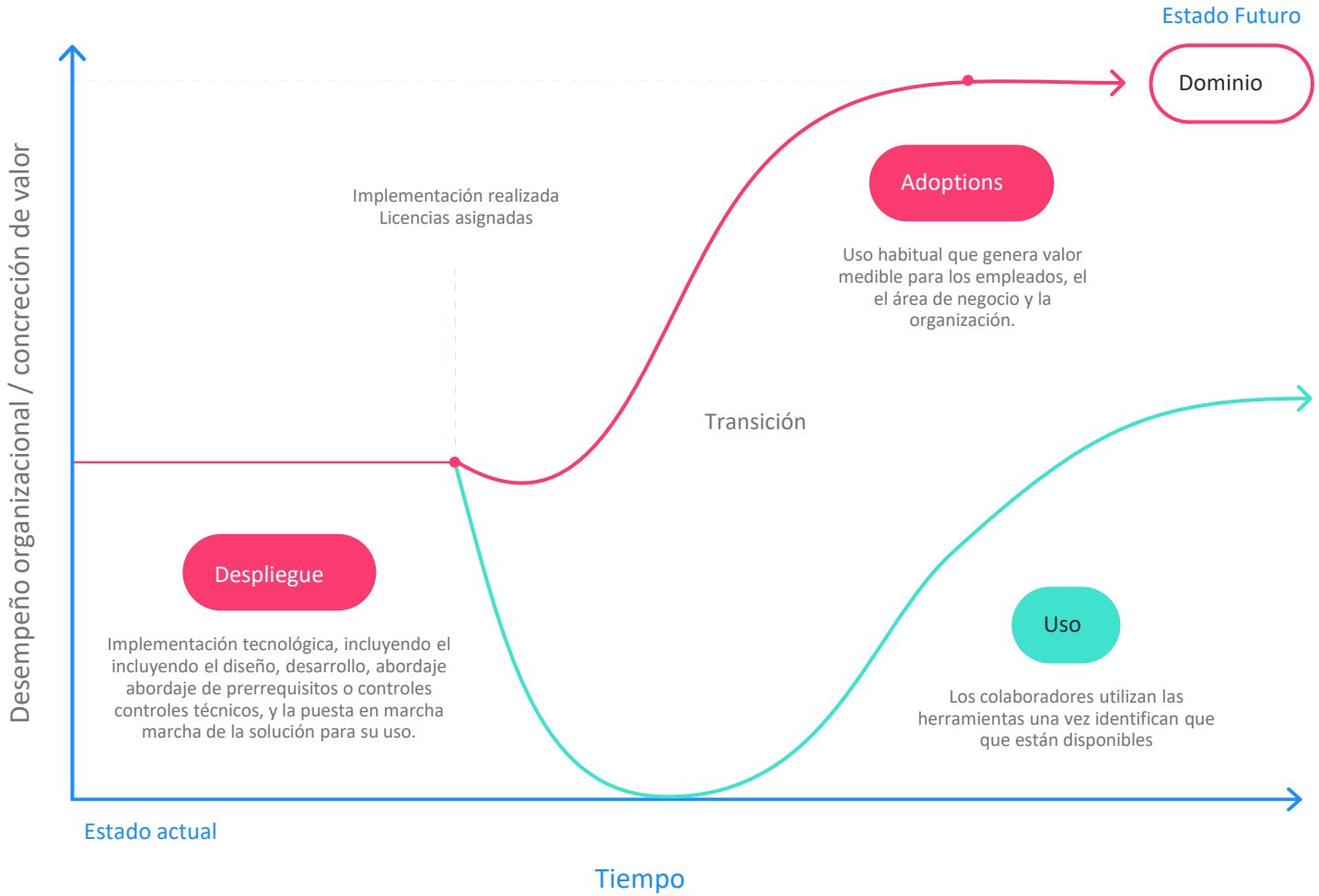
Múltiples soluciones, unificadas para ofrecer una seguridad integral.

Transforme las operaciones con IA y automatización.

Proceso de adopción

Impulsar el cambio humano requiere buenas prácticas

Beneficios definidos en el caso de negocio



Con gestión del cambio

Mayor probabilidad de adopción de MS365 y de concretar los beneficios esperados.

Sin gestión del cambio

Transición más compleja, empleados menos comprometidos y con mayor resistencia. Mayor tiempo hasta lograr beneficios.

7 veces más probabilidades de cumplir o superar los objetivos

del proyecto cuando se aplican excelentes prácticas de gestión del cambio, en comparación con prácticas deficientes.(Prosci, 2024)

Recorrido de adopción

Implementar tecnología

Requiere asegurar previamente:

- Patrocinador
- Casos de uso + KPI
- Seguridad de datos

Cambio humano

Preparar a la organización y a los colaboradores para el proceso de transformación de la IA a través de de programas de adopción.

Los flujos de trabajo se apoyan entre sí para obtener el máximo valor y ROI

Preparar > Incorporar > Generar impacto > Expandir y optimizar

Preparación técnica

Aborde la implementación y optimización técnica, incluida la gobernanza, la seguridad, el cumplimiento y la administración.

Lideres presentes a lo largo del proceso

Nuestro Framework de adopción e implementación - Fases

Gestión del cambio

1. Preparar

Establecer una base sólida para la implementación, asegurando la alineación estratégica, la preparación técnica y la identificación de los primeros casos de uso.

2. Incorporar

Fomentar la adopción y el uso efectivo de la plataforma a través de programas de habilitación
y comunicación.

3. Generar impacto

Medir el impacto de Copilot en en la organización y optimizar su optimizar su uso basándose en en los resultados y la retroalimentación

4. Expandir y optimizar

Escalar la implementación
a nuevos escenarios y usuarios, transformando los procesos de negocio y fomentando la mejora continua.

Impulsa el aprendizaje continuo y la optimización.

Gracias

¡Innovemos juntos!

We Love Tech
By POSSUMUS

Build software
Build value
Positive experiences

info@possumus.tech
Tel. 0810 345 0562
www.possumus.tech

possumustech
@possumus.tech
@PossumusTech
possumus.tech