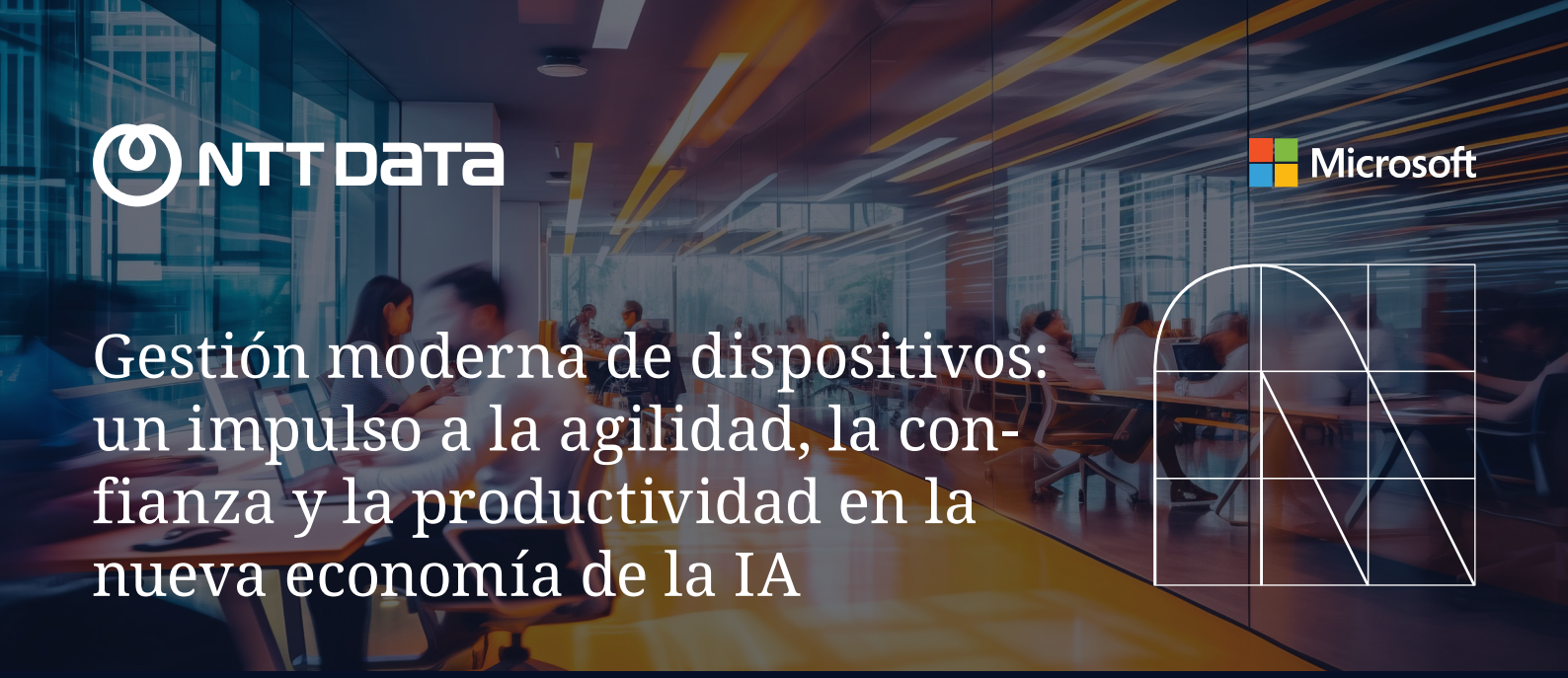


Gestión moderna de dispositivos: un impulso a la agilidad, la confianza y la productividad en la nueva economía de la IA

Descubre cómo transformar tu empresa con un sistema de gestión de dispositivos moderno, basado en la IA e integrado con el ecosistema de Microsoft.

Mejora la resiliencia empresarial, potencia la agilidad operativa y genera confianza digital con información práctica que transforma la gestión de puntos finales en una ventaja estratégica para lograr resultados cuantificables que contribuyen al éxito empresarial.

Resumen ejecutivo

El entorno de trabajo digital se encuentra en un punto de inflexión. Las organizaciones ya no se limitan a reaccionar al cambio. Ahora son proactivas y están reinventando la forma de trabajar, los espacios de trabajo y las tecnologías que dan forma a la experiencia de los empleados. Según el Índice de tendencias laborales de Microsoft de 2023, "el 73 % de los empleados desean que se mantengan las opciones flexibles de trabajo remoto". El trabajo híbrido, la integración de la IA y las operaciones distribuidas se han convertido en algo habitual, lo que obliga a las empresas a modificar su gestión de puntos finales para pasar de una configuración táctica de los sistemas de IT a soluciones que faciliten el trabajo de los empleados. En la actualidad, la gestión de dispositivos es una capacidad fundamental para lograr resiliencia empresarial, agilidad operativa y confianza digital. Los directivos de IT deben garantizar que todos los puntos finales (independientemente de si son propiedad de la empresa, están gestionados por los empleados o son asistidos por IA) son seguros y productivos, cumplen con la normativa y están gobernados de forma inteligente. Para lograrlo, es necesario dejar atrás las herramientas heredadas y los modelos de gestión aislados y pasar a un ecosistema unificado, inteligente y proactivo.

Este informe examina los cambios radicales que se están dando en las expectativas de los trabajadores, la postura de riesgo empresarial y las obligaciones de cumplimiento y sostenibilidad, una revolución que está transformando las estrategias de puntos finales. También analiza la arquitectura de gestión de dispositivos de Microsoft, que ofrece resultados empresariales tangibles como la mejora de la experiencia del usuario, el refuerzo de la seguridad y la protección de datos, el cumplimiento normativo y la gobernanza de IA a escala.

El informe presenta un plan de acción para CIOs, CTOs, y ejecutivos de tecnología, proporcionando una hoja de ruta que se ha aplicado con éxito en múltiples proyectos de transformación global liderados por partners como NTT DATA, que ha ayudado a las empresas a modernizar su infraestructura de dispositivos, reducir los costes operativos y lograr resultados cuantificables.

La oportunidad es clara: las organizaciones que incorporen un sistema de gestión de dispositivos seguro y adaptable en su ADN digital superarán a sus homólogos en aspectos clave como la agilidad, la rentabilidad, la retención de empleados y el cumplimiento normativo. El reto está en eliminar las brechas operativas con una hoja de ruta por etapas que alinee los cambios en las infraestructuras con las ambiciones empresariales. Este informe proporciona esa hoja de ruta.

Introducción

Las empresas están viviendo una profunda transformación que afecta tanto a sus estructuras como a su comportamiento. Las operaciones empresariales han dejado de ser algo circunscrito a oficinas físicas, infraestructuras fijas y horarios de trabajo convencionales. Las plantillas actuales son dinámicas y distribuidas, con fluidez digital y una dependencia cada vez mayor del acceso en tiempo real a datos y servicios. Al mismo tiempo, los directivos tienen que lidiar con un entorno macroeconómico volátil caracterizado por la escalada de la ciberseguridad, la incertidumbre geopolítica, los cambios normativos y una fuerte presión para mejorar los resultados con recursos reducidos.

Esta convergencia de personas, riesgos y tecnología ha trasladado la relevancia estratégica de la gestión de dispositivos a los niveles más altos de toma de decisiones. La estrategia de dispositivos, una tarea que antes era responsabilidad del equipo interno de back end, ahora está directamente vinculada a la resiliencia empresarial, la mitigación de riesgos, el rendimiento de los trabajadores y la innovación digital.

Esta evolución tiene consecuencias evidentes. Los retrasos en el proceso de incorporación ya no son un problema que afecta únicamente al departamento de IT, sino que representan una pérdida de productividad y una experiencia negativa para los empleados. Los dispositivos obsoletos y los protocolos ineficientes de actualizaciones de seguridad exponen a la organización a riesgos operativos y de reputación. La falta de información sobre el cumplimiento de los dispositivos dificulta que se pueda escalar la IA de forma responsable o cumplir con los cambiantes requisitos de los informes de ESG.

En esta nueva realidad, los líderes de IT han dejado de ser meros guardianes de la tecnología para convertirse en una figura clave que hace posible las operaciones. Sus obligaciones se han ampliado, y ahora incluyen la implementación de entornos de trabajo digitales seguros, alineados e inteligentes que permiten el trabajo híbrido, aceleran la innovación y generan confianza a escala. En este informe exploramos el ecosistema moderno de dispositivos de Microsoft (Intune, Autopilot, Entra ID, Defender, Purview y Copilot) y su capacidad para servir de base en la creación de entornos de trabajo digitales seguros, escalables y preparados para la IA.

Las organizaciones que trabajan con integradores expertos como NTT DATA ya han comenzado a utilizar estos entornos para reducir los tiempos de formación y lograr productividad rápidamente, hacer cumplir las medidas de gobernanza de IA y alinear la gestión de los dispositivos con las prioridades empresariales.

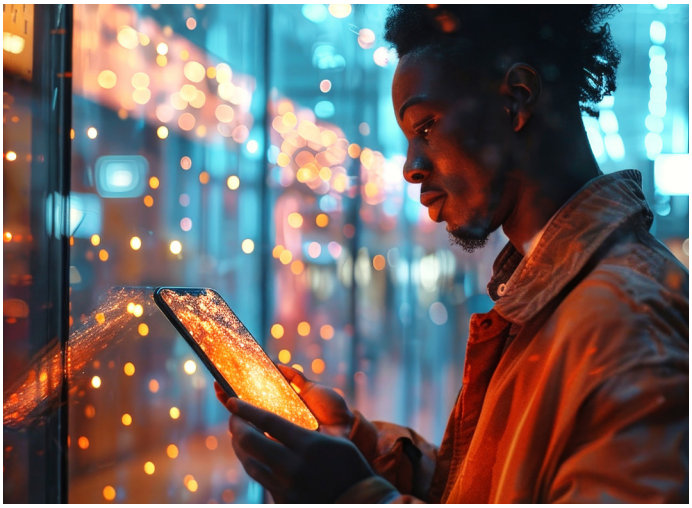
Cómo se está transformando el ecosistema laboral

La disrupción tecnológica, la evolución demográfica y las nuevas normativas laborales han traído consigo un cambio fundamental en la composición y las expectativas de las plantillas. Ahora los empleados trabajan en un entorno digital ampliado que puede incluir desde el hogar personal y espacios de coworking hasta aeropuertos, oficinas de clientes o fábricas. Estén donde estén, todos ellos esperan contar con acceso ininterrumpido, seguro e inmediato a aplicaciones y datos empresariales críticos. Esta forma de trabajar desde cualquier lugar ha dejado obsoletos los modelos de IT limitados al perímetro de la empresa.

Al mismo tiempo, el auge de la IA generativa ha introducido nuevos paradigmas en la productividad, los accesos al conocimiento y la colaboración entre humanos y máquinas. Las herramientas como Microsoft 365 Copilot y Copilot en Intune están integrándose en la forma de trabajar. Ayudan a tomar mejores decisiones, automatizar tareas y aumentar la productividad de las personas y sus equipos.

En lo demográfico, la generación Z y los mileniales, que son ahora la mayoría de los trabajadores, esperan experiencias digitales similares a las de las plataformas de consumo que utilizan a diario. Buscan autonomía, personalización e interacciones sin fricciones. Por otro lado, los trabajadores de oficios críticos necesitan dispositivos resilientes y adaptados a su trabajo que les permitan llevar a cabo tareas críticas sin latencia ni fallos. Además, la alta dirección precisa un sistema de colaboración móvil seguro que ayude a tomar decisiones de impacto en tiempo real.

Esta diversidad de roles, necesidades y estilos de trabajo supone todo un reto para los directivos de IT, que deben proporcionar una infraestructura de trabajo ágil, inclusiva y también alineada con las innovaciones en herramientas, marcos de seguridad y métricas empresariales. Para adaptarse a estos cambios a escala, **es necesario disponer de sistemas de gestión de dispositivos modernos y equipados con un arquitectura que priorice el cumplimiento y esté preparada para la IA.**



Desafíos empresariales y cometido de los directivos de IT

En todos los sectores, las organizaciones se enfrentan a una lista creciente de retos estratégicos y operativos. El aumento de las ciberamenazas y de las expectativas de los clientes, la mayor presión normativa y la necesidad constante de mejorar la eficiencia sin dejar de lado la retención del talento son solo algunos de ellos. El entorno laboral se encuentra en el epicentro de estas disrupciones.

Las estrategias tradicionales de gestión de puntos finales, basadas en controles estáticos de los dispositivos, aprovisionamientos manuales y herramientas fragmentadas, no pueden responder a las exigencias de este nuevo entorno. Exponen a la empresa a riesgos operativos, aumentan el coste total de propiedad y erosionan la confianza y el compromiso de los empleados.

Todos estos factores están ampliando rápidamente el papel de los responsables de IT. Los CIOs y CTOs ya no se ocupan únicamente de garantizar el tiempo de actividad. Ahora se les exige que diseñen entornos de trabajo digitales resilientes, seguros e inteligentes que contribuyan a los resultados empresariales. Estas nuevas responsabilidades incluyen implementar sistemas de aprovisionamiento escalables, asegurar la visibilidad en tiempo real sobre el cumplimiento de los dispositivos, garantizar el uso seguro de la IA y crear experiencias digitales de calidad para los empleados.

Sus obligaciones están claras: Las compañías de IT deben ahora convertirse en un aliado estratégico de la productividad, la innovación y la confianza de los empleados. Las soluciones de trabajo seguras por diseño, escalables por defecto y centradas en las personas proporcionan la base de infraestructura necesaria para alcanzar este objetivo.

Macrotendencias en la gestión moderna de dispositivos

Las empresas globales operan en un entorno marcado por la creciente dependencia digital, el incremento de las amenazas de seguridad, el aumento de las expectativas de los trabajadores y la intensificación de la supervisión normativa. Estas macrofuerzas están transformando la gestión de dispositivos, que pasa de ser una función táctica de IT a un pilar estratégico del rendimiento empresarial.

Hemos identificado siete tendencias clave que definen lo que hay tener en cuenta de cara al futuro para anticiparse, diseñar arquitecturas y operar en este nuevo ecosistema:

1. Consolidación del trabajo híbrido y accesos que no dependen de la ubicación

Según el informe Gartner Future of Work Trends PostCOVID-19 de 2022, “más del 70 % de los trabajadores del conocimiento esperan ya disponer de opciones de trabajo flexibles”. El trabajo híbrido ya no es únicamente una respuesta a la disrupción provocada por la pandemia, sino que se ha convertido en un modelo habitual en la arquitectura de las operaciones empresariales. Hoy en día, el trabajo es algo fluido, sin fronteras y asíncrono. Se da por hecho el acceso a aplicaciones empresariales críticas desde múltiples dispositivos y ubicaciones sin detrimento de la seguridad, la velocidad o la experiencia del usuario. Estos cambios obligan a los directores de Sistemas de Información a replantearse los perímetros tradicionales de la red e invertir en plataformas que permitan el acceso desde cualquier lugar sin incumplir las obligaciones de cumplimiento y seguridad de la empresa.

Los sistemas de gestión de dispositivos modernos de Microsoft, cuando se implementan con la ayuda de un partner de confianza como NTT DATA, agilizan los procesos de formación e incorporación, permiten centralizar los protocolos de cumplimiento de las políticas y ofrecen asistencia en tiempo real a plantillas con una gran diversidad de funciones y ubicaciones. La capacidad para operar desde cualquier sitio se ha convertido en una ventaja competitiva, pero este modelo requiere un nuevo planteamiento de compra, seguridad y gobierno de los puntos finales, donde estos se traten como extensiones dinámicas de la

2. Adopción de marcos de seguridad de confianza cero

Según el estudio Market Guide for Zero Trust Network Access publicado por Gartner en 2022, "para el 2025, el 60 % de las organizaciones habrán adoptado un planteamiento de confianza cero como punto de partida para la seguridad". La frecuencia, velocidad y sofisticación de las ciberamenazas ha aumentado notablemente, dejando obsoletos los sistemas de defensa tradicionales basados en el perímetro. En respuesta a esta situación, el modelo de confianza cero se ha convertido en el marco de seguridad de referencia para las empresas que operan con plantillas distribuidas y un número de puntos finales cada vez mayor. Este enfoque supone no dar automáticamente por sentada la fiabilidad de ningún usuario, dispositivo o conexión de red.

La solución de administración de dispositivos móviles de Microsoft (MDM) es un componente fundamental del marco de confianza cero, ya que verifica continuamente todos los usuarios, dispositivos y solicitudes de acceso. Este enfoque valida la postura del dispositivo, aplica ajustes de cumplimiento y monitoriza las anomalías en tiempo real, ofreciendo información de contexto para las decisiones y aplicando estas últimas de forma dinámica.

3. Integraciones de IA que aumentan la productividad y la rentabilidad

La IA está transformando los modelos operativos de las empresas Sus aplicaciones, que van desde los asistentes de IA generativa hasta las automatizaciones inteligentes, se están integrando en flujos de trabajo, procesos y plataformas para escalar las operaciones, mejorar la eficiencia y diferenciarse ante la competencia. Según el informe Microsoft Copilot Early Access de 2023, "Microsoft 365 Copilot ha demostrado mejoras de productividad de hasta un 29 % en la ejecución de tareas y la calidad de la redacción".

Microsoft Intune está transformando la gestión de puntos finales y ampliando las innovaciones de IA para IT con la introducción de los agentes de Security Copilot. Estos agentes permiten mejorar la postura de seguridad, impulsar la productividad y simplificar las operaciones de IT. Su implementación reduce la presión a la que están sometidos los equipos de IT y seguridad, que deben gestionar puntos finales de gran complejidad y anticiparse a amenazas que cambian continuamente.

Otro estudio de Microsoft de 2024, Randomized Controlled Trials for Security Copilot for IT Administrators, reveló que "los profesionales de IT que utilizan Security Copilot completaban sus tareas con un 35 % más de precisión". Ahora, Copilot en Intune está ampliando sus capacidades con los agentes de Security Copilot. Estos agentes ofrecen herramientas potentes y adaptables de automatización que agilizan las tareas críticas de IT y seguridad, y ayudan a los equipos a trabajar con más agilidad y confianza. El primero de ellos es el Agente de corrección de vulnerabilidades, disponible desde mayo de 2025 en una versión preliminar pública, que aplica automatizaciones de IA a la corrección de vulnerabilidades y supone un gran avance en la gestión de puntos finales.

No obstante, la adopción de la IA va acompañada de nuevas exigencias en el rendimiento de los dispositivos, el acceso a los datos, los controles de políticas y la gobernanza. Los servicios de NTT DATA para la implementación de sistemas de gestión de dispositivos proporcionan puntos finales que cumplen con la normativa, protegen los accesos de nivel superior a los datos sensibles y monitorizan el uso de la IA en todos los roles y funciones empresariales, preparando la organización para la IA. Estos sistemas permiten impulsar la productividad al tiempo que se garantiza la seguridad de los datos y la gobernanza.

4. Asistencia técnica para modelos BYOD y diversidad de los ecosistemas de dispositivos

Hoy en día, los puntos finales desde los que acceden los trabajadores son muy heterogéneos. Este ecosistema incluye desde dispositivos propiedad de la empresa hasta teléfonos personales, tabletas o equipos reforzados para trabajar en las condiciones más exigentes. Se están imponiendo dos nuevos modelos que reflejan una filosofía empresarial centrada en los trabajadores. Por un lado, el BYOD, donde los trabajadores aportan sus propios dispositivos. Por otro, el modelo COPE, donde los dispositivos son propiedad de la empresa pero los empleados los utilizan también con fines personales. A pesar de sus ventajas evidentes, estos modelos complican significativamente la visibilidad, la asistencia y el cumplimiento de políticas en los puntos finales.

Las plataformas modernas de gestión de dispositivos, como Microsoft Intune, permiten disfrutar de una experiencia ininterrumpida, independientemente de quién sea el propietario del dispositivo. Con la ayuda de NTT DATA, las organizaciones pueden ofrecer a sus trabajadores un entorno de dispositivos fluido y heterogéneo, algo esencial para garantizar su satisfacción, productividad y seguridad.

5. Alineación con los objetivos de sostenibilidad y ESG

Según el estudio ESG and IT Asset de NTT DATA de 2022, "si se amplía el ciclo de vida de los dispositivos en un año, la huella de carbono de los puntos finales puede reducirse en un 30 %". La presión de los inversores, las expectativas de los consumidores y los cambios legislativos globales han convertido la sostenibilidad en una prioridad estratégica. Ahora las empresas deben rendir cuentas de su huella de carbono, de los residuos electrónicos y del consumo de energía en toda la cadena de valor, incluidos los dispositivos de IT.

Los modelos modernos de gestión de dispositivos contribuyen a alcanzar los objetivos de ESG, ya que permiten implementar configuraciones de ahorro de energía, ampliar la vida útil de los dispositivos mediante mantenimiento predictivo y obtener más información sobre su uso. Gracias a estas capacidades, las organizaciones pueden reducir los residuos electrónicos, optimizar los ciclos de actualización e integrar la sostenibilidad en su estrategia de infraestructura digital. Con una amplia experiencia global en proyectos de modernización de IT alineados con los compromisos empresariales de ESG, NTT DATA es un partner estratégico en materia de sostenibilidad, ya que ofrece información práctica y modelos de ejecución de eficacia demostrada para acelerar el impacto.

6. Cumplimiento y gobernanza de datos, cada vez más importantes

Con el aumento de normativas globales de protección de datos, el cumplimiento ha dejado de ser una simple formalidad legal y se ha convertido en una prioridad clave para la dirección. Según la encuesta IDC Future of Trust 2023, "más del 76 % de los directivos globales consideran que la gobernanza de datos es un aspecto crítico de la estrategia empresarial". Las empresas deben demostrar responsabilidad, transparencia y control en todo lo relacionado con los accesos a los datos, así como su procesamiento y almacenamiento, tanto en dispositivos como en entornos de nube.

El sistema de gestión moderna de dispositivos, integrado con Microsoft Purview, refuerza la protección de datos, previene amenazas internas y proporciona trazabilidad de calidad forense para las auditorías. Estas capacidades garantizan un cumplimiento continuo, escalable y demostrable, incluso en sectores altamente regulados o jurisdicciones gobernadas por estándares como la HIPAA o el RGPD.

7. La experiencia digital del empleado (DEX), una métrica de rendimiento clave

Según el informe Qualtrics X-Data and Gartner Workforce Trends de 2023, "las empresas que invierten en DEX superan a sus competidoras en un 22 % en la retención de empleados y en un 17 % en la productividad". En NTT DATA creemos que la experiencia del empleado se ha convertido en un KPI empresarial cuantificable, con impacto directo en el compromiso, la productividad y la retención de los trabajadores. En los lugares de trabajo digitales, la calidad de las interacciones entre el usuario y su dispositivo suelen determinar la percepción que este tiene de la organización. Las plataformas de gestión de dispositivos modernos permiten monitorizar, comparar y mejorar la experiencia digital de los empleados, ya que reducen los puntos de fricción, automatizan los servicios de asistencia técnica y facilitan la personalización. Cuando las tecnologías de la información se vuelven invisibles pero facilitan realmente el trabajo, se consigue una plantilla con altos niveles de rendimiento y compromiso. Con este enfoque, el departamento de IT deja de ser un servicio de asistencia para convertirse en un componente clave del éxito del empleado.

Hacia la madurez digital

Aunque casi todo el mundo coincide en la importancia de los sistemas modernos de gestión de dispositivos, muchas empresas siguen dependiendo de herramientas obsoletas, equipos que trabajan en silos y procesos reactivos, algo insostenible en una era marcada por el trabajo híbrido, la aceleración de la IA y los ciberriesgos constantes.

Los departamentos de IT tienen que trabajar a menudo en entornos fragmentados, gestionando múltiples plataformas de puntos finales con políticas poco coherentes y automatizaciones limitadas. Esta situación no solo expone a las empresas a las violaciones de seguridad. También provoca desgaste e insatisfacción de los trabajadores, altos costes de asistencia técnica, errores de cumplimiento y adopción de la IA sin que esta esté respaldada por un modelo de gobernanza.

En las organizaciones que no cuentan con un sistema automatizado y unificado de gestión de puntos finales, el proceso de incorporación más sencillo puede tardar días, ya que exige configuraciones manuales y múltiples aprobaciones innecesarias. Las aplicaciones empresariales no se entregan a tiempo, las actualizaciones de seguridad se aplican de forma irregular y el departamento de IT carece de información fiable sobre qué dispositivos cumplen la normativa. Estas fricciones dan lugar a usos no autorizados de las tecnologías de la información, lo que supone un riesgo no supervisado y una reducción de las capacidades de control del departamento de IT. Sin analíticas integradas, los responsables de IT no pueden comparar experiencias, predecir fallos ni demostrar el impacto en el negocio.

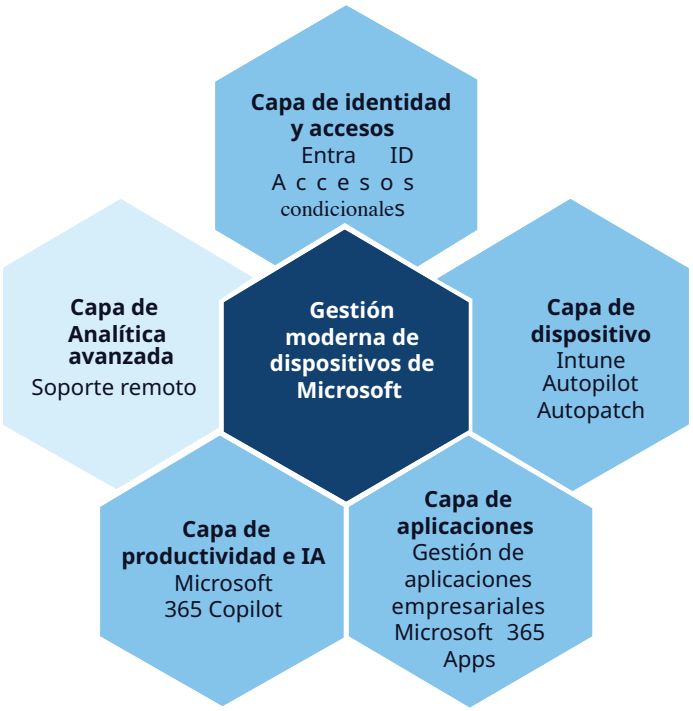
Gracias a la colaboración de NTT DATA con Microsoft, muchas organizaciones han podido resolver estos problemas para obtener resultados destacables: centralización de la gestión de puntos finales, medición de la experiencia digital del empleado y reducción del tiempo de incorporación en más de un 50 % en implementaciones que afectaban a toda la empresa.

Caso de éxito: NTT DATA colaboró con una de las aerolíneas más grandes del mundo en su transición hacia un entorno de trabajo digital moderno, ayudando en la implementación de soluciones de gestión de dispositivos de Microsoft como Intune y Autopilot. La iniciativa sirvió para modernizar y unificar los servicios de dispositivos y movilidad en más de 30.000 dispositivos distribuidos en 400 ubicaciones de todo el mundo. Como resultado, las llamadas al servicio de asistencia se redujeron en un 24 %, lo que mejoró notablemente la satisfacción de los empleados y la eficiencia operativa. El proyecto de colaboración con NTT DATA permitió alinear dinámicamente las operaciones de IT con prioridades empresariales como la gestión de picos en temporada alta, la asistencia en ubicaciones críticas y el mantenimiento proactivo. El problema de los equipos heredados no se resuelve simplemente cambiando de herramientas. Requiere modificar por completo la estrategia de puntos finales, desde la implementación y la gobernanza hasta la asistencia técnica y la evaluación a lo largo de todo el ciclo de vida del empleado. Exige que la gestión de dispositivos se incorpore a los responsables de la alta dirección como un proceso integrado en las estrategias laborales, la postura de riesgo, la arquitectura de cumplimiento y los proyectos de experiencia digital.

La solución: Consigue un impacto de negocio inmediato a través del sistema de gestión moderna de dispositivos de Microsoft

Las soluciones de gestión moderna de dispositivos de Microsoft ofrecen una base consolidada, integral y nativa de la nube desde la que abordar las necesidades de productividad y seguridad. Este conjunto de soluciones, basado en los principios del modelo de confianza cero, ha sido diseñado para entornos híbridos y está alineado con los principios de continuidad del negocio. Ofrece un modelo operativo unificado que integra aprovisionamientos, gestión, protección, gobernanza, productividad y automatización.

Con Microsoft Intune, Autopilot, Autopatch, Defender, Purview y 365 Copilot, las empresas pueden automatizar los procesos de incorporación a escala, implementar modelos de gestión de configuraciones, aplicar políticas de seguridad dinámicas, permitir la adopción responsable de IA, integrar el cumplimiento en las operaciones y mejorar la experiencia digital de los empleados. El resultado es un espacio de trabajo digital más ágil, seguro y preparado para el futuro.



Capacidades clave:

1. **Microsoft Entra ID,** una base para proteger las identidades en entornos híbridos o nativos de la nube. Esta solución es normalmente el primer paso para establecer un modelo de confianza cero, ya que permite crear accesos condicionales, controles basados en políticas y sistemas eficientes de autenticación de usuarios en todos los dispositivos y aplicaciones.
2. **Microsoft Intune,** que ofrece visibilidad y sistemas de gestión centralizados y basados en la nube en todos los terminales (ordenadores de sobremesa o portátiles, dispositivos móviles y entornos virtuales). Con esta solución, los empleados ven implementadas únicamente las aplicaciones empresariales y de productividad que necesitan para su trabajo, lo que garantiza una postura de seguridad uniforme y el cumplimiento de la normativa, además de permitir la orquestación de políticas y la configuración remota.
3. **Windows Autopilot,** que permite la implementación de dispositivos sin intervención de los usuarios, lo que reduce drásticamente el tiempo de incorporación y permite crear experiencias de usuario estandarizadas para todos los roles y ubicaciones. Es perfecto para entornos de trabajo híbridos.
4. **Microsoft Defender xDR,** que ofrece protección avanzada contra amenazas y respuesta en tiempo real, utilizando analíticas de IA para identificar y neutralizar amenazas a nivel de dispositivo, correo electrónico, aplicaciones e identidad.
5. **Microsoft 365 Copilot,** que incorpora IA directamente en el flujo de trabajo para mejorar la productividad. La gestión de dispositivos garantiza, además, accesos seguros y reglamentarios a las fuentes de datos necesarias.
6. **Microsoft Purview,** que aplica políticas de gobernanza, protege los datos, defiende los recursos sensibles de la empresa de las amenazas internas y previene la exfiltración de datos, además de facilitar el cumplimiento de estándares y marcos regulatorios como el HIPAA, el RGPD y el marco de gestión de riesgos de IA del NIST gracias a sus capacidades integradas de clasificación de datos y auditoría.
7. **Windows Autopatch,** que automatiza la gestión de parches para que los dispositivos estén siempre actualizados, sin necesidad de intervenciones manuales y sin interrumpir el trabajo, para que los equipos de TI puedan dedicarse a iniciativas estratégicas en lugar de a operaciones rutinarias de mantenimiento.

En conjunto, estas soluciones garantizan resultados tangibles: reducción del coste de la asistencia técnica, mejora de la postura de seguridad, rapidez en la incorporación y mayor satisfacción de los empleados. El enfoque de la plataforma de Microsoft evita la proliferación de herramientas, simplifica el cumplimiento y alinea la gestión de dispositivos con la estrategia general de transformación digital.

Gracias a nuestra experiencia en la implementación de las soluciones modernas de gestión de Microsoft en entornos complejos, podemos ayudarte a acceder rápidamente a estas ventajas a escala. Te ofrecemos fiabilidad en todas las etapas de modernización de tus dispositivos, desde el diseño de la hoja de ruta hasta la gestión del cambio, y te ayudamos a lograr resultados tangibles en aspectos como la productividad, la optimización de costes, la continuidad del negocio, la seguridad de las operaciones, el cumplimiento de la normativa y la preparación de tus equipos para la IA.

Hoja de ruta de implementación con el modelo de madurez de Microsoft

La implementación de una estrategia moderna de gestión de dispositivos no es una tarea puntual, es un proceso que evoluciona a través de etapas definidas. El modelo de madurez de Microsoft ofrece un marco estructurado para evaluar el estado actual, identificar qué capacidades faltan y planificar la ruta que hay que seguir para lograr un entorno de gestión de dispositivos completamente integrado y optimizado. En cada una de sus fases se genera un valor tangible y se incrementa progresivamente la resiliencia, la seguridad y la productividad a largo plazo, en un proceso que parte del simple mantenimiento de los sistemas y finaliza con la habilitación digital.

1.ª etapa: Tradicional — Operaciones fragmentadas, visibilidad limitada y propensión a riesgos

La mayoría de las organizaciones comienzan con un modelo de gestión de dispositivos heredado que se caracteriza por herramientas de gestión en silos, políticas y controles estáticos y aprovisionamientos manuales. Es necesario contar con técnicos en el entorno local para dar acceso a los recursos empresariales, y la información sobre el cumplimiento o la postura ante amenazas es, en el mejor de los casos, fragmentada. Las políticas de seguridad no son coherentes, no se evalúa la experiencia del usuario, y la incorporación es lenta y requiere mucho trabajo.

Situación de la organización: alto coste de los servicios de asistencia técnica, procesos de incorporación lentos, aplicación desigual de las medidas de seguridad y mala experiencia del usuario.

Cometido del departamento de IT: en esta etapa es necesario comprender el ecosistema de dispositivos existente, alinearse con grupos de interés clave y crear las estructuras de gobernanza donde se apoyará la transformación. Los responsables de IT deben evaluar el estado actual de todo el inventario de dispositivos, las herramientas de puntos finales, la postura de seguridad y los procesos de cumplimiento. El objetivo es crear una hoja de ruta que prepare a la organización para pasar a un modelo de gestión centralizado, donde las mejoras técnicas estén alineadas con las necesidades de los trabajadores y los objetivos empresariales.

2.ª etapa: Avanzada — Operaciones estandarizadas, gobernadas y gestionadas, pero que siguen siendo reactivas

En esta etapa, las organizaciones inician su proceso de modernización. Una vez completada la evaluación y definida la arquitectura de gobernanza, las organizaciones empiezan a estandarizar políticas de referencia para los puntos finales, a consolidar sus herramientas y a activar las soluciones básicas de gestión de dispositivos de Microsoft. Se implementa Intune para crear un sistema de control centralizado, se configura Autopilot para permitir la implementación de dispositivos sin intervención de los usuarios y se activa Defender para responder a las amenazas. Los accesos de los usuarios a los dispositivos están gobernados por políticas de identidad híbrida y acceso condicional.

Acciones estratégicas:

- Se establece la base de las identidades híbridas o nativas de la nube con Microsoft Entra ID.
- Se centraliza la gestión de dispositivos con Intune para implementar y configurar las aplicaciones.
- Se pone en marcha un sistema de implementación de dispositivos sin intervención de los usuarios con Windows Autopilot.
- Se implementa un marco de confianza cero con accesos condicionales.
- Se implementa Defender para la protección y respuesta a amenazas.

Beneficios para la empresa: mejora de la experiencia de los empleados en todos los dispositivos, mayor control operativo, procesos de incorporación más rápidos, menor superficie de ataque, mitigación proactiva de las amenazas y optimización de costes en la etapa inicial.

3.ª etapa: Óptima — Integrada, automatizada y basada en analíticas

La etapa óptima marca un punto de inflexión, donde se pasa del simple cumplimiento de las políticas a la optimización proactiva. Los motores de analíticas procesan datos de telemetría del estado del dispositivo, información sobre el uso y señales de seguridad para desarrollar acciones predictivas. Autopatch automatiza la gestión de actualizaciones y el cumplimiento. Microsoft Purview habilita la gobernanza y la protección de los datos.

Capacidades implementadas:

- Windows Autopatch para automatizar la gestión de actualizaciones
- Analíticas avanzadas con monitorización y telemetría proactivas del estado del dispositivo
- Clasificación y cifrado de datos sensibles, y políticas de prevención de pérdida de datos (DLP) con Microsoft Purview

Beneficios para la empresa: tiempo de inactividad casi nulo, estructura de datos segura y sistema de gobernanza que cumple con las exigencias de las auditorías.

4.ª etapa: Estratégica — Escalable, inteligente y alineada con la empresa

En esta etapa, la gestión de dispositivos queda totalmente integrada en el modelo de negocio y el tejido digital de la empresa. Se establece un marco de confianza cero para dispositivos, identidades, datos, aplicaciones y redes. Microsoft 365 Copilot añade productividad a los flujos de trabajo, y los sistemas de gobernanza de la IA implementados garantizan el uso ético de estas herramientas de productividad. Se incorporan los controles de dispositivos a los informes de ESG, y se utilizan las métricas DEX en los procesos de RR.HH. y de planificación de plantillas. Las estrategias de puntos finales se extienden a los procesos de fusiones y adquisiciones, a las contrataciones globales y a nuevos modelos de negocio.

Capacidades implementadas:

- Marco de confianza cero
- Microsoft 365 Copilot
  - Marcos de gobernanza de la IA con Microsoft Pur-

Transformación organizacional:

- Estrategia de dispositivos alineada con la empresa
- Las métricas de los puntos finales mejoran la experiencia digital del empleado y los informes de ESG
- La confianza cero y la preparación para la IA pasan a ser estándares en toda la empresa

NTT DATA ayuda a las empresas a implementar estas capacidades e integrarlas en las operaciones utilizando el modelo de madurez de Microsoft, que ofrece una hoja de ruta de eficiencia demostrada para lograr una mejora progresiva. Alinear la estrategia, las herramientas y la ejecución permite pasar de la simple gestión de dispositivos a un espacio de trabajo digital resiliente, seguro y basado en IA que genera un valor empresarial tangible.

Etapa	Operaciones	Operaciones y postura del dispositivo	Gobernanza e información	Capacidades implementadas	Impacto empresarial
Tradicional	Fragmentadas	Aprovisionamientos manuales, con herramientas y políticas silos	Sin gobernanza ni monitorización básica del inventario	Herramientas heredadas On-premises	Alto coste, baja visibilidad y propensión a riesgos
Avanzada	Reactivas	Implementación de dispositivos sin intervención de los usuarios e incorporación automatizada de los empleados, identidad híbrida/en la nube, implementación y configuración más rápida de las aplicaciones, accesos dinámicos basados en condiciones, procesos estandarizados de control de políticas y protección/respuesta ante amenazas.	Gestión del cumplimiento e inventario unificado de recursos	Entra ID, Intune, Autopilot, Conditional Access y Defender xDR	Mayor productividad y seguridad reforzada que permiten optimizar costes
Optimizada	Proactivas	Automatización de las actualizaciones, seguridad de datos y telemetría con IA en tiempo real	Analíticas y telemetría, calificación de riesgos y gobernanza que cumple con las exigencias de las auditorías	Autopatch, Purview y Analíticas avanzadas	Mejora de la experiencia del empleado y estructura de datos segura que ayudan a la retención de talento y reducen casi por completo el tiempo de inactividad
Estratégica	Inteligentes, automatizadas y basadas en IA	Dispositivos con capacidad de recuperación autónoma, basados en confianza cero y preparados para la IA	Métricas DEX, iniciativas ESG y gobernanza de la IA	Gobernanza de IA con Purview, Microsoft 365 Copilot y confianza cero	Gestión de dispositivos alineada con las estrategias empresariales

La gestión de dispositivos pasa a ser una palanca estratégica para la agilidad y la confianza empresarial

La gestión moderna de dispositivos ha pasado de ocupar una posición secundaria en las operaciones de IT a convertirse en protagonista de la estrategia empresarial. En la nueva realidad marcada por el trabajo híbrido, la productividad basada en IA y un número cada vez mayor de ciberamenazas, la forma de gestionar los dispositivos afecta directamente al rendimiento de los empleados, los costes para la empresa, la exposición al riesgo y la velocidad operativa.

La plataforma de gestión de dispositivos de Microsoft **permite pasar de un modelo de operaciones de IT fragmentadas y reactivas a un sistema de gestión de puntos finales seguro, automatizado e inteligente basado en la confianza cero**. Este modelo acelera la incorporación, refuerza la seguridad, ayuda a utilizar la IA de forma inteligente y reglamentaria, y permite ofrecer experiencias digitales estandarizadas, todo ello a escala.

Estas mejoras no son solo logros técnicos, sino que se traducen en resultados empresariales tangibles. Se reduce el coste de la asistencia técnica, se consigue productividad en menos tiempo, aumenta la satisfacción de los trabajadores y las empresas están mejor preparadas para las auditorías y el cumplimiento. Todas estas métricas son las que preocupan a los ejecutivos de hoy.

En el mundo empresarial actual, la madurez digital no es solo una iniciativa tecnológica: es una ventaja diferencial. Este documento técnico ofrece un plan de acción para ayudar a los directivos de IT que se enfrentan a esta complejidad. Analiza los cambios en las demandas de los trabajadores, las macrotendencias que afectan a las estrategias de puntos finales y las brechas operativas que obstaculizan la ejecución. Pero, sobre todo, explica cómo el ecosistema de gestión moderna de dispositivos de Microsoft permite transformar los puntos finales, que pasan de ser una fuente de gastos heredada a convertirse en un motor de agilidad, confianza y compromiso del talento.

NTT DATA y Microsoft comparten una visión común: ofrecer entornos de dispositivos seguros, diversos e independientes de la ubicación que generen un impacto empresarial tangible. Ambas organizaciones se alinean para permitir experiencias de usuario fluidas, seguridad proactiva y operaciones de IT escalables, todo ello basado en un marco de confianza cero y preparación para la IA. Gracias a nuestro enfoque estratégico compartido, las empresas pueden modernizar el lugar de trabajo con confianza, logrando un equilibrio entre el control y la flexibilidad, así como entre el rendimiento y la rentabilidad.

Sobre NTT DATA y Microsoft

Según el informe NTT DATA Global Partnership de 2023, "NTT DATA está reconocida como una de las principales empresas integradoras de sistemas globales (GSI) de Microsoft, y ofrece soluciones seguras para entornos de trabajo digitales en más de 50 países".

NTT DATA y Microsoft son partners estratégicos globales desde hace mucho tiempo, y trabajan juntos para ayudar a las empresas a modernizar sus entornos de TI y a obtener resultados en menos tiempo. Los servicios que ofrecemos combinan las plataformas líderes de seguridad y nube de Microsoft con nuestros conocimientos expertos y capacidades globales, que nos permiten ofrecer soluciones de transformación digital fiables y end-to-end.

NTT DATA cuenta con décadas de experiencia en el diseño, la implementación y la gestión de ecosistemas de Microsoft en entornos con gran complejidad y mucha regulación. Desde la implementación de Microsoft Intune y Defender en toda la empresa hasta la activación segura de Microsoft 365 Copilot y la gobernanza de puntos finales con Microsoft Purview, NTT DATA garantiza un proceso de modernización alineada con la seguridad, el cumplimiento y la estrategia empresarial a largo plazo.

Juntos, NTT DATA y Microsoft ofrecen experiencia, tecnología y escala operativa para construir lugares de trabajo digitales seguros, inteligentes y productivos, diseñados para las necesidades de hoy y preparados para el crecimiento del mañana.

Anexo

- **Los trabajadores esperan flexibilidad:**
- "Más del 70 % de los trabajadores del conocimiento en todo el mundo han adoptado un modelo de trabajo híbrido o esperan que este siga existiendo tras la pandemia". — Gartner, Future of Work Trends PostCOVID-19, 2022.
- **La gestión moderna de dispositivos reduce costes:** "Las organizaciones que consolidan la gestión de puntos finales logran una reducción del 30 % en los costes operativos y del 25 % en los incidentes de seguridad". — Forrester Total Economic Impact™ Study of Microsoft Endpoint Manager, 2021.
- **El trabajo híbrido se ha convertido en la norma:** "El 73 % de los empleados quiere que se mantengan las opciones de trabajo remoto flexible". — Microsoft Work Trend Index, 2023.
- **La confianza cero es un imperativo estratégico:** "Para el 2025, el 60 % de las organizaciones habrán adoptado un planteamiento de confianza cero como punto de partida para la seguridad". — Gartner Market Guide for Zero Trust Network Access, 2022.
- **La IA impulsa la productividad de los empleados:** "Microsoft 365 Copilot ha demostrado mejoras de productividad de hasta un 29 % en la ejecución de tareas y la calidad de la redacción". — Microsoft Copilot Early Access Report, 2023.
- **El cumplimiento y la gobernanza son prioridades directivas:**
"Más del 76 % de los directivos globales consideran que la gobernanza de datos es un aspecto crítico de la estrategia empresarial". — IDC Future of Trust Survey, 2023.
- **La experiencia digital del empleado (DEX) afecta a la retención:**
"Las empresas que invierten en DEX superan a sus competidoras en un 22 % en la retención de empleados y en un 17 % en la productividad". — Qualtrics X-Data y Gartner Workforce Trends, 2023.
- **Sostenibilidad y optimización del ciclo de vida del dispositivo:**
"Si se amplía el ciclo de vida de los dispositivos en un año, la huella de carbono de los puntos finales puede reducirse en un 30 %". — NTTT DATA ESG and IT Asset Study, 2022.
- **Colaboración entre NTT DATA y Microsoft:**
"NTT DATA está reconocida como una de las principales empresas integradoras de sistemas globales (GSI) de Microsoft, y ofrece soluciones seguras para entornos de trabajo digitales en más de 50 países". — NTT DATA Global Partnership Report, 2023.

Más información sobre NTT DATA

Visita nttdata.com

Somos un innovador global para servicios empresariales y tecnológicos. Nuestro objetivo es ayudar a nuestros clientes en sus procesos de innovación, optimización y transformación para que puedan conseguir el éxito en sus proyectos. Somos Global Top Employer, y contamos con expertos en más de 50 países, además de un sólido ecosistema de partners. NTT DATA forma parte del Grupo NTT.