

# Gerenciamento moderno de dispositivos: impulsionando agilidade, confiança digital e produtividade em um cenário orientado por IA



Descubra como o gerenciamento moderno de dispositivos, impulsionado por IA e integrado ao ecossistema Microsoft, pode revolucionar a sua empresa.

**Reforce a resiliência dos negócios, aumente a agilidade operacional e consolide a confiança digital com insights acionáveis que transformam a gestão de endpoints em uma vantagem estratégica, gerando resultados mensuráveis para o sucesso empresarial.**

## Resumo Executivo

O ambiente de trabalho digital entrou em uma nova fase decisiva. As organizações deixaram de apenas reagir às mudanças — agora redesenham ativamente como o trabalho acontece, onde acontece e quais tecnologias moldam a experiência dos colaboradores. Segundo o Microsoft Work Trend Index 2023, “73% dos colaboradores querem continuar com opções flexíveis de trabalho remoto”. Com o avanço do modelo híbrido, da integração da IA e das operações distribuídas, o gerenciamento de endpoints precisa deixar de ser apenas uma função tática de TI para se tornar um pilar estratégico da força de trabalho.

Atualmente, o gerenciamento moderno de dispositivos é uma capacidade essencial para garantir resiliência, agilidade e confiança digital. Os líderes de TI devem garantir que cada endpoint — seja corporativo, pessoal ou assistido por IA — esteja seguro, em conformidade, produtivo e governado com inteligência. Isso exige a superação de ferramentas legadas e modelos fragmentados, migrando para um ecossistema unificado, inteligente e proativo.

Este white paper analisa as mudanças estruturais nas expectativas da força de trabalho, no perfil de riscos, nas exigências de conformidade e nas metas de sustentabilidade que estão redefinindo a estratégia de endpoints. A arquitetura de gerenciamento moderno da Microsoft entrega resultados concretos para os negócios — como melhoria da experiência do usuário, reforço da segurança e da proteção de dados, alinhamento regulatório e governança de IA em larga escala.

Esse white paper apresenta também um roteiro estratégico voltado a CIOs, CTOs e executivos de tecnologia que lideram transformações empresariais — um plano já validado em projetos globais conduzidos por parceiros como a NTT DATA, que têm ajudado empresas

a modernizar sua infraestrutura de dispositivos, reduzir custos operacionais e gerar impactos mensuráveis.

A oportunidade é clara: organizações que incorporam um gerenciamento seguro e adaptativo de dispositivos ao seu DNA digital estarão à frente em agilidade, eficiência de custos, retenção de talentos e prontidão para atender às exigências regulatórias. O desafio está em superar as lacunas operacionais com uma jornada estruturada, alinhando a evolução da infraestrutura com os objetivos estratégicos da empresa. Este white paper apresenta o caminho para colocar esse roteiro estratégico em prática.

## Introdução

A empresa moderna está passando por uma transformação estrutural e comportamental profunda. As operações empresariais já não estão mais restritas a escritórios físicos, infraestrutura local ou jornadas tradicionais. A força de trabalho se tornou dinâmica, geograficamente distribuída, digitalmente fluente e cada vez mais dependente de acesso a dados e serviços em tempo real. Ao mesmo tempo, as lideranças executivas enfrentam um cenário macroeconômico volátil, marcado pela escalada das ameaças cibernéticas, incertezas geopolíticas, crescentes exigências regulatórias e intensa pressão por fazer cada vez mais com menos recursos.

Essa convergência entre pessoas, riscos e tecnologia elevou a relevância estratégica do gerenciamento de dispositivos aos mais altos níveis da tomada de decisão empresarial. Antes visto como uma tarefa secundária da TI, o tema agora está diretamente ligado à resiliência dos negócios, mitigação de riscos, desempenho da força de trabalho e inovação digital.

Considere as implicações: atrasos no onboarding deixaram de ser apenas um problema de TI — agora representam perda de produtividade e impacto negativo na experiência dos colaboradores. Dispositivos desatualizados e atualizações de segurança inconsistentes expõem a organização a riscos operacionais e reputacionais. A falta de visibilidade sobre a conformidade dos dispositivos compromete a capacidade de escalar a IA de forma responsável e de atender às novas exigências de transparência relacionadas a critérios ESG.

Nesse novo cenário, os líderes de TI não são apenas responsáveis pela tecnologia — passaram a ser agentes estratégicos que impulsionam o negócio. Sua missão agora inclui entregar ambientes digitais seguros, consistentes e inteligentes, que ofereçam todo o suporte ao trabalho híbrido, acelerem a inovação e promovam a confiança em escala. Este white paper explora como o ecossistema moderno de dispositivos da Microsoft — que inclui Intune, Autopilot, Entra ID, Defender, Purview e Copilot — oferece uma base robusta para construir ambientes digitais seguros, escaláveis e preparados para a IA.

Organizações que contam com integradores experientes como a NTT DATA já começaram a explorar esses ambientes para reduzir o tempo de produtividade, implementar governança de IA e alinhar as operações de dispositivos com as prioridades de negócio.

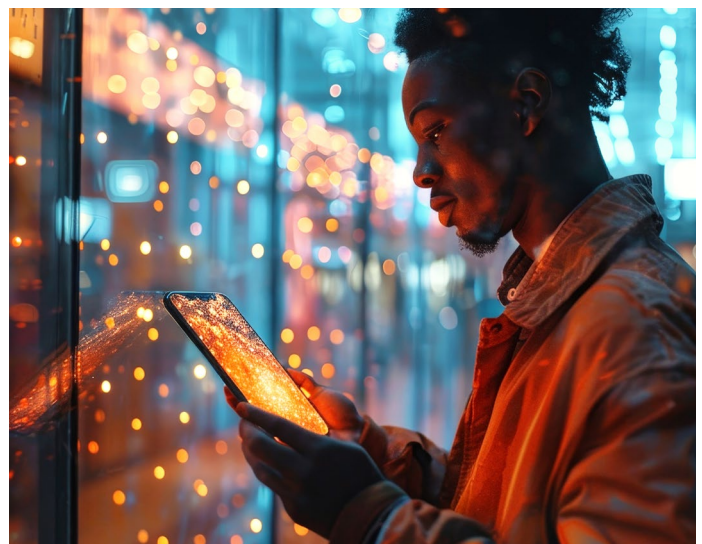
## Como a força de trabalho moderna está mudando

A composição e as expectativas da força de trabalho passaram por uma mudança fundamental, impulsionada por uma confluência de disrupção tecnológica, evolução demográfica e transformação nas normas do ambiente profissional. Atualmente, os colaboradores atuam em um ambiente de trabalho digital descentralizado — trabalhando de home offices, espaços de coworking, aeroportos, sedes de clientes e ambientes industriais — com a expectativa de acesso seguro, instantâneo e sem interrupções a aplicações e dados críticos para o negócio. Essa nova dinâmica de trabalho tornou obsoletos os modelos tradicionais de TI baseados em perímetro.

Ao mesmo tempo, a ascensão da IA Generativa introduziu novos paradigmas de produtividade, acesso ao conhecimento e colaboração entre humanos e máquinas. Ferramentas como o Microsoft 365 Copilot e o Copilot no Intune estão sendo integradas ao cotidiano das equipes. Essas soluções ajudam os colaboradores a tomar melhores decisões, automatizar tarefas e aumentar a produtividade individual e coletiva.

Do ponto de vista geracional, os colaboradores das gerações Z e Millennials — que já representam a maioria da força de trabalho — esperam experiências digitais que reflitam as plataformas de consumo que utilizam no dia a dia. Eles buscam autonomia, personalização e interações fluídas. Já os colaboradores operacionais precisam de dispositivos resilientes e adequados ao contexto, que ofereçam suporte à tarefas críticas sem falhas ou latência. Por sua vez, os executivos exigem colaboração segura em dispositivos móveis para tomar decisões de alto impacto em tempo real.

Essa diversidade de perfis, necessidades e estilos de trabalho impõe aos líderes de TI o desafio de construir uma infraestrutura de ambiente de trabalho que seja responsiva, inclusiva e alinhada a novas ferramentas, frameworks de segurança e métricas de negócio. O gerenciamento moderno de dispositivos, com arquitetura orientada à conformidade e à prontidão para IA, é agora essencial para sustentar essa evolução em escala.





## Transformação digital em curso: o novo papel da liderança de TI

Em todos os setores, as organizações enfrentam uma lista crescente de desafios estratégicos e operacionais. Entre eles estão o aumento das ameaças cibernéticas, o aumento das expectativas dos clientes, o maior rigor regulatório e a demanda constante por mais eficiência — tudo isso em meio ao desafio contínuo de reter talentos. O ambiente de trabalho se tornou o ponto de convergência desses desafios.

As abordagens tradicionais de gerenciamento de endpoints — centradas em controles estáticos, provisionamento manual e ferramentas isoladas — já não acompanham a complexidade do cenário atual. Elas aumentam o risco operacional, elevam o custo total de propriedade e comprometem a confiança e reduzem o engajamento dos colaboradores.

Nesse cenário, o papel da liderança de TI assume uma nova dimensão estratégica dentro das organizações. CIOs e CTOs deixaram de ser responsáveis apenas pela estabilidade dos sistemas: agora têm a missão de projetar ambientes digitais resilientes, seguros e inteligentes, com impacto direto nos resultados do negócio. Isso envolve provisionamento em escala, visibilidade em tempo real da conformidade dos dispositivos, uso seguro de IA e experiências digitais de alta qualidade para os colaboradores.

A missão é clara: o departamento de TI deve atuar como agente estratégico da produtividade, da inovação e da confiança organizacional. A adoção de soluções modernas de ambiente de trabalho — com segurança incorporada desde o início do projeto, escaláveis por padrão e centradas nas pessoas por definição — forma a base necessária para essa transformação.

## Tendências globais que impulsionam o gerenciamento moderno de dispositivos

Empresas globais operam em um cenário caracterizado por crescente dependência digital, ameaças de segurança cada vez mais sofisticadas, expectativas elevadas da força de trabalho e pressão regulatória constante. Essas forças estão posicionando o gerenciamento de dispositivos como um pilar estratégico da performance empresarial — deixando de ser uma função estritamente operacional. Sete tendências-chave estão moldando as prioridades da liderança de TI neste novo paradigma.

### Trabalho híbrido consolidado e acesso seguro de qualquer lugar

Segundo o relatório Gartner Future of Work Trends Post-COVID-19, 2022, “mais de 70% dos trabalhadores do conhecimento agora esperam modelos de trabalho flexíveis”. O trabalho híbrido deixou de ser uma resposta emergencial e passou a integrar, de forma definitiva, a arquitetura das operações modernas. Agora, o trabalho é descentralizado, contínuo e sem barreiras físicas. Os colaboradores esperam acessar as principais aplicações da empresa em qualquer dispositivo e de qualquer lugar — sem abrir mão de segurança, desempenho ou experiência do usuário. Essa nova realidade exige que os CIOs repensem a lógica dos perímetros fixos e priorizem plataformas capazes de oferecer acesso contínuo e seguro, com governança robusta e compatível com os padrões corporativos.

O gerenciamento moderno de dispositivos da Microsoft, quando implementado por parceiros estratégicos como a NTT DATA, permite simplificar o processo de onboarding, padronizar a aplicação de políticas e oferecer suporte proativo e em tempo real a uma força de trabalho ampla e diversificada — seja em termos geográficos ou funcionais. A possibilidade de operar independentemente da localização deixou de ser exceção e passou a ser um diferencial competitivo. Para sustentar essa realidade, é fundamental tratar cada endpoint como uma extensão inteligente, segura e adaptável da infraestrutura corporativa.



## Zero Trust como novo paradigma de segurança empresarial

Segundo o estudo Gartner Market Guide for Zero Trust Network Access (2022), "até 2025, 60% das organizações adotarão o Zero Trust como ponto de partida para suas estratégias de segurança." Diante do aumento da frequência, velocidade e sofisticação das ameaças cibernéticas, os modelos tradicionais de defesa baseados em perímetro se tornaram obsoletos. Diante desse cenário, o Zero Trust firmou-se como o modelo de segurança preferencial entre organizações com força de trabalho distribuída e ecossistemas de dispositivos em constante expansão. Essa estrutura parte do princípio de que nenhum usuário, dispositivo ou conexão deve ser confiável por padrão.

O gerenciamento moderno de dispositivos da Microsoft é um elemento central na arquitetura de Zero Trust — com verificação contínua de cada usuário, dispositivo e solicitação de acesso. Essa abordagem permite validar a postura dos dispositivos, aplicar configurações de conformidade e monitorar desvios em tempo real, garantindo decisões de acesso contextuais e aplicação dinâmica de políticas.

## IA como aceleradora de produtividade e eficiência operacional

A inteligência artificial está redefinindo o modelo operacional das empresas. De assistentes baseados em IA Generativa à automação inteligente, as organizações estão incorporando a IA em fluxos de trabalho, processos e plataformas para escalar resultados, aumentar a eficiência e diferenciar-se competitivamente. Segundo o relatório Microsoft Copilot Early Access Report (2023), "o Microsoft 365 Copilot demonstrou ganhos de produtividade de até 29% em tarefas de escrita e conclusão de atividades."

O Microsoft Intune está transformando a gestão de endpoints e ampliando a inovação em IA para TI com a introdução dos agentes do Security Copilot. Esses agentes fortalecem a postura de segurança, aumentam a produtividade e simplificam as operações de TI, ajudando as equipes a lidar com a complexidade crescente dos ambientes de endpoint e com as ameaças em constante evolução.

Um estudo experimental da Microsoft (Security Copilot for IT Administrators, 2024) revelou que "profissionais de TI usando o Security Copilot foram 35% mais precisos na execução de tarefas". O Microsoft Intune está transformando a gestão de endpoints e ampliando a inovação em IA para TI com a introdução dos agentes do Security Copilot. Esses agentes fortalecem a postura de segurança, aumentam a produtividade e simplificam as operações de TI, ajudando as equipes a lidar com a complexidade crescente dos ambientes de endpoint e com as ameaças em constante evolução. O primeiro desses agentes no Intune é o "Agente de Remediação de Vulnerabilidades". O agente foi lançado em versão prévia pública limitada em maio de 2025, representando um avanço importante na automação de correções de vulnerabilidades com suporte de IA.

A adoção da IA também impõe novas exigências em relação ao desempenho dos dispositivos, acesso a dados, controle de políticas e governança. A NTT DATA apoia essa transformação com serviços de gerenciamento de dispositivos preparados para IA — provisionando endpoints em conformidade, protegendo acessos privilegiados a conjuntos sensíveis de dados e monitorando o uso de IA em diferentes perfis e áreas da organização. Com isso, promove a produtividade sem comprometer a integridade dos dados ou a supervisão da governança.

## Expansão do suporte ao BYOD e à diversidade do ecossistema de dispositivos

A força de trabalho atual opera em um ecossistema de múltiplos dispositivos — incluindo equipamentos corporativos, smartphones pessoais, tablets e dispositivos robustos específicos por setor. O avanço dos modelos bring your own device (BYOD) e corporate-owned, personally enabled (COPE) reflete uma abordagem centrada na experiência do colaborador. No entanto, essa diversidade amplia significativamente a complexidade de visibilidade, suporte e conformidade de políticas nos endpoints.

Plataformas modernas como o Microsoft Intune oferecem uma experiência unificada, independentemente da propriedade ou do ambiente operacional. A NTT DATA permite que as organizações mantenham esse ecossistema fluido e diverso de dispositivos — hoje fundamental para a produtividade, a segurança e a satisfação dos colaboradores.

## Alinhamento com metas de sustentabilidade e ESG

Segundo o estudo NTT DATA ESG and IT Asset Study (2022), "estender o ciclo de vida dos dispositivos em um ano pode reduzir em até 30% a pegada de carbono associada aos endpoints." A sustentabilidade deixou de ser um diferencial e tornou-se uma prioridade estratégica, impulsionada por pressões de investidores, expectativas de consumidores e novas regulamentações globais. As empresas estão sendo cobradas por sua pegada de carbono, geração de resíduos eletrônicos e consumo de energia em toda a cadeia de valor, incluindo os ativos de TI.

O gerenciamento moderno de dispositivos contribui para os compromissos de ESG ao permitir configurações energeticamente eficientes, ampliar a vida útil dos ativos por meio de manutenção preditiva e melhorar a visibilidade sobre a utilização de dispositivos. Essas capacidades ajudam a reduzir o lixo eletrônico, otimizar os ciclos de renovação e incorporar a sustentabilidade à estratégia de infraestrutura digital. A experiência global da NTT DATA na convergência entre modernização de TI e compromissos de ESG a posiciona como um parceiro estratégico valioso — promovendo impacto com base em insights acionáveis e modelos de execução comprovados.

## Foco ampliado em conformidade e governança de dados

Com a proliferação das regulamentações globais de proteção de dados, a conformidade deixou de ser uma formalidade legal e passou a ser uma prioridade estratégica para a alta liderança. Segundo a pesquisa IDC Future of Trust 2023, “mais de 76% dos executivos globais consideram a governança de dados fundamental para a estratégia de negócios.” As organizações precisam demonstrar responsabilidade, transparência e controle sobre como os dados são acessados, processados e armazenados em dispositivos e ambientes de cloud.

O gerenciamento moderno de dispositivos, integrado ao Microsoft Purview, fortalece a proteção de dados, mitiga riscos internos e fornece trilhas de auditoria com nível forense. Isso garante uma conformidade contínua, escalável e defensável — mesmo em setores altamente regulados e em jurisdições com exigências rigorosas, como HIPAA e GDPR.

## Experiência digital do colaborador (DEX) como métrica estratégica de desempenho

De acordo com dados da Qualtrics X-Data e do relatório Gartner Workforce Trends 2023, “empresas que investem em DEX superam seus pares em 22% na retenção de talentos e 17% em produtividade.” A NTT DATA reconhece que a experiência do colaborador se consolidou como um KPI empresarial mensurável — com impacto direto sobre engajamento, desempenho e retenção. Em ambientes digitais, a forma como os profissionais interagem com seus dispositivos influencia diretamente sua percepção sobre a organização.

Plataformas modernas de gerenciamento de dispositivos permitem monitorar, avaliar e aprimorar a DEX, reduzindo pontos de atrito, automatizando o suporte e promovendo experiências personalizadas. Quando o TI se torna invisível e eficiente, a empresa se beneficia de uma força de trabalho altamente engajada e com alto desempenho. Isso transforma o TI de um serviço de suporte em um agente colaborador para o sucesso dos profissionais.

## Impulsionando a prontidão organizacional

Mesmo com ampla consciência sobre os benefícios do gerenciamento moderno de dispositivos, muitas empresas ainda operam com soluções ultrapassadas, estruturas fragmentadas e abordagens reativas — um cenário que não acompanha as exigências do trabalho híbrido, da aceleração da IA e da intensificação dos riscos cibernéticos.

As equipes de TI enfrentam ambientes fragmentados — com múltiplas plataformas de endpoint, políticas inconsistentes e pouca automação. Essa lacuna expõe a empresa não apenas a falhas de segurança, mas também à perda de talentos,

aumento dos custos de suporte, queda na satisfação dos usuários, riscos regulatórios e à adoção de IA sem diretrizes claras ou governança adequada.

Em organizações sem gerenciamento automatizado e unificado, processos simples como a integração de um novo colaborador podem levar dias, exigindo configurações manuais e aprovações redundantes. Aplicativos corporativos não são entregues dentro do prazo, atualizações de segurança são aplicadas de forma inconsistente e o TI perde visibilidade sobre o nível de conformidade dos dispositivos. Esse cenário favorece o crescimento da TI paralela — introduzindo riscos não monitorados e reduzindo o controle da área de tecnologia. Sem análises integradas, líderes de TI não conseguem avaliar a experiência do usuário, prever falhas ou demonstrar impacto nos resultados do negócio.

A parceria entre NTT DATA e Microsoft tem permitido que as organizações superem essas barreiras — com a implantação de um gerenciamento unificado de endpoints, o desenvolvimento de métricas para DEX e a redução do tempo de integração em mais de 50% em algumas implantações em escala empresarial.

Um exemplo prático: a NTT DATA colaborou com uma das maiores companhias aéreas do mundo para modernizar seu ambiente de trabalho digital com a implementação de soluções Microsoft como Intune e Autopilot. A iniciativa unificou os serviços de mobilidade e dispositivos em mais de 30 mil endpoints distribuídos por 400 localidades ao redor do mundo. O resultado foi uma redução de 24% nas chamadas ao service desk, com ganhos mensuráveis em satisfação dos colaboradores e eficiência operacional. A parceria também permitiu que o cliente alinhasse dinamicamente as operações de TI às prioridades do negócio — como a gestão de picos sazonais, o suporte a unidades críticas e a garantia de manutenção proativa.

Assim, superar o déficit deixado por soluções legadas exige mais do que substituir ferramentas. É necessário um redesenho estrutural da forma como os dispositivos são provisionados, gerenciados, protegidos e avaliados ao longo de todo o ciclo de vida do colaborador. Isso exige que os líderes de TI posicionem o gerenciamento de dispositivos como uma disciplina estratégica no nível da liderança executiva — integrada à estratégia de força de trabalho, à postura de risco, à arquitetura de conformidade e à agenda de experiência digital.

## A solução: Impacto imediato com o gerenciamento moderno de dispositivos da Microsoft

O portfólio de gerenciamento moderno de dispositivos da Microsoft oferece uma base unificada, abrangente e nativa em cloud para atender aos dois grandes desafios da era digital: produtividade e segurança. Fundamentada nos princípios de Zero Trust, desenvolvida para ambientes híbridos e alinhada às estratégias de continuidade dos negócios, a solução reúne provisionamento, gerenciamento, proteção, governança, produtividade e automação em um modelo operacional unificado. Isso permite que os líderes de TI deixem de atuar de forma reativa e passem a desempenhar um papel estratégico na entrega de valor.

Com Microsoft Intune, Autopilot, Autopatch, Defender, Purview e 365 Copilot, as organizações podem: automatizar o onboarding em escala, aplicar políticas de configuração, reforçar a segurança com regras dinâmicas, adotar IA de forma responsável e operacionalizar a conformidade — tudo isso enquanto aprimoram a experiência digital dos colaboradores. O resultado é um ambiente de trabalho digital mais seguro, ágil e preparado para o futuro.



### Principais funcionalidades incluem:

**1. Microsoft Entra ID** é a base para uma identidade segura em ambientes híbridos ou nativos em cloud. Geralmente, representa o primeiro passo na jornada de Zero Trust de uma organização — viabilizando acesso condicional, controles baseados em políticas e autenticação de usuários eficiente em todos os dispositivos e aplicativos.

- 2. Microsoft Intune** oferece visibilidade centralizada e gerenciamento baseado em cloud para todos os dispositivos de endpoint — desktops, laptops, dispositivos móveis e ambientes virtuais — fornecendo aplicativos de produtividade e negócios quando necessário, garantindo postura de segurança consistente com políticas de configuração padrão, aplicação de conformidade, configuração remota e orquestração de políticas.
- 3. Windows Autopilot** permite o provisionamento zero-touch, reduzindo drasticamente o tempo de integração do colaborador e proporcionando uma experiência padronizada para os usuários, independentemente de função ou localização — ideal para cenários de trabalho híbrido.
- 4. Microsoft Defender xDR** oferece proteção avançada contra ameaças e resposta em tempo real, usando análises baseadas em IA para identificar e neutralizar ameaças em dispositivos, e-mails, aplicativos e identidades.
- 5. Microsoft 365 Copilot** incorpora a IA diretamente ao fluxo de trabalho, potencializando a produtividade dos colaboradores, enquanto o gerenciamento de dispositivos assegura acesso seguro e em conformidade às fontes de dados necessárias.
- 6. Microsoft Purview** aplica políticas de governança, protege dados, resguarda os recursos sensíveis da empresa contra ameaças internas, evita a exfiltração de dados e atende a normas regulatórias como HIPAA, GDPR e NIST AI RFM, por meio de classificação automatizada de dados e recursos integrados de auditoria.
- 7. Windows Autopatch** automatiza a gestão de atualizações, garantindo que os dispositivos estejam sempre atualizados sem comprometer a produtividade dos usuários ou exigir intervenção manual — permitindo que as equipes de TI se concentrem em iniciativas estratégicas, em vez de manutenção rotineira.

Essas soluções, em conjunto, ajudam os líderes de TI a gerar resultados mensuráveis: redução de custos de suporte, melhoria na postura de segurança, onboarding mais rápido e maior satisfação dos colaboradores. A abordagem de plataforma da Microsoft reduz a fragmentação de ferramentas, simplifica a conformidade e alinha o gerenciamento de dispositivos com estratégias mais abrangentes de transformação digital.

A expertise da NTT DATA na implementação do pacote moderno de gerenciamento Microsoft em ambientes complexos garante que esses benefícios sejam alcançados com rapidez e de forma abrangente. Do desenho da jornada à gestão da mudança, a empresa assegura execução com confiança, viabilizando resultados tangíveis como produtividade da força de trabalho, otimização de custos, continuidade dos negócios, operações seguras, alinhamento regulatório e prontidão para a IA.



## Roteiro de implementação para líderes de TI com base no modelo de maturidade de adoção da Microsoft

Implementar uma estratégia moderna de gerenciamento de dispositivos não é um evento pontual — é uma jornada que evolui por estágios bem definidos. O modelo de maturidade de adoção da Microsoft fornece uma estrutura clara e progressiva que ajuda os líderes de TI a avaliarem seu estado atual, identificarem lacunas de capacidades e planejarem uma trajetória para um ambiente de gerenciamento de dispositivos totalmente integrado e otimizado. Cada fase entrega valor progressivo, ao mesmo tempo que reforça a resiliência operacional, a postura de segurança e a produtividade da força de trabalho — ajudando os líderes de TI a evoluírem da manutenção de dispositivos para a capacitação digital.

### **Estágio 1: Tradicional — operações fragmentadas, visibilidade limitada e alto risco**

A maioria das organizações começa com um modelo de gerenciamento legado, caracterizado por ferramentas isoladas, controles e políticas estáticas, e provisionamento manual. Os dispositivos geralmente exigem presença física para acessar recursos corporativos, e a visibilidade sobre conformidade ou postura de ameaças é, na melhor das hipóteses, fragmentada. As políticas de segurança são inconsistentes, a experiência do usuário não é mensurada e o onboarding é lento e trabalhoso.

**Realidade organizacional:** custos elevados de suporte, prazos longos de onboarding, aplicação inconsistente das políticas de segurança e experiência do usuário insatisfatória.

**Foco do TI:** nesse estágio o objetivo é compreender o ecossistema atual de dispositivos, alinhar com os stakeholders e estabelecer as estruturas de governança necessárias para viabilizar a transformação. Os líderes de TI devem conduzir uma avaliação do atual cenário, considerando o inventário de dispositivos, as ferramentas de endpoint, a postura de segurança e os processos de conformidade. O objetivo é construir um roteiro estratégico para preparar o gerenciamento centralizado — um plano que alinhe as atualizações tecnológicas às necessidades da força de trabalho e aos objetivos estratégicos da organização.

### **Estágio 2: Avançado — operações padronizadas, governadas e gerenciadas, mas ainda reativas**

As organizações neste estágio iniciam sua jornada de modernização. Com a avaliação e a arquitetura de governança já estabelecidas, passam a padronizar políticas de endpoint, consolidar ferramentas e ativar as principais soluções de gerenciamento de dispositivos da Microsoft. O Intune é implantado para fornecer controle centralizado; o Autopilot, configurado para viabilizar o provisionamento zero-touch; e o Defender, ativado para resposta a ameaças. Políticas de identidade híbrida e de acesso condicional regulam a relação entre usuários, dispositivos e permissões de acesso.

#### **Ações estratégicas:**

- Estabelecer identidade em cloud ou híbrida com Microsoft Entra ID
- Centralizar o gerenciamento de dispositivos com Intune — distribuindo apps e configurações
- Ativar provisionamento zero-touch com Windows Autopilot
- Implementar modelo Zero Trust com acesso condicional
- Proteger e responder a ameaças com Microsoft Defender

**Benefícios empresariais:** melhor experiência do colaborador em todos os dispositivos, maior controle operacional, onboarding mais rápido, redução da superfície de ataque, mitigação proativa de ameaças e início da otimização de custos.

### **Estágio 3: Otimizado — operações integradas, automatizadas e orientadas por análises**

Esse estágio representa uma mudança determinante da conformidade com as políticas para uma otimização proativa. Telemetria de integridade dos dispositivos, insights de uso e sinais de segurança alimentam mecanismos de análise que impulsionam ações preditivas. O Autopatch automatiza o gerenciamento de atualizações e a conformidade. O Microsoft Purview viabiliza a proteção de dados e a governança.

#### **Capacidades implantadas:**

- Windows Autopatch para gestão automatizada de atualizações
- Análises avançadas com telemetria proativa de integridade dos dispositivos
- Classificação e criptografia de dados sensíveis, e políticas de DLP com Microsoft Purview

**Benefícios empresariais:** operação contínua com interrupções mínimas, proteção abrangente da arquitetura de dados e governança auditável e em conformidade,

**Estágio 4: Estratégico — escalável, inteligente e alinhado aos objetivos do negócio**

Neste estágio, o gerenciamento de dispositivos está totalmente integrado ao modelo operacional e à estrutura digital da organização. O modelo Zero Trust é institucionalizado em todos os níveis — dispositivos, identidades, dados, aplicativos e redes. O Microsoft 365 Copilot amplia a produtividade diretamente no fluxo de trabalho dos colaboradores, enquanto estruturas de governança de IA garantem o uso ético dessas ferramentas. Os controles de dispositivos passam a compor os relatórios de ESG, enquanto as métricas de DEX orientam tanto a área de RH quanto o planejamento da força de trabalho. As estratégias de endpoints escalam de forma fluida em fusões e aquisições, contratações globais e novos modelos de negócio.

**Capacidades implantadas:**

- Modelo Zero Trust
- Microsoft 365 Copilot
- Frameworks de governança de IA com Microsoft Purview

**Transformação organizacional:**

- Estratégia de dispositivos alinhada aos objetivos do negócio
- Métricas de endpoints orientam os relatórios de DEX e ESG
- Zero Trust e prontidão para IA tornam-se práticas padrão em toda a empresa

A NTT DATA oferece suporte as empresas na implementação e operacionalização dessas capacidades, utilizando o modelo de maturidade da Microsoft como um roteiro comprovado para avanços contínuos. Ao alinhar estratégia, ferramentas e execução, os líderes de TI deixam de apenas gerenciar dispositivos e passam a habilitar ambientes digitais resilientes, seguros e prontos para IA, gerando valor real para o negócio.

Estágio	Operações	Postura e operações de dispositivos	Governança e insights	Capacidades implantadas	Impacto nos negócios
Tradicional	Fragmentadas	Provisionamento manual, ferramentas e políticas isoladas	Sem governança, apenas rastreamento básico de inventário	Ferramentas legadas locais	Alto custo, baixa visibilidade e exposição a riscos
Avançado	Reativas	Provisionamento zero-touch e integração automatizada de colaboradores, identidade híbrida/cloud, implantação mais ágil de aplicativos e configurações, acesso dinâmico baseado em condições, controle padronizado de políticas e proteção e resposta a ameaças.	Gerenciamento de conformidade, inventário unificado	Entra ID, Intune, Autopilot, Acesso Condicional, Defender xDR	Maior produtividade da força de trabalho e segurança reforçada, resultando em otimização de custos
Otimizado	Proativas	Atualizações automatizadas, segurança de dados e telemetria em tempo real com IA	Análises, telemetria, pontuação de risco, governança pronta para auditoria	Autopatch, Purview e análises avançadas	Melhor experiência do colaborador e proteção dos dados — favorecendo retenção de talentos e mínimo tempo de interrupção
Estratégico	Inteligentes, automatizadas e orientadas por IA	Dispositivos autogerenciáveis com Zero Trust e prontos para IA	Métricas de DEX, iniciativas de ESG e governança de IA	Governança de IA com Purview, Microsoft 365 Copilot e Zero Trust	Gerenciamento de dispositivos alinhado à estratégia do negócio



## Transformando o gerenciamento de dispositivos em um pilar estratégico de agilidade e confiança

O gerenciamento moderno de dispositivos deixou de ser uma função restrita ao back office de TI e passou a ocupar o centro da estratégia corporativa. Em um cenário moldado pelo trabalho híbrido, pela produtividade impulsionada por IA e pelo aumento das ameaças cibernéticas, a forma como as empresas administram seus dispositivos impacta diretamente o desempenho dos colaboradores, os custos do negócio, a exposição a riscos e a velocidade operacional.

A plataforma de gerenciamento de dispositivos da Microsoft permite que os líderes de TI avancem de operações fragmentadas e reativas para um gerenciamento de endpoints seguro, automatizado e inteligente, baseado no modelo de Zero Trust. A plataforma permite um processo de onboarding mais rápido, maior robustez em segurança, uso de IA de forma inteligente e em conformidade, além de experiências digitais consistentes — em escala empresarial.

Essas melhorias não representam apenas ganhos técnicos: resultam em benefícios concretos para o negócio, como menores custos de suporte, redução do tempo até a produtividade, maior satisfação da força de trabalho e melhor preparo para auditorias e conformidade. São essas as métricas que importam para os executivos de hoje.

No ambiente corporativo atual, a fluência digital não é apenas uma iniciativa tecnológica — é um diferencial competitivo. Este white paper oferece um roteiro sólido para os líderes de TI que enfrentam essa complexidade. Esse documento analisa as demandas da força de trabalho, as macro-tendências que orientam a estratégia de endpoints e as lacunas operacionais que limitam a execução dos negócios. Mais importante ainda, mostra como o ecossistema de gerenciamento moderno de dispositivos da Microsoft permite às organizações transformar os endpoints de um centro de custos legado em um motor dinâmico de agilidade, confiança e engajamento de talentos.

A NTT DATA e a Microsoft atuam em conjunto para entregar ambientes de dispositivos seguros, diversos e independentes de localização, capazes de gerar impacto mensurável nos negócios. Ambas organizações estão alinhadas em viabilizar experiências de usuário perfeitas, segurança proativa e operações de TI escaláveis — baseadas no framework de Zero Trust e na prontidão para IA. Essa abordagem estratégica conjunta garante que as empresas modernizem seu ambiente de trabalho com confiança, equilibrando controle e flexibilidade, desempenho e eficiência de custos.



# Sobre a parceria entre NTT DATA e Microsoft

De acordo com o NTT DATA Global Partnership Report 2023, “a NTT DATA é reconhecida como um dos principais Integrador de Sistemas Globais (GSI) da Microsoft, entregando soluções seguras para o ambiente de trabalho digital em mais de 50 países.”

**A NTT DATA e a Microsoft** mantêm uma parceria estratégica de longa data, com atuação conjunta para ajudar as empresas a modernizar seus ambientes de TI e acelerar seus resultados de negócios. Ao combinar as plataformas de cloud e segurança avançada da Microsoft com a sólida expertise setorial e a capacidade global de entrega da NTT DATA, as organizações têm acesso a soluções confiáveis de transformação digital de ponta a ponta.

A NTT DATA reúne décadas de experiência no desenvolvimento, implantação e gestão de ecossistemas baseados em Microsoft — inclusive em contextos altamente regulamentados e complexos. De implementações empresariais do Microsoft Intune e Defender à habilitação segura do Microsoft 365 Copilot e à governança de endpoints com o Microsoft Purview, a NTT DATA assegura que a modernização esteja sempre alinhada à segurança, à conformidade e à estratégia de negócios de longo prazo.

Juntas, a NTT DATA e a Microsoft entregam a expertise, a tecnologia e a escalabilidade operacional necessárias para ajudar empresas a construir ambientes de trabalho digitais seguros, inteligentes e produtivos — prontos para os desafios de hoje e preparados para o crescimento de amanhã.

## Anexos

- **Forças de trabalho exigem flexibilidade:** “Mais de 70% dos trabalhadores do conhecimento em todo o mundo adotaram um modelo de trabalho híbrido ou esperam um após a pandemia.” — Gartner, Future of Work Trends Post-COVID-19, 2022.
- **Gerenciamento moderno de dispositivos reduz custos e riscos:** “As organizações que consolidam o gerenciamento de endpoints observam uma redução de 30% nos custos operacionais e uma diminuição de 25% nos incidentes de segurança.” — Forrester Total Economic Impact™ Study of Microsoft Endpoint Manager, 2021.
- **O trabalho híbrido consolida-se como padrão global:** “73% dos colaboradores querem opções flexíveis de trabalho remoto de forma permanente.” — Microsoft Work Trend Index, 2023.
- **Zero Trust consolida sua posição como pilar estratégico:** “Até 2025, 60% das organizações adotarão o zero trust como ponto de partida para a segurança.” — Gartner, Market Guide for Zero Trust Network Access, 2022.
- **IA acelera a produtividade dos colaboradores:** “O Microsoft 365 Copilot apresentou melhorias de até 29% na conclusão de tarefas e na qualidade da escrita.” — Microsoft Copilot Early Access Report, 2023.
- **Conformidade e governança ganham espaço na agenda dos executivos:** “Mais de 76% dos executivos globais consideram a governança de dados fundamental para a estratégia de negócios.” — IDC Future of Trust Survey, 2023.
- **Experiência digital do colaborador (DEX) fortalece a retenção:** “As empresas que investem em DEX superam seus concorrentes em 22% na retenção de colaboradores e em 17% na produtividade.” — Qualtrics X-Data and Gartner Workforce Trends, 2023.
- **Sustentabilidade ganha força com a otimização do ciclo de vida dos dispositivos:** “Estender o ciclo de vida dos dispositivos em um ano pode reduzir a pegada de carbono dos endpoints em até 30%.” — NTT DATA ESG and IT Asset Study, 2022.
- **A parceria entre a NTT DATA e a Microsoft:** “A NTT DATA é reconhecida como um dos principais Global Systems Integrators (GSI) da Microsoft, entregando soluções seguras de ambiente de trabalho digital em mais de 50 países.” — NTT DATA Global Partnership Report, 2023.

## Saiba mais sobre a NTT DATA

Visite [br.nttdata.com](https://br.nttdata.com)

A NTT DATA é uma inovadora global confiável de serviços de negócios e tecnologia, ajudando os clientes a inovar, otimizar e transformar para o sucesso. Como Global Top Employer, temos diversos especialistas em mais de 50 países e um robusto ecossistema de parceiros. A NTT DATA faz parte do Grupo NTT.

