Melhores práticas para gerenciamento de dispositivos simples e seguro

Produtividade móvel para a sua empresa.
Liberdade de escolha para os funcionários.
Segurança e controle total para a TI.

A escolha dos funcionários tornou-se um dos pilares da estratégia da TI moderna. Ao permitir que as pessoas escolham os melhores dispositivos para suas necessidades, as organizações podem melhorar a produtividade, a flexibilidade e até mesmo a satisfação no trabalho. Com a estratégia certa, a TI pode garantir que as políticas e as tecnologias adequadas estejam em vigor para proteger as informações corporativas, reduzindo os custos e proporcionando uma excelente experiência aos usuários.

Sua estratégia deve permitir que sua organização:

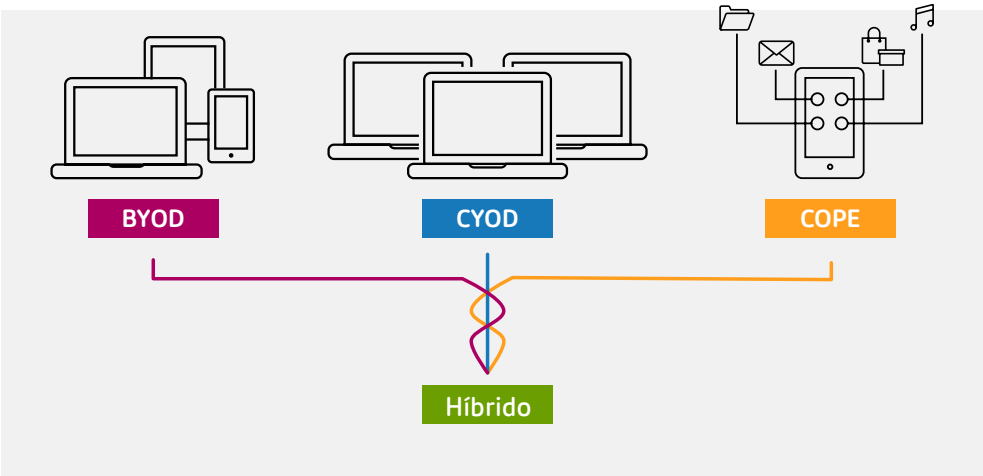
- **Capacite as pessoas** a escolherem seus próprios dispositivos para melhorar a produtividade, a colaboração e a mobilidade.
- **Proteja as informações confidenciais** contra perda e roubo, ao mesmo tempo em que aborda os mandatos de privacidade, conformidade e gerenciamento de riscos.
- **Reduza os custos e simplifique o gerenciamento** por meio de provisionamento de autoatendimento e gerenciamento e monitoramento automatizados.
- **Simplifique a TI** com uma única solução abrangente para gerenciar e proteger dados, aplicativos e dispositivos.

Aqui estão 8 melhores práticas para projetar uma estratégia que combina simplicidade para funcionários com segurança, controle e gerenciamento efetivos para TI:

1. Escolha de uma política

Como a mobilidade e a consumerização continuam a transformar a TI, existem várias políticas que combinam a liberdade de escolha com maior controle para a TI:

- Traga seu próprio dispositivo (BYOD): Permite que as pessoas usem dispositivos pessoais para trabalhar.
- Escolha o seu próprio dispositivo (CYOD): Permite que os funcionários escolham um dispositivo de propriedade da empresa a partir de um pequeno pool de dispositivos para usar para fins de trabalho.



- Propriedade da empresa, pessoalmente habilitada (COPE): Permite que os funcionários escolham um dispositivo da empresa a partir de uma lista aprovada e usem seus próprios aplicativos, bem como aplicativos corporativos no dispositivo.
- Abordagem híbrida: Uma combinação pode ser usada para capacitar a mobilidade da maneira certa para diferentes usuários e grupos. Por exemplo, o COPE pode ser usado lado a lado com o CYOD ou o BYOD.

Embora as nuances das políticas possam variar, todas compartilham os princípios mais fundamentais do gerenciamento unificado de endpoints (UEM), inclusive suas implicações de segurança. As principais diferenças tem a ver com os custos.

Os usuários do BYOD pagam por seus próprios dispositivos e planos de dados, às vezes com um pagamento parcial ou total feito pela empresa. Para COPE e CYOD, a empresa paga pelo uso de dispositivos e dados. Uma política BYOD também pode precisar abordar algumas considerações além do escopo do COPE e do CYOD, como por exemplo, se os funcionários devem receber horas extras para verificar e-mails depois do trabalho ou nos fins de semana.

2. Elegibilidade e inscrição

Deixe claro quem tem permissão para usar dispositivos pessoais, seja em uma base ad hoc para complementar um endpoint corporativo, como substituto permanente de um dispositivo corporativo ou qualquer situação parecida. Isso pode ser visto como um privilégio a ser ganho, uma resposta à uma demanda de um funcionário, um requisito para determinados tipos de funções, um risco excessivo para alguns casos de uso ou, mais provavelmente, uma combinação dessas coisas.

Uma maneira de determinar a elegibilidade é aplicar critérios, como por exemplo, tipo de trabalhador, frequência de viagem, performance ou a necessidade de acesso off-line a dados confidenciais. No entanto, a elegibilidade é definida em um nível amplo, os gerentes devem sempre ter a aprovação final sobre quais membros da equipe são candidatos apropriados para receber um estipêndio. Os gerentes também podem ser aconselhados a aplicar o BYOD, o COPE ou o CYOD dentro do contexto de outros incentivos, privilégios e medidas disciplinares do departamento.

Os contratados geralmente são os candidatos ideais para o BYOD. Muitas organizações já esperam que os contratados tragam seus próprios dispositivos, e a exigência que eles façam isso ajuda no cumprimento da contratação independente.

3. Dispositivos permitidos

Para evitar ter uma diversidade incontrolável de dispositivos, você pode limitar o tipo de dispositivos móveis que sua empresa dará suporte. A granularidade dessa política dependerá dos requisitos do usuário, dos riscos de segurança e dos recursos de suporte. Em geral, quanto mais detalhada for sua política em termos de tipos de dispositivo, versões do sistema operacional e números de modelo, mais recursos serão necessários para testar e dar o suporte adequado aos dispositivos especificados.

Para manter a propriedade clara, os participantes do BYOD devem comprar seus dispositivos pessoais por meio de canais comuns ao consumidor, em vez de comprar pelo departamento de compras de uma organização. Você pode disponibilizar descontos para funcionários em fornecedores corporativos de seu relacionamento na empresa.

Algumas pessoas também podem querer equipamentos suplementares, como monitores ou teclados. Só não se esqueça de especificar quem irá adquirir e possuir cada item.

4. Lançamento

A comunicação é vital para uma implementação bem-sucedida. Dê orientações para ajudar as pessoas a decidirem se querem participar e como escolher o dispositivo certo para as suas necessidades. Eles também devem entender como os dados podem ser acessados, usados e armazenados, e a maneira apropriada de configurar e usar contas relacionadas ao trabalho para aplicativos e serviços não gerenciados do consumidor.

Os dados corporativos devem ser mantidos estritamente segregados para dar suporte aos requisitos de descoberta eletrônica e políticas de retenção de dados; e-mails de trabalho nunca devem ser enviados de contas pessoais. Políticas de uso aceitáveis devem ser aplicadas da mesma forma nos dispositivos BYO que são nos dispositivos corporativos.

É importante também oferecer um programa de adoção para os usuários para ajudar os participantes a colocar tudo para funcionar. Um e-mail de boas vindas com um link para o portal de autoatendimento pode ajudar as pessoas a se tornarem mais produtivas mais rápido.

5. Compartilhamento de custos

Reduzir custos é um dos principais benefícios do BYOD, em que as pessoas pagam parte ou todo o custo de vários dispositivos pessoais usados para o trabalho. Um estipêndio oferecido pelas empresas normalmente varia entre 18% e 20% do custo do dispositivo. Os participantes devem estar cientes de que qualquer estipêndio é tratado como receita para fins fiscais Em regiões com maiores taxas de imposto de renda pessoal, você pode querer aumentar o estipêndio de acordo para manter o subsídio líquido consistente para todos os participantes.

Se você optar por fornecer um subsídio, isso deve refletir a vida total da participação de cada indivíduo. Os subsídios devem ser renovados em intervalos regulares para garantir que os dispositivos pessoais não ultrapassem o que seria esperado para um dispositivo empresarial Se um participante sair da empresa durante um ciclo de BYOD, talvez seja necessário recuperar uma parte do estipêndio.

Lembre-se de que o compartilhamento de custos tem implicações ao apresentar seu programa BYOD à organização. Um lançamento feito de uma vez só pode aumentar os custos conforme as pessoas se inscrevem - e reivindicam seus pagamentos - em todos os pontos do ciclo de atualização do endpoint. Oferecer o programa às pessoas à medida que elas chegam ao fim do ciclo de vida de seus dispositivos espalhará o impacto. Por outro lado, as organizações que não oferecem um estipêndio podem incentivar a participação total desde o primeiro dia.

Além disso, qualquer política BYOD, com ou sem compartilhamento de custos, deve esclarecer quem pagará pelo acesso à rede fora do firewall corporativo, seja por meio de uma rede móvel, Wi-Fi pública ou banda larga doméstica.

6. Segurança e conformidade

Um requisito crucial para dispositivos de propriedade de funcionários e da empresa é proteger os dados sem afetar a experiência do usuário. Para programas que permitem aplicativos e dados pessoais em dispositivos usados para o trabalho, o gerenciamento de aplicativos móveis (MAM) permite manter os aplicativos e dados pessoais e corporativos separados do conteúdo corporativo.

Instalar aplicativos corporativos em dispositivos pessoais aumenta o risco. Mas, uma estratégia que combina gerenciamento unificado de endpoints, virtualização de aplicativos e desktops e compartilhamento seguro de arquivos torna isso desnecessário. As informações corporativas permanecem seguras em seu datacenter ou nuvem. E, nos casos em que os dados precisem residir no dispositivo móvel, você pode proteger os dados da empresa por meio de mecanismos de conteinerização, criptografia e apagamento remoto. Você também pode desativar a impressão ou o acesso ao armazenamento do lado do cliente, como unidades locais e armazenamento USB.

Você pode controlar e proteger o acesso a aplicativos e dados com políticas baseadas na propriedade, no status ou no local do dispositivo. Inscreva e gerencie qualquer dispositivo, defina os requisitos de senha, detecte dispositivos jail-broken e faça uma limpeza completa ou seletiva de um dispositivo que esteja fora de conformidade, tenha sido perdido ou roubado ou que pertença a um funcionário ou contratado que foi embora. Garanta a segurança dos aplicativos por meio de acesso seguro por meio de túneis de aplicativos, listas negras, listas de permissões e políticas dinâmicas e sensíveis ao contexto.

Para proteger sua rede, você pode aplicar a tecnologia NAC (controle de acesso à rede), que autentica as pessoas que se conectam à rede e verifica se os dispositivos têm antivírus e patches de segurança atualizados.

Fora do firewall, a virtualização e a criptografia podem diminuir a maioria das vulnerabilidades de segurança de Wi-Fi, criptografia WEP, acesso sem fio, 3G/4G e outros métodos de acesso do consumidor. Os recursos de segurança de rede fornecem visibilidade e proteção contra ameaças móveis internas e externas; bloqueio de dispositivos desonestos, usuários não autorizados e aplicativos não compatíveis; e a integração com sistemas de informação de segurança e gerenciamento de eventos (SIEM).

No caso de um participante BYOD sair da organização, ou se a política relevante for violada ou um dispositivo de propriedade pessoal for perdido ou roubado, a TI deve ter um mecanismo para encerrar o acesso instantaneamente a dados e aplicativos, inclusive o desprovisionamento automático de contas SaaS relacionadas ao trabalho e apagamento seletivo de dispositivos perdidos. Essa funcionalidade também é essencial para dispositivos COPE ou CYOD, possibilitando a realocação de um dispositivo corporativo para um novo usuário sem a possibilidade de que os dados deixados no dispositivo caiam nas mãos de um usuário que não tenha autorização para acessá-los.

Em vez de permitir um BYOD aberto, no qual as pessoas podem trazer qualquer dispositivo para acessar aplicativos e dados corporativos, algumas organizações escolhem uma abordagem gerenciada Nesse cenário, a TI gerencia o dispositivo de propriedade pessoal diretamente, inclusive registro, validação, autorização e acesso a recursos do dispositivo.

7. Monitoramento e gerenciamento

O monitoramento e o gerenciamento contínuos são essenciais para garantir a conformidade com as políticas e determinar seu retorno sobre o investimento.

Algumas soluções UEM aumentam a produtividade e a eficácia da TI automatizando vários aspectos de monitoramento e gerenciamento, como a especificação das ações a serem tomadas em resposta a várias violações. Estes podem incluir totalmente ou seletivamente: limpar o dispositivo, definir o dispositivo como fora de conformidade, revogar o dispositivo ou enviar uma notificação ao usuário para corrigir um problema dentro de um certo limite de tempo - por exemplo, remover um aplicativo que está na lista negra - antes que uma ação mais severa seja tomada.

8. Suporte e manutenção de dispositivos

Um programa BYOD geralmente reduz a manutenção de TI necessária para cada dispositivo porque o usuário também é o proprietário. A política deve explica detalhadamente como várias tarefas de suporte e de manutenção serão abordadas e pagas para evitar maior complexidade e carga de trabalho para a TI. Na maioria dos programas CYOD ou COPE, a TI é totalmente responsável pelo suporte e manutenção de dispositivos.

Como o Citrix Workspace permite o gerenciamento seguro de dispositivos

Qualquer programa de gerenciamento de dispositivos deve incluir tecnologias que deem acesso seguro a aplicativos e arquivos corporativos em dispositivos pessoais. O Citrix Workspace inclui todos os principais recursos necessários para tornar o BYOD, o CYOD e o COPE simples, seguros e eficazes para qualquer organização. Ele combina gerenciamento unificado de endpoints, virtualização de aplicativos e de desktops Windows, compartilhamento seguro de arquivos e entrega de aplicativos para que você possa disponibilizar aplicativos e dados corporativos em qualquer dispositivo que as pessoas usem para trabalhar, mantendo a segurança e o controle.

Unified Endpoint Management (Gerenciamento de pontos de extremidade unificado)

Obtenha provisionamento e controle baseados em identidade de aplicativos, dados e dispositivos, des-provisionamento automático de contas para usuários que foram embora e apagamento seletivo de dispositivos perdidos. O Citrix Workspace não só permite gerenciar dispositivos, inclusive a IoT, mas também possibilidade segurança e controle no nível dos aplicativos para que você possa proteger os dados corporativos sem afetar o uso de conteúdo pessoal em dispositivos BYOD, CYOD ou COPE O gerenciamento de endpoints do Citrix Workspace permite que você escolha qual estratégia do MAM é melhor para você, MAM de plataforma, como Samsung KNOX ou Appconfig, Citrix MDX (que fornece um nível adicional de criptografia de aplicativos sem inscrição de dispositivo) ou Intune MAM.

Virtualização de desktop e aplicativos Windows

Em vez de instalar e gerenciar aplicativos e desktops Windows em cada dispositivo individual, você pode entregá-los como serviços on-demand disponíveis em qualquer dispositivo. Como os aplicativos e dados são gerenciados em um datacenter ou nuvem, a TI mantém a proteção centralizada de dados, conformidade, controle de acesso e administração de usuários tão facilmente em dispositivos pessoais quanto em corporativos - dentro do mesmo ambiente unificado.

Loja de aplicativos

Dê às pessoas acesso com um único clique a aplicativos móveis, Web, SaaS, corporativos e Windows a partir de uma loja de aplicativos unificada. Independente do dispositivo escolhido pelas pessoas, computadores Windows ou Mac, iOS, Android ou produtos móveis baseados em Windows ou Google Chromebooks, a experiência do usuário é a mesma em todos os dispositivos, locais e redes.

Acesso seguro

Uma estrutura de gerenciamento unificada permite que a TI proteja, controle e otimize o acesso a aplicativos, desktops e serviços em qualquer dispositivo, junto com auditoria e relatórios para dar suporte à conformidade e à proteção de dados. Somente a Citrix oferece uma micro-VPN exclusiva para proteger ainda mais os dados dos aplicativos entre o dispositivo móvel e os recursos corporativos por trás do firewall.

Compartilhamento de arquivos seguros

As pessoas podem compartilhar e colaborar de maneira segura seus arquivos com qualquer pessoa dentro ou fora da organização, além de sincronizar arquivos entre dispositivos. O controle de acesso baseado em políticas, auditoria, relatórios e o apagamento remoto de dispositivos ajudam a manter o conteúdo corporativo seguro.

Com as políticas e as tecnologias certas, você pode equilibrar a liberdade de escolha dos funcionários com segurança e controle para TI. Saiba mais sobre como o Citrix Workspace pode ajudá-lo a tornar o gerenciamento de dispositivos simples e seguro no site www.citrix.com/workspace

Vendas corporativas
América do Norte | 800-424-8749
Mundial | +1 408-790-8000

Escritórios
Matriz | 851 Cypress Creek Road Fort Lauderdale, FL 33309 United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054 United States