TRANSFORMAÇÃO DIGITAL NAS EMPRESAS:

COLABORADORES 2.0

TELECOM

ÍNDICE

INTRODUÇÃO 3
O NOVO PARADIGMA 6
SEGURANÇA E SUPORTE 11
DA TEORIA À PRÁTICA 16
A RESPOSTA AO PROBLEMA 21
CONCLUSÃO 24
SOBRE A AR TELECOM 26

INTRODUÇÃO

A tecnologia revoluciona tudo onde toca – e o conceito de posto de trabalho não é exceção. As organizações têm de se adaptar a esta nova realidade, e devem fazê-lo em duas importantes frentes: Mitigando os riscos de privacidade e segurança que o acesso anytime, anywhere dos colaboradores à informação digital representa; e prestando-lhes o devido suporte para antecipar problemas como a fuga de informação, a quebra de sigilo ou danos reputacionais.

Segundo a IDC, o número de colaboradores com mobilidade no território nacional em 2018 ultrapassa os 2,8 milhões de pessoas. Ou seja, 64% da população ativa em Portugal não tem uma forma de trabalhar que se possa considerar fixa, valor que se traduz numa taxa de crescimento anual média de 6,7% face ao período homólogo anterior.

Também a IDC, através do seu estudo DX MaturityScape que analisa o estado de maturidade da transformação digital nas empresas, estima que 75% das organizações que sobrevivam nos próximos 10 anos conhecerão então o sucesso neste capítulo.

Isto significa uma coisa: A transformação digital é cada vez mais uma certeza, seja por força da revolução dos negócios, seja por força da revolução dos colaboradores – também eles cada vez mais móveis e digitais.

Um dos melhores indicadores da transformação digital das organizações é a cada vez maior substituição das ferramentas de trabalho de filosofia estática (on-premises) por soluções modernas baseadas na cloud. Isso é bem visível no cada vez menor número de meios informáticos tradicionais que vemos nas mesas. São cada vez menos os computadores de secretária e cada vez mais os laptops, tablets e smartphones.

Esta revolução ao nível da mobilidade corporativa traz evidentes benefícios ao negócio, mas obriga a que o conceito de perímetro de segurança tradicional seja revisto. Tudo o que está dentro de portas é fácil de trancar e controlar, mas cada dispositivo móvel ligado à rede ou que transporte informação corporativa representa um risco isolado que pode comprometer a integridade do bem comum.

Os riscos e desafios são de vária ordem:

As empresas digitais devem encontrar o ponto de equilíbrio entre os benefícios que os equipamentos móveis podem oferecer e o reconhecimento de que esses mesmos dispositivos se tornaram um ponto de ataque atraente para o cibercrime.

Cabe ao CIO encontrar uma forma de ultrapassar estas questões e garantir o melhor proveito para a empresa sem prejudicar o colaborador nem afetar o seu potencial desempenho, encarando os dispositivos móveis como equipamentos integrados nas suas políticas corporativas de suporte aos utilizadores.

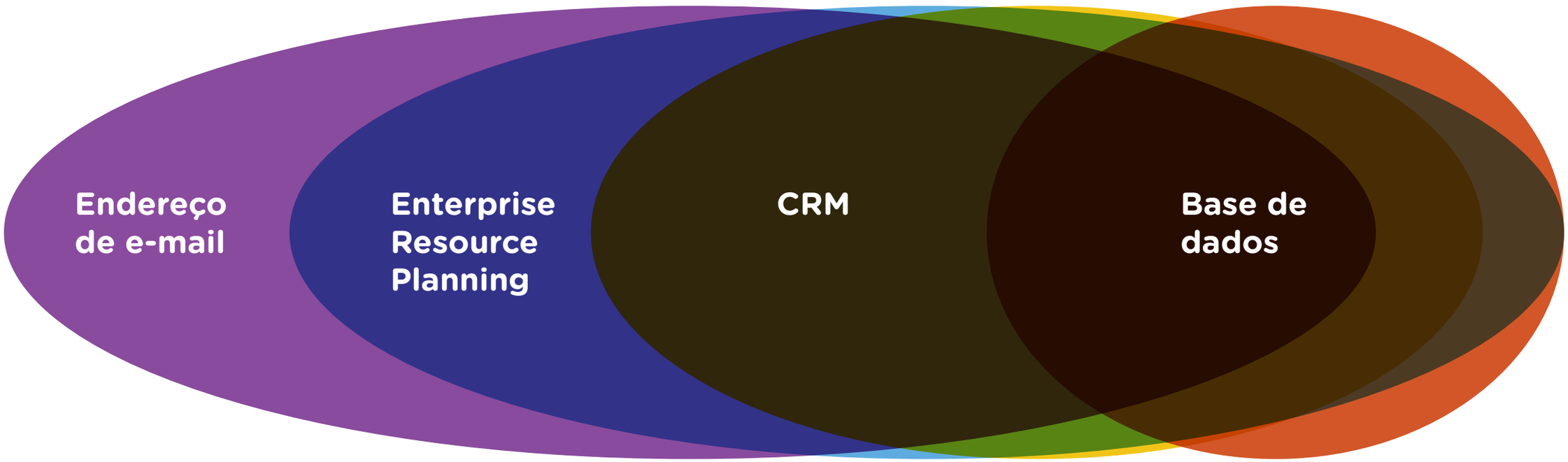
O NOVO PARADIGMA

As empresas já não são unidades estanques e isoladas. São organismos cada vez mais abertos e participativos, onde os negócios se desenvolvem a alta velocidade e os colaboradores trabalham em constante movimento por todo o mundo, precisando de ter um meio online que lhe garanta acesso anytime, anywhere à rede corporativa e às suas ferramentas de trabalho. Vejamos este novo paradigma em cinco pontos fundamentais.

REALIDADE

As TI já não se aplicam apenas das portas das empresas para dentro. Devem estar sempre ao lado dos colaboradores quando estão em reunião num cliente, em viagem profissional, a trabalhar a partir de casa ou num espaço de coworking. O espaço de trabalho já não se resume a uma simples secretária – aliás, o seu ambiente de trabalho é hoje cada vez mais dinâmico e heterogéneo.

Sendo inevitável esta aposta na mobilidade, regista-se uma tendência crescente do Bring Your Own Device – ou BYOD –, que como o nome sugere traduz-se na aceitação na rede informática do dispositivo móvel do próprio colaborador enquanto ferramenta no seu local de trabalho, usando-a para obter acesso privilegiado a recursos da empresa, nomeadamente os mais habituais:



Esta medida permite reduzir custos financeiros para a organização, mas levanta obviamente riscos de segurança. Todavia, a compra de dispositivos móveis a operadores de comunicações também não resolve o problema da gestão dos dispositivos móveis e de suporte, nem tão pouco ajuda no apoio técnico aos colaboradores.

A mobilidade traz mais liberdade aos colaboradores, mas também lança ao CIO e às equipas de TI maiores desafios à proteção e segurança. Se antes se seguia uma estratégia de proteção pelo perímetro físico da empresa, agora há que estudar a segurança e a proteção de informação em dispositivos que entram e saem das suas instalações ficando totalmente fora desses perímetros bem estabelecidos.

DESAFIO

Com acesso permanente à Internet, e com as suas ferramentas de trabalho sempre à mão através de apps dedicadas ou via cloud, os colaboradores podem agora trabalhar a partir de qualquer espaço, hora e lugar. Para isso, precisam de soluções 100% funcionais (sejam elas de terceiros ou criadas à medida) e 99,999% disponíveis. No entanto, isto também significa que têm acesso a redes sociais e outras formas de entretenimento e diversão pessoal.

Isto representa um maior desafio para as empresas. As soluções de segurança utilizadas que anteriormente se aplicavam continuam a fazer sentido, mas devem ser reforçadas – desde os antivírus ao URL filtering, passando pela encriptação de dados e pelas políticas de segurança – de modo a adaptarem-se à proteção dos dispositivos móveis dos colaboradores.

AMEAÇA

As políticas de gestão de TI devem ser capazes de controlar os computadores e outros aparelhos pessoais móveis que são usados pelos funcionários dentro de todo o ambiente corporativo. Caso contrário, a empresa pode ficar exposta a uma série de ameaças digitais e de fuga de informação.

No caso do BYOD, embora traga avanços significativos nos negócios ao incutir maior produtividade aos funcionários pelo uso da própria tecnologia no trabalho, poderá resultar em sérias violações das políticas de segurança corporativas.

Outra questão que urge ponderar é o facto de ser muito mais fácil e frequente a perda de um smartphone ou de um portátil do que a perda dos tradicionais equipamentos informáticos, como os volumosos computadores desktop.

O FATOR HUMANO

O novo paradigma não funciona se os colaboradores não se sentirem envolvidos. Efetivamente, os utilizadores terão de se adaptar a uma nova realidade, sendo que uns conseguirão fazê-lo mais facilmente do que outros – a grande verdade é que ninguém nasce ensinado. Isto faz levantar uma outra necessidade: a de formar e consciencializar os colaboradores para os riscos envolvidos com este novo paradigma. Nesta matéria, evite cometer estes cinco erros cruciais:

- **Permitir que tragam qualquer tipo de dispositivo**
- **Deixar pouco claro que tipos de apps é permitido usar**
- **Não comunicar internamente questões como a monitorização**
- **Subestimar a importância da proteção por palavra-passe**
- **Não dar o apoio e formação necessários ou quando solicitados**

Outra boa dica: Procure obter feedback dos colaboradores para garantir que a sua estratégia está a cumprir os objetivos. Por exemplo, pergunte-lhes diretamente se estão satisfeitos com o programa de formação, se gostariam de adicionar mais dispositivos à lista autorizada ou se têm alguma dúvida ou preocupação que deva ser devidamente abordada.

ENQUADRAMENTO LEGAL

A implementação do Regulamento Geral de Proteção de Dados (RGPD) fez com que os requisitos de segurança sobre os dados pessoais se tornassem ainda mais exigentes. Por exemplo, caso as políticas de gestão das TI não sejam capazes de controlar os computadores e outros aparelhos pessoais móveis que estiverem a ser utilizados pelos funcionários dentro do ambiente corporativo, a empresa pode ficar exposta a uma série de ameaças digitais e de fuga de informação, com consequentes repercussões a nível reputacional e também possivelmente coimas ou sanções impostas por via da legislação.

SEGURANÇA E SUPORTE

OS CIOs também têm de olhar para estes dispositivos móveis, como a área de IT olha para os postos de trabalho, já que a complexidade no suporte ao utilizador é crescente e multi-device. Esta nova realidade tem que ser vista numa perspectiva de suporte a devices e não só como suporte a utilizadores

Assim, as TI devem encarar o suporte a dispositivos móveis como parte integrante do plano de suporte ao utilizador de todo o seu parque informático.

Esta tendência é praticamente imparável e já está aliás em prática em muitas organizações – cabe-lhe a si, na qualidade de CIO, abordar o problema da sua empresa de uma forma o mais prática possível. As cinco questões que se seguem resumem uma boa forma de colocar em prática as políticas, os procedimentos e as soluções para ajudar a reduzir os riscos.

COMO GARANTIR A SEGURANÇA DOS DADOS?

Uma das principais razões para as empresas resistirem à introdução de dispositivos móveis nas suas redes informáticas prende-se com preocupações de segurança – e isso é absolutamente uma preocupação válida. Todos nos lembramos no passado de ameaças como o WannaCry e outros ataques cibernéticos, que tiraram proveito de vulnerabilidades conhecidas e deixaram bastante claro que os utilizadores nem sempre cumprem a sua parte no que concerne a instalar atualizações e patches de segurança. Se a isto juntarmos softwares críticos, como antivírus ou antimalware, o risco pode aumentar para um nível de tal forma alarmante que as equipas de TI acabarão por não ter controlo sobre os dispositivos pessoais dos funcionários.

Urge manter os endpoints em segurança. Os colaboradores estão a ligar-se via redes Wi-Fi não protegidas? Usam links potencialmente maliciosos nas redes sociais? Os seus familiares usam esse mesmo dispositivo? Se não tiver medidas em vigor para precaver todos estes cenários, basta uma resposta afirmativa a uma destas três perguntas para poder comprometer a sua rede ou os seus dados corporativos.

Por exemplo, uma das formas mais simples de aumentar a segurança é garantir que todos os dados corporativos são armazenados num data center seguro e não nos endpoints individuais, mantendo assim os dados do endpoint isolados quando estiverem a ser acedidos localmente.

AS APPS EMPRESARIAIS CRÍTICAS FUNCIONARÃO NORMALMENTE NOS DISPOSITIVOS?

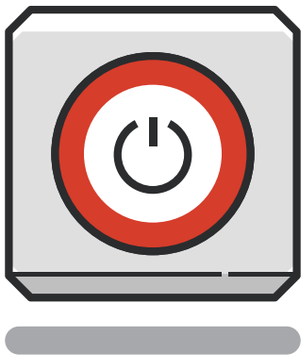
O aumento da produtividade é um dos objetivos da introdução de dispositivos móveis como motor da transformação digital do posto de trabalho, razão pela qual as apps essenciais para o negócio terão de funcionar no dispositivo escolhido pelo (ou atribuído ao) funcionário – mesmo que apenas um colaborador use um dispositivo iOS enquanto todos os outros usam Windows.

É aqui – ao nível das várias versões de sistemas operativos – que a questão pode tornar-se mais profunda e complicada. Por exemplo, se uma aplicação legacy não for compatível com a atualização mais recente do sistema, os utilizadores poderão de repente simplesmente deixar de conseguir aceder a uma app com a qual estavam a trabalhar no dia anterior, e tudo isto por causa de algo aparentemente tão simples e inocente como são as atualizações de SO recomendadas para o dispositivo.

Por isso, e antes de permitir que os funcionários optem por um programa de BYOD, assegure-se de que tem uma lista bem documentada de apps e respetivos requisitos de dispositivo ou de sistema operativo, ou se há uma solução que resolva os problemas de compatibilidade conhecidos.

QUE RESPONSABILIDADES CABEM ÀS TI?

No caso de os dispositivos serem atribuídos pela empresa, fica evidentemente claro quem é responsável pela resolução de problemas: O CIO e a sua equipa de TI. No caso do BYOD a resposta recai numa área cinzenta. Se o dispositivo de um colaborador não estiver a funcionar, ele acaba por não ser produtivo. Ora, sendo o dispositivo de propriedade pessoal é responsabilidade das TI resolver o problema? E serão as TI responsáveis pelas correções e atualizações das apps?



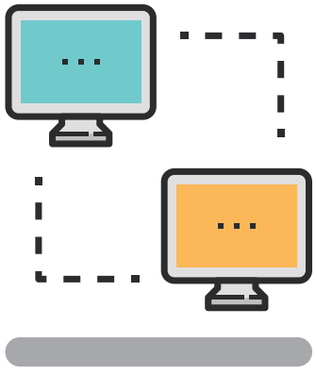
As perguntas são muitas e de vária ordem, pelo que é fundamental que existam políticas escritas e ferramentas apropriadas na gestão de dispositivos móveis que disponibilizem às TI respostas para quando houver confronto com estas questões. As políticas também devem deixar claras as expectativas para os utilizadores, para que eles compreendam que as TI podem abordá-los e irão fazê-lo quando for necessário controlar o dispositivo pessoal do funcionário ao ser utilizado no seio da empresa. Um exemplo simples deste poder é obrigar à remoção de software não autorizado ou que consuma demasiados recursos.

Um exemplo simples é a área de IT das Organizações, passar a disponibilizar um Store APP para as únicas aplicações que podem ser instaladas nos dispositivos de forma segura e controlar a atualização de sistema operativo no equipamento assim como a forma deste mesmo se conectar de forma segura às APPs oficiais da organização.

E SE O DISPOSITIVO DE UM COLABORADOR NÃO ESTIVER A FUNCIONAR?

Se o colaborador estiver a usar um dispositivo atribuído pela empresa, as TI simplesmente têm de lidar com esse equipamento defeituoso e fornecer ao utilizador um dispositivo de substituição, seja esta temporária ou permanente. Dependendo do tipo de trabalho que estiver em questão, convém que exista um plano de backup de dados em ação e que seja feito regularmente – só assim o colaborador poderá aceder aos seus documentos e aplicações na nova área de trabalho tal como fazia até então com a ferramenta de trabalho anterior.

Já se o colaborador estiver a usar o seu próprio dispositivo, a situação poderá ser diferente. A empresa tem dispositivos de backup disponíveis? Com que rapidez se deve esperar que o utilizador substituía um laptop que deixou de funcionar? E o que é que acontece quando ele deixar a empresa? Pode sair do programa BYOD e receber rapidamente um dispositivo da empresa?



Mais uma vez, todas estas questões devem ser contempladas minuciosamente nas políticas para que não haja impacto negativo na produtividade dos colaboradores – logo, da empresa.

COM QUE FREQUÊNCIA SE DEVE REVER A EFICÁCIA DAS POLÍTICAS?

A tecnologia evolui a um ritmo muito rápido. É imperativo que as políticas de transformação digital do posto de trabalho se tornem documentos vivos e com tecnologia de gestão dos mesmos de vanguarda e que sejam analisadas e atualizadas regularmente. Recomendamos que crie uma política que defina expectativas, que descreva como os cenários serão abordados e que incorpore um cronograma com revisões regulares de modo a garantir que essa política permanecerá atualizada e eficaz, dentro do seu Service Desk interno ou externo.

Se o BYOD é algo de novo para a empresa, é melhor começar com um programa piloto limitado antes de lançar a política para a empresa como um todo. Desta forma, dará tempo à organização para solucionar problemas, ajustar a política conforme necessário e consolidar as melhores soluções de segurança antes que uma grande quantidade de dados corporativos possa ser colocada em risco.

Mesmo depois de a política ser implementada, urge certificar de que ela é regularmente revista juntamente com as principais partes interessadas, incluindo gestores de linhas de negócios, executivos e membros das equipas de TI e de segurança da empresa. Esta vasta amplitude de inputs dará à organização a capacidade de abordar quaisquer preocupações sob um ponto de vista holístico, em vez de resolver um problema criando outro.

DA TEORIA À PRÁTICA

Seguir um conjunto de práticas recomendadas e ter uma boa ferramenta de Mobile Device Management (MDM) é meio caminho andado para garantir uma transição digital de sucesso.

Inclua na sua atual equipa de ServiceDesk o suporte a dispositivos móveis na sua plenitude.

CONSULTE A CHECKLIST DE 10 PASSOS QUE PREPARÁMOS PARA SI, E NÃO SE ESQUEÇA DE ADOPTAR UMA BOA FERRAMENTA DE MDM

1. CRIE POLÍTICAS CLARAS.

É importante garantir que as políticas sejam bem percetíveis para os colaboradores, de modo a que estes entendam como podem ou não usar os seus dispositivos corporativos. Não se esqueça de abordar possíveis riscos de segurança e privacidade – lembre-se sempre que esses dispositivos são utilizados não só para fins profissionais, mas também para fins pessoais e de lazer.

2. REÚNA FEEDBACK INTERNO

Ouça primeiro departamentos tão importantes como os Recursos Humanos ou o Jurídico e estabeleça depois os riscos e os requisitos, colocando sempre a segurança à frente de qualquer decisão que venha a tomar. Não se esqueça de que as partes interessadas terão sempre diferentes necessidades e expectativas. Saiba o que têm a dizer e procure obter este importante apoio antes de definir a estratégia.

3. PREPARE UM PLANO DE AÇÃO

Mesmo que todos os dispositivos estejam protegidos e seguros, tenha sempre uma resposta preparada para o pior cenário: a probabilidade de violação de dados ou de ataque. Este plano de ação deverá contemplar não só a recomendada imposição de atualizações regulares de software e aplicações, como também o recurso a soluções mais radicais que permitam fazer a limpeza remota de dispositivos perdidos.

4. NÃO CORRA RISCOS DE SEGURANÇA

Usar apenas palavras-passe não chega para proteger os dados da empresa. Faça uma avaliação de risco para identificar quaisquer perigos que possam advir também dos ambientes móveis. Certifique-se de que as redes estão seguras, as passwords são alteradas periodicamente e os backups feitos regularmente, e monitorize as suas redes constantemente para detetar possíveis ameaças.

5. ATENÇÃO AOS DISPOSITIVOS A AUTORIZAR

Sabemos hoje que uns dispositivos podem ser mais seguros do que outros, e por isso poderá compensar que seja a própria empresa a adquirir dispositivos que possam ser melhor monitorizados e mantidos protegidos e em segurança. No entanto, uma grande parte dos colaboradores acabará por usá-los também nas suas vidas pessoais, o que poderá torná-los ligeiramente vulneráveis.

6. SEPARE TRABALHO E LAZER

Pondere por isso criar uma blacklist de aplicações proibidas ou uma whitelist com as apps que deseja permitir, podendo neste caso restringir a utilização apenas aos colaboradores devidamente autorizados e com diferentes tipos de permissões. Importante: Nunca monitorize o uso pessoal para proteger a privacidade do colaborador e adie ao máximo bloquear o acesso a redes sociais e sites como o YouTube, especialmente se o colaborador tiver um bom desempenho.

7. APOSTE NA MONITORIZAÇÃO

Na parte profissional considere usar sistemas que rastreiem quem está a usar o quê e para que fim. Veja isto como uma forma de simplificar a segurança na sua rede, inclusive pela colocação de dados e aplicações corporativas confidenciais em contentores seguros de dados. Por exemplo, ao separar dados pessoais e comerciais será mais fácil controlar e definir políticas específicas para cada um dos âmbitos.

8. FATOR HUMANO VS. TECNOLÓGICO

Implemente níveis de acesso adequados ao papel de cada colaborador na organização. E seja flexível, pois a variedade de plataformas móveis disponíveis irá tornar a integração complexa. Se tem sistemas legacy, substitua-os para garantir compatibilidade e suporte. Não menos importante: Reavalie as suas políticas regularmente para garantir que a sua organização não fica para trás.

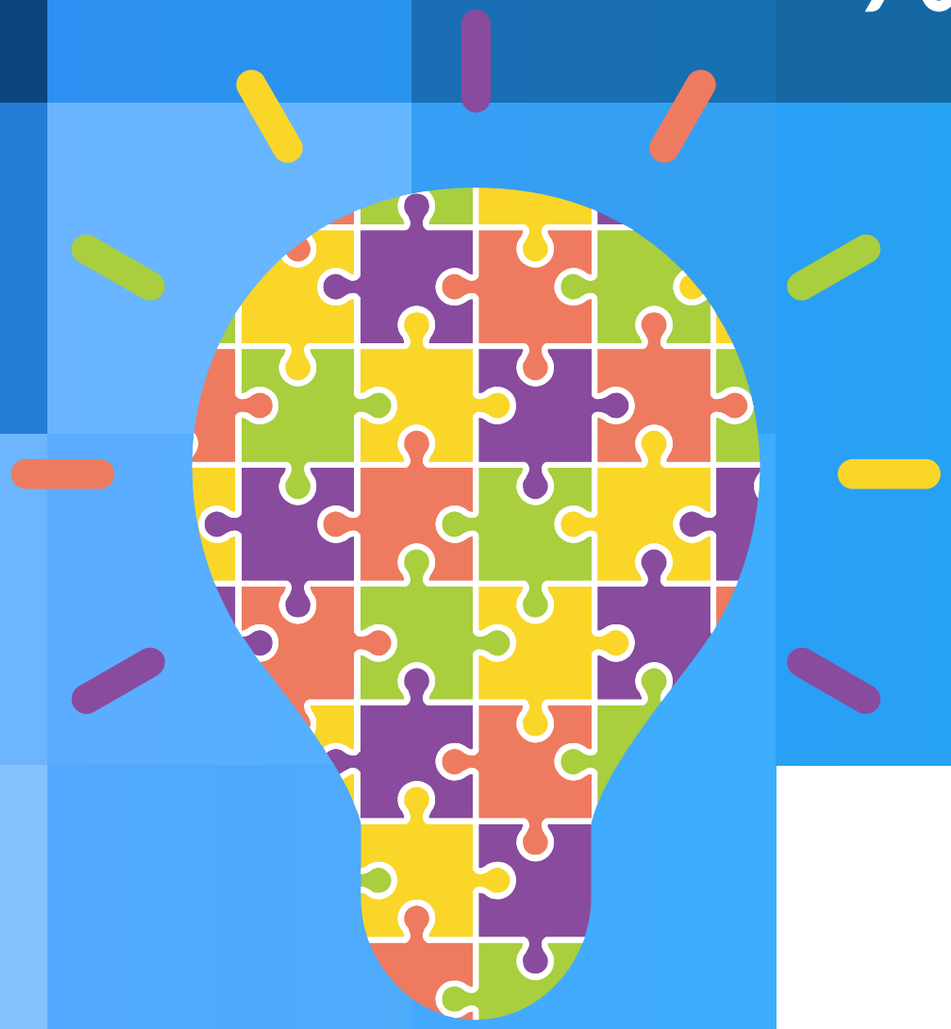
9. DAR LUGAR À FORMAÇÃO

Os colaboradores devem estar sempre o mais e melhor informados sobre quaisquer riscos de segurança. Desde a segurança básica do smartphone (downloads e palavras-passe) até aos riscos impostos pela introdução de dispositivos externos e pela integração com a Internet das coisas (IoT), passando pelo uso de códigos PIN fortes, redes seguras e encriptação de dados, deverão estar cientes dos perigos.

10. DEFINA A ESTRATÉGIA DE SAÍDA

Quando um colaborador sair da organização, certifique-se de que é feita a eliminação dos dados corporativos em quaisquer dispositivos usados profissionalmente. Isto inclui a desativação de emails e contas desse colaborador na empresa, a limpeza de dispositivos (atribuídos pela empresa ou pessoais) e o cancelamento definitivo de acesso a quaisquer dados confidenciais e protegidos.

A RESPOSTA AO PROBLEMA



As empresas e organizações têm de se adaptar a esta nova realidade. Para isso, devem apostar em soluções igualmente criativas e personalizáveis que se adequem tanto às suas necessidades de proteção da empresa como dos seus colaboradores, tudo isto sem restringir a sua mobilidade.

Muitas empresas ponderam – e bem – externalizar estes serviços de TI a um parceiro de confiança, contratualizando níveis de SLA que garantam rácios de qualidade e cumprimento à altura dos desafios e exigências que os negócios impõem.

A Ar Telecom tem a capacidade de prestar este suporte e proteção, independentemente dos dispositivos utilizados. Através dos seus serviços de End User Support, disponibiliza suporte 24 horas por dia aos utilizadores e aos seus equipamentos, incluindo dispositivos móveis.

SERVICE DESK

Partindo do tradicional e sobejamente conhecido conceito de Help Desk para resolução das questões levantadas diretamente pelo utilizador, o Service Desk permite ir mais além ao fazer uma eficiente gestão dos postos de trabalho e do atendimento, tudo isto seguindo as melhores práticas de implementação de acordo com as normas ITIL vigentes.

SUPORTE LOCAL OU REMOTO

Serviço de apoio informático aos utilizadores das empresas prestado no local remotamente, focado na satisfação e produtividade da organização. A oferta Ar Telecom foca-se nos processos essenciais que permitem a operação contínua das tarefas diárias do utilizador, fazendo uma gestão eficaz dos incidentes e dando resposta aos pedidos.

GESTÃO DE PLATAFORMAS

Prestação de serviços de suporte à criação, manutenção e certificação de imagens dos computadores instalados na rede informática. Inclui ainda a distribuição centralizada de software para os postos de trabalho, bem como Security Patching dos sistemas operativos e correção de vulnerabilidades e problemas de segurança que venham a surgir.

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

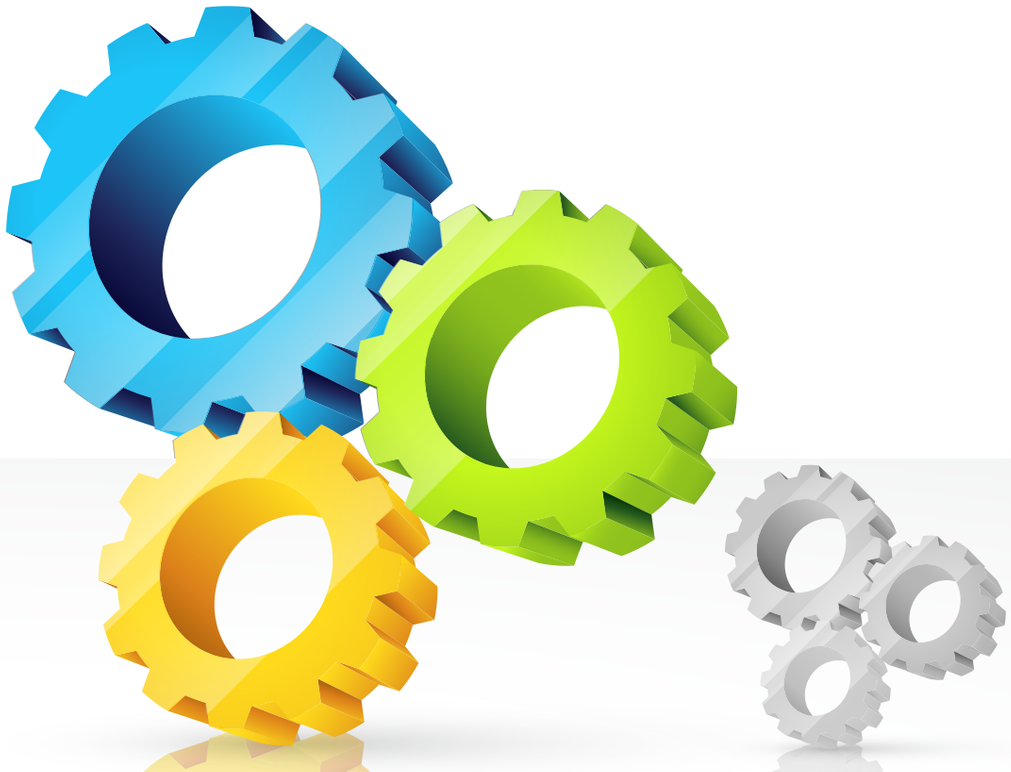
Integração de soluções de segurança (endpoints, perímetro, rede interna – SIEM – e integridade da informação), sempre oriundas de fabricantes líderes de mercado e tendo em conta as necessidades específicas do segmento empresarial. Esta visão integrada garante o usufruto de uma estratégia tecnológica coerente.

GESTÃO DOS SISTEMAS INFORMÁTICOS

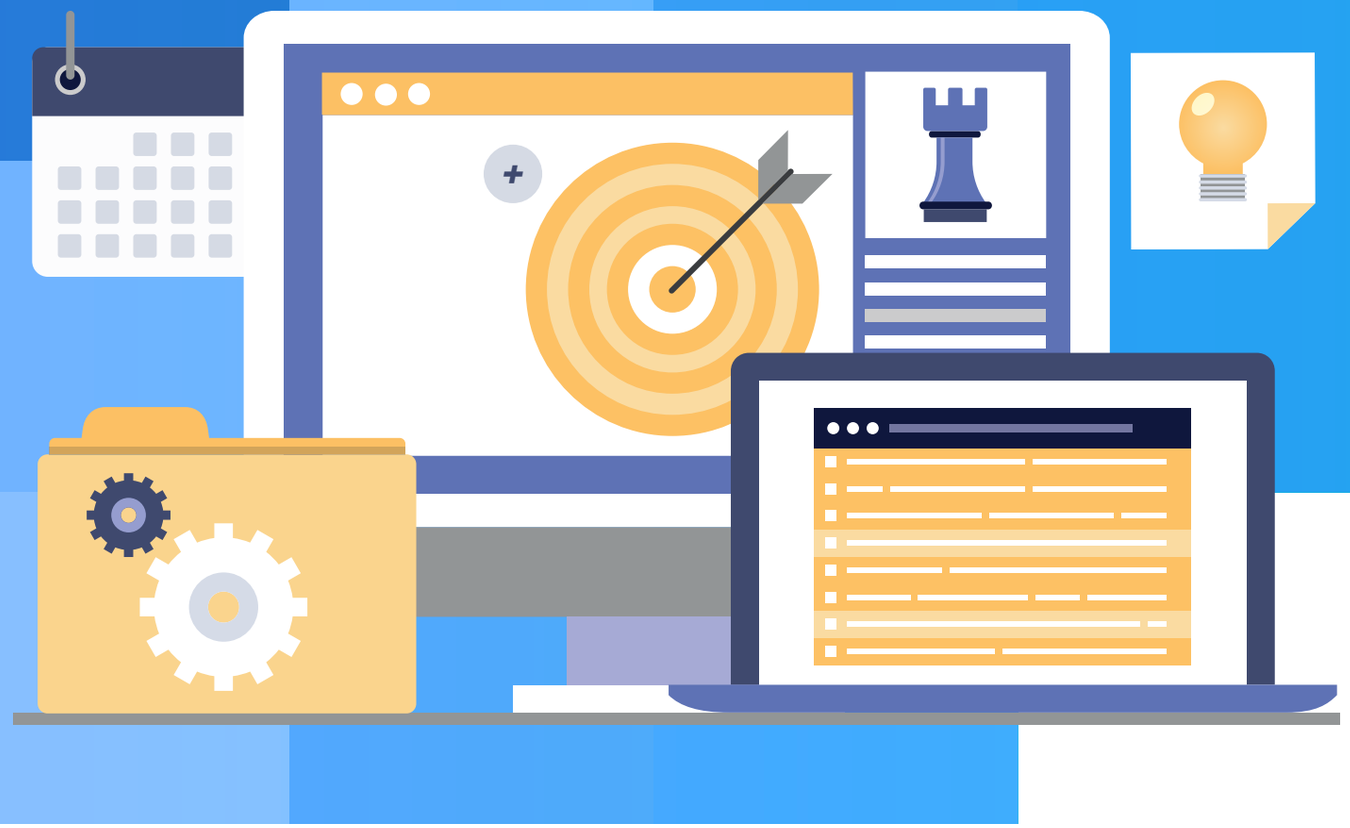
Independentemente da plataforma – seja ela cloud, server, database, groupware, middleware, storage ou networking –, a Ar Telecom dispõe das competências necessárias para monitorizar, operar e administrar sistemas e infraestruturas na cloud (pública, privada ou híbrida) ou nas instalações físicas do cliente (on-premises).

GESTÃO DE DISPOSITIVOS MÓVEIS

Os endpoints tradicionais são hoje muito mais do que computadores desktop Windows, Mac e Linux, podendo ter a forma de smartphones ou tablets baseados também em Android ou iOS. A Ar Telecom pode gerir todo este ecossistema de uma forma centralizada, rápida e segura, e sem impacto no desempenho do colaborador.



CONCLUSÃO



A oferta de End-User Services da Ar Telecom foca-se nos processos essenciais que permitem a operação contínua das tarefas diárias do utilizador, fazendo uma gestão eficaz dos incidentes e dando resposta aos pedidos em todos os dispositivos corporativos – sejam eles laptops, desktops, impressoras, telemóveis, tablets ou servidores.

Este é um passo necessário rumo a uma correta transformação digital do posto de trabalho, com evidentes benefícios para os colaboradores e para as organizações.

Ao adotar os serviços Ar Telecom, estará a usufruir da nossa vasta experiência e conhecimento em quatro áreas fundamentais: **Competências; Processos; Recursos e ferramentas; Analítica**.

As nossas soluções são desenhadas para proporcionar valor em 5 áreas críticas:

QUALIDADE

- Sistema de gestão da qualidade para prevenção de falhas
- Soluções de automação que minimizam erros humanos
- Processos, ferramentas e métricas implementadas com sucesso em vários clientes

EXPERIÊNCIA TÉCNICA E NA INDÚSTRIA

- Modelo de serviço com processo de melhoria contínua integrado na operação
- Equipas especializadas em diversas tecnologias
- Experiência na prestação de serviços de outsourcing

ADAPTABILIDADE E FLEXIBILIDADE

- Encargos em função dos recursos fornecidos
- Flexibilidade para alocar recursos em função das necessidades de picos de projeto

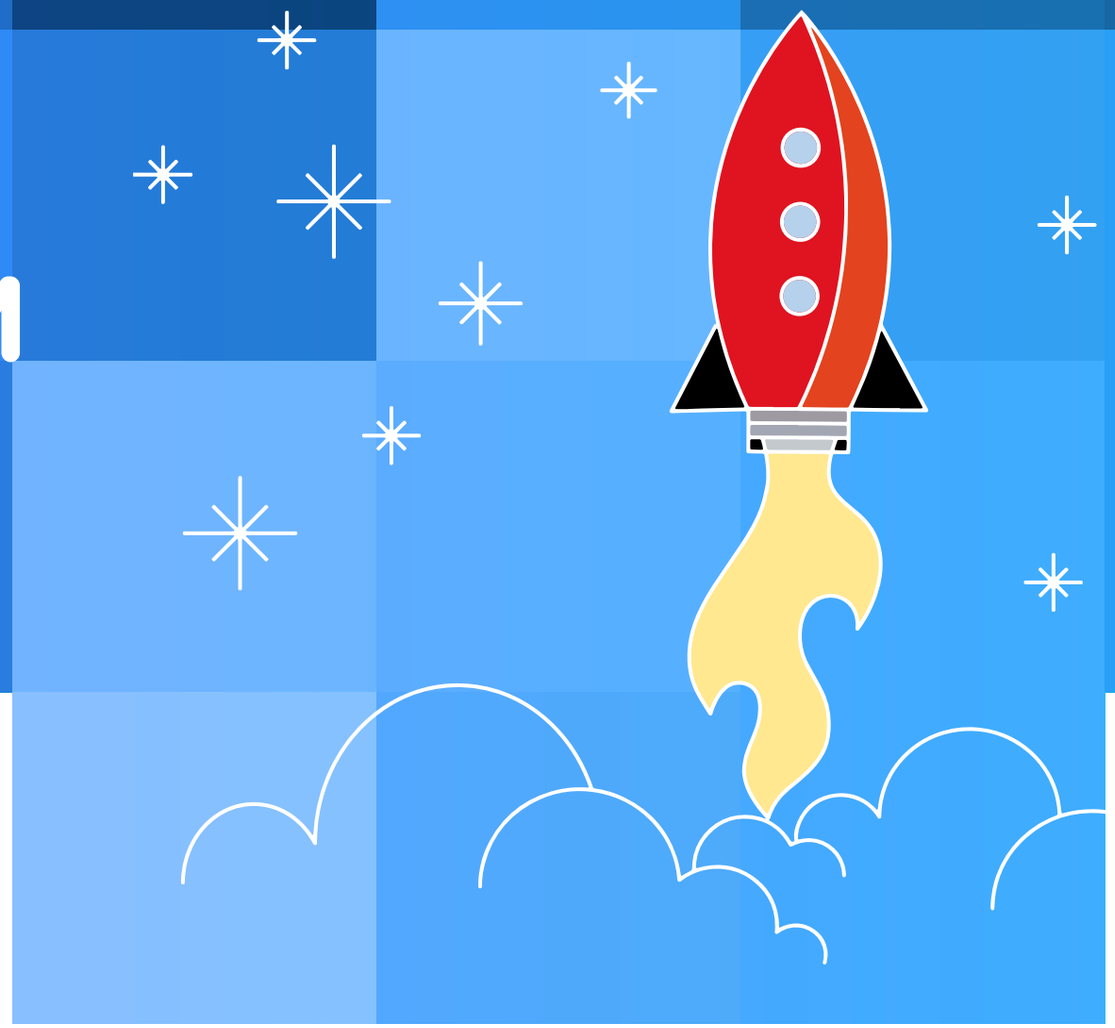
GESTÃO DE RISCO

- Equipas estendidas, com processos e ferramentas comuns, minimizam a dependência de recursos individuais
- Rede de alianças e parcerias com diversos fornecedores

BENEFÍCIO FINANCEIRO

- Experiência na otimização do serviço pela automação de atividades e aumento de qualidade, com consequente redução do volume de incidentes, através de melhoria contínua

SOBRE A AR TELECOM



Nascemos há 18 anos da ambição de transformar o setor das comunicações em Portugal. Somos uma empresa sólida, autónoma, responsável, orientada para o cliente e comprometida com o investimento contínuo em novas soluções. Merecemos a confiança dos nossos clientes, aos quais dedicamos uma lealdade incondicional que se reflete na sua satisfação e fidelidade.

Disponibilizamos uma oferta completa de soluções cloud e managed services, para que o departamento de TI de cada empresa se dedique a projetos estratégicos e que exigem recursos focados e dedicados.

O conhecimento das especificidades de cada setor de atividade, para melhor adequar as soluções às necessidades de cada cliente, é uma das garantias dadas pela Ar Telecom.

PRECISA DE AJUDA? ENTRE EM CONTACTO CONNOSCO!