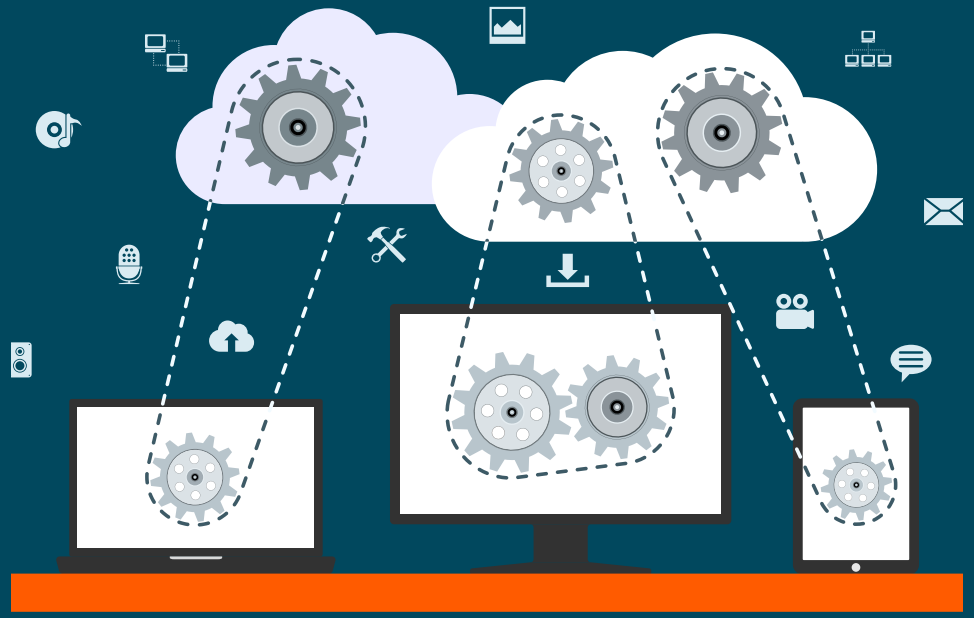
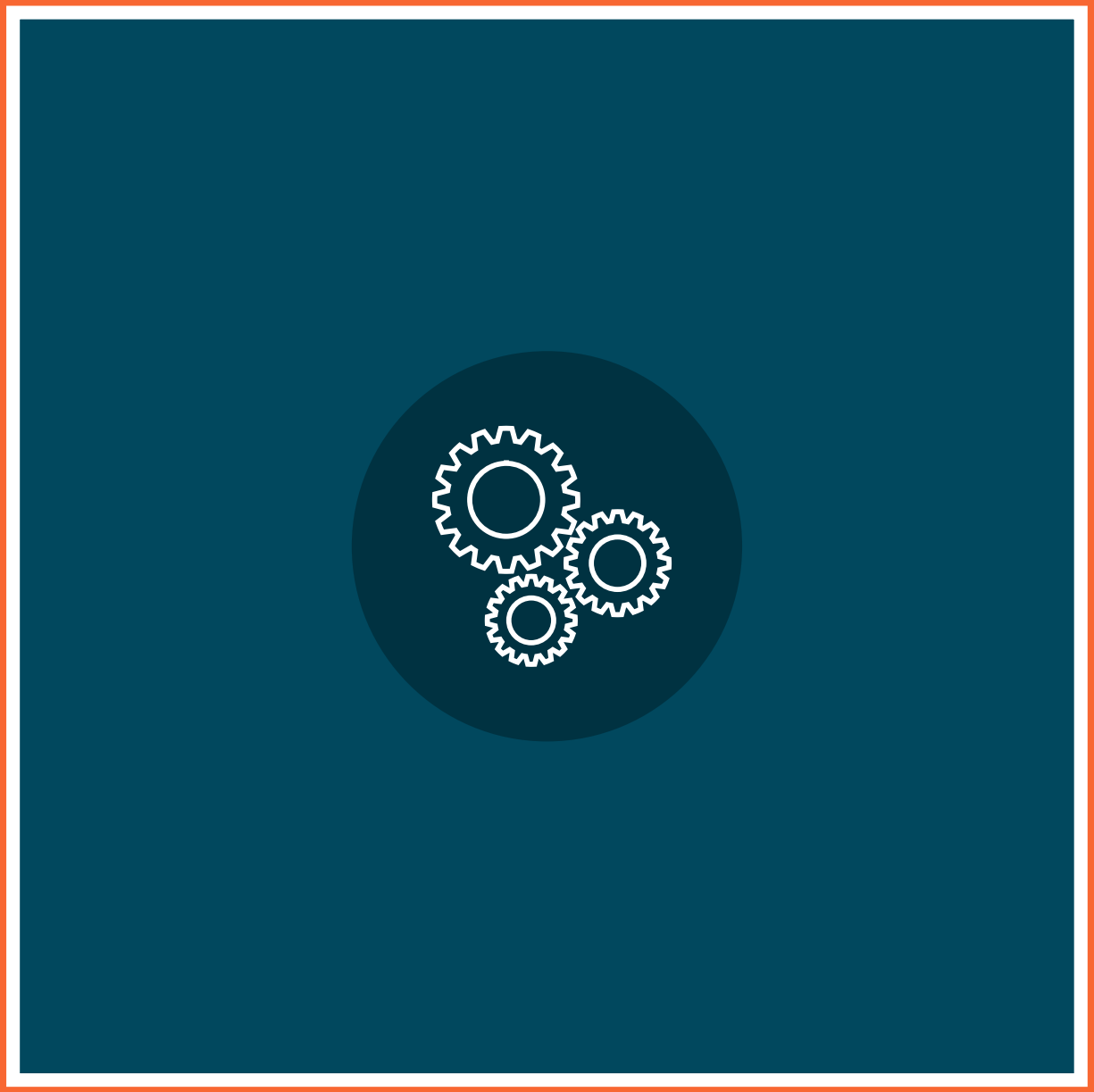
NÃO ARRISQUE PERDER TUDO:
GUIA COMPLETO DE BACKUP NAS EMPRESAS



ASCENT
OUTSOURCING TI



INTRODUÇÃO

Empresas dependem dos seus ativos de TI para se manter eficientes e com alta performance. Afinal, em meios digitais, os profissionais conseguem atuar com **integração elevada**, trocando informações e reduzindo distâncias.

Isso permite que o empreendimento consiga competir por **novos consumidores e parceiros comerciais**, ainda que o país esteja em crise. Contudo, conforme as ferramentas de TI são integradas ao ambiente de trabalho, o número de dados que circulam em meios digitais cresce continuamente.

Além disso, a presença da tecnologia nas rotinas internas eleva as chances de um ataque de malware atingir o negócio. O que cria um risco operacional elevado: em caso de falhas ou ataques, a companhia corre o risco de perder informações importantes para a execução de atividades diárias.

Assim, para proteger o negócio, entram em ação as **políticas de backup de dados**.

Elas podem ser implementadas a qualquer momento e, em um cenário ideal, dão ao empreendimento a capacidade de proteger seus registros digitais, tornando a infraestrutura de TI mais confiável e robusta.

Então, se você quer saber como as políticas de backup podem ser implementadas no seu negócio e qual é a sua importância para a empresa, continue lendo este e-book. Aqui veremos algumas dicas para criar uma **rotina de backup eficaz**, e como companhias de outsourcing podem auxiliar nesse processo.

Boa leitura!

SEGURANÇA CORPORATIVA

De fato, nos últimos anos, a segurança corporativa tornou-se um tópico de grande importância para gestores de várias áreas. Seja pela presença da Internet das Coisas no ambiente corporativo — algo que contribui para o aumento do número de brechas internas — ou pelo crescimento de ondas de ataques, como a do malware WannaCry e o malware Petya, as companhias correm o risco constante de ser atingidas e perder dados importantes.

Para **se proteger** disso, os negócios têm como alternativa uma série de medidas. Em primeiro lugar, o uso de softwares de monitoramento e a criação de políticas de controle de acesso reduzem as chances de um ataque não ser detectado rapidamente e causar um grande impacto na rotina do negócio.

Além disso, a **manutenção de fluxos de atualização ágil** elimina brechas de segurança e traz mais confiabilidade para os sistemas internos. E, nesse cenário, a **rotina de backup** auxilia o empreendimento a ter mais capacidade de atuação na proteção dos ativos de TI.

Grosso modo, a criação de cópias de sistemas e arquivos críticos permite que a empresa consiga recuperar dados caso algum problema ocorra, maximizando a confiabilidade das políticas de segurança digital.

OS TIPOS DE BACKUP

Um dos passos básicos das políticas de backup é o uso de diferentes tipos de mídias para armazenar os dados. O ideal é que, ao menos, duas **soluções sejam utilizadas**, garantindo que, em caso de falhas, a empresa terá mais chances de **restaurar os seus dados**.

Entre essas mídias que podem ser utilizadas, destacamos:

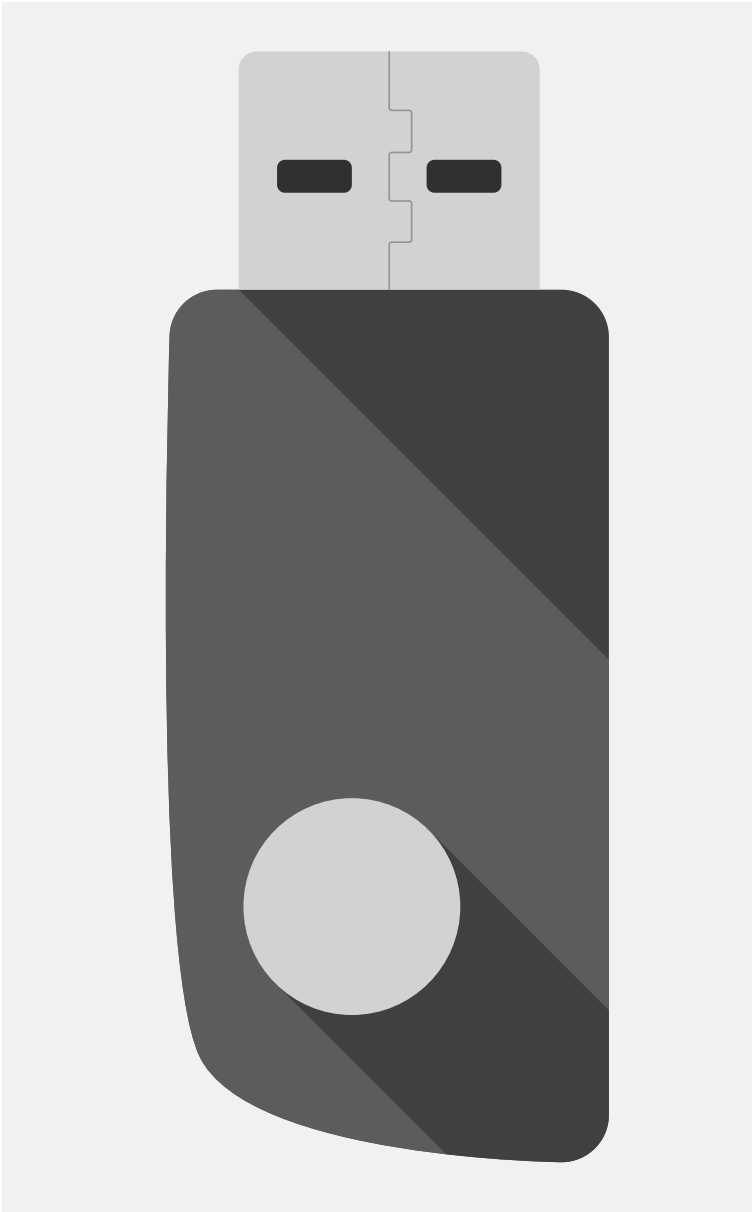
PEN DRIVES E HDS EXTERNOS

As mídias externas são utilizadas por muitos empreendimentos pelo seu baixo custo e facilidade de manipulação.

O uso de pen drives ou HDs externos para salvar dados permite que a companhia faça cópias de vários arquivos em um mesmo local e, se necessário, migre informações para outros dispositivos facilmente. No entanto, **essa estratégia deve ser evitada sempre que possível**.

Isso porque mídias externas são furtadas facilmente, tanto por conta do seu tamanho quanto por serem projetadas para não ficar permanentemente em um local.

E vale destacar, ainda, que os dados do usuário podem ser comprometidos a qualquer momento: HDs são suscetíveis a problemas causados por interferências eletromagnéticas e, assim como pen drives, a danos físicos. Como consequência, a empresa pode perder o acesso às suas informações, inviabilizado-as permanentemente.



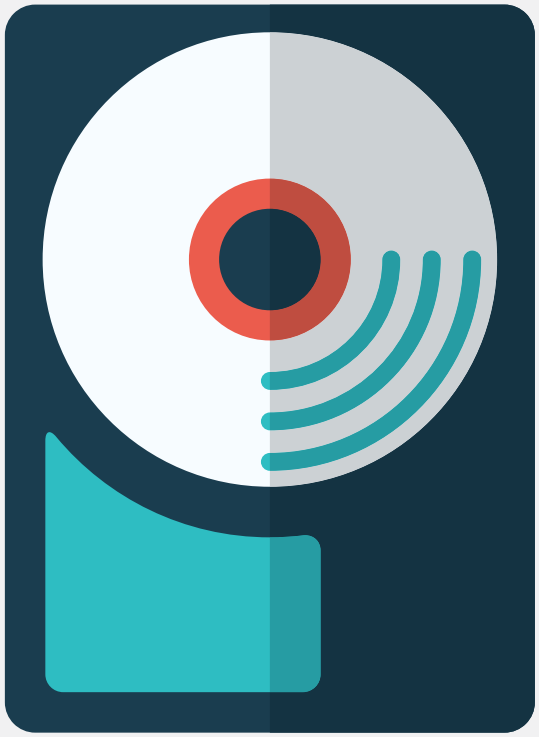
NAS

Sigla para Network-Attached Storage (Armazenamento Conectado à Rede, em uma tradução livre) o NAS é um dispositivo utilizado para conectar unidades de armazenamento a uma rede.

Ele dispõe de uma interface para configuração das mídias e, em alguns casos, ainda **permite que as unidades sejam gerenciadas por meio de tecnologias como a RAID**. Assim, a companhia pode agendar backups em várias máquinas e direcioná-los para um único local.

Grosso modo, o NAS atuará como um **pequeno servidor**, unificando o local em que os registros do negócio são salvos.

Como medida de segurança, também é possível configurar a criptografia nos dados, impedindo o acesso não autorizado às informações. Além disso, pode-se manter um sistema RAID para garantir mais confiabilidade aos backups, evitando que falhas impeçam o acesso aos registros.



CDS/DVDS

CDs e DVDs também podem ser utilizados como ferramenta de backup. Por meio deles, a companhia consegue armazenar em um disco de baixo custo uma grande quantidade de arquivos.

Contudo, assim como HDs externos e pen drives, essa é uma das piores escolhas que podem ser feitas pelo negócio. CDs e DVDs não só têm mais facilidade de sofrer danos que prejudicam permanentemente o acesso aos dados (como quebras e arranhões), mas também **são menos seguros**.

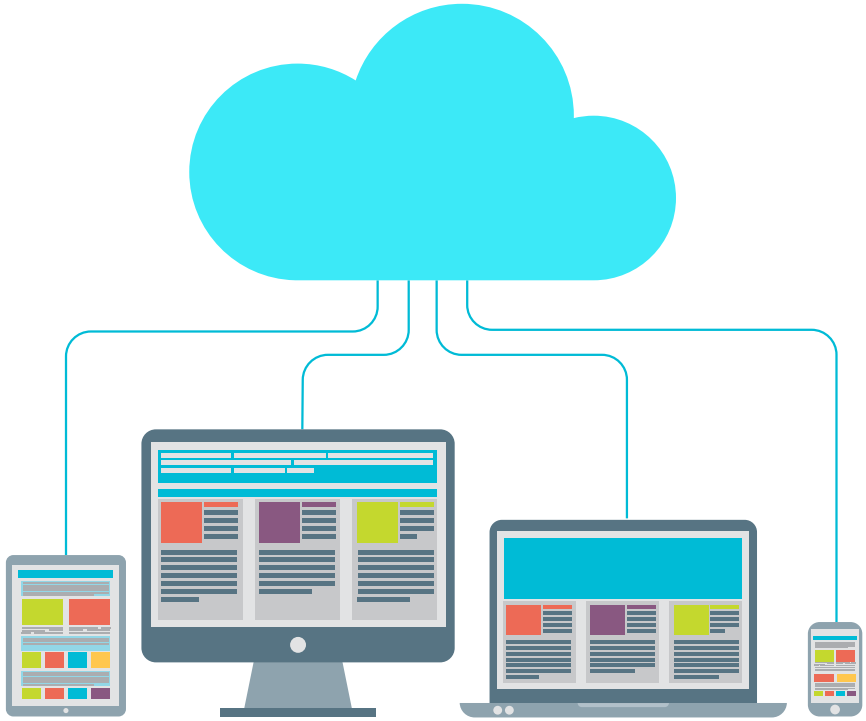
Além disso, tais mídias não permitem a alteração ou remoção de arquivos, prejudicando o versionamento dos dados: sempre que uma nova versão for criada, uma nova gravação deverá ser feita. Portanto, evite esse tipo de solução ao máximo. Discos de DVD podem ter um baixo custo, mas não são capazes de trazer ao empreendimento a segurança necessária para o armazenamento eficiente das suas informações corporativas.

SERVIÇOS DE CLOUD BACKUP

Os serviços de cloud backup ganharam popularidade nos últimos anos por fornecer uma **forma simples e integrada** para a criação de rotinas de backup flexíveis.

Essa alternativa pode ser implementada com soluções profissionais ou por meio do investimento em cloud computing do tipo IaaS (Infrastructure as a Service, ou Infraestrutura como Serviço, em português). Nesse caso, o negócio utiliza um software próprio para gerenciar seus dados e manter as suas próprias políticas de backup.

Além disso, backups na nuvem têm como uma de suas principais vantagens o fato de serem **mais escaláveis**. Assim, festores podem modificar o espaço disponível para o armazenamento sempre que for necessário.



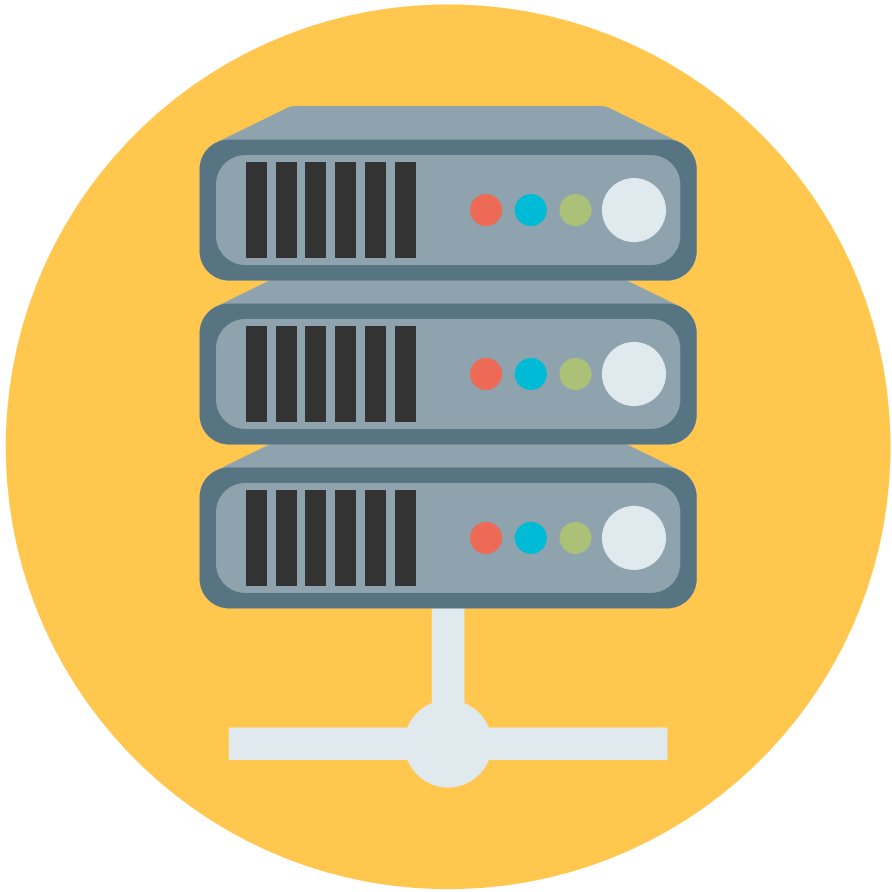
E essa escalabilidade do backup em ambientes de regras de segurança são aplicadas com maior agilidade quando comparamos essa tecnologia com outras do mercado. Sem contar que é **possível restaurar arquivos** remotamente — algo fundamental se a máquina não estiver fisicamente acessível.

SERVIDORES INTERNOS

O uso de servidores internos também é uma medida que pode ser adotada pelo negócio. Apesar da complexidade que pode apresentar, essa opção permite que a companhia tenha total controle sobre os mecanismos utilizados nos processos de backup e a sua configuração.

A empresa poderá definir o tipo de mídia utilizada nesse processo, políticas de segurança e controles de acesso. Além disso, as máquinas estarão em um local controlado pelo negócio, reduzindo ainda mais as chances de terceiros obterem qualquer acesso às informações.

Por outro lado, os gastos com manutenção e troca de hardware serão todos de responsabilidade da empresa. Sempre que for necessário trocar uma peça ou atualizar um software, por exemplo, os recursos para tais processos sairão diretamente do orçamento do setor de TI.



ROTINA DE BACKUP

Para proporcionar segurança, de fato, o backup não deve ser feito apenas uma vez por ano. É importante que o negócio tenha uma rotina para a criação de cópias de sistemas e arquivos contínua. E deve-se priorizar os dados mais importantes, dando ao negócio a capacidade de manter uma infraestrutura sólida e confiável.

A companhia deve avaliar a frequência com que os dados são alterados e como a sua perda impacta o empreendimento, para identificar a frequência ideal da criação dos arquivos.

Informações importantes, mas que não são modificadas frequentemente, por exemplo, podem ser copiadas em intervalos maiores. Por outro lado, dados críticos ou que são modificados constantemente precisam de **backups mais regulares**.

Como citado anteriormente, é importante que o negócio utilize mais de uma ferramenta para armazenar os seus dados. Isso impede que, caso a falha também atinja o backup, o negócio não consiga restaurar os seus dados.

Testes devem ser realizados regularmente, para que a companhia possa validar a integridade dos seus backups. Então, instrua técnicos a avaliar se os arquivos estão restauráveis. E não se esqueça de **treinar os profissionais** para que eles consigam recuperar dados com agilidade e segurança.

Também é importante que o negócio tenha mecanismos que impeçam o acesso aos dados por pessoas não autorizadas, o que causaria grandes prejuízos para a empresa.

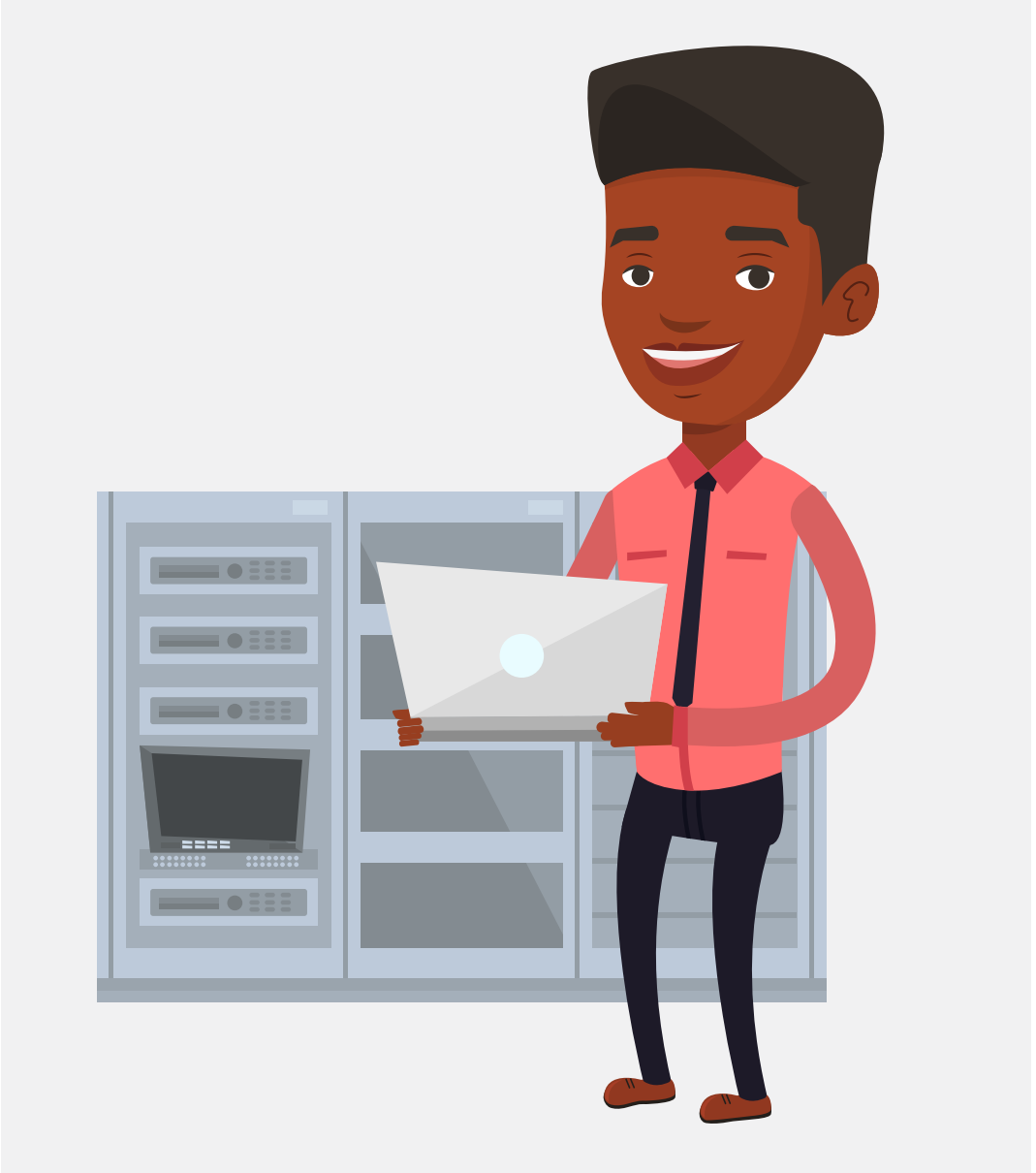
Afinal, se um backup for extraviado, os conteúdos de um sistema ou de um setor inteiro poderão ser restaurados em outros dispositivos, revelando segredos do negócio e projetos internos a terceiros. Por isso, sefina uma política de segurança para armazenar as informações em um **local confiável**.

TERCEIRIZAÇÃO: UMA ALTERNATIVA

A terceirização de processos de TI tem sido adotada por várias empresas como uma forma de reduzir custos, aumentar a capacidade dos profissionais de TI de focar nas suas atividades críticas e atingir melhor performance.

Além disso, o outsourcing dá ao empreendimento a capacidade de encontrar a melhor rotina de acordo com o seu perfil, melhorando o impacto das políticas de TI.

Assim, se a empresa não possuir um setor de TI estruturado, ou desejar focar os seus recursos operacionais com outras rotinas, o processo de backup pode ser direcionado para uma companhia especializada.



Os profissionais designados ficarão responsáveis por todos os processos, da criação das cópias à definição das mídias utilizadas. Técnicos de TI avaliam a infraestrutura do negócio, os objetivos de médio e longo prazo, o perfil corporativo e normas internas para identificar como a cópia de arquivos deve ser planejada e executada.

Isso permite que o backup seja integrado diretamente na rotina da companhia, otimizando as rotinas sem impactar na produtividade do empreendimento.

O agendamento das atividades de criação de cada cópia, por exemplo, será definido de acordo com a rotina dos setores, evitando que os backups impactem negativamente a produtividade de profissionais internos. A definição das mídias, por outro lado, buscará o máximo de custo-benefício para o empreendimento.

Além disso, a política de backup estará alinhada com os padrões do mercado, tornando simples o seu alinhamento com as regras de compliance internas e a legislação local.

CONCLUSÃO

Sabemos que a infraestrutura de TI tem desempenhado um papel-chave no dia a dia de várias empresas. Por meio de equipamentos computacionais e softwares, profissionais estão **inovando cada vez mais**.

O atendimento a clientes ganhou direcionamentos mais precisos. A rotina do profissional ganhou **maior mobilidade**. Sem contar que, ao mesmo tempo, times podem atuar integrados, independentemente do local em que cada pessoa se encontra.

Nesse cenário, como vimos, ter uma política de **backup é crucial** para garantir que seus serviços sejam continuamente executáveis e robustos.

Logo, as empresas devem investir em rotinas para criar sempre cópias de seus arquivos e sistemas, **evitando o risco** de que esses dados não sejam recuperados após um problema qualquer que possa ocorrer com os hardwares e softwares.

Em outras palavras, investir na criação e implementação de uma rotina de backups deve ser visto pela empresa como uma **aplicação estratégica de recursos**. Assim, a companhia passa a ter mais capacidade de atender a demandas de clientes, sabendo que sempre terá uma infraestrutura de TI disponível quando necessário.

Além disso, o backup ainda torna a **companhia mais competitiva**. Afinal, esse processo garante que o negócio está comprometido com a necessidade de manter dados em ambiente confiável e robusto, algo valorizado pelo mercado como um diferencial competitivo.

ASCENT
OUTSOURCING TI

A velocidade da evolução tecnológica atual determina que empresas que tenham acesso rápido e com qualidade à informação se posicionem à frente dos seus concorrentes. Transformar dados em informação e garantir a sua correta circulação entre a corporação é se credenciar como uma instituição a frente do seu tempo. O **Grupo ASCENT** é especialista em Tecnologia de Informação e se preparou para essa realidade.

Somos focados na inovação, relacionamento e suporte à gestão. Temos uma característica forte e amplamente reconhecida no mercado de ser uma empresa determinada e comprometida com a qualidade do trabalho realizado. Uma empresa jovem que não mede esforços na busca de melhoria e aperfeiçoamento contínuo e o entendimento completo do negócio principal dos seus clientes. Atuamos na área de Business Intelligence e Outsourcing de TI, aumentando os resultados dos nossos clientes e diminuindo seus riscos operacionais.

Comprometimento e eficácia é a marca dos nossos profissionais – qualificados e com experiência em grandes projetos, estão sempre voltados para os objetivos e desafios dos nossos clientes. O investimento contínuo na atualização profissional é nossa preocupação primária. Enfim, a **ASCENT** se orgulha de ser uma empresa caracterizada pela transparência e comprometimento no relacionamento com seu cliente. Esse é o maior compromisso da nossa empresa. Este é o nosso perfil: Uma empresa jovem, ágil e com visão voltada sempre para o futuro.