

1. Gerenciamento de ativos

Toda organização possui um **processo formal** para aquisição de bens e serviços de terceiros. Esse é um componente essencial do **processo de compras**, que geralmente envolve diversas aprovações dentro da empresa.

O processo normalmente começa com o **usuário final**, que pode precisar de um software ou hardware específico. Esse usuário trabalha em conjunto com o departamento de **TI** e o setor de **compras** para adquirir os produtos ou serviços necessários.

Antes de concluir a compra, é feita uma **análise orçamentária** para determinar se o departamento pode arcar com os custos do produto ou serviço. Além disso, são necessárias **aprovações formais** de diferentes setores, incluindo a **TI, compras** e, muitas vezes, a **gestão da empresa**.

O processo de compra geralmente envolve **negociações** com os fornecedores para garantir que a empresa obtenha o melhor preço e as condições mais favoráveis. Essas negociações podem incluir discussões sobre **preço, termos de licenciamento** e outros detalhes contratuais.

Depois que as negociações são concluídas, a compra pode ser formalizada. O fornecedor então entrega os bens ou serviços, e a empresa recebe uma **fatura** pelo custo da aquisição.

As faturas normalmente vêm com **termos de pagamento**, que podem exigir que a empresa pague o valor total **imediatamente** ou dentro de um período, como **30 ou 60 dias**.

Se a empresa estiver comprando um **produto físico**, ele será registrado em um **sistema central de rastreamento de ativos**. Esse sistema permite acompanhar a **vida útil** do produto, desde a aquisição até o descarte.

A primeira etapa do rastreamento de ativos é determinar **quem tem controle** sobre o item e atribuir a posse no sistema. Por exemplo, se um funcionário recebe um **laptop**, ele é registrado no nome dessa pessoa, e qualquer atualização ou manutenção necessária será feita com base nessa atribuição.

O sistema também classifica os itens por **tipo de dispositivo**, como **laptops, desktops, dispositivos móveis** ou outros sistemas. Além disso, a empresa precisa diferenciar se o ativo é **hardware ou software**, pois isso afeta a forma como ele é contabilizado.

- **Hardware** é um **gasto de capital** e pode ser depreciado ao longo do tempo, afetando a tributação da empresa.
- **Software** geralmente **não se deprecia**, sendo considerado um **gasto operacional**, com tributação diferente.

O rastreamento de ativos não é útil apenas para a **aquisição**, mas também para **gerenciar o ciclo de vida** do produto. Com ele, a empresa pode realizar inventários, acompanhar a localização dos ativos e registrar manutenções ou substituições.

Por exemplo, o sistema pode listar **todos os laptops e roteadores da empresa**, permitindo que a equipe de suporte técnico saiba quais dispositivos estão disponíveis e onde estão localizados.

O rastreamento de ativos também auxilia o **help desk**, pois permite associar um usuário a um **chamado técnico** e fornecer detalhes sobre o modelo do dispositivo. Isso facilita o trabalho dos técnicos ao solucionar problemas.

Além disso, um **desktop** não é apenas um único equipamento. Ele contém vários componentes, como **CPU, memória, discos de armazenamento, teclado, mouse** e outros periféricos. O rastreamento de ativos pode listar o dispositivo como um **único item** ou detalhar cada um de seus componentes separadamente.

Para facilitar a identificação, muitas empresas utilizam **etiquetas de ativos** com um **código de barras ou número de série**. Essas etiquetas ajudam a associar fisicamente o dispositivo ao sistema de rastreamento e também servem como um **recurso de segurança**, especialmente se o equipamento for perdido ou roubado.

Quando um **dispositivo precisa ser reutilizado**, pode ser necessário remover todos os **dados da empresa** para garantir que não possam ser recuperados, principalmente se o equipamento for descartado ou doado.

Existem diferentes **métodos de sanitização de mídia**, dependendo do destino do equipamento:

- Se o dispositivo for **descartado**, todos os dados devem ser **apagados permanentemente**.
- Se ele for **reutilizado internamente**, pode ser necessário apenas **excluir arquivos sensíveis**.

Para reutilizar **discos de armazenamento**, o ideal é utilizar um **software de apagamento seguro**, garantindo que ninguém possa recuperar os dados excluídos.

Se a empresa quiser garantir que **nenhum dado seja recuperado**, ela pode optar por **destruir fisicamente o disco rígido**. Isso pode ser feito de várias maneiras:

1. **Trituradores industriais ou pulverizadores**, que destroem completamente o disco.
2. **Perfuração com furadeiras ou martelos**, que danificam os pratos do disco, tornando impossível a recuperação dos dados.
3. **Desmagnetização (Degaussing)**, que usa um campo eletromagnético para apagar todas as informações do disco e inutilizá-lo.

4. **Incineração**, método mais extremo, que garante que ninguém jamais poderá reutilizar o disco.

Para grandes volumes de dispositivos descartados, muitas empresas contratam **serviços terceirizados de destruição de discos**. Essas empresas não apenas destroem os discos, mas também fornecem um **certificado de destruição**, confirmando que os dados foram eliminados de forma irreversível.

2.Retenção de Dados

Assim como há momentos em que é necessário **destruir dados**, também existem situações em que é essencial **manter informações armazenadas** por longos períodos.

A retenção de dados pode incluir:

- **Fontes de dados originais**
- **Cópias e backups**
- **Registros financeiros e empresariais**

Dependendo das **leis e regulamentações**, algumas empresas são **obrigadas** a armazenar certos tipos de dados por **anos**. Por exemplo:

- **E-mails corporativos** podem precisar ser arquivados por um período determinado.
- **Registros financeiros** podem ter requisitos legais de armazenamento.

Muitas organizações possuem **políticas e procedimentos específicos** para retenção de dados, garantindo que informações essenciais sejam preservadas.

Além da obrigatoriedade legal, manter dados pode ser uma **boa prática de segurança**, especialmente se for integrada a um **plano de backup**. Isso garante que arquivos importantes possam ser recuperados caso sejam excluídos acidentalmente ou perdidos devido a falhas de hardware.

Se a empresa enfrentar uma **situação de desastre**, os dados retidos podem ser usados para restaurar as operações em outro local.

Diferentes tipos de dados exigem **diferentes períodos de retenção**, por isso é fundamental entender:

1. **Quais informações precisam ser mantidas?**
2. **Por quanto tempo elas devem ser armazenadas?**
3. **Quais são as melhores práticas para protegê-las?**

Com um planejamento adequado, a empresa pode garantir que seus dados estejam seguros e acessíveis sempre que necessário.