

# Facilitando a conformidade com a Lei Geral de Proteção de Dados



# O que é LGPD e quando entra em vigor?

A LGPD é a nova Lei Geral de Proteção de Dados do Brasil, que cria um novo marco legal para a proteção de dados pessoais, estabelecendo maiores direitos aos indivíduos e maiores obrigações para as organizações que administram dados pessoais em relação ao Brasil.

A LGPD entra em vigor em Agosto de 2020.

## Âmbito de aplicação da LGPD

- a) A operação de tratamento de dados realizada no Brasil ou dados que tenham sido coletados no Brasil;
- b) Tratamento de dados pessoais de indivíduos no Brasil, se tal tratamento se relacionar à oferta de bens ou serviços a tais pessoas – independente de onde ocorra o tratamento ou da nacionalidade ou localização da empresa.

## Definições

- **Dados pessoais:** Qualquer dado que se relacione a um indivíduo, uma pessoa física identificada ou identificável.
- **Dado anonimizado:** Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- **Dado pessoal sensível:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- **Controlador:** A pessoa física ou jurídica que decide sobre o tratamento de dados pessoais.
- **Processador:** A pessoa física ou jurídica que processa dados pessoais para ou em nome do controlador.

# Como a LGPD impacta o meu negócio?

## Aumenta as proteções dos titulares de dados pessoais

Os titulares de dados têm direito de

- Acessar seus dados pessoais
- Corrigir erros em seus dados pessoais
- Apagar seus dados pessoais
- Opor-se ao tratamento de seus dados pessoais
- Exportar seus dados pessoais

## Exige a notificação de violações de segurança de dados pessoais

Quando ocorrer uma violação de segurança de dados pessoais:

- O processador deve notificar o controlador prontamente
- O controlador deve notificar o titular dos dados prontamente, se a violação representar um risco a seus direitos

## Incrementa o dever de proteção dos dados pessoais

As organizações devem:

- Proteger dados pessoais com medidas de segurança apropriadas
- Obter os consentimentos necessários para o processamento de dados
- Manter registros com informações detalhadas sobre o processamento dos dados

## Impõe penalidades significativas por descumprimento

Multas de 2% do faturamento anual da empresa no país (até 50M de Reais).

- Dano reputacional e das possíveis indenizações decorrentes de ações dos titulares dos dados afetados.

# A LGPD é sobre proteger dados pessoais em qualquer lugar e em qualquer momento.

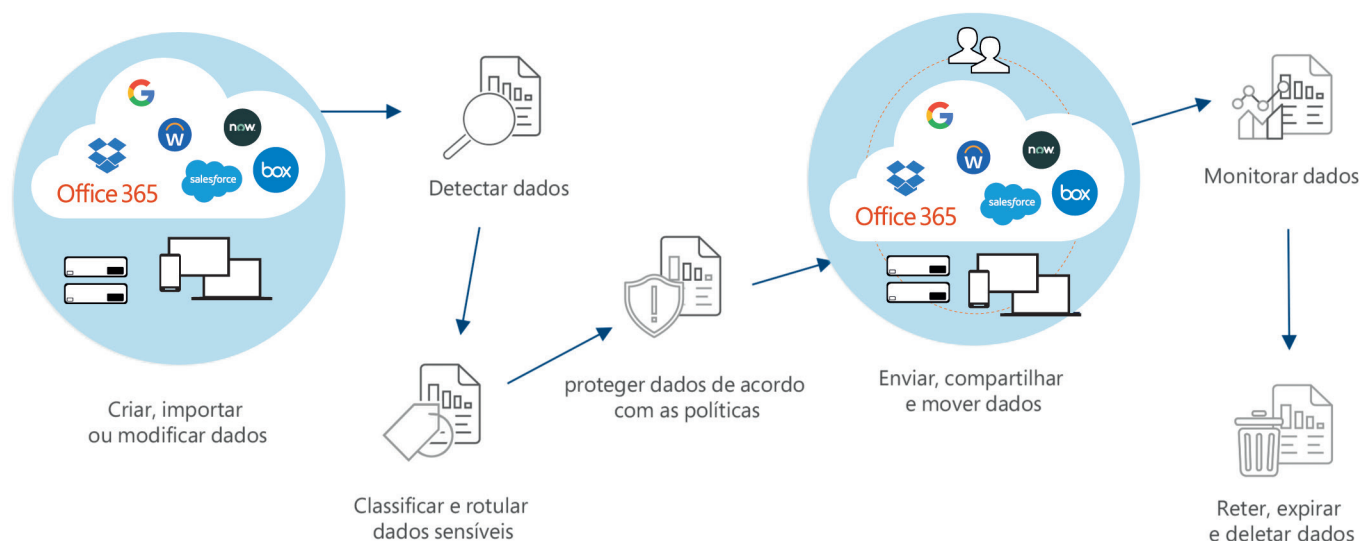














Fig 1: Ciclo de vida da Informação

# Tecnologia Microsoft 365 para acelerar a conformidade com a LGPD

## Recursos detalhados nos cenários a seguir:

 <b>Azure Active Directory / Conditional Access</b>	 <b>Intune (MDM &amp; MAM)</b>	 <b>Azure Information Protection</b>	 <b>Privileged Identity Management</b>
 <b>Identity Protection</b>	 <b>Advanced Data Governance</b>	 <b>Advanced e-Discovery</b>	 <b>Data Loss Prevention</b>
 <b>Multi-Factor Authentication</b>	 <b>Cloud App Security</b>	 <b>Advanced Threat Protection</b>	 <b>Behavioral Analytics for Threat Protection</b>

## Cenários e Desafios mais comuns na jornada de LGPD

1. Como descobrir dados pessoais em dados não estruturados.
2. Como assegurar a proteção dos dados em estrutura local, na nuvem e em dispositivos móveis.
3. Como garantir e restringir acesso aos dados.
4. Como ter visibilidade e controle de dados armazenados em aplicações na nuvem.
5. Como detectar ameaças antes que causem danos maiores.
6. Como comprovar que os esforços necessários de conformidade estão sendo realizados.
7. Como executar pedidos de dados de titulares.

# 1. Como descobrir dados pessoais em dados não estruturados

Toda organização tem muitos dados, inclusive dados pessoais. Estes podem residir em uma estrutura local, no Office 365 ou em outros aplicativos de nuvem. Independentemente de onde estiverem, precisamos identificar estes dados pessoais e classificá-los de acordo. Como exemplo, é preciso varrer seus diretórios em estrutura local e sites do SharePoint buscando por dados sensíveis e, quando forem encontrados, relatá-los de volta para você ou classificar e proteger diretamente de acordo com definições prévias.

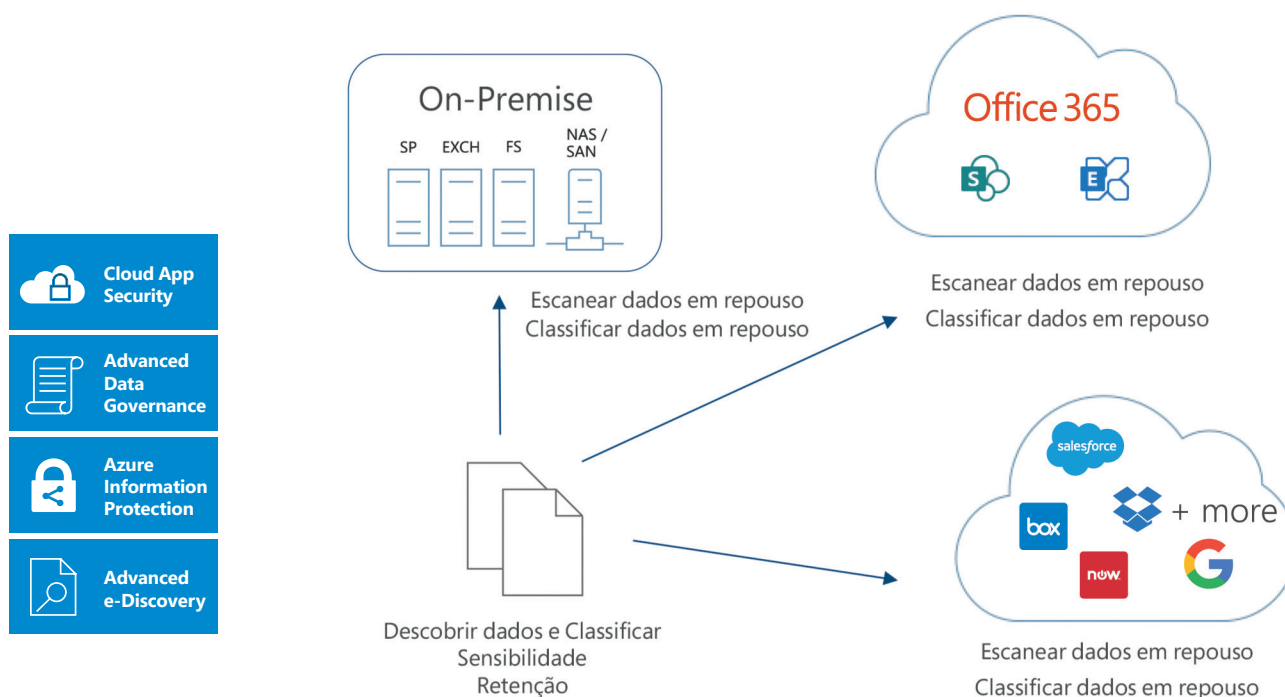


Fig 2: Identificar dados sensíveis em dados não estruturados.

## Recursos Microsoft 365 para lhe ajudar:

- Office 365 e Discovery search pode ser usado para encontrar texto e metadados em conteúdos espalhados em seus ativos do Office 365—SharePoint Online, OneDrive for Business, Microsoft Teams, e Exchange Online.
- Microsoft Cloud App Security é um serviço abrangente que provê visibilidade, controle e proteção para dados e aplicações na nuvem. Você pode ter visibilidade de quais aplicações estão em uso na sua rede – identificando mais de 13 mil aplicações em todos os dispositivos – além de uma avaliação de risco para cada aplicação.
- Advanced Data Governance usa inteligência e insights assistidos por máquina para ajudar a encontrar, classificar, definir políticas, e tomar ações para gerenciar o ciclo de vida dos dados que são mais importantes para a sua organização.
- Office 365 Advanced e Discovery, baseado em aprendizado de máquina, ajuda a identificar rapidamente documentos que são relevantes para um tema específico (como uma investigação de conformidade, por exemplo) e com melhor precisão do que buscas tradicionais através de palavras chaves ou revisões manuais de uma vasta quantidade de arquivos. O Advanced e Discovery pode reduzir significativamente os custos e esforços para identificar documentos relevantes e relações entre dados através de aprendizado de máquina treinado para explorar de maneira inteligente grandes conjuntos de dados.
- Microsoft Azure Information Protection ajuda a identificar quais são as suas informações sensíveis e onde elas residem. Você pode buscar por dados marcados com uma classificação específica ou identificar dados sensíveis automaticamente quando um email ou arquivo é criado, de acordo com as políticas da sua organização.

## 2. Como assegurar que meus dados estejam protegidos na infra local, na nuvem e em dispositivos móveis

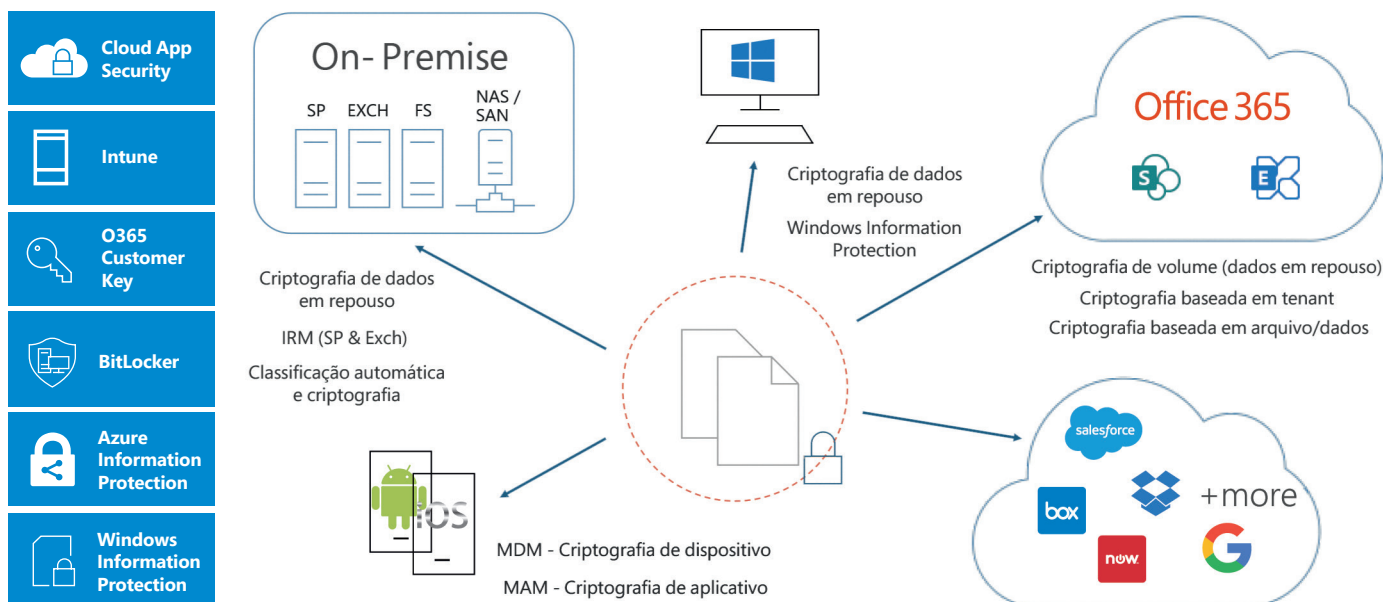


Fig 3: Proteção dados onde eles estiverem.

### A sua organização provavelmente tem dados pessoais em diversas aplicações, e é possível protegê-los de diversas maneiras:

#### Dados que residam na infra local

Uma das atividades que você precisa fazer é proteger os dados em repouso, o que pode ser feito com criptografia de disco. Podemos contar com uma camada de proteção adicional, utilizando o gerenciamento de direitos de informação no SharePoint e no Exchange que utiliza criptografia no nível do arquivo. Esta criptografia viajará com o arquivo aonde ele for, e a classificação e proteção podem ser automáticas, evitando possíveis descuidos dos usuários.

#### Dispositivo

Você poderá habilitar a criptografia de disco para proteger os dados em repouso. Além disso, você poderá separar dados corporativos de dados pessoais e fornecer controles e proteções adicionais a dados corporativos.

#### No Office 365

Todos os dados em repouso no O365 já estão criptografados, isso é o que chamamos de criptografia de volume. Esta criptografia de disco é semelhante à criptografia de base que você tem em seus servidores Windows. O Office 365 oferece uma camada adicional de criptografia no nível do aplicativo para conteúdos do Office 365. Isso é chamado de criptografia de serviço. A chave do cliente (O365 Customer key) é criada na criptografia de serviço e permite que você forneça e controle chaves que são usadas para criptografar seus dados em repouso no Office 365. A chave do cliente ajuda a cumprir as obrigações de conformidade porque você controla as chaves de criptografia que o Office 365 usa para descriptografar dados. E por fim, a última camada de proteção é no nível do arquivo antes de carregá-lo para a aplicação.

#### Para outros aplicativos de nuvem

Você pode proteger/criptografar o arquivo antes de carregá-lo nos aplicativos de nuvem. Ao usar um proxy embutido, isso também pode ser feito no momento do upload, garantindo que todos os dados que entram em um aplicativo de nuvem sejam criptografados.

### E por fim, dispositivos móveis

Através da gestão de dispositivos (MDM), podemos impor a encriptação de dispositivos para garantir que os dados em repouso estejam protegidos. Isso nem sempre é possível, especialmente no caso em que seus usuários tragam seus próprios dispositivo (BYOD). Logo, você pode optar por mover a camada de criptografia para o aplicativo móvel em vez do dispositivo e aplicar controles adicionais sobre aonde os dados podem ir (por exemplo, impedir que os dados corporativos se movam a um aplicativo pessoal (não gerenciado)). Você poderá fazer uma combinação entre os dois para melhor proteger os seus dados.

## 3. Como garantir e restringir acesso aos dados

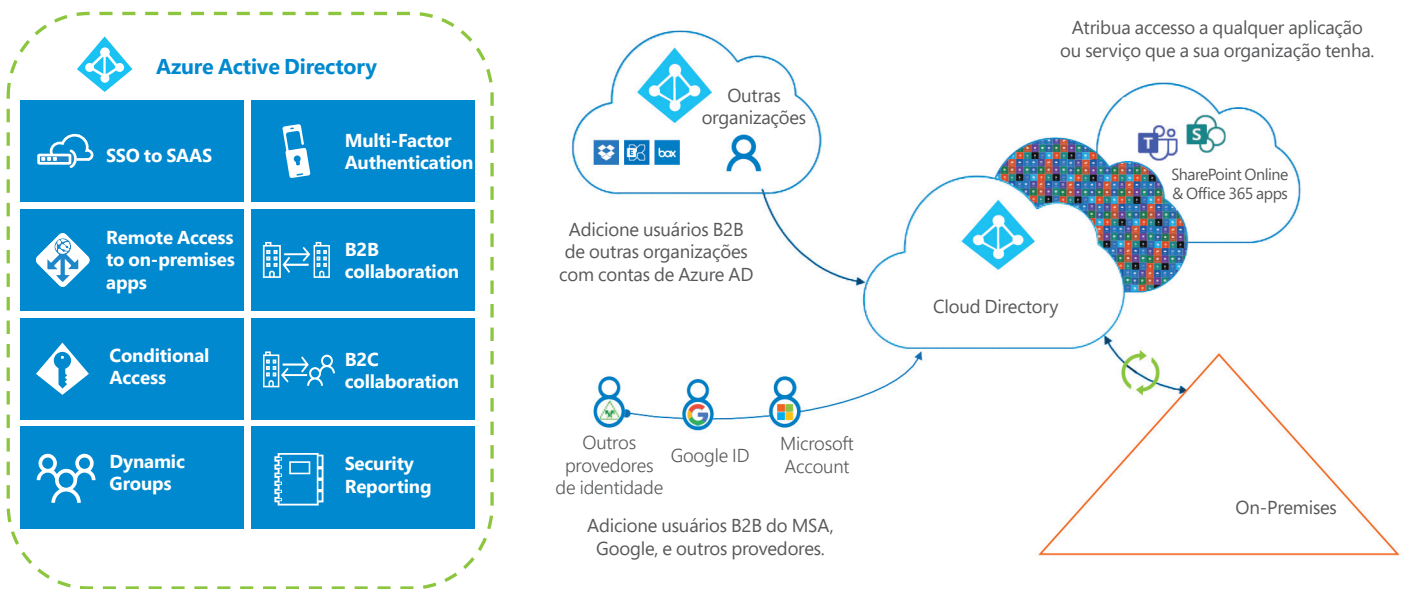


Fig 4: Gestão de identidade e acesso.

A forma como protegemos nossos dados e informações mudou, uma vez que com aplicações em nuvem e dispositivos móveis, temos cada vez menos controle do nosso perímetro de segurança. Mas ainda há uma coisa comum entre quase todos os locais onde os dados são armazenados, que é a identidade para acessar esses dados, o que nos faz colocar a gestão de identidade no centro da nossa estratégia de proteção de dados.

Os usuários finais não são bons em lidar com diferentes combinações de nome de usuário/senha para diferentes recursos que eles precisam acessar (os mesmos buscarão padrões e/ou combinações fáceis para as senhas). Fáceis para um algoritmo descobrir e difíceis para o usuário lembrar. No entanto, estes usuários já têm uma identidade que eles estão usando em seu dia a dia, e podemos nos utilizar dela para garantir o acesso a informação apenas a usuários que o podem fazer por direito.

Portanto, o primeiro passo é estender essa identidade para um diretório de nuvem por meio de uma ponte de identidade. Isto dará aos usuários finais um login único em aplicativos de nuvem, mas também abrirá opções para recursos de autoatendimento, como redefinições de senha e acesso remoto a aplicativos locais, além de recursos como múltiplos fatores de autenticação para trazer uma camada adicional de proteção.

### Recursos Microsoft 365 para lhe ajudar:

- Azure Active Directory (AAD) é uma solução de gestão de identidade e acesso na nuvem. O AAD gerencia identidades e controla o acesso a aplicações e dados na nuvem ou na infra local. Com o Azure Active Directory Privileged Identity Management, você pode atribuir acesso Just-In-Time (JIT) para usuários ADMIN, que expira após o período previsto de uso.

## 4. Como ter visibilidade e controle de dados armazenados em aplicações na nuvem

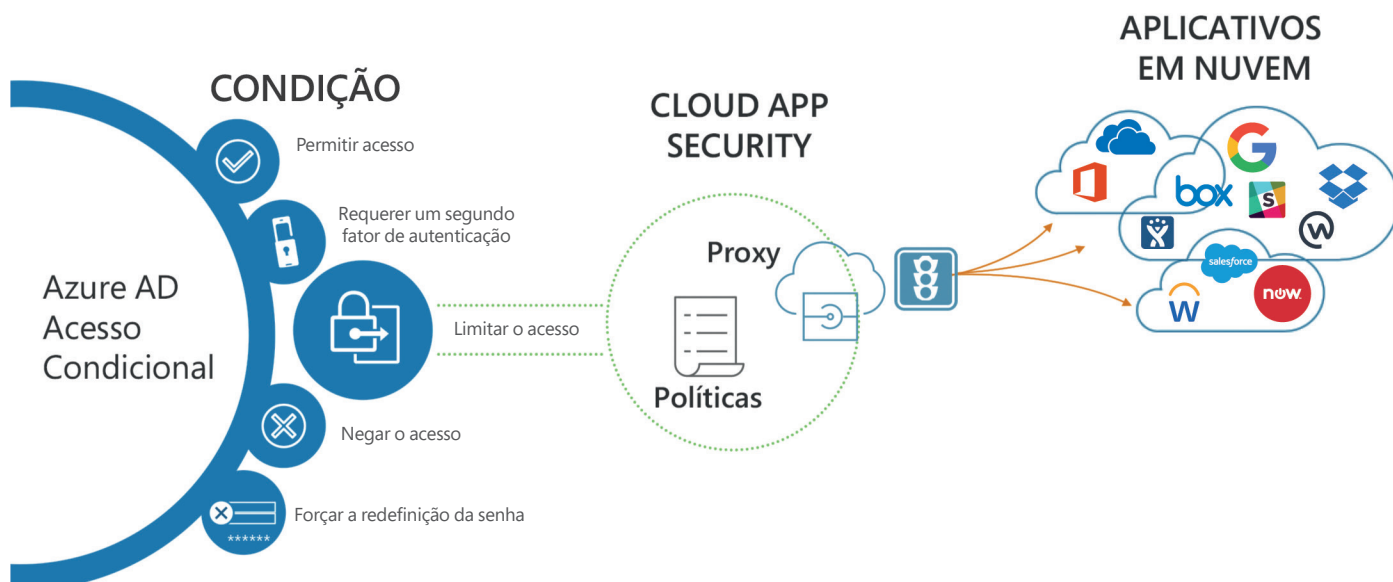


Fig 5: Controle e visibilidade de aplicações na nuvem.

A mudança para a nuvem aumenta a flexibilidade para os funcionários e reduz o custo de TI, mas introduz novos desafios e complexidades para manter sua organização segura. Possibilitando aos funcionários assinarem um serviço de nuvem sem envolver a TI, conhecido como "Shadow IT".

A primeira etapa é descobrirmos quais os aplicativos de nuvem estão em uso e avaliarmos se estes aplicativos são adequados para a nossa organização.

Em seguida, é necessário controlar o acesso destes aplicativos em nuvem, (através de um dispositivo gerenciado ou local confiável) ou bloqueá-los, caso identificado alto risco dos mesmos.

E por fim, é importante proteger os dados contidos nestes aplicativos. Por exemplo: através de criptografia ou impedindo que os dados sejam baixados para dispositivos não gerenciados.

### Recursos Microsoft 365 para lhe ajudar:

Microsoft Cloud App Security é um serviço abrangente que provê visibilidade, controle e proteção para dados em aplicações na nuvem. Você pode ter visibilidade de quais aplicações estão em uso na sua rede – identificando mais de 13 mil aplicações em todos os dispositivos – assim como obter uma avaliação de risco através de relatórios avançados.



## 5. Como detectar ameaças antes que causem danos maiores

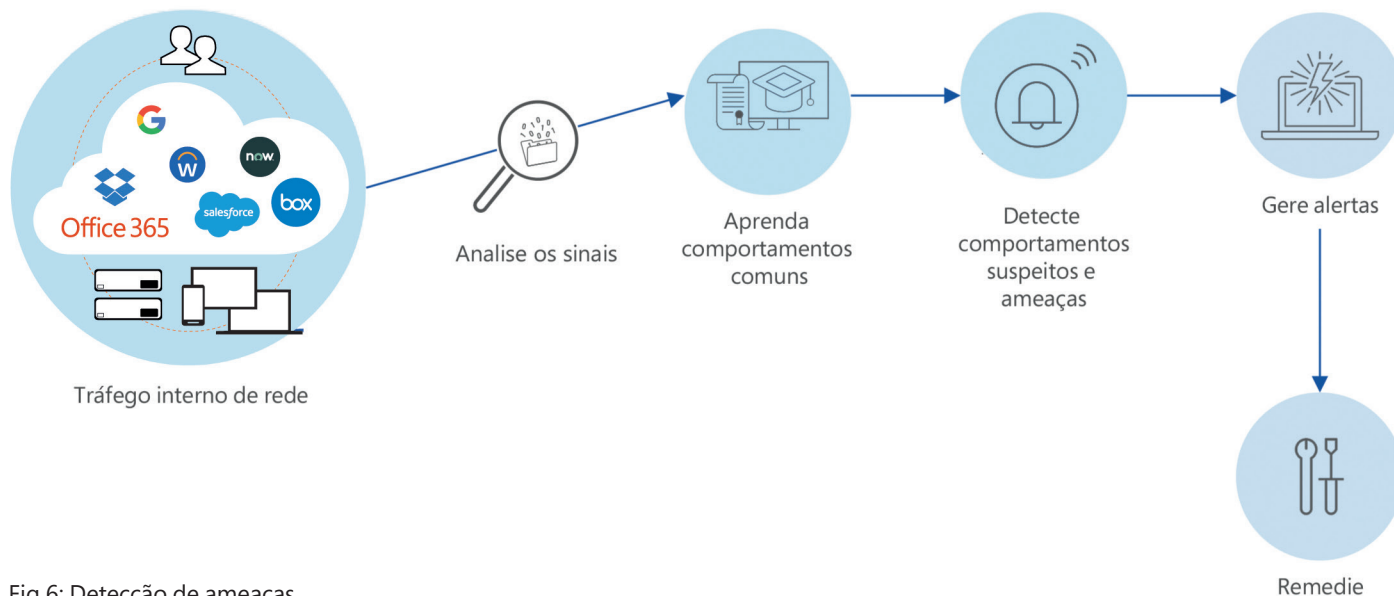


Fig 6: Detecção de ameaças.

Quando um vazamento acontece você quer detectá-lo o mais rápido possível para minimizar seu impacto, além de entender quais registros foram afetados. Com a LGPD, você deverá notificar quando houver um vazamento de dados.

Se alguma atividade fora do comum for detectada, receber alertas imediatamente, nos ajuda a monitorar comportamentos suspeitos como downloads em massa ou malwares. Estes alertas permitirão, em alguns casos, evitar um vazamento e, no caso de um vazamento ocorrer, permitirão correlacionar todos os dados e atividades a fim de determinar o impacto do vazamento e por fim, estancá-lo.

### Recursos Microsoft 365 para lhe ajudar:

- O Microsoft Advanced Threat Protection (Azure ATP, O365 ATP e Microsoft Defender ATP) ajuda os times de segurança a detectar, investigar, contextualizar e responder às ameaças em sua rede.
- **Proteja Identidades com Azure Advanced Threat Protection**  
Bloqueie logins maliciosos. Detecte e barre ameaças. Tenha uma visão abrangente do que está acontecendo na sua rede.
- **Proteja emails, aplicações, dados e documentos com O365 Advanced Threat Protection**  
Utilize-se de relatórios e inteligência para prevenir ameaças como Phishing e ataques Zero-day com o Office 365.
- **Proteja os dispositivos com Microsoft Defender Advanced Threat Protection**  
Investigue e responda automaticamente a ameaças complexas em seus dispositivos em minutos.
- **Proteja sua infra e/ou estrutura híbrida**  
Detecte e bloqueie atividades maliciosas em workloads on-premises ou na nuvem usando relatórios. Proteja seus servidores, dados, e informações de ataques sofisticados.

## 6. Como provar que os esforços corretos estão sendo executados para estar em conformidade com a lei

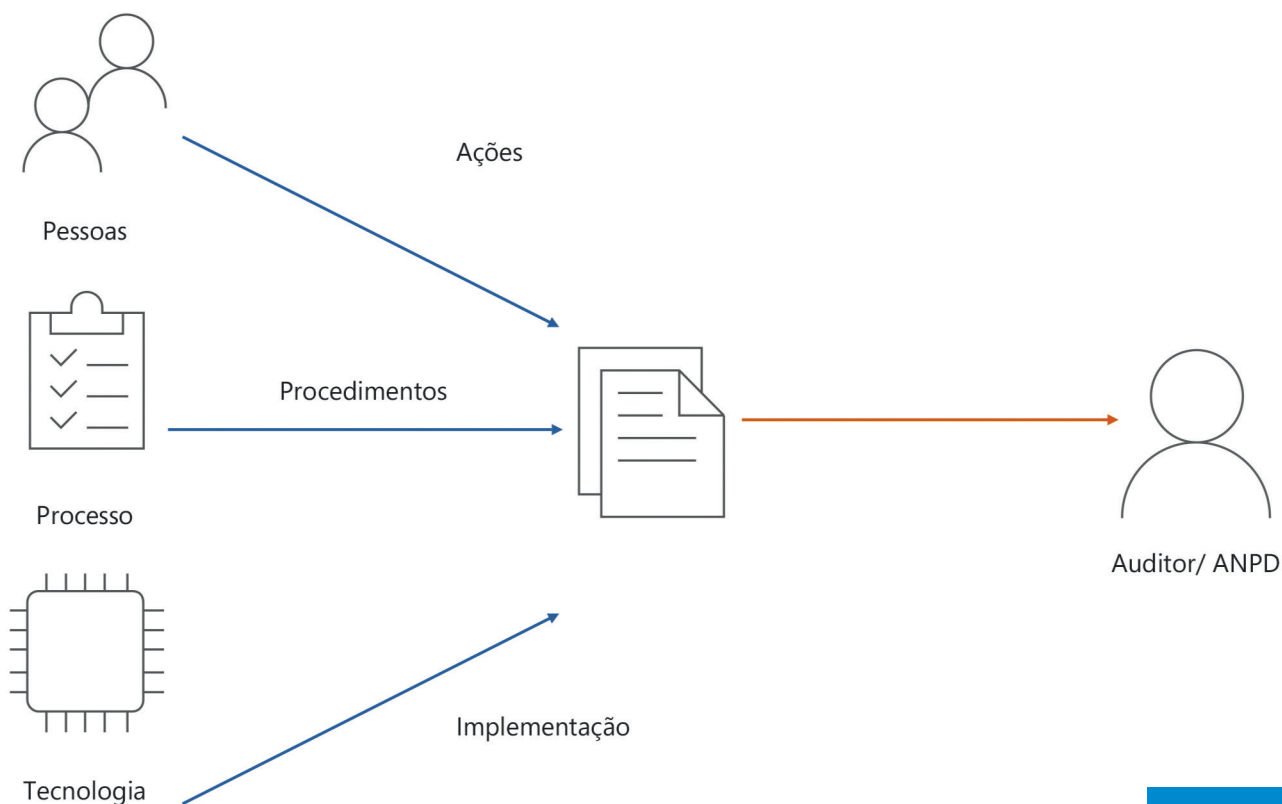


Fig 7: Pessoas, processos e tecnologia para a LGPD.



### A LGPD é sobre pessoas, processos & tecnologia.

Para mostrar a conformidade, precisamos documentar ações, procedimentos e implementação. Podemos apresentá-lo ao auditor/ Agência Nacional quando solicitado para mostrar que temos agido com o melhor de nossas capacidades para estar em conformidade com a lei. Uma das maneiras mais fáceis de fazer isso é com a ajuda de uma ferramenta, como o Compliance Manager.

#### Recursos Microsoft 365 para lhe ajudar:

O Compliance Manager, é uma ferramenta de avaliação de riscos baseada em workflows e está disponível hoje no Service Trust Portal, ajuda a acompanhar, atribuir e verificar as atividades de conformidade da sua organização na plataforma Microsoft. Disponível apenas para GDPR neste momento.

## 7. Como localizar dados de um titular

### Encontre dados associados com o indivíduo

- ✓ Busque dados no Exchange Online, Sharepoint Online, Onedrive for business (incluindo Teams e Grupos) e pastas públicas
- ✓ Busque dados pessoais através dos mais de 80 templates já construídos ou construa os seus próprios.
- ✓ Baixe dados para revisão futura antes de enviar aos titulares

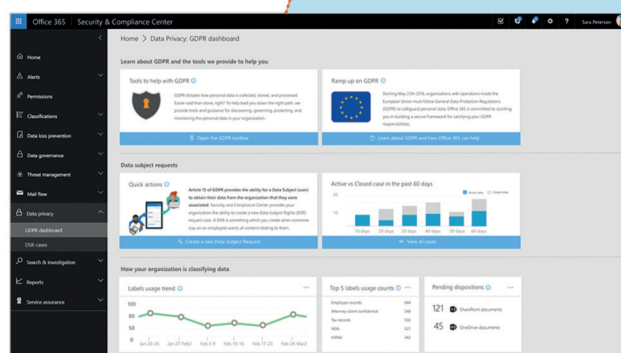


Fig 8: Pedido de dados de um titular.

Uma das ferramentas que oferecemos para simplificar os processos é a pesquisa de conteúdo do Office 365, O365 Content Search.

O O365 Content Search é uma ferramenta de descoberta eletrônica com recursos novos e aprimorados de dimensionamento e desempenho. Ele permite que você execute pesquisas de descoberta eletrônica em grandes volumes de conteúdo, sem limites para o número de locais de conteúdo a pesquisar. Alguns exemplos: pesquisar simultaneamente conteúdo em todas as caixas de correio, nas pastas públicas do Exchange, em todos os sites do SharePoint Online e nas contas do OneDrive for Business.

Depois de executar uma pesquisa de conteúdo bem-sucedida, você pode exportar os resultados da pesquisa para um computador local. Quando você exporta os resultados de e-mail, eles são baixados para o seu computador como arquivos PST. Quando você exporta conteúdo do SharePoint e OneDrive para sites de negócios, cópias de documentos nativos do Office são exportadas. Documentos e relatórios adicionais são incluídos com os resultados de pesquisa exportados.

Além disso, qualquer mensagem de email criptografada pelo RMS incluída nos resultados de uma pesquisa de conteúdo será descriptografada quando você exportá-las (como mensagens individuais). Esse recurso de descriptografia é habilitado por padrão para membros do grupo de funções do eDiscovery Manager.



Uma solução completa, inteligente e segura que capacita os funcionários



Libera a  
criatividade



Criado para o  
trabalho em equipe



Integrado para  
fins de simplicidade



Segurança  
inteligente



Entre em contato com seu representante Microsoft para conhecer mais sobre soluções de segurança e conformidade. A Microsoft está comprometida com a sua jornada de conformidade para a Lei Geral de Proteção de Dados.

<https://www.microsoft.com/pt-br/lgpd>