Microsoft

Lei Geral de Proteção de Dados com Microsoft 365

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 LGPR se aplica a:

a) A operação de tratamento seja realizada no Brasil ou os dados tenham sido coletados no Brasil;

b) Tratamento de dados pessoais de pessoas 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.
- **Operador:** A pessoa física ou jurídica que processa dados pessoais para ou em nome do controlador.

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

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

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

Impõe penalidades significativas por descumprimento

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

Isto além do dano reputacional e das possíveis indenizações decorrentes de ações dos titulares dos dados afetados.

Microsoft

A LGPD é sobre proteger informações sensíveis em qualquer lugar e em qualquer momento

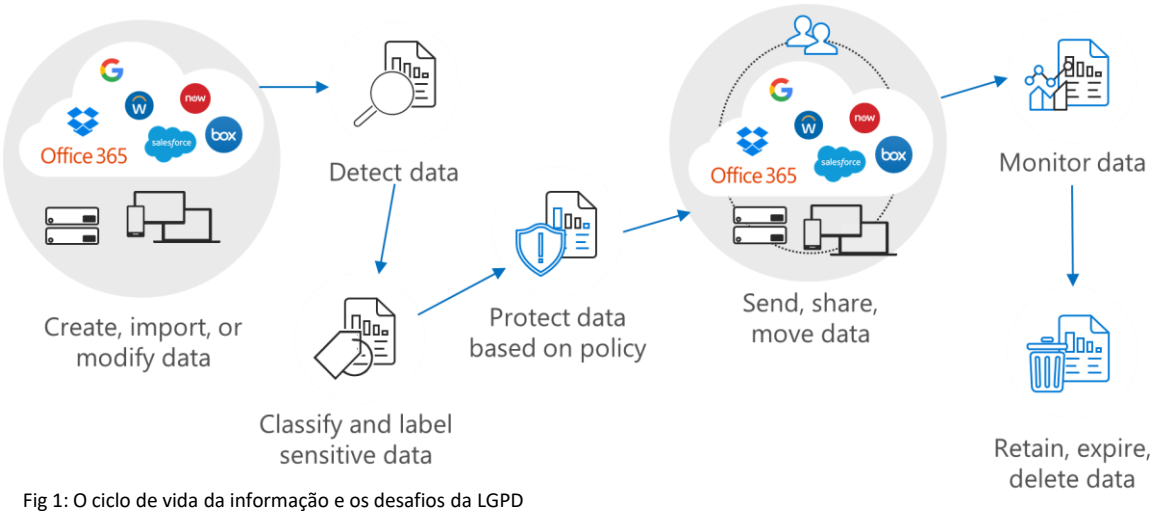

Fig 1: O ciclo de vida da informação e os desafios da LGPD

Desafios mais comuns de LGPD

1- Como descobrir dados sensíveis 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 visibiliade e controle de dados armazenados em aplicações na Nuvem;
5- Como detector 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 sensíveis em dados não estruturados

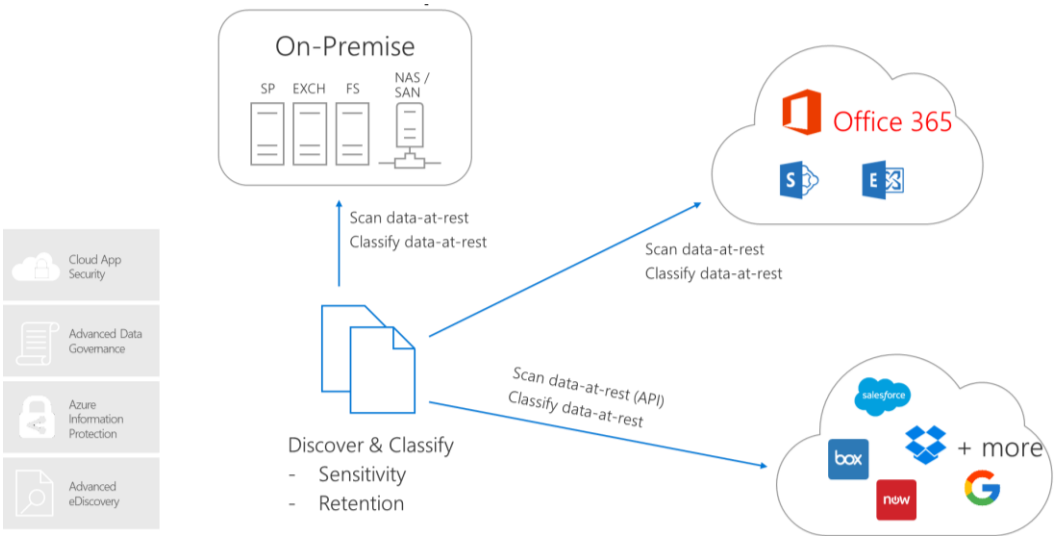

Fig 2: O desafio de dados em repouso em diferentes fontes de armazenamento

Toda organização tem muitos dados, inclusive dados sensíveis. Estes podem residir numa estrutura local, no Office 365, em outros aplicativos de nuvem ou na sua infra local. Independente de onde estejam, é preciso identificar estes dados sensíveis 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 automaticamente os dados, de acordo com definições prévias.

- *Office 365 eDiscovery search pode ser usado para encontrar texto e metadata em conteúdos espalhados em seus ativos do Office 365—SharePoint Online, OneDrive for Business, Skype for Business Online, and Exchange Online.*

- *Microsoft Cloud App Security é um serviço abrangente que prove 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 – e também ter uma avaliação de risco e analíticos.*

- *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 eDiscovery, baseado em aprendizado de máquina, pode te ajudar a identificar rapidamente documentos que são relevantes para um tema específico (como uma investigação de conformidade, por exemplo) e com melhor precisão que buscas trdicionais através de palavras-chaves ou revisões manuais de uma vasta quantidade de arquivos. O Advanced eDiscovery pode reduzir significantemente os custos e esforços para identificar documentos relevantes e relações entre dados através de aprendizado de máquina para treinar o Sistema para explorer 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

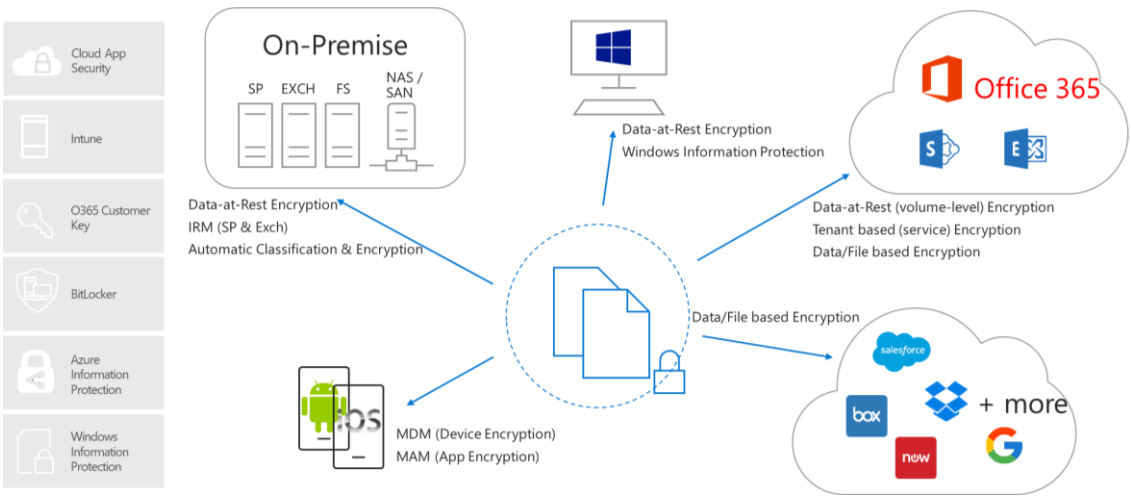

Fig 3: A Complexidades de proteger dados em diferentes aplicações e dispositivos

Você provavelmente tem dados sensíveis espalhados em diversas aplicações, e é possível potegê-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. Você, também, pode se utilizar de uma camada de proteção adicional, se utilizando do gerenciamento de direitos de informação no SharePoint e no Exchange que criptografará no nível do arquivo. Esta encriptação irá viajar com o arquivo aonde ele for, e a classificação e proteção podem ser automáticas, evitando possiveis erros de usuários.

Dispositivo
Você poderá habilitar a criptografia de disco para proteger os dados em repouso. Além disso, você poderá adicionar a separação de dados, separando os 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 nível de volume. Esta é a 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 o 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

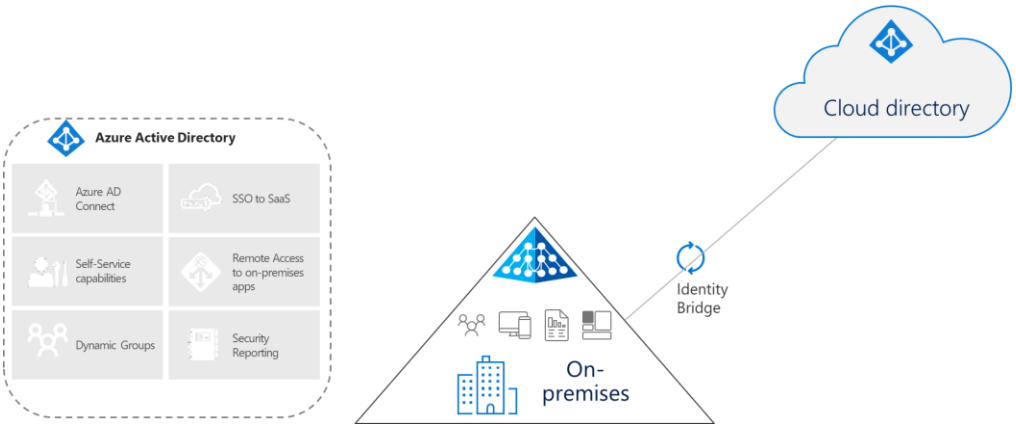

Fig 4: Gestão híbrida de Identidade e Acesso

Gestão de Identtidade e controle de 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 e 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 realmente 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 s as senhas)). Fáceis para um algoritmos 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 valher 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 logon único em aplicativos de nuvem, mas também abrirá opções para recursos de autoatendimento, como redefinições de senha de autoatendimento e acesso remoto a aplicativos locais, além de recursos como múltiplos fatores de autenticação para trazer uma camada adicional de proteção.

- *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 assignar acesso Just-In-Time (JIT) para usuários ADMIN, que expira após o período previsto de uso.*

4 - Como ter visibiliade e controle de dados armazenados em aplicações na nuvem

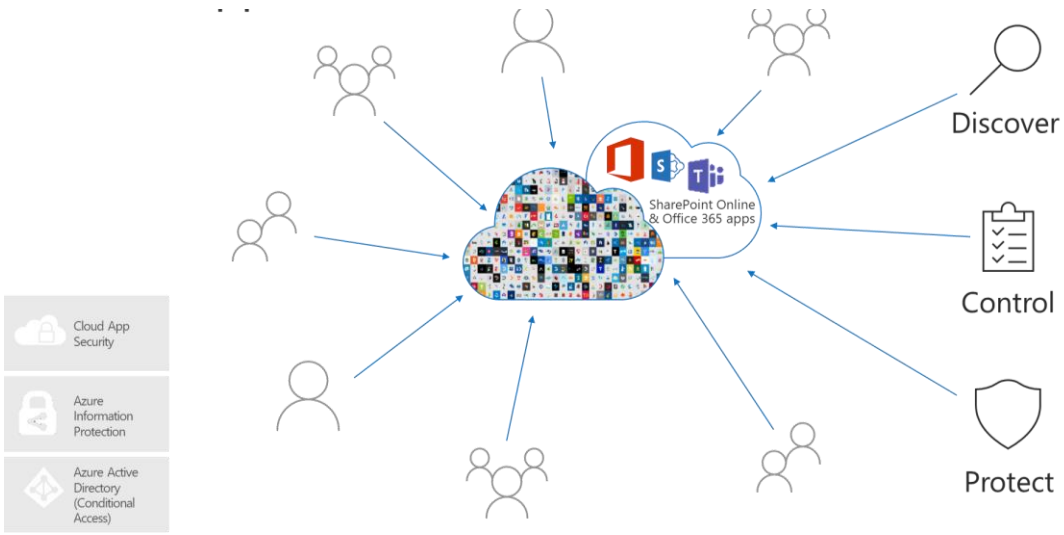

Fig 5: Visibilidade e Controle de dados em múltiplas nuvens.

A mudança para a nuvem aumenta a flexibilidade para os funcionários e reduz o custo de TI, mas também introduz novos desafios e complexidades para manter sua organização segura. É muito mais fácil para os funcionários assinarem um serviço de nuvem sem envolver a TI. Isto é o que chamamos de Shadow IT.

A primeira etapa que precisamos fazer é descobrir os aplicativos de nuvem que estão em uso dentro da organização e então fazer uma avaliação se esse aplicativo é adequado para a nossa organização.

Em seguida, precisamos começar a controlar esses aplicativos de nuvem. Isso pode significar que queremos bloquear o acesso a eles porque descobrimos que o risco do aplicativo é muito alto, mas também pode significar que queremos controlar como o aplicativo é acessado (por exemplo, somente de um dispositivo gerenciado ou de um local confiável).

E por fim, é importante começar a proteger os dados que estão nestes aplicativos. Isso pode significar que queremos que os dados sejam criptografados ou que queremos impedir que os dados sejam baixados para dispositivos não gerenciados, por exemplo.

- *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 – e também ter uma avaliação de risco e analíticos.*

5- Como detectar ameaças antes que causem danos maiores

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, será necessário reportar vazamentos de dados em até 72 horas após a detecção.

Imediatamente quando alguma atividade fora do comum é detectada, queremos receber um alerta, isto significa que você deseja monitorar comportamentos suspeitos como downloads em massa ou malwares. Estes alertas permitirão, em alguns casos, evitar uma vazamento e, no caso de um vazamento ocorrer, permitirão correlacionar todos os dados e atividades a fim de determinar o impacto da vazamento e por fim, estancá-lo.

- *O Microsoft Advanced Threat Protection (Azure ATP, O365 ATP and Win 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***

Bloquei logins maliciosos. Detecte e barre ameaças. Tenha uma visão abrangente com o Azure Active

- ***Proteja emails, aplicações, dados e documentos com O365 Advanced Threat Protection***

Aplique analíticos e inteligência para prevenir contra ameaças como Phishing e ataques que 0-day com o Office 365.

- ***Proteja os dispositivos com Windows Defender Advanced Threat Protection***

Investigue e responda automaticamente a ameaças complexas em seus dispositivos em minutos.

- ***Proteja sua infra estrutura híbrida***

Detecte e bloqueie atividades maliciosas em workloads on-premises ou na nuvem usando analíticos. Proteja seus servidores, dados, e informações de ataques sofisticados.

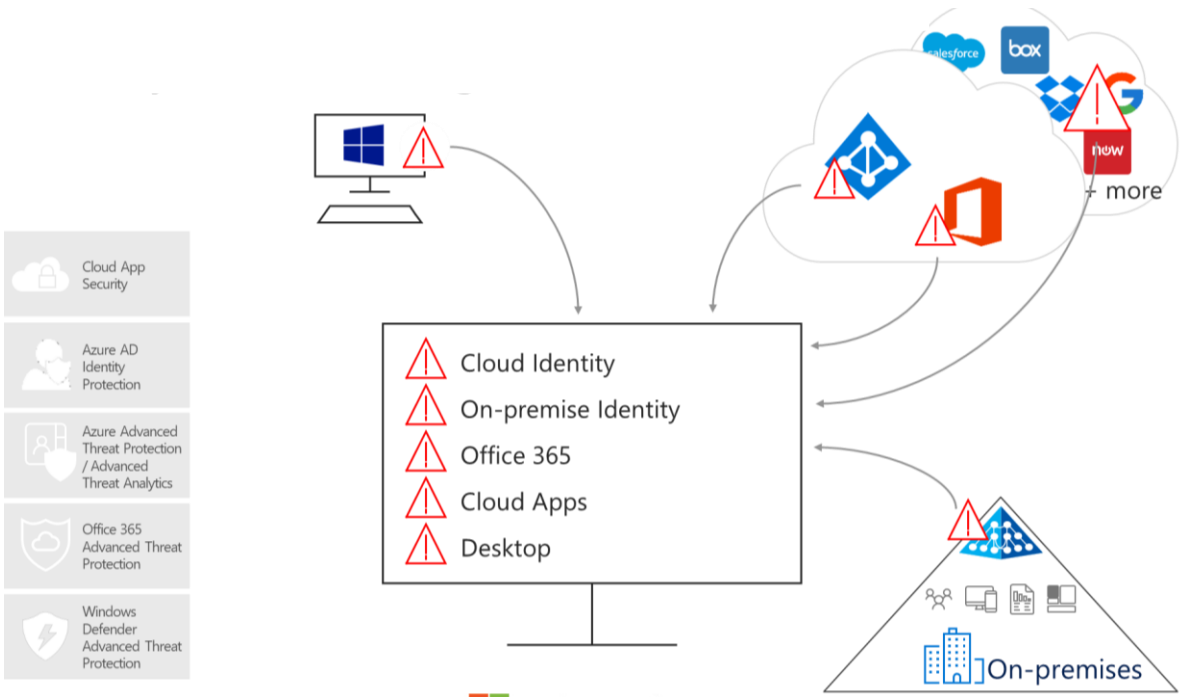

Fig 6: Correlação de sinais para detecção avançada c

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

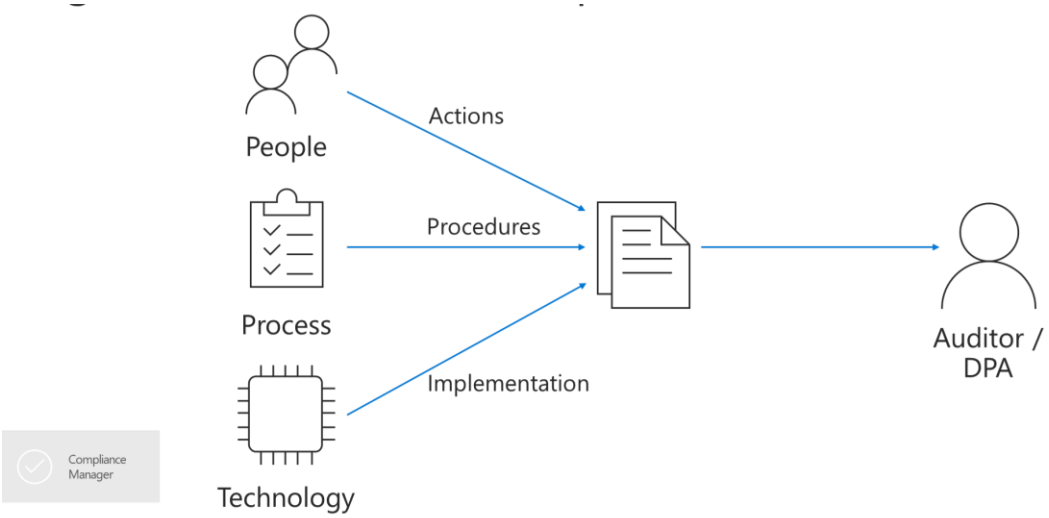

Fig 7: Pessoas, Processos e Tecnologia na jornada de conformidade com a LGPD.

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.*

- O Compliance Manager, é uma ferramenta de avaliação de riscos baseada em workpflows e está disponível hoje no Service Trust Portal, te ajuda a acompanhar, assignar 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

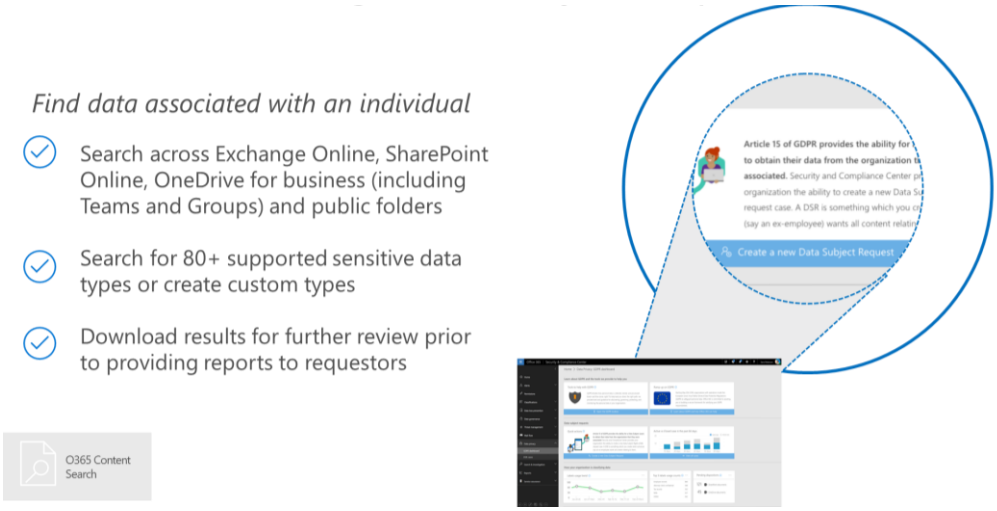

Fig 8: Recuperação de dados de titulares

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; Não há limites para o número de locais de conteúdo que você pode pesquisar. Você pode pesquisar todas as caixas de correio, todas as pastas públicas do Exchange e todos os sites do SharePoint Online e as contas do OneDrive for Business em uma única pesquisa de conteúdo. Também não há limites para o número de pesquisas que podem ser executadas ao mesmo tempo.

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.*

Microsoft 365

A complete, intelligent, secure solution to empower employees

Unlocks creativity

Built for teamwork

Integrated for simplicity

Intelligent security

Microsoft

Entre em contato com seu representate 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/trustcenter/privacy/gdpr