ANEEL
AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA

Procedimento Operacional para a Governança do Microsoft Power Platform

SEI nº 48500.007095/2025-44

Índice Analítico

1. Objetivo

Estabelecer os procedimentos, recomendações e detalhamentos da Política de Governança para o Desenvolvimento Distribuído de soluções de Tecnologia da Informação (TI) para o Microsoft Power Platform.

2. Histórico de Revisões

Versão	Descrição	Data	Atualizado por	Aprovado por
1.0	Elaboração do documento	18/02/2025	Thiago Luiz Leite Ribeiro da Costa	Adriana de Carvalho Drummond Vivan

3. UORG Responsável

SGI

4. Área Responsável

SGI / CSNGP / Coordenação de Soluções Negociais e Geoprocessamento

5. Abrangência

As soluções de TI desenvolvidas na Power Platform devem ser limitadas em escopo e impacto. Se desenvolvidas no âmbito do "Faça Você Mesmo", essas soluções não podem ter uma abrangência corporativa, ou seja, não devem ser projetadas para atender a toda a organização ou afetar múltiplas unidades organizacionais.

Além disso, as soluções de TI desenvolvidas na Power Platform não podem estar associadas a processos de alta criticidade, que são aqueles essenciais para a operação segura e eficiente da ANEEL.

6. Requisitos para atribuição de licenças premium

Para atribuir licenças premium do Power Automate e do Power Apps para desenvolvedores negociais, é essencial considerar tanto os tipos de licenças disponíveis quanto as responsabilidades dos desenvolvedores negociais.

Tanto as licenças vinculadas ao Microsoft Copilot 365 quanto as licenças premium podem ser usadas por desenvolvedores para criar e automatizar soluções de TI que atendam às necessidades específicas da ANEEL, garantindo conformidade com as normas de governança e segurança.

A atribuição de uma licença Premium se verifica necessária somente quanto há a aplicação de uso de conectores Premium, os quais podem ser verificados nesta URL: Lista de todos os conectores Premium | Microsoft Learn

A licença Power Apps (Premium ou vinculada ao Microsoft Copilot 365) permite o uso do Power Apps, uma plataforma que possibilita a criação de aplicativos personalizados para atender às necessidades específicas de negócios. Esta licença é baseada em usuário, o que significa que cada usuário individual precisa de uma licença para acessar e utilizar o Power Apps.

A licença Power Automate (Premium ou vinculada ao Microsoft Copilot 365) permite o uso do Power Automate, uma ferramenta que permite automatizar fluxos de trabalho entre aplicativos e serviços. Esta licença

também é baseada em usuário, permitindo que cada usuário individual utilize o Power Automate para automatizar processos de negócios.

Entretanto, tanto para Power Apps quanto para Power Automate, caso sejam necessários uso de conectores Premium, são necessárias licenças Premium.

Os desenvolvedores negociais têm várias necessidades que justificam a atribuição de licenças premium para ferramentas como Power Automate e Power Apps. Contudo, para que as licenças premium sejam adequadamente atribuídas, eles devem considerar os seguintes requisitos:

- Cumprir com as normas de governança de dados e de segurança da informação vigentes na ANEEL, bem como com as instruções e procedimentos operacionais da SGI;
- Desenvolver novas soluções de TI negociais conforme as necessidades e normas da ANEEL;
- Realizar atualizações e correções de erros nas soluções existentes;
- Manter documentação técnica detalhada sobre as soluções de TI negociais;
- Testar novas soluções para garantir que atendam aos requisitos funcionais e de segurança;
- Garantir que o código desenvolvido esteja em conformidade com os padrões técnicos da SGI e de segurança;
- Manter-se capacitados na utilização da Microsoft Power Platform para o desenvolvimento distribuído. O requisito de capacitação para a Power Platform é de 20 horas a cada dois anos.

Uma vez atribuídas as licenças premium do Power Automate e do Power Apps, os desenvolvedores negociais devem cumprir rigorosamente com os requisitos estabelecidos, incluindo a capacitação de 20 horas a cada dois anos. Caso contrário, a licença não será atribuída ou poderá ser retirada e seus aplicativos e fluxo serão descontinuados.

É fundamental que os desenvolvedores se mantenham atualizados e em conformidade com as normas de governança de dados e de segurança da informação, bem como com as instruções e procedimentos operacionais da SGI, para garantir a continuidade do uso das ferramentas e a eficácia no desenvolvimento de soluções de TI negociais

7. Gestão do Ciclo de Vida de Aplicações (ALM1 - Application Lifecycle Management)

7.1 Uso de Soluções

No Microsoft Power Platform, as **soluções** são usadas para transportar aplicativos e componentes de um ambiente para outro ou para aplicar um conjunto de personalizações a aplicativos existentes. Elas são essenciais para o gerenciamento do ciclo de vida das aplicações (ALM) no Power Apps e Power Automate.

Recomenda-se a utilização de soluções para transportar aplicativos e componentes de um ambiente para outro ou para aplicar um conjunto de personalizações a aplicativos existentes.

7.2 Recursos das soluções:

As soluções no Microsoft Power Platform são ferramentas que permitem aos desenvolvedores e administradores gerenciar e transportar aplicativos e componentes entre diferentes ambientes. Elas facilitam a

[1] ALM (Application Lifecycle Management): Gestão do ciclo de vida do aplicativo desde sua concepção até sua descontinuação.

aplicação de personalizações e a implementação de novos recursos em aplicativos existentes. As soluções possuem os seguintes recursos:

- As soluções incluem metadados e algumas entidades com dados de configuração e não contêm dados corporativos.
- As soluções podem conter vários componentes diferentes do Microsoft Power Platform, como aplicativos baseados em modelo, aplicativos de tela, mapas de sites, fluxos, entidades, formulários, conectores personalizados, recursos da Web, conjuntos de opções, gráficos e campos. Observa-se que nem todas as entidades podem ser incluídas em uma solução. Por exemplo, as tabelas de sistema Usuário do Aplicativo, API Personalizada e Configuração da Organização não podem ser adicionadas a uma solução.
- As soluções são empacotadas como uma unidade a ser exportada e importada para outros ambientes ou desconstruídas e verificadas no controle do código-fonte como código-fonte de ativos. As soluções também são usadas para aplicar alterações a soluções existentes.
- As soluções gerenciadas são usadas para implantar a qualquer ambiente que não seja um ambiente de desenvolvimento para essa solução. Isso inclui testes, teste de aceitação do usuário (UAT), teste de integração do sistema (SIT) e ambientes de produção. As soluções gerenciadas podem ser atendidas (atualização, patch e exclusão) independentemente de outras soluções gerenciadas em um ambiente. Como prática recomendada do ALM, as soluções gerenciadas devem ser geradas por um servidor de compilação e consideradas um artefato de compilação.
- As atualizações de solução gerenciada são implantadas à versão anterior da solução gerenciada. Isso não cria uma camada de solução adicional. Não é possível excluir componentes usando uma atualização.
- Um patch[2] contém somente as alterações de uma solução pai gerenciada. Deve-se usar patches somente ao fazer pequenas atualizações (semelhante a um hotfix[3]) e ao exigir que ele possa ser desinstalado. Quando os patches são importados, eles são sobrepostos no topo da solução primária. Não é possível excluir componentes usando um patch.
- Ao se atualizar uma solução, será instalada uma nova camada de solução imediatamente acima da camada base e quaisquer patches existentes. Isso exclui todos os patches existentes e a camada base.
-
- As atualizações da solução excluirão os componentes existentes, mas que não serão mais incluídos na versão atualizada.

7.3 Detalhamento do ALM na Power Platform

7.3.1 Papéis e recomendações:

Os pipelines no Power Platform têm como objetivo tornar o gerenciamento do ciclo de vida dos aplicativos (ALM) mais acessível para os usuários do Power Platform. Eles oferecem funcionalidades de automação do ALM, bem como integração e entrega contínuas (CI/CD[4]), facilitando o uso dessas ferramentas por criadores, administradores e desenvolvedores de todos os níveis.

[2] Patch é um pequeno programa de computador que pode ser adicionado a um software existente para corrigir problemas, melhorar a funcionalidade ou atualizar o sistema.

[3] Hotfix é uma correção rápida e específica aplicada a um software para resolver problemas críticos, como bugs ou falhas de segurança.

[4] CI/CD (Continuous Integration/Continuous Deployment): Práticas de integração e entrega contínua no desenvolvimento de software.

Para garantir a consistência, rastreabilidade e automação nas entregas de soluções e aplicativos, recomenda-se:

- **Administrador:** Os pipelines são uma ferramenta importante para administradores, permitindo configurar, gerenciar e monitorar os fluxos de desenvolvimento e implantação. Isso assegura que as entregas sejam consistentes e rastreáveis.
- **Desenvolvedor Cidadão:** Embora os desenvolvedores departamentais geralmente não sejam desenvolvedores profissionais, eles também podem se beneficiar do uso de pipelines. Esses recursos garantem que suas soluções sejam implantadas de maneira organizada e controlada, permitindo uma automação simplificada e adaptada às suas necessidades.
- **Desenvolvedor Profissional:** Desenvolvedores profissionais podem utilizar o Azure DevOps[5] para gerenciar código-fonte, realizar testes automatizados, controle de versão e integrar CI/CD (Integração Contínua/Entrega Contínua) ao ciclo de desenvolvimento.

Importante ressaltar que todos os aplicativos deverão passar por toda a esteira de ambientes, incluindo desenvolvimento, homologação e produção.

7.3.2 Processo de ALM:

O Application Lifecycle Management (ALM), ou Gerenciamento do Ciclo de Vida de Aplicações, é um conjunto de processos, práticas e ferramentas que gerenciam o ciclo de vida de um aplicativo desde a concepção até a sua descontinuação. No contexto da Power Platform, o ALM abrange a gestão de aplicativos, fluxos de trabalho automatizados, chatbots e relatórios, assegurando que eles sejam desenvolvidos, testados, implantados e mantidos de forma eficiente e segura.

a. Planejamento

A etapa de planejamento da aplicação no processo de ALM é fundamental para garantir o sucesso do desenvolvimento e implementação do aplicativo. Durante essa fase, são definidos os requisitos, o escopo e os objetivos do projeto. Isso inclui a identificação das necessidades dos usuários, a especificação das funcionalidades desejadas e a definição dos critérios de sucesso.

Além disso, o planejamento envolve a criação de um cronograma detalhado, a alocação de recursos e a identificação de possíveis riscos e estratégias de mitigação. É também nessa etapa que são estabelecidos os marcos e as entregas do projeto, garantindo que todas as partes interessadas estejam alinhadas e cientes das expectativas.

b. Desenvolvimento

A etapa de desenvolvimento da aplicação no processo de ALM é onde a criação e a codificação do aplicativo realmente acontecem. Durante essa fase, os desenvolvedores trabalham para transformar os requisitos e especificações definidos na etapa de planejamento em um produto funcional.

Os desenvolvedores utilizam práticas de desenvolvimento ágil, que incluem a divisão do trabalho em sprints ou iterações curtas, permitindo ajustes rápidos e contínuos com base no feedback. Eles escrevem o código, criam

[5] Azure DevOps: Plataforma da Microsoft para controle de versão, gerenciamento de projetos e automação de pipelines.

as interfaces de usuário, integram sistemas e garantem que todas as funcionalidades estejam implementadas conforme planejado.

Os desenvolvedores devem criar soluções modulares e reutilizáveis, bem documentadas e seguindo as melhores práticas de codificação.

Além disso, a fase de desenvolvimento envolve testes contínuos para identificar e corrigir bugs o mais cedo possível, garantindo que o aplicativo esteja funcionando corretamente antes de avançar para a próxima etapa.

Todo o código deve ser gerenciado por meio de um sistema de controle de versão, preferencialmente utilizando o Azure DevOps para gerenciar versões, revisar códigos e integrar mudanças.

c. **Teste**

Nesta etapa o aplicativo é movido para o ambiente de homologação é fundamental para garantir que o aplicativo funcione conforme o esperado e esteja livre de defeitos. Durante essa fase, são realizados diversos tipos de testes, como testes unitários, de integração, de sistema e de aceitação, para validar que todas as partes do aplicativo estão operando corretamente e de forma integrada.

Os testes unitários verificam a funcionalidade de componentes individuais do código, enquanto os testes de integração asseguram que diferentes módulos do aplicativo funcionem bem juntos. Os testes de sistema avaliam o comportamento do aplicativo como um todo, e os testes de aceitação garantem que o produto atenda aos requisitos e expectativas dos usuários.

Além disso, a fase de teste envolve a identificação e correção de bugs, bem como a realização de testes de desempenho e segurança para assegurar que o aplicativo seja robusto e confiável antes de ser implantado no ambiente de produção.

d. **Implantação**

A etapa de implantação da aplicação no processo de ALM é onde o aplicativo é transferido do ambiente de desenvolvimento para o ambiente de produção, tornando-o disponível para os usuários finais. Durante essa fase, são realizadas várias atividades para garantir uma transição suave e bem-sucedida.

Primeiramente, é importante preparar o ambiente de produção, configurando servidores, bancos de dados e outros recursos necessários. O ambiente de produção deve ser preparado com base nos resultados dos testes, assegurando que todas as configurações de segurança estejam implementadas corretamente. Em seguida, o aplicativo é implantado, o que pode envolver a cópia de arquivos, a configuração de serviços e a execução de scripts de inicialização.

Recomenda-se a adoções de práticas de CI/CD (Integração Contínua/Entrega Contínua) para automatizar a implantação, utilizando ferramentas como Azure DevOps para facilitar a entrega contínua.

Após a implantação, são realizados testes finais para garantir que o aplicativo esteja funcionando corretamente no ambiente de produção. Isso inclui verificar a conectividade, a funcionalidade e o desempenho do aplicativo. Além disso, é essencial monitorar o aplicativo de perto nas primeiras horas ou dias após a implantação para identificar e resolver rapidamente quaisquer problemas que possam surgir.

e. **Monitoramento e Manutenção**

A etapa de monitoramento e manutenção da aplicação no processo de ALM é essencial para garantir que o aplicativo continue funcionando de maneira eficiente e segura após a implantação. Durante essa fase, o

desempenho do aplicativo é constantemente supervisionado para identificar e resolver quaisquer problemas que possam surgir.

O monitoramento envolve a coleta de dados sobre o uso do aplicativo, desempenho, erros e outros indicadores-chave. Isso permite que a equipe de desenvolvimento detecte rapidamente quaisquer anomalias ou falhas e tome medidas corretivas antes que afetem os usuários finais. Neste sentido, deve ser estabelecido um plano de ação para resolução rápida de incidentes, minimizando o impacto no usuário final.

Para o monitoramento, recomenda-se a implementação de ferramentas como *Azure Monitor* e *Application Insights*, para alertar sobre possíveis problemas de performance, segurança ou falhas operacionais.

A manutenção inclui a aplicação de atualizações e patches para corrigir bugs, melhorar a segurança e adicionar novas funcionalidades, documentando todas as alterações e garantindo que sejam testadas antes de sua aplicação em produção. Também envolve a realização de ajustes e otimizações contínuas para garantir que o aplicativo continue atendendo às necessidades dos usuários e se adapte a mudanças no ambiente de negócios ou na tecnologia.

f. **Descontinuação**

A etapa de descontinuação da aplicação no processo de ALM é o momento em que o aplicativo é retirado de uso, seja por ter sido substituído por uma versão mais nova, por não ser mais necessário ou por não atender mais aos requisitos do negócio. Durante essa fase, várias atividades são realizadas para garantir uma transição suave e minimizar o impacto nos usuários.

Primeiramente, é importante comunicar a descontinuação aos usuários e partes interessadas, fornecendo informações sobre prazos e alternativas disponíveis. Em seguida, o aplicativo é gradualmente desativado, o que pode envolver a migração de dados para novos sistemas, a desativação de servidores e a remoção de acessos.

Além disso, é essencial garantir que todos os dados e informações sensíveis sejam devidamente arquivados ou destruídos, conforme as políticas de segurança e conformidade. A documentação do processo de descontinuação também é importante para futuras referências e auditorias.

8. Ambientes

8.1 Usos dos ambientes

Os ambientes são espaços virtuais utilizados para armazenar, gerenciar e compartilhar dados corporativos, aplicativos e processos empresariais. Eles são essenciais para separar aplicativos que podem ter diferentes funções, requisitos de segurança ou públicos-alvo.

a. **Ambiente de Produção**

O ambiente de produção é essencial para garantir que os aplicativos e sistemas estejam prontos para uso pelos usuários finais.

- **Objetivo:** O principal objetivo do ambiente de produção é hospedar aplicativos essenciais de negócios que estão prontos para uso pelos usuários finais. Ele é destinado ao uso para trabalhos permanentes em uma organização e deve ser configurado para suportar cargas de trabalho reais.

- **Usos Típicos:** Os usos típicos do ambiente de produção incluem a hospedagem de fluxos de trabalho automáticos em uso contínuo e o armazenamento de dados de produção no Dataverse[6]. Esse ambiente é utilizado para garantir que os aplicativos funcionem corretamente e atendam às necessidades dos usuários finais sem interrupções.
- **Segurança:** A segurança no ambiente de produção é uma prioridade. Ele deve ter controle total para garantir que apenas usuários autorizados possam acessar e modificar os dados e aplicativos. Isso inclui a implementação de medidas de segurança robustas, como autenticação, autorização, criptografia de dados e monitoramento contínuo para detectar e responder a possíveis ameaças.

b. **Ambiente de Desenvolvimento**

O ambiente de desenvolvimento é essencial para a criação e teste de aplicativos antes de sua implantação em produção.

- **Objetivo:** O principal objetivo do ambiente de desenvolvimento é fornecer um espaço isolado onde os desenvolvedores possam criar, modificar e testar aplicativos sem afetar a versão ativa do produto de software. Ele permite que os desenvolvedores experimentem novas funcionalidades, integrem sistemas e realizem ajustes necessários antes de mover o aplicativo para o ambiente de produção. Esses são ambientes destinados para uso compartilhado entre os desenvolvedores (sejam desenvolvedores cidadãos ou desenvolvedores profissionais).
- **Usos Típicos:** Os usos típicos do ambiente de desenvolvimento incluem o desenvolvimento e teste de aplicativos, fluxos de trabalho e integrações de maneira isolada. Os desenvolvedores utilizam esse ambiente para escrever, depurar e aplicar patches no código, garantindo que todas as funcionalidades estejam implementadas conforme planejado. Além disso, é um espaço para experimentação com novas funcionalidades ou conectores, utilizando dados fictícios ou isolados para evitar impacto nos dados de produção.
- **Segurança:** A segurança no ambiente de desenvolvimento é controlada, mas menos restritiva em comparação com o ambiente de produção. O acesso é geralmente limitado aos desenvolvedores e administradores, e grupos de segurança não podem ser atribuídos a ambientes de desenvolvedor. É importante implementar controle de versão de código e logs de atividade para rastreamento das modificações realizadas. Além disso, treinamentos periódicos sobre boas práticas de desenvolvimento são essenciais para garantir que os desenvolvedores sigam as diretrizes de segurança estabelecidas.

c. **Ambiente de Teste**

O ambiente de teste é essencial para garantir que os aplicativos funcionem corretamente antes de serem implantados no ambiente de produção.

- **Objetivo:** O principal objetivo do ambiente de teste é fornecer um espaço controlado onde os desenvolvedores e testadores possam validar a funcionalidade, desempenho e segurança dos aplicativos sem afetar o ambiente de produção. Ele permite a identificação e correção de falhas, vulnerabilidades e problemas de desempenho em um estágio inicial do ciclo de vida da aplicação.

[6] Dataverse é uma plataforma de dados da Microsoft Power Platform que permite armazenar e gerenciar dados de maneira estruturada e segura, facilitando a integração com outros serviços e aplicativos.

- **Usos Típicos:** Os usos típicos do ambiente de teste incluem a execução de testes unitários, de integração, de sistema e de aceitação. Esse ambiente é utilizado para simular cenários reais de uso, garantindo que todas as funcionalidades do aplicativo estejam operando conforme esperado. Além disso, é um espaço para realizar testes de desempenho e segurança, utilizando dados fictícios ou anonimizados para evitar impacto nos dados de produção.
- **Segurança:** A segurança no ambiente de teste é crucial para garantir que os testes sejam realizados de maneira segura e controlada. O ambiente de teste deve ser isolado do ambiente de produção e de outros ambientes de teste para evitar interferências. Além disso, é importante implementar controles de acesso rigorosos, garantindo que apenas usuários autorizados possam acessar e modificar os dados e configurações do ambiente de teste.

d. **Ambiente de Sandbox**

O ambiente de Sandbox é uma ferramenta valiosa para experimentação e inovação, permitindo que desenvolvedores e analistas testem novas ideias e funcionalidades sem o risco de impactar os ambientes de produção.

- **Objetivo:** O principal objetivo do ambiente de Sandbox é fornecer um espaço isolado e seguro para a experimentação e inovação. Ele permite que os usuários testem novas funcionalidades, configurações e integrações sem afetar os sistemas de produção.
- **Usos Típicos**: Os usos típicos do ambiente de Sandbox incluem experimentações e inovações, permitindo que os desenvolvedores modifiquem configurações e testem novos recursos sem as restrições dos ambientes de produção e teste.
- **Segurança:** A segurança no ambiente de Sandbox é garantida pelo isolamento total do ambiente de produção, o que assegura que as experiências não interfiram com as operações diárias. Os ambientes de Sandbox são temporários e serão redefinidos ou descartados após o uso.

e. **Ambiente de Trial**

O ambiente de Trial, também conhecido como ambiente de avaliação, é utilizado para suportar necessidades de teste de curto prazo e é automaticamente limpo após um período específico.

- **Objetivo:** O principal objetivo do ambiente de Trial é fornecer um espaço temporário para testes e avaliações de curto prazo. Ele permite que os usuários experimentem novas funcionalidades, configurações e integrações sem afetar os sistemas de produção.
- **Usos Típicos:** Os usos típicos do ambiente de Trial incluem a realização de testes de funcionalidades, avaliações de desempenho e experimentações com novas configurações. Esse ambiente é ideal para testar rapidamente novas ideias ou soluções antes de decidir se devem ser implementadas em um ambiente mais permanente. Ele é limitado a um por usuário e expira após 30 dias, garantindo que os recursos sejam utilizados de forma eficiente e que não haja acúmulo de ambientes desnecessários.
- **Segurança:** A segurança no ambiente de Trial é garantida pelo isolamento total do ambiente de produção, o que assegura que as experiências não interfiram com as operações diárias. O acesso ao ambiente de Trial é geralmente restrito aos administradores, e os dados utilizados são fictícios ou anonimizados para proteger informações sensíveis durante os testes.

f. **Ambiente Microsoft Dataverse for Teams**

O Microsoft Dataverse for Teams é uma plataforma de dados Low-Code integrada ao Microsoft Teams, que permite aos usuários criar aplicativos, bots e fluxos personalizados diretamente no Teams usando Power Apps, Microsoft Copilot Studio e Power Automate. Os ambientes do Dataverse for Teams são criados automaticamente para a equipe selecionada quando é criado um aplicativo no Teams usando o aplicativo pela primeira vez ou quando é instalado um aplicativo do catálogo de aplicativos.

- **Objetivo:** O principal objetivo do Dataverse for Teams é fornecer um ambiente simplificado e integrado para a criação e gerenciamento de aplicativos e dados dentro do Microsoft Teams. Ele facilita a colaboração e a inovação, permitindo que as equipes criem soluções personalizadas sem a necessidade de sair do Teams.
- **Usos Típicos:** Os usos típicos do Dataverse for Teams incluem a criação de aplicativos, bots e fluxos que são específicos para as necessidades de uma equipe. Por exemplo, uma equipe pode criar um aplicativo para gerenciar tarefas, um bot para responder a perguntas frequentes ou um fluxo para automatizar processos de aprovação. Todos os dados, aplicativos, bots e fluxos criados no Teams são armazenados no banco de dados do Dataverse for Teams dessa equipe.
- **Segurança:** A segurança no Dataverse for Teams é garantida pelo alinhamento com as construções do Microsoft Teams. Os membros do Teams são mapeados automaticamente para o seu tipo de associação do Teams (proprietários, membros e convidados), com um direito de acesso atribuído pelo sistema. Além disso, a SGI pode se envolver efetivamente com novos criadores e garantir que a capacidade do Dataverse for Teams seja usada de maneira eficaz, aplicando políticas específicas e chamando a limpeza de ativos não utilizados. O Dataverse for Teams também oferece governança de nível empresarial e implantação de solução com um clique na loja de aplicativos do Microsoft Teams.

8.2 Ambiente Padrão

O ambiente padrão é um espaço criado automaticamente pelo Power Apps para cada locatário[7] e é compartilhado por todos os usuários desse locatário.

Todos os funcionários de uma organização que utilizam o Power Platform têm acesso ao ambiente padrão e são adicionados automaticamente à função de Criador, permitindo que qualquer usuário licenciado crie aplicativos e fluxos de trabalho dentro desse ambiente.

As seguintes recomendações ajudam a manter a organização e a segurança do ambiente padrão, garantindo que ele seja utilizado de forma eficiente e controlada.

a. **Definir administradores**

Para garantir uma gestão eficiente e segura do ambiente padrão no Power Platform, é essencial definir administradores de sistema confiáveis. Os administradores da Microsoft 365 Power Platform não recebem mais automaticamente permissões de administrador do Dataverse no ambiente padrão, e nenhum outro usuário é adicionado como administrador nesse ambiente. Para evitar um bloqueio administrativo, recomenda-se conceder

[7] Um locatário é uma entidade ou organização que possui uma assinatura do Microsoft Power Platform e gerencia os ambientes e recursos dentro dessa assinatura

o direito de acesso como administrador do sistema a alguns usuários confiáveis, sem, no entanto, atribuir-lhes a função de administrador da Power Platform. Isso permite que esses administradores gerenciem e mantenham o ambiente, garantindo que ele funcione de maneira eficiente e segura.

É igualmente importante monitorar o uso do ambiente padrão e identificar aplicativos e fluxos órfãos ou não utilizados. Utilizar ferramentas como o CoE (Centro de Excelência) pode ajudar a entender o que está acontecendo nos ambientes e estabelecer processos para limpar esses itens regularmente, evitando a sobrecarga do ambiente. Implementar políticas para colocar aplicativos em quarentena quando necessário, como durante revisões ou atualizações, também é uma prática recomendada. Isso permite que os criadores editem os aplicativos enquanto os usuários não podem acessá-los até que a quarentena seja removida, garantindo a segurança e a eficiência do ambiente padrão.

b. **Renomear o ambiente padrão**

Renomear o ambiente padrão no Power Platform é uma prática recomendada para melhorar a clareza e a gestão dos recursos. Ao renomear o ambiente padrão para algo mais descritivo, como "Ambiente de produtividade pessoal", você evidencia a intenção do ambiente e facilita a sua identificação e uso pelos usuários. Isso ajuda a evitar confusões e garante que todos entendam o propósito específico desse ambiente, promovendo uma utilização mais eficiente e organizada dos recursos disponíveis.

c. **Gerenciar o ambiente padrão**

Gerenciar o ambiente padrão no Power Platform é essencial para garantir a eficiência e a segurança dos recursos. Como todos os funcionários de uma organização têm acesso a esse ambiente, é essencial implementar formas de controle para evitar a sobrecarga com aplicativos e fluxos órfãos ou não utilizados. Utilizar ferramentas como o Centro de Excelência (CoE) pode fornecer informações sobre o uso do ambiente, permitindo que os administradores monitorem e analisem as atividades, identifiquem padrões de uso e tomem decisões informadas sobre a alocação de recursos e a necessidade de limpeza regular.

Além disso, é recomendável estabelecer políticas claras para a criação e manutenção de aplicativos e fluxos no ambiente padrão. Isso inclui definir processos para a revisão e aprovação de novos aplicativos, bem como para a desativação de aplicativos que não são mais necessários. Implementar políticas de quarentena para aplicativos durante revisões ou atualizações também pode ajudar a garantir que apenas aplicativos seguros e funcionais estejam disponíveis para os usuários. Ao adotar essas práticas, os administradores podem manter o ambiente padrão organizado, seguro e eficiente, promovendo a produtividade e a inovação dentro da organização.

d. **Fluxos órfãos e não utilizados**

Recomenda-se a realização de auditorias regulares para identificar fluxos que não foram executados em um período de seis meses. Esses fluxos devem ser analisados para determinar se ainda são necessários ou se podem ser desativados. A desativação de fluxos não utilizados não só libera recursos do sistema, mas também reduz o risco de falhas e problemas de segurança associados a fluxos desatualizados ou mal configurados.

Além disso, é importante estabelecer diretrizes claras para a criação e manutenção de fluxos. Os criadores de fluxos devem ser incentivados a documentar suas criações e a transferir a propriedade dos fluxos quando mudarem de função ou deixarem a organização. Isso garante que os fluxos permaneçam sob a supervisão de alguém responsável e evita que se tornem órfãos. A implementação de um sistema de notificações para alertar os

administradores sobre fluxos inativos também pode ser uma medida eficaz para manter a integridade e a eficiência do ambiente de trabalho.

e. **Análise de uso e reorganização**

Para garantir uma gestão adequada de aplicativos e fluxos amplamente adotados ou essenciais para a organização, é fundamental realizar uma análise de uso regular. Embora o ambiente padrão seja voltado à produtividade pessoal, criadores podem desenvolver soluções que se tornem amplamente utilizadas. O painel do Power BI no Kit de Início do CoE pode ser uma ferramenta valiosa para identificar esses aplicativos e fluxos. Quando mais de 10 funcionários utilizam uma solução de produtividade pessoal, o CoE da Power Platform deve avaliar se ela deve ser movida para um ambiente dedicado ou compartilhado. Essa avaliação ajuda a garantir que os recursos críticos sejam gerenciados de forma eficiente e segura.

Além disso, a reorganização desses aplicativos e fluxos é essencial para manter a integridade e a eficiência do ambiente de trabalho. A tabela de parâmetros no Kit de Início do CoE pode fornecer diretrizes claras para essa avaliação. Ao mover soluções amplamente utilizadas para ambientes dedicados, a organização pode melhorar a colaboração, a segurança e a manutenção dessas ferramentas. Essa prática não só otimiza o uso dos recursos, mas também garante que as soluções críticas estejam sempre disponíveis e funcionando corretamente para todos os usuários.

Tabela 1 - Tabela de parâmetros no Kit de Início do CoE

Parâmetros	Definir critérios	Ambiente
Número de usuários	1–10 usuários	Padrão
	7–30 usuários	Compartilhado
	>30 usuários	Dedicado
Natureza de dados	Altamente confidencial	Dedicado
	Confidencial	Compartilhado
	Não confidencial	Padrão
Impacto monetário ou de reputação para os negócios	Sim	Compartilhado ou dedicado
	Não	Padrão
Requer ALM	Sim	Compartilhado ou dedicado
	Não	Padrão

f. **Quarentena**

Para garantir a segurança e a integridade do ambiente de trabalho, é essencial implementar uma política de quarentena para aplicativos na Power Platform. No ambiente padrão, pode ser necessário colocar um aplicativo em quarentena em situações como a necessidade de desabilitação temporária para revisão, quando o aplicativo foi compartilhado com muitos usuários e precisa ser desativado, ou durante uma atualização ou migração para outro ambiente. Durante o período de quarentena, os criadores podem continuar editando o aplicativo, mas os usuários não conseguem executá-lo. Isso permite que os administradores realizem as revisões e ajustes necessários sem interromper o uso geral do sistema.

Além disso, é importante estabelecer procedimentos claros para a reavaliação e reintegração de aplicativos após o período de quarentena. Para restaurar o acesso aos usuários com quem o aplicativo foi compartilhado, é necessário remover a quarentena, e apenas os administradores têm permissão para alterar o estado de quarentena

de um aplicativo. Esse processo garante que apenas aplicativos seguros e confiáveis sejam utilizados, minimizando os riscos de falhas e problemas de segurança. A implementação de uma política de quarentena eficaz ajuda a manter um ambiente de trabalho seguro e eficiente, protegendo os dados e recursos da organização.

8.3 Formulários do SharePoint

A Power Platform está profundamente integrada ao ecossistema empresarial da Microsoft, o que permite que qualquer criador desenvolva automações e aplicativos essenciais para si ou para sua equipe. Uma das integrações mais potentes acontece entre o SharePoint e a Power Platform.

Com o Power Apps, os criadores podem facilmente criar ou personalizar formulários do SharePoint. Ao gerar um formulário personalizado no SharePoint, é criado um aplicativo de tela no ambiente padrão.

Para evitar sobrecarregar o ambiente padrão com esses aplicativos, recomenda-se criar um ambiente separado para armazenar os formulários personalizados do SharePoint. Dessa forma, os administradores da Power Platform podem isolar esses formulários dos aplicativos de produtividade gerais.

- Crie um ambiente separado ou designe um já existente para armazenar os formulários personalizados do SharePoint.
- Conceda a função de criador de ambiente a todos os usuários responsáveis por criar ou atualizar formulários no novo ambiente.
- Use o seguinte cmdlet do PowerShell para definir o ambiente do formulário do SharePoint: Set-AdminPowerAppSharepointFormEnvironment --EnvironmentName '<EnvironmentName>'.

É importante considerar dois pontos:

- Os formulários do SharePoint já existentes não são migrados para o novo ambiente.
- Se o ambiente de formulários do SharePoint for excluído após a configuração, os formulários personalizados serão perdidos, e a interface do SharePoint retornará ao formulário padrão. Novos formulários personalizados serão novamente criados no ambiente padrão.

O cmdlet Set-AdminPowerAppSharepointFormEnvironment aplica-se exclusivamente a formulários personalizados do SharePoint criados no Power Apps. Os fluxos criados no Power Automate a partir do SharePoint sempre utilizam o ambiente padrão.

8.4 Estratégia de ambientes

A estratégia de ambientes aplicada no caso da ANEEL visa garantir a segurança, eficiência e governança dos aplicativos e fluxos desenvolvidos na Power Platform, alinhando-se às melhores práticas de Application Lifecycle Management (ALM). A Figura 1 detalha a estratégia de ambientes aplicada para a ANEEL.

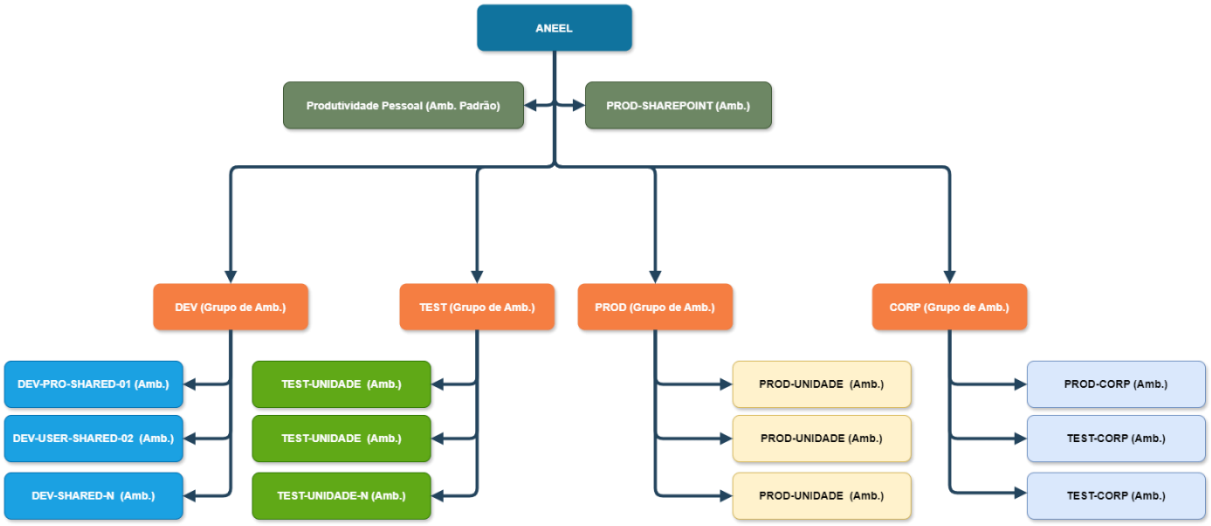

Figura 1 - Estratégia de ambientes aplicada para a ANEEL

a. **Produtividade Pessoal**

O ambiente de **Produtividade Pessoal** é destinado a usuários que criam aplicativos ou fluxos para uso pessoal, sem colaboração. Esses usuários são direcionados para ambientes de desenvolvimento pessoal bloqueados, com recursos limitados e regras de **Data Loss Prevention** (DLP)[8] mais restritivas, o que reduz o risco devido à natureza individual do ambiente e requer governança mínima.

b. **Formulários do SharePoint**

O ambiente de **Formulários do SharePoint** é dedicado exclusivamente ao armazenamento e gerenciamento de formulários do SharePoint, com acesso concedido apenas a usuários responsáveis pela criação e atualização desses formulários.

c. **Desenvolvimento e Teste**

Já os ambientes de **Desenvolvimento** e de **Teste** oferecem espaços separados e ajustados conforme o nível de experiência dos desenvolvedores. Esses ambientes podem ser compartilhados ou dedicados, separando desenvolvedores iniciantes, que têm políticas mais restritivas, dos avançados, que possuem maior liberdade, permitindo a implementação de políticas apropriadas para diferentes níveis de usuários.

[8] DLP, ou Data Loss Prevention, é uma estratégia de segurança que visa proteger dados sensíveis contra perda, vazamento ou acesso não autorizado, monitorando e controlando a transferência de informações dentro e fora da organização.

d. **Produção por Unidade Organizacional**

O ambiente de **Produção por Unidade Organizacional** é projetado para a criação de ferramentas e automações específicas de cada unidade organizacional. Esse ambiente pode armazenar dados confidenciais e utilizar conectores avançados, exigindo governança rigorosa e a implementação de processos de gestão do ciclo de vida de aplicações (ALM). Ambientes de desenvolvimento e teste são usados para trabalho de pré-produção, e apenas soluções gerenciadas são permitidas na produção, com revisões recorrentes de segurança e privacidade.

Apenas usuários que pertencem à unidade organizacional terão acesso a esse ambiente, garantindo que as informações e ferramentas sejam utilizadas exclusivamente por quem realmente precisa delas.

Para manter a segurança e a integridade das soluções, o ambiente de Produção por Unidade Organizacional requer governança rigorosa e a implementação de processos de gestão do ciclo de vida de aplicações (ALM). Isso inclui o uso de ambientes de desenvolvimento e teste para trabalho de pré-produção, garantindo que as soluções sejam devidamente testadas antes de serem implantadas na produção.

Apenas soluções gerenciadas são permitidas na produção, o que significa que todas as alterações e atualizações passam por um processo de revisão e aprovação. Além disso, são realizadas revisões recorrentes de segurança e privacidade para assegurar que as soluções estejam em conformidade com as políticas e regulamentos da organização

e. **Produção Corporativo**

Por fim, o ambiente de **Produção Corporativo** é controlado pela SGI e destinado a soluções utilizadas por toda a ANEEL. Esse ambiente tem a capacidade de armazenar dados altamente confidenciais e usar conectores avançados, exigindo um alto nível de governança e controle devido ao risco elevado. A gestão do ciclo de vida de aplicações (ALM) é imprescindível, com ambientes de teste e homologação utilizados antes da produção, e apenas soluções gerenciadas são permitidas na produção, com revisões frequentes de segurança e privacidade.

Além disso, a implementação de políticas de prevenção contra perda de dados (DLP) é fundamental para proteger os dados organizacionais, classificando os conectores em grupos de dados comerciais, não comerciais e bloqueados. A integração com ferramentas como o Azure DevOps para automatizar tarefas comuns de desenvolvimento e implantação também é recomendada, garantindo a consistência e a qualidade das implementações. Em resumo, a conformidade das soluções no ambiente de Produção Corporativo é garantida por meio de um processo rigoroso de ALM, revisões frequentes de segurança e privacidade, e a personalização das regras de acordo com as necessidades específicas de cada solução.

Esses ambientes são projetados para atender às necessidades específicas dos usuários e garantir que os aplicativos e fluxos sejam gerenciados de maneira eficiente e segura, alinhando-se às melhores práticas de ALM e políticas de DLP.

8.5 Recomendações

a. **Uso de ambientes de desenvolvedor**

Ambientes de desenvolvedores individuais são recomendados para fornecer aos criadores um espaço de trabalho dedicado para construir soluções com pouco código, garantindo o mais alto nível de isolamento em relação a outros ambientes. No entanto, se a organização prefere limitar a quantidade de ambientes de desenvolvedor, é

mais eficiente optar por vários ambientes compartilhados, em vez de permitir que os criadores usem o ambiente padrão.

Nesse contexto, a criação de ambientes de desenvolvedor fica restrita a ambientes compartilhados de desenvolvimento, que são do tipo produção. Esses ambientes podem ser organizados conforme a estrutura organizacional, localização geográfica ou outros critérios relevantes. É possível agrupar esses ambientes para assegurar que sejam aplicadas regras de governança consistentes. Além disso, é importante garantir que os criadores tenham permissão para desenvolver soluções Low-Code no ambiente designado a eles.

b. **Grupos e regras de ambiente**

À medida que a adoção do Power Platform cresce, o número de ambientes que requerem administração e governança também aumenta. Com o aumento desses ambientes, torna-se cada vez mais difícil garantir a aplicação uniforme de configurações e políticas de governança em todos eles. Para simplificar esse processo, o recurso de grupos de ambientes permite a criação de grupos nomeados, nos quais os ambientes podem ser organizados de forma semelhante à organização de documentos em uma pasta, facilitando a gestão e a aplicação de políticas consistentes.

Sempre que possível, deve ser utilizado grupos de ambientes para simplificar a governança em sua organização. Esses grupos permitem que os administradores apliquem políticas de governança por meio de regras personalizáveis, assegurando a consistência entre os ambientes e evitando desorganização. Administradores da Microsoft Power Platform podem criar grupos de ambientes que funcionam como contêineres para reunir ambientes com necessidades semelhantes. Os grupos podem ser organizados de acordo com critérios como departamento, projeto, centro de custo, ou qualquer outro relevante, proporcionando uma abordagem sistemática para gerenciar vários ambientes de forma integrada.

c. **Configurações de Segurança**

A maioria das configurações de segurança que impactam os ambientes são definidas individualmente para cada um deles. No entanto, algumas modificações podem ser feitas no nível do locatário para apoiar a sua estratégia de gestão de ambientes.

Recomendações

- Considerar a desativação da funcionalidade "Compartilhar com Todos" no Power Platform, permitindo que apenas administradores possam compartilhar ativos com todos os usuários.
- Avaliar a proteção da integração com o Exchange para aumentar a segurança.
- Implementar isolamento entre locatários, ajudando a reduzir o risco de exfiltração de dados entre diferentes locatários.
- Restringir a criação de novos ambientes de produção aos administradores. Essa medida ajuda a manter o controle, evitando consumo de capacidade não planejada e reduzindo o número de ambientes que precisam ser gerenciados. Se os usuários precisarem solicitar novos ambientes à equipe de TI central, será mais fácil monitorar em quais projetos estão trabalhando.

8.6 Segurança do ambiente Padrão

O ambiente padrão desempenha um papel importante no suporte às personalizações de produtividade no Microsoft 365. No entanto, como parte das melhores práticas recomendadas para gestão de ambientes, é ideal

reduzir ao máximo o uso desse ambiente. O ideal é que os desenvolvedores utilizem seus próprios ambientes isolados para criação. Embora não seja possível impedir completamente o acesso ao ambiente padrão, é viável restringir as ações que podem ser realizadas nele. As seguintes recomendações devem ser consideradas na segurança do ambiente padrão:

- Usar o roteamento de ambiente para redirecionar os criadores a seus próprios ambientes de trabalho, seja individual ou compartilhado, para o desenvolvimento de soluções Low-Code.
- Fazer uma revisão dos administradores que possuem acesso ao ambiente padrão e limite essa permissão apenas às funções essenciais.
- Considerar renomear o ambiente padrão para um nome mais informativo, como "Produtividade Pessoal".
- Implementar uma política de prevenção contra perda de dados (DLP) no ambiente padrão, bloqueando novos conectores e permitindo que os criadores utilizem apenas conectores básicos ou desbloqueáveis. Os conectores que não podem ser bloqueados devem ser movidos para o grupo de dados corporativos, enquanto os conectores bloqueáveis devem ser transferidos para o grupo de dados restritos.
- Criar uma regra para bloquear todos os padrões de URL relacionados a conectores personalizados.

A proteção do ambiente padrão deve ser tratada com prioridade. Esse processo deve ser realizado em conjunto com a segurança do tenant[9], como uma das primeiras etapas na implementação da estratégia de gestão de ambientes. Sem essas medidas, os criadores terão mais liberdade para adicionar ativos ao ambiente padrão. Com as proteções e roteamento adequados, eles serão encorajados a utilizar seus próprios ambientes de criação.

8.7 Segurança dos outros ambientes

A ANEEL, semelhante à maioria das organizações, possui diversos ambientes além do padrão. O nível de segurança necessário para cada um pode variar de acordo com os aplicativos e dados que ele armazena. Ambientes de desenvolvimento geralmente possuem regras mais flexíveis em comparação com os ambientes de produção. Alguns ambientes de produção demandam o mais alto nível de proteção.

Ao definir a estratégia de ambientes, é fundamental identificar níveis de segurança comuns para cada um deles e os recursos que garantem essa proteção.

[9] **Tenant** é uma instância única de um serviço em nuvem dedicada a uma organização específica, garantindo isolamento e segurança dos dados e recursos dessa organização.

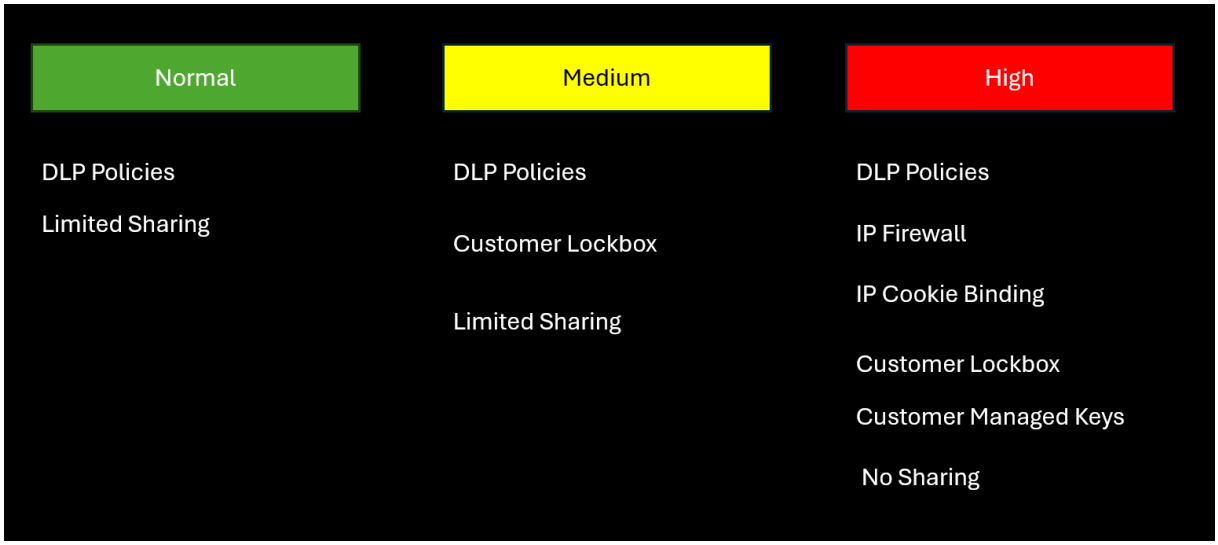

Figura 2 - Um exemplo de três camadas de segurança para os ambientes e os recursos correspondentes a cada uma.

8.8 Alinhar políticas de DLP a estratégia

As políticas de dados representam um elemento essencial em uma estratégia ampla de governança para controlar os serviços utilizados por recursos Low-Code em um ambiente. Embora os grupos de ambientes não possuam uma regra específica para impor uma política de DLP a um ambiente, é viável alinhar a estratégia de DLP com os grupos de ambientes. Por exemplo, pode ser criada uma política DLP com um nome idêntico ou semelhante ao de um grupo de ambientes e aplicá-la aos ambientes pertencentes a esse grupo.

8.9 Melhores práticas e recomendações

a. **Novos Ambientes**

Ao desenvolver a estratégia, é importante considerar a criação de ambientes que suportem adequadamente uma carga de trabalho. A análise deve equilibrar os benefícios do isolamento oferecido por um ambiente, como a capacidade de restringir mais alguns ambientes do que outros para fins de segurança, com as desvantagens, como o atrito gerado para os usuários que precisam compartilhar dados entre aplicativos.

Ao avaliar se um aplicativo ou automação deve ter seu próprio ambiente, é necessário considerar os diferentes estágios do ciclo de vida do aplicativo separadamente. Durante o desenvolvimento, isolar o aplicativo de outros é crucial. Quando vários aplicativos são desenvolvidos em um único ambiente, corre-se o risco de criar dependências indesejadas entre eles.

Como recomendação geral, sempre que possível, os ambientes de desenvolvimento devem ser de uso único, temporários e facilmente recriados. Testar vários aplicativos no mesmo ambiente pode ser adequado se eles forem executados em conjunto na produção. De fato, não realizar testes com os aplicativos que serão utilizados na produção pode resultar em problemas de compatibilidade não detectados.

Ao considerar o **ambiente de produção** de um aplicativo, é essencial levar em conta as seguintes questões:

- **Compatibilidade**: O aplicativo é compatível com os aplicativos existentes no ambiente? Por exemplo, dois aplicativos que utilizam a tabela "Contato" do Dataverse para finalidades diferentes podem gerar conflitos. Além disso, os aplicativos são compatíveis com a política de DLP vigente?
- **Requisitos de conformidade**: Existem normas ou exigências especiais de conformidade para a separação de dados? A confidencialidade dos dados demanda isolamento? Há restrições que proíbem a incorporação desses dados em outros conjuntos?
- **Confidencialidade dos dados**: Os dados são altamente sensíveis? A exfiltração desses dados poderia causar danos financeiros ou reputacionais à organização? O isolamento em um ambiente separado pode proporcionar maior controle sobre a segurança.
- **Necessidade de integração de dados**: O aplicativo precisa acessar dados de outros aplicativos e, por isso, deve ser implantado junto com eles? Por exemplo, dois aplicativos que usam a tabela "Cliente" devem estar hospedados no mesmo ambiente. Separá-los pode gerar duplicação de dados e problemas com a manutenção dessas informações.
- **Residência de dados**: Os dados exigem uma residência regional específica? Em certos casos, o mesmo aplicativo ou automação pode precisar ser implantado em ambientes regionais para garantir o isolamento adequado e a conformidade com as exigências de residência de dados.
- **Distribuição geográfica dos usuários**: A maioria dos usuários está localizada na mesma região do ambiente? Se o ambiente estiver na EMEA, mas a maioria dos usuários residir nos EUA, compartilhar o mesmo ambiente pode comprometer o desempenho.
- **Necessidade de novos administradores**: Será necessário designar novos administradores ou os administradores atuais serão suficientes? Se o novo aplicativo demandar mais administradores, eles serão compatíveis com os atuais, considerando que todos terão permissões de administrador para todos os aplicativos no ambiente?
- **Ciclo de vida do aplicativo**: Qual é a expectativa de vida útil do aplicativo? Se o aplicativo ou automação for temporário ou de curta duração, pode não ser aconselhável instalá-lo em um ambiente que hospeda aplicativos mais permanentes.
- **Facilidade de uso pelos usuários**: Os usuários enfrentarão dificuldades em utilizar múltiplos ambientes para acessar diferentes aplicativos? Isso pode afetar desde a localização de um aplicativo em dispositivos móveis até a geração de relatórios que precisam reunir dados de vários ambientes.

b. **Capacidade**

Cada ambiente (além dos ambientes de teste e de desenvolvedor) consome 1 GB para o provisionamento inicial. A capacidade é compartilhada no locatário, por isso é necessário alocá-la de forma adequada para quem realmente precisa.

Para economizar capacidade, considerar as seguintes práticas:

- **Gerenciar ambientes de teste e produção compartilhados**: Ao contrário dos ambientes de desenvolvimento, as permissões nos ambientes de teste e produção devem ser restritas, limitando o acesso do usuário apenas para testes.
- **Automatizar a limpeza de ambientes de desenvolvimento temporários** e incentivar o uso de ambientes de teste para experimentos ou provas de conceito.

c. **Grupos de ambientes**

Os grupos de ambientes são bastante flexíveis e permitem atender a diferentes necessidades específicas da sua organização. Aqui estão algumas formas de considerar o agrupamento de ambientes ao definir sua estratégia de ambiente:

- **Por serviço ou componente, como:** Desenvolvimento, teste e produção;
- **Por departamentos, grupos de negócios ou centros de custo**;
- **Por projetos**;
- **Por localização**, caso a maioria dos ambientes em uma região compartilhe necessidades de governança semelhantes; isso também pode facilitar a conformidade com regulamentações e legislações regionais.

d. **Nomeando ambientes e grupos**

Ao definir a estratégia, é importante considerar como os ambientes e grupos são nomeados:

- **Visibilidade dos nomes**: Os nomes dos ambientes são visíveis para administradores, criadores e usuários. Embora os grupos de ambientes geralmente sejam usados apenas por administradores, criadores com privilégios podem encontrá-los ao criar ambientes.
- **Nomenclatura automática**: Os ambientes de desenvolvedores criados automaticamente seguem o formato "<Ambiente> do nome do usuário", como "Ambiente de Júlio Almeida". Já os grupos de ambiente não são nomeados automaticamente.
- **Unicidade dos nomes**: Embora não seja necessário que os nomes de ambientes e grupos sejam únicos, é recomendável evitar duplicações para evitar confusão.
- **Limite de caracteres**: Os nomes são limitados a 100 caracteres, mas quanto mais curtos, mais fáceis de usar.
- **Convenção de nomenclatura**: Estabeleça um padrão de nomenclatura consistente.
- **Facilitação de administração e automação**: Nomes consistentes ajudam os administradores a entender a função dos grupos e ambientes, além de facilitar automações e relatórios.
- **Estágio do ciclo de vida no nome**: Uma prática comum é incluir o estágio do ciclo de vida no nome do ambiente, como "Desenvolvimento da Contoso", "Teste da Contoso" ou "Produção da Contoso", para diferenciar ambientes com o mesmo conteúdo, mas finalidades distintas.
- **Incluir departamento ou unidade de negócios**: Se o ambiente for dedicado a um grupo específico, inclua o nome do departamento ou unidade de negócios.
- **Padrão de nome**: Uma convenção útil pode ser o formato <estágio do ciclo de vida>-<região>-<unidade de negócios>-<finalidade>, como "Prod-EUA-Finanças-Folha de Pagamento".
- **Nomes curtos e descritivos**: Mantenha os nomes concisos e informativos.
- **Evolução dos grupos**: Pense na evolução e no crescimento dos grupos ao longo do tempo, garantindo que a convenção de nomenclatura se adapte a essas mudanças.
- **Evitar informações confidenciais nos nomes**: Não inclua informações sensíveis, já que os nomes podem ser vistos por qualquer pessoa com acesso ao centro de administração.

8.10 Acessos aos ambientes

O acesso aos ambientes na Power Platform deve ser cuidadosamente gerenciado para garantir a segurança e a eficiência das operações.

a. **Desenvolvimento**

No ambiente de Desenvolvimento, o acesso é concedido a criadores e desenvolvedores de aplicativos. Esses usuários precisam, no mínimo, do direito de acesso de **Criador de Ambiente** para criar recursos. É importante que os usuários de aplicativos não tenham acesso a este ambiente, garantindo que apenas aqueles envolvidos no desenvolvimento possam interagir com os recursos disponíveis.

b. **Teste**

No ambiente de Teste, o acesso é restrito a administradores e pessoas que estão realizando testes. Criadores, desenvolvedores e usuários de aplicativos de produção não devem ter acesso a este ambiente. Os usuários de teste devem ter privilégios suficientes para realizar os testes necessários, assegurando que as soluções sejam devidamente verificadas antes de serem movidas para a produção.

c. **Produção**

O ambiente de Produção é acessível a administradores e usuários de aplicativos. Os usuários devem ter acesso suficiente para realizar as tarefas associadas aos aplicativos que utilizam. No entanto, os criadores e desenvolvedores de aplicativos não devem ter acesso a este ambiente ou devem ter apenas privilégios no nível de usuário, garantindo que as operações de produção sejam realizadas de forma segura e controlada.

d. **Distribuído**

O ambiente Distribuído também é acessível a administradores da SGI e usuários de aplicativos. Assim como no ambiente de Produção, os usuários devem ter acesso suficiente para realizar as tarefas necessárias, enquanto os criadores e desenvolvedores de aplicativos não devem ter acesso ou devem ter apenas privilégios no nível de usuário. Isso assegura que as operações distribuídas sejam gerenciadas de maneira eficiente e segura.

e. **Padrão**

Por fim, no ambiente Padrão, todos os usuários do locatário podem, por padrão, criar e editar aplicativos em um ambiente padrão do Dataverse com um banco de dados. No entanto, é altamente recomendável criar ambientes para finalidades específicas e conceder as funções e os privilégios apropriados apenas para as pessoas que realmente necessitam. Isso ajuda a manter a organização e a segurança dos recursos disponíveis na Power Platform.

Recomenda-se que, nos ambientes de teste, produção e nos ambientes corporativos, apenas os responsáveis pela implantação dos aplicativos e fluxos de trabalho possuam permissões de Administrador. Todos os demais usuários devem ter permissões limitadas a usuário básico.

As práticas recomendadas reforçam a importância de separar rigorosamente os acessos em cada fase do ciclo de vida do aplicativo. Desenvolvedores não devem ter acesso ao ambiente de produção, e usuários de negócios não devem ter acesso a ambientes de desenvolvimento, conforme recomendado.

8.11 Recomendações sobre os ambientes

- **Ambientes isolados:** Manter ambientes de desenvolvimento, teste e produção isolados para evitar conflitos e garantir que as mudanças sejam testadas antes da implantação final.
- **Nomenclatura clara:** Utilizar uma nomenclatura clara e consistente para os ambientes para facilitar a identificação e o gerenciamento.
- **Controle de acesso:** Garantir que apenas usuários autorizados tenham permissão para configurar e executar pipelines. Definir políticas de segurança robustas para proteger os ambientes.
- **Segregação de funções:** Separar as funções de desenvolvimento, teste e implantação para minimizar riscos e garantir a conformidade.
- **Testes em ambientes aproximados:** Realizar testes em ambientes que espelhem o ambiente de produção para identificar e corrigir problemas antes da implantação final.
- **Deploy[10] incremental:** Realizar deploys incrementais e pequenos para reduzir o risco de grandes mudanças e facilitar a identificação de problemas.

9. Aplicativos

9.1 Propriedade de Aplicativo

A política de propriedade em aplicativos da plataforma Power Apps visa assegurar que a gestão e o controle desses aplicativos sejam devidamente mantidos dentro da organização. Estão assim definidos:

- **Criador original**: A pessoa que desenvolve o aplicativo é automaticamente designada como o proprietário. Essa função concede o controle sobre o acesso e a capacidade de realizar modificações no aplicativo.
- **Transferência de propriedade**: O proprietário tem a opção de transferir a titularidade do aplicativo para outro usuário ou grupo, o que é particularmente útil em casos de mudança de função ou desligamento de um usuário.

9.2 Abandono de aplicativos

O "abandono de aplicativos" ocorre quando um aplicativo ou fluxo de trabalho criado na plataforma Power Platform é deixado sem suporte ou manutenção pelo desenvolvedor, equipe ou departamento responsável. Isso pode ocorrer por diversos motivos, como:

- **Mudança de função ou saída de funcionário**: O desenvolvedor original pode ter mudado de função ou deixado a empresa, resultando na falta de um responsável para manutenção e suporte.
- **Mudança de prioridades**: O foco do desenvolvedor ou da equipe pode mudar para outros projetos, o que leva ao abandono do aplicativo.
- **Falta de recursos**: A organização pode não dispor de recursos suficientes para continuar o suporte ao aplicativo, especialmente se ele não for crítico.
- **Obsolescência**: O aplicativo pode se tornar obsoleto devido a mudanças nos processos de negócios, tecnologia ou necessidades da empresa, levando à sua descontinuação.

Quando um aplicativo é abandonado, vários problemas podem surgir, como bugs não corrigidos, incompatibilidade com atualizações da plataforma e vulnerabilidades de segurança. Além disso, os usuários podem perder confiança na solução devido à falta de suporte e à experiência comprometida.

[10] **Deploy** é o processo de colocar um software ou aplicativo em operação, tornando-o disponível para uso em um ambiente de produção.

Para mitigar esses riscos, é essencial que as organizações adotem boas práticas de gestão de aplicativos, como garantir **documentação adequada, monitoramento contínuo e estratégias de transição**. Isso ajuda a assegurar que os aplicativos essenciais continuem funcionando de maneira segura e eficiente.

A prática recomendada para proteger a SGI e os usuários é: **se o desenvolvedor original não puder continuar a dar suporte ou não encontrar alguém para assumir essa função, o aplicativo deverá ser removido.**

As três opções recomendadas para lidar com o abandono de aplicativos ou fluxos de trabalho são:

- Outro desenvolvedor assume a propriedade do aplicativo;
- A responsabilidade é transferida para a equipe da SGI, na ausência de um desenvolvedor;
- O aplicativo deve ser removido.

9.3 Transferência de Propriedade

A transferência de propriedade garante que outro desenvolvedor ou a equipe de TI assuma a responsabilidade sobre um aplicativo ou fluxo, assegurando que o novo proprietário tenha as habilidades e permissões necessárias. Aqui estão os procedimentos de acordo com o tipo de aplicação:

Os Aplicativos Canvas[11] permitem múltiplos coproprietários, e a propriedade pode ser transferida diretamente pelo portal Power Apps. Além disso, é obrigatório nomear um coproprietário secundário.

Já os Aplicativos Orientados a Modelos não suportam múltiplos coproprietários. A transferência de propriedade é realizada com o suporte de administradores usando ferramentas como PowerShell ou CoE Starter Kit, e o proprietário original deve abrir um chamado para a SGI para que a transferência seja executada.

Quanto aos Fluxos, eles também permitem múltiplos coproprietários, e a propriedade pode ser transferida diretamente pelo portal Power Apps. Assim como nos Aplicativos Canvas, é obrigatória a nomeação de um coproprietário secundário.

a. Razões para a transferência de aplicativos

Existem várias razões para a transferência de aplicativos. A continuidade do negócio é uma delas, garantindo que os aplicativos essenciais continuem funcionando sem interrupções, mesmo quando o desenvolvedor original não está mais disponível ou não pode dar suporte.

A segurança e conformidade também são cruciais, assegurando que os aplicativos que lidam com dados sensíveis ou regulamentados sejam geridos por equipes com as qualificações adequadas para manter a conformidade com políticas de segurança e regulamentações legais.

Além disso, a escalabilidade e suporte são importantes, pois aplicativos que crescem em complexidade ou em número de usuários podem precisar de suporte mais especializado e recursos que equipes de TI dedicadas ou departamentos especializados podem fornecer.

Mudanças de prioridades também podem exigir a transferência de aplicativos, especialmente quando as prioridades de desenvolvimento mudam e os aplicativos que não estão mais no foco principal do desenvolvedor original precisam continuar recebendo o suporte necessário.

Por fim, mudanças de estrutura organizacional, como fusões, aquisições ou reestruturações, podem exigir que os aplicativos sejam realocados para refletir a nova organização de departamentos ou equipes.

[11] Aplicativo Canvas: Aplicativo que permite múltiplos coproprietários e é flexível na transferência de propriedade.

b. **Casos em que a transferência deve ser considerada**

Existem vários casos em que a transferência de aplicativos deve ser considerada. O número de usuários com os quais o aplicativo é compartilhado é um fator importante, pois aplicativos amplamente utilizados dentro da organização geralmente requerem mais suporte e supervisão.

A frequência de uso, medida pelos usuários ativos diários do aplicativo, pode indicar a importância do aplicativo para as operações diárias.

Quando o desenvolvedor original deixa a empresa ou muda de função, a transferência do aplicativo garante que ele continue a ser gerido adequadamente.

Para aplicativos que são vitais para as operações diárias ou estratégicas da organização, a transferência para uma equipe especializada pode garantir suporte contínuo e melhorias constantes. Quando um aplicativo começa a ser amplamente utilizado ou se torna mais complexo, pode ser necessário transferi-lo para uma equipe que possa gerenciar melhor os novos desafios técnicos e de suporte.

Aplicativos que começam a lidar com dados sensíveis ou confidenciais devem ser geridos por equipes com as habilidades e controles de segurança necessários. Transferir a propriedade de aplicativos importantes pode fazer parte de um plano de sucessão ou redundância, garantindo que não haja um único ponto de falha na gestão do aplicativo.

c. **Habilidades Necessárias para Dar Suporte ao Aplicativo**

Para garantir que o novo proprietário de um aplicativo Power Apps tenha as habilidades necessárias, é essencial seguir um processo estruturado de treinamento, documentação e suporte contínuo. Abaixo estão as principais políticas para o processo de repasse e transição de propriedade:

a. **Treinamento**
- Desenvolver um treinamento personalizado focado no aplicativo.
- Identificar lacunas de conhecimento que o novo proprietário possa ter.
- Organizar sessões de treinamento focadas nas áreas onde o novo proprietário precisa de mais suporte.
- Considerar realizar workshops presenciais ou virtuais para o repasse de conhecimento detalhado.

b. **Documentação**
- Criar uma documentação completa do aplicativo que inclua:
  - Estrutura e arquitetura do aplicativo;
  - Fluxos de trabalho e lógica de negócios;
  - Conexões de dados e configurações;
  - Manuais de usuário e procedimentos de manutenção (se possível).

c. **Sessões de Repasse de Conhecimento**
- Realizar sessões em que o desenvolvedor atual apresenta o aplicativo ao novo proprietário.
- Explicar os principais componentes do aplicativo.
- Permitir que o novo proprietário faça perguntas e esclarecer dúvidas durante essas sessões.

d. **Mentoria e Suporte Contínuo**
- Definir um período de mentoria, em que o desenvolvedor original esteja disponível para suporte.
- Estabelecer um canal de comunicação para suporte contínuo, caso o novo proprietário precise de ajuda adicional.

e. **Licenciamento e Acessos**

- Assegurar que o novo proprietário tenha a licença necessária para utilizar o Power Apps e suas conexões.
- Garantir que o novo proprietário tenha acesso ao ambiente, solução, aplicativo e conexões necessárias para suportar o aplicativo adequadamente.

9.4 Acesso Baseado em Função (RBAC[12])

Para controlar quem pode acessar dados e recursos restritos ou confidenciais e o que esses usuários podem fazer, é fundamental atribuir direitos de acesso adequados. Esses direitos determinam como diferentes usuários interagem com diferentes tipos de registros. É possível criar ou modificar direitos de acesso, além de alterar os direitos atribuídos aos usuários. Um mesmo usuário pode ter múltiplos direitos de acesso, e esses privilégios são cumulativos, ou seja, o usuário receberá todos os privilégios disponíveis em cada função atribuída.

9.5 Funções Predefinidas para Power Apps e Power Automate

A atribuição de funções na Power Platform, especialmente para desenvolvedores, não é uma tarefa simples. Existem duas funções predefinidas que devem ser consideradas:

- **Criador de Ambiente**: Esse perfil permite criar recursos dentro de um ambiente, como aplicativos, conexões, APIs personalizadas e fluxos de trabalho no Power Automate. No entanto, essa função não concede privilégios de acesso aos dados do ambiente, apenas permite criar e gerenciar fluxos de dados e aplicativos de tela.
- **Personalizador de Sistemas**: Tem permissão total para personalizar o ambiente e visualizar todos os dados de tabelas personalizadas. Porém, em tabelas como Contas, Contatos e Atividades, o usuário só pode visualizar registros que ele próprio criou.

Muitas vezes, um desenvolvedor precisará dos privilégios de ambas as funções para criar aplicativos. Contudo, é essencial seguir o **princípio do menor privilégio**, que garante que os usuários tenham apenas o acesso necessário para suas atividades, evitando a concessão de permissões excessivas.

a. **Atribuição de Funções para Desenvolvedores**

As funções para desenvolvedores são atribuídas no nível de ambiente. Caso um desenvolvedor trabalhe em múltiplas equipes, ele precisará de permissões em vários ambientes. Idealmente, permissões de desenvolvedor devem ser concedidas apenas em ambientes de desenvolvimento e teste, e em produção somente quando necessário.

b. **Funções Predefinidas para Outros Usuários**

Para gerenciar usuários com outros papéis, utilize funções predefinidas na Power Platform:

- **Administrador de Ambiente**: Pode executar todas as ações administrativas em um ambiente, como adicionar ou remover usuários, provisionar bancos de dados Dataverse, gerenciar recursos e criar políticas de prevenção contra perda de dados.

[12] RBAC (Role-Based Access Control): Controle de acesso baseado em funções para garantir que os usuários tenham apenas as permissões necessárias

- **Usuário Básico**: Essa função permite que o usuário execute aplicativos no ambiente e realize tarefas em registros que possui, com privilégios nas tabelas de negócios principais, como Conta, Contato e Atividade.

c. **Recomendações de Permissões para Administradores**

Para uma gestão eficaz da Power Platform, os administradores precisam ter funções adequadas. As organizações devem decidir se a administração será:

- **Centralizada**: Onde os administradores são definidos no nível do locatário.
- **Descentralizada**: Com administradores definidos no nível de ambiente.
- **Ambos**: Com permissões atribuídas no locatário e em ambientes específicos, como desenvolvimento e teste.

Para administradores no modelo centralizado, a função de Administrador da Power Platform deve ser atribuída a ambientes sem Dataverse. Já em ambientes com Dataverse, será necessário atribuir a função de Administrador de Sistema.

d. **Outras Considerações ao Definir Papéis e Permissões**

- Integrar o Microsoft Teams aos ambientes da Power Platform para uma gestão mais eficiente de projetos.
- Realizar revisões periódicas de permissões para garantir que o acesso continue apropriado.
- Sempre atribuir o menor nível de permissão possível para evitar concessões desnecessárias de acesso.
- Documentar claramente os processos de gestão de usuários e permissões.
- Informar os usuários sobre suas responsabilidades e melhores práticas de segurança ao usar a Power Platform.

9.6 Autenticação de Fluxos de Trabalho Críticos

O uso de contas de serviço para autenticação em fontes de dados no Microsoft Power Automate é crucial para garantir a segurança, confiabilidade e gestão eficiente dos fluxos de trabalho, especialmente em processos críticos. Essas contas garantem que as conexões com fontes de dados sejam consistentes, sem depender de credenciais de funcionários que podem ser alteradas ou desativadas, como em casos de desligamentos ou mudanças de função. Quando o fluxo de trabalho utiliza a credencial de um usuário autenticado e ela é desativada, o fluxo para de funcionar até que novas credenciais sejam configuradas. Contas de serviço eliminam esse risco, mantendo a continuidade do fluxo de trabalho mesmo com alterações de credenciais dos usuários.

a. **Estratégia Eficaz para o Uso de Contas de Serviço no Microsoft Power Automate**

Para criar uma estratégia eficiente, é necessário levar em consideração diversos aspectos relacionados à segurança, governança e eficiência operacional. A seguir estão as principais práticas:

- **Gestão de Contas de Serviço:** É fundamental que as contas de serviço sejam criadas e gerenciadas de forma controlada. Apenas administradores designados devem ter permissão para criar essas contas, garantindo que o processo seja seguro. Cada conta de serviço precisa ser documentada com detalhes como o propósito de uso, permissões associadas e quem é o responsável por gerenciá-la.
- **Política de Permissões e Acessos:** As contas de serviço devem ser configuradas com o princípio do menor privilégio, ou seja, devem possuir apenas as permissões necessárias para executar suas funções no Power

Automate. As permissões devem ser concedidas exclusivamente para usuários experientes com Power Automate, evitando acessos desnecessários que possam comprometer a segurança.
- **Revisões periódicas:** Realizar revisões regulares das permissões das contas de serviço para garantir que continuam adequadas e necessárias.
- **Uso exclusivo para automação:** As contas de serviço devem ser usadas apenas para fluxos automatizados e não devem ser acessadas manualmente por usuários.

b. **Implementação de Políticas de Segurança e Governança**

Seguindo essas diretrizes, a gestão das contas de serviço no Microsoft Power Automate será mais segura, eficiente e em conformidade com as melhores práticas de segurança e governança. Isso reduz o risco de falhas nos fluxos de trabalho críticos e evita interrupções desnecessárias, garantindo a continuidade operacional.

10. Reutilização de Componentes

10.1 Componentes

Os componentes funcionam como blocos de construção reutilizáveis para aplicativos de tela, permitindo que os desenvolvedores criem controles personalizados que possam ser utilizados tanto dentro de um único aplicativo quanto em vários, por meio de uma biblioteca de componentes. Eles podem incorporar funcionalidades avançadas, como propriedades personalizadas, e viabilizar recursos mais complexos.

Esses componentes são especialmente vantajosos para o desenvolvimento de aplicativos maiores com padrões de controle semelhantes. Quando uma definição de componente é atualizada no aplicativo, todas as suas instâncias refletem essas mudanças automaticamente. Além disso, os componentes minimizam a duplicação de trabalho, eliminando a necessidade de copiar e colar controles, o que também contribui para a melhoria do desempenho. Eles também incentivam o desenvolvimento colaborativo e padronizam a aparência de uma organização ao se adotar uma biblioteca de componentes.

Recomenda-se o uso de uma biblioteca de componentes ao criar componentes com foco em reutilização. Alterações feitas diretamente em um aplicativo afetam apenas aquele aplicativo específico. No entanto, ao utilizar uma biblioteca de componentes, é possível editar e publicar essas atualizações para múltiplos aplicativos simultaneamente.

10.2 Biblioteca de componentes

Bibliotecas de componentes no Power Apps são coleções de componentes reutilizáveis que se pode criar, armazenar e compartilhar entre diferentes aplicativos dentro da Power Platform. Esses componentes são blocos de construção que encapsulam um conjunto de funcionalidades e design, permitindo que sejam utilizados de forma consistente em várias aplicações, sem precisar recriar o mesmo conteúdo repetidamente. As principais características das bibliotecas de componentes são:
- **Reutilização:** Os componentes criados em uma biblioteca podem ser reutilizados em diferentes aplicativos, economizando tempo e esforço no desenvolvimento.
- **Centralização:** Uma biblioteca de componentes centraliza o gerenciamento de componentes comuns, o que facilita a manutenção e atualizações. Quando um componente é atualizado na biblioteca, a mudança pode ser propagada para todos os aplicativos que o utilizam.

- **Consistência:** Ao utilizar componentes de uma biblioteca, garante-se uma aparência e comportamento consistentes em todos os aplicativos da organização, promovendo uma melhor experiência do usuário e uma identidade visual unificada.
- **Customização:** Embora os componentes sejam reutilizáveis, eles podem ser configurados ou parametrizados dentro de cada aplicativo para atender a necessidades específicas, mantendo a flexibilidade.

As bibliotecas de componentes são fundamentais para organizações que buscam eficiência e consistência no desenvolvimento na Power Platform. Elas permitem economizar tempo ao eliminar a necessidade de recriar componentes comuns, garantindo que elementos sejam desenvolvidos uma vez e depois reutilizados em vários aplicativos. Isso não apenas reduz a quantidade de erros, já que os componentes são testados e validados previamente, mas também facilita a atualização, permitindo que alterações em um componente sejam aplicadas de forma uniforme a todos os aplicativos que o utilizam.

10.3 Principais casos de uso

Os cenários mais comuns para o uso de bibliotecas de componentes no Power Apps são aqueles em que a reutilização, a consistência e a eficiência são essenciais para o desenvolvimento de aplicativos.

- **Cabeçalhos e rodapés:** Elementos como cabeçalhos, rodapés, barras de navegação e menus, que precisam ser usados em diversos aplicativos, podem ser criados uma única vez e reaproveitados em várias aplicações, garantindo uma aparência e comportamento uniformes.
- **Botões padronizados:** Botões com estilos, ícones e comportamentos específicos (como salvar, cancelar, enviar) podem ser padronizados e utilizados em diferentes aplicativos.
- **Menus de navegação:** Barras laterais ou menus de navegação que fornecem links para várias seções de um aplicativo ou para diferentes aplicativos de um conjunto.
- **Paginadores:** Componentes que permitem a navegação entre páginas de dados ou etapas de um processo.
- **Barras de progresso:** Usadas para mostrar o avanço em processos, como formulários com várias etapas ou listas de verificação.
- **Notificações e alertas:** Componentes que exibem mensagens de erro, sucesso ou outras notificações, seguindo um padrão visual e de comportamento.
- **Logotipos e identidade visual:** Componentes que incorporam logotipos, paletas de cores e outros elementos de identidade visual que precisam ser consistentes em todos os aplicativos.
- **Pop-ups e modais:** Janelas de diálogo ou pop-ups que solicitam confirmação ou oferecem informações adicionais ao usuário.

  Esses componentes facilitam a criação de aplicativos padronizados e eficientes.

11. Políticas de Dados e Conectores

11.1 Política de Dados

As políticas de prevenção contra perda de dados (DLP) funcionam como barreiras para evitar que os usuários exponham acidentalmente dados da organização, além de proteger a segurança das informações no locatário. Elas estabelecem diretrizes sobre quais conectores estão habilitados para cada ambiente e quais podem ser utilizados em conjunto. Os conectores são categorizados como comerciais, não comerciais ou bloqueados. Um

conector classificado como comercial só pode ser combinado com outros conectores desse grupo dentro do mesmo aplicativo ou fluxo.

11.2 Estratégias para criação de DLPs

A criação de Políticas de Prevenção de Perda de Dados (DLP) é uma estratégia essencial para proteger informações sensíveis e garantir a conformidade com regulamentações de segurança. As DLPs são definidas como um conjunto de regras e procedimentos que identificam, monitoram e protegem dados confidenciais contra acessos não autorizados, vazamentos e outras ameaças. A implementação eficaz de DLPs envolve várias etapas, recomendações e, em alguns casos, exceções que devem ser consideradas.

Como administrador que está assumindo um ambiente ou começando a dar suporte ao uso do Power Apps e Power Automate, uma das primeiras ações a serem tomadas é a configuração das políticas de DLP. Após estabelecer um conjunto básico de políticas, é fundamental focar no tratamento de exceções e criar políticas de DLP direcionadas para implementar essas exceções, uma vez que forem aprovadas.

a. **Etapas para a criação de DLPs**

O primeiro passo na criação de DLPs é a definição dos objetivos e escopo. Isso inclui identificar os tipos de dados que precisam ser protegidos, como informações pessoais, financeiras, propriedade intelectual, entre outros. Em seguida, é necessário realizar uma avaliação de risco para entender as possíveis ameaças e vulnerabilidades associadas aos dados. Com base nessa avaliação, as organizações podem desenvolver políticas específicas que definam como os dados devem ser protegidos e quais ações devem ser tomadas em caso de violação.

A implementação das DLPs envolve a configuração de ferramentas e tecnologias que monitoram e controlam o fluxo de dados dentro e fora da organização. Além disso, é importante treinar os funcionários sobre as políticas de DLP e as melhores práticas de segurança, garantindo que todos estejam cientes de suas responsabilidades na proteção dos dados.

Recomenda-se observar os seguintes pontos para procedimentos de DLP em ambientes de produtividade compartilhada de usuários e equipes:

- Criar uma política que abarque todos os ambientes, exceto os selecionados (como os de produção), restringindo os conectores disponíveis nesta política ao Office 365 e outros microsserviços padrões, bloqueando o acesso ao restante. Essa política deve ser aplicada ao ambiente padrão, aos ambientes de treinamento internos e a quaisquer novos ambientes que forem criados.
- Desenvolver políticas de DLP mais flexíveis e apropriadas para ambientes de produtividade compartilhada de usuários e equipes, permitindo o uso de conectores como serviços do Azure e Office 365, de acordo com as necessidades e onde a organização armazena dados comerciais.

Para ambientes de produção (unidade de negócios e projeto), sugere-se o seguinte:

- Excluir esses ambientes das políticas de produtividade compartilhada.
- Trabalhar com as unidades de negócio e os projetos para definir quais conectores e combinações serão utilizados, e criar uma política específica para incluir apenas os ambientes selecionados.
- Permitir que os administradores desses ambientes categorizem conectores personalizados como dados comerciais, se necessário.
- Criar o mínimo possível de políticas por ambiente, já que não há uma hierarquia estrita entre políticas de locatário e ambiente. Durante o design e a execução, todas as políticas aplicáveis ao ambiente serão

avaliadas em conjunto para determinar se o recurso está em conformidade ou violação. Muitas políticas fragmentam o uso de conectores e podem tornar difícil a identificação de problemas pelos criadores.

- Centralizar a gestão das políticas de DLP com políticas de nível de locatário, utilizando políticas de ambiente apenas para categorização de conectores personalizados ou para casos de exceção.

Para garantir a eficácia das DLPs, é recomendável realizar auditorias e revisões periódicas das políticas e procedimentos. Isso ajuda a identificar possíveis falhas e a fazer ajustes necessários para melhorar a segurança dos dados. Também é importante manter-se atualizado com as mudanças nas regulamentações de segurança e adaptar as políticas de DLP conforme necessário.

b. **Exceções à estratégia de criação de DLPs**

No entanto, existem exceções à estratégia de criação de DLPs que devem ser consideradas. Em alguns casos, pode ser necessário permitir exceções para determinados usuários ou departamentos que precisam de acesso a dados sensíveis para realizar suas funções. Essas exceções devem ser cuidadosamente avaliadas e documentadas, garantindo que haja controles adequados para monitorar e registrar o acesso aos dados. Além disso, é importante considerar a flexibilidade das políticas de DLP para acomodar mudanças nas necessidades de negócios e nas tecnologias utilizadas pela organização.

Com uma estratégia básica de Políticas de Prevenção de Perda de Dados (DLP) estabelecida, é essencial planejar como lidar com exceções de maneira eficaz e segura. As exceções podem surgir por diversas razões, como necessidades específicas de negócios ou requisitos técnicos. Para gerenciar essas exceções, é importante seguir um processo estruturado que garanta a segurança dos dados e a conformidade com as políticas organizacionais.

- **Negar a solicitação:** A primeira abordagem para lidar com exceções é negar a solicitação. Essa opção deve ser considerada quando a exceção não é justificada ou quando pode comprometer a segurança dos dados. Negar a solicitação ajuda a manter a integridade das políticas de DLP e a evitar riscos desnecessários. No entanto, é importante comunicar claramente os motivos da negação ao solicitante e, se possível, oferecer alternativas que atendam às suas necessidades sem comprometer a segurança.
- **Adicionar o conector à política DLP padrão:** Outra abordagem é adicionar o conector à política DLP padrão. Isso permite que a exceção seja tratada dentro das regras já estabelecidas, garantindo que os dados continuem protegidos conforme as diretrizes da política padrão. Essa opção é útil quando a exceção é justificada e pode ser gerenciada sem a necessidade de criar políticas adicionais. Ao adicionar o conector à política DLP padrão, é essencial revisar e ajustar as regras existentes para garantir que a nova inclusão não introduza vulnerabilidades.
- **Incluir os ambientes na lista de exceções para a política global de DLP e criar uma política específica para o caso de uso com a exceção:** Por fim, pode-se incluir os ambientes na lista de exceções para a política global de DLP e criar uma política específica para o caso de uso com a exceção. Essa abordagem permite um controle mais granular e adaptado às necessidades específicas, garantindo que a segurança dos dados seja mantida sem comprometer a flexibilidade operacional. Criar uma política específica para o caso de uso com a exceção permite definir regras e controles personalizados que atendam às particularidades da exceção, enquanto a inclusão na lista de exceções para a política global de DLP assegura que a exceção seja monitorada e gerenciada de forma centralizada.

Ao lidar com exceções nas políticas de DLP, é fundamental seguir um processo estruturado que inclua a negação de solicitações não justificadas, a adição de conectores à política DLP padrão e a criação de políticas específicas para casos de uso excepcionais. Essas abordagens garantem que as exceções sejam gerenciadas de

maneira segura e eficaz, mantendo a integridade das políticas de DLP e protegendo as informações sensíveis da organização.

Em resumo, a criação de DLPs envolve a definição clara dos objetivos e escopo, a avaliação de riscos, a implementação de ferramentas e tecnologias adequadas, o treinamento dos funcionários e a realização de auditorias periódicas. As exceções à estratégia de DLP devem ser cuidadosamente gerenciadas para garantir que a segurança dos dados não seja comprometida. Com uma abordagem abrangente e bem planejada, as organizações podem proteger eficazmente suas informações sensíveis e garantir a conformidade com as regulamentações de segurança.

11.3 Cenário de DLP da ANEEL

Considerando as recomendações apresentadas e alinhando com a estratégia sugerida na seção Estratégias de Ambiente, um cenário da ANEEL é este apresentado na Figura a seguir.

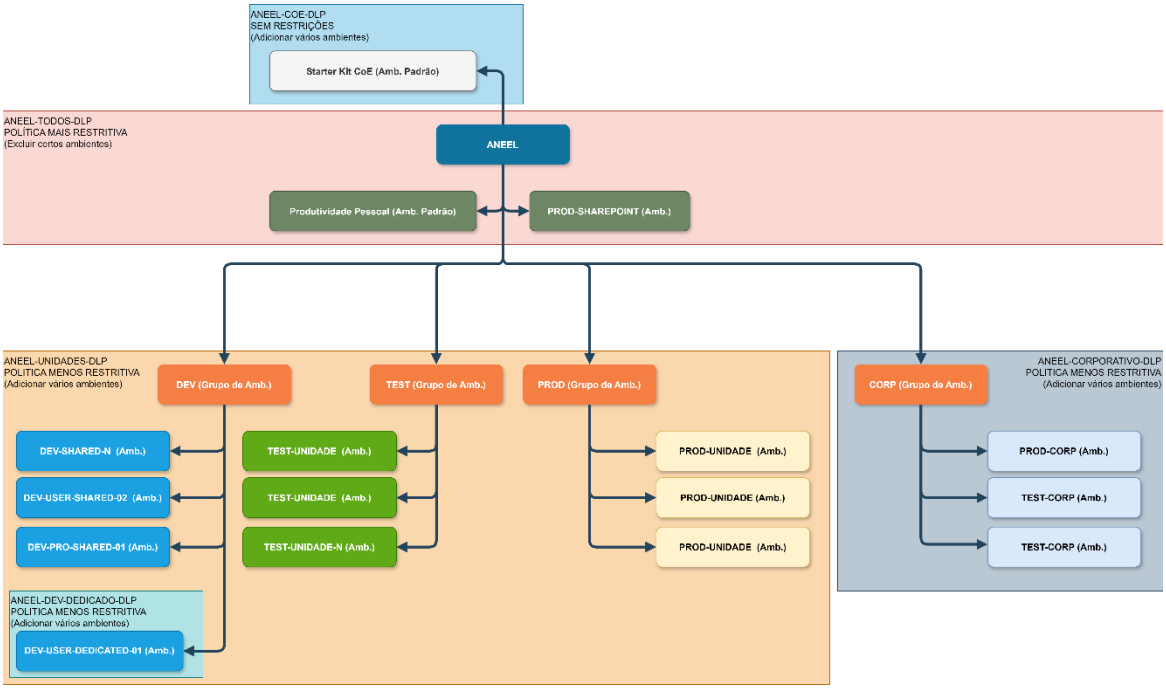

Figura 3 - Cenário de DLP recomendado para a ANEEL

O cenário de Políticas de Prevenção de Perda de Dados (DLP) recomendado para a ANEEL envolve a implementação de várias políticas específicas para diferentes ambientes e necessidades.

a. **ANEEL-TODOS-DLP**

A política ANEEL-TODOS-DLP é uma política DLP mais restritiva, aplicável a todos os ambientes do locatário, exceto aqueles classificados como DEV, TEST, PROD e CORP. Nesta política, os conectores permitidos se restringem ao Office 365 e outros microsserviços padrão, bloqueando o acesso ao restante. Ela abrange o ambiente padrão, o

ambiente dos formulários do SharePoint, além de novos ambientes que ainda não foram incluídos em uma política DLP.

b. **ANEEL-UNIDADES-DLP**

A política ANEEL-UNIDADES-DLP e a política ANEEL-DEV-DEDICADO-DLP são voltadas para ambientes compartilhados, dedicados e das unidades (DEV, TEST, PROD), onde os usuários podem criar aplicativos para casos de uso voltados à produtividade de equipes e usuários. Esses ambientes têm uma política de DLP em nível de locatário associada, que é menos rígida em comparação com uma política padrão, permitindo o uso de outros conectores além dos serviços do Office 365. Como esse ambiente não é padrão, os administradores podem gerenciar de maneira ativa a lista de criadores, adotando uma abordagem em camadas para os ambientes de produtividade compartilhada. O acesso dos criadores é cuidadosamente gerido, e conectores próprios ou de terceiros são disponibilizados conforme a definição dos administradores da Power Platform.

c. **ANEEL-CORP-DLP**

A política ANEEL-CORP-DLP é direcionada aos ambientes corporativos, geridos pela equipe de TI da ANEEL. Esses ambientes também possuem uma política de DLP em nível de locatário associada, com um nível de risco menor que a política padrão, permitindo a utilização de conectores além do Office 365. Como apenas os administradores de TI têm permissão para publicar nesse ambiente, eles podem controlar ativamente a lista de criadores e de conectores usados.

d. **ANEEL-COE-DLP**

Por fim, a política ANEEL-COE-DLP é destinada ao ambiente do Start Kit CoE, que possui um propósito específico. Neste caso, a administração da política de DLP para o ambiente é delegada diretamente a um administrador confiável da equipe do CoE. Esse ambiente foi excluído de todas as políticas de locatário, sendo gerido apenas por uma política DLP de nível de ambiente, o que representa uma exceção, e não a regra.

Essas políticas de DLP são fundamentais para garantir a segurança e a conformidade dos dados dentro da ANEEL, permitindo um controle mais granular e adaptado às necessidades específicas de cada ambiente e uso.

11.4 Conectores

Os conectores na Power Platform são componentes essenciais que permitem a integração de aplicativos, dados e dispositivos na nuvem. Eles funcionam como pontes que conectam a Power Platform a diversas fontes de dados, serviços e APIs, facilitando a automação de processos e a criação de soluções personalizadas. Os conectores são fundamentais para a funcionalidade do Power Apps, Power Automate e outros serviços da Power Platform, permitindo que os usuários acessem e manipulem dados de maneira eficiente e segura.

a. **Classificação dos conectores**

A classificação dos conectores é uma parte crucial da gestão de políticas de prevenção contra perda de dados (DLP). Os conectores são classificados em três categorias principais: Negócio, Não Comercial[13] e Bloqueado.

Conectores classificados como "Negócio" podem ser usados em conjunto com outros conectores do mesmo grupo em um determinado aplicativo ou fluxo. No entanto, se um recurso estiver utilizando um conector comercial, ele não poderá usar conectores não comerciais simultaneamente.

Conectores classificados como "Não Comercial" podem ser usados juntos, mas não podem ser combinados com conectores comerciais.

Já os conectores "Bloqueados" não podem ser utilizados em nenhum recurso do Power Apps ou Power Automate.

É importante notar que todos os conectores premium da Microsoft e conectores de terceiros, tanto padrão quanto premium, podem ser bloqueados, enquanto os conectores padrão da Microsoft e conectores do Common Data Service não podem ser bloqueados.

b. **Conectores que não podem ser bloqueados**

Existem conectores que são essenciais para o funcionamento da Microsoft Power Platform e, portanto, não podem ser bloqueados. Esses conectores garantem que os principais cenários de uso dos usuários permaneçam funcionais.

Entre os conectores que não podem ser bloqueados, estão os conectores padrão do Microsoft Enterprise Plan, como Dataverse, Aprovações e Notificações, bem como conectores específicos da Microsoft Power Platform que fazem parte dos recursos fundamentais da plataforma. O Dataverse, por exemplo, é o único conector premium que não pode ser bloqueado, pois é um elemento essencial da Power Platform. Outros conectores não bloqueáveis incluem Excel Online (Negócios), Microsoft 365 Outlook, OneDrive para Empresas, SharePoint, Power BI, entre outros.

- **Conectores da plataforma Core Power:** Aprovações; Notificações; Dataverse; Dataverse (ambiente atual) e Notificações do Power Apps (v1 e v2).
- **Conectores padrão do Microsoft Enterprise Plan:** Defensor para aplicativos em nuvem; Voz do cliente do Dynamics 365; Excel Online (Negócios); Kaizala; Grupos do Microsoft 365; Grupos de e-mail do Microsoft 365 (visualização); Microsoft 365 Outlook; Usuários do Microsoft 365; Equipes da Microsoft; Microsoft To-Do (Negócios); OneDrive para Empresas; OneNote (Negócios); Planejador; Power BI; SharePoint; Turnos; Skype para Empresas Online e Yammer.

Se um conector que atualmente não pode ser bloqueado já estiver classificado no grupo Bloqueado (por exemplo, porque foi bloqueado em um momento em que as restrições eram diferentes), ele permanecerá nesse grupo até que a política seja modificada. Ao tentar salvar a política, o usuário receberá uma mensagem de erro, sendo impedido de concluir o processo até que o conector desbloqueável seja movido para um grupo de dados Comercial ou Não Comercial.

Em resumo, os conectores desempenham um papel vital na Power Platform, permitindo a integração e automação de processos. A classificação dos conectores em Negócio, Não Comercial e Bloqueado ajuda a gerenciar a segurança e a conformidade dos dados, enquanto a lista de conectores que não podem ser bloqueados assegura que os principais cenários de uso permaneçam operacionais. Com uma gestão adequada dos conectores, as organizações podem maximizar a eficiência e a segurança de suas soluções na Power Platform.

[13] Os termos "Negócio" e "Não Comercial" são apenas rótulos sem significado específico. O que importa é o agrupamento em si dos conectores, e não o nome do grupo.

12. Monitoramento e Análise

12.1 Relatório sobre uso de recursos

Um dos princípios essenciais na administração do Microsoft Power Platform é garantir uma visão completa de como a organização está utilizando o Power Apps e o Power Automate. Obter insights sobre a adoção dessas ferramentas permite q um gerenciamento e proteção da plataforma de maneira eficiente, identificando padrões de uso e incentivando os desenvolvedores a aumentarem a adoção.

Para executar atividades de monitoramento e análise, utilizar o CoE (Center of Excellence). Ele fornece uma implementação de modelo que usa conectores de gerenciamento e administrador, além de um painel no Power BI, que possibilita obter insights sobre o uso do locatário.

As práticas recomendadas para o monitoramento de aplicativos e fluxos de trabalho no Power Apps e Power Automate incluem:

a. **Monitorar os complementos de capacidade de armazenamento**

A seção de capacidade de análise possibilita monitorar tanto o uso da capacidade de armazenamento quanto a disponibilidade no seu locatário. A partir de uma visão abrangente de todos os ambientes, é possível realizar uma análise mais detalhada de cada ambiente individual, permitindo obter informações como a entidade que mais utiliza armazenamento, exibida em um formato de linha do tempo. Para monitorar a capacidade e os complementos de armazenamento, acessar o centro de administração do Power Platform.

Como administrador, você deve:

- Verificar regularmente a capacidade disponível para garantir que novos ambientes possam ser criados pelos usuários no locatário.
- Revisar o armazenamento principal utilizado pelos ambientes para identificar os ambientes que mais consomem recursos.
- Observar picos inesperados no uso de banco de dados, arquivos e gráficos de log em ambientes individuais.
- Revisar os complementos de capacidade, como aprovações no aplicativo do Power Apps, fluxos por processos empresariais, visualizações de páginas do portal, entradas no portal ou créditos do AI Builder, e atribuir essa capacidade a ambientes específicos.

b. **Monitorar o uso do Power Apps**

As análises para o ambiente do administrador podem ser acessadas no centro de administração do Microsoft Power Platform. Os relatórios administrativos oferecem uma visão sobre o uso em nível de ambiente, erros e desempenho do serviço, contribuindo para a governança e o gerenciamento de mudanças para os usuários. Vale destacar que esses relatórios estão disponíveis apenas para aplicativos de tela, não abrangendo os aplicativos baseados em modelo.

Como administrador, é importante:

- Acompanhar a adoção geral, monitorando insights sobre a frequência de uso dos aplicativos e quando eles estão sendo utilizados.
- Verificar o uso dos aplicativos, tanto em navegadores quanto em versões de players móveis, além de identificar em quais plataformas estão sendo executados.

- Monitorar regularmente o desempenho geral do serviço para garantir que a experiência do usuário durante a interação com os serviços da plataforma seja eficiente.

c. **Monitorar o uso do Power Automate**

Administradores de ambiente podem acessar análises para o Power Automate diretamente no centro de administração do Microsoft Power Platform. Esses relatórios fornecem informações detalhadas sobre execuções, uso, erros, tipos de fluxos criados, fluxos compartilhados e conectores associados a diversos tipos de fluxos, como fluxos automatizados, de botão, agendados, de aprovação e de processo empresarial. No entanto, esses relatórios não incluem insights para fluxos de área de trabalho.

Como administrador, é essencial:

- Monitorar o uso e buscar insights sobre os tipos de fluxos que estão sendo utilizados.
- Observar os erros por tipo para identificar possíveis problemas recorrentes.
- Detectar usos inesperados de dados, analisando os conectores, e ajustar as políticas de prevenção contra perda de dados no ambiente para garantir a segurança e integridade da plataforma.

O monitoramento de aplicativos e fluxos de trabalho também pode ser facilitado pelo CoE. O CoE Starter Kit coleta dados sobre todos os aplicativos, fluxos, conectores e outros recursos no ambiente. Ele gera relatórios detalhados que mostram a utilização de cada recurso, quem o criou, a última modificação e muito mais. Com ele, é possível identificar rapidamente aplicativos e fluxos que não são usados há muito tempo ou que têm poucos usuários, sinalizando possíveis problemas ou oportunidades de otimização.

d. **Monitorar o uso do Microsoft Dataverse**

O monitoramento do uso do Microsoft Dataverse é uma prática essencial para garantir a eficiência, segurança e integridade dos dados dentro de uma organização. A análise do Dataverse no centro de administração do Power Platform fornece detalhes sobre o uso do Dataverse em um ambiente específico. É possível alterar os ambientes selecionados utilizando filtros e ajustando o intervalo de datas conforme necessário. As seguintes métricas devem ser acompanhadas no monitoramento do Microsoft Dataverse:

- **Adoção:** A adoção do Dataverse deve ser acompanhada de perto para entender como os usuários estão interagindo com a plataforma. Isso inclui monitorar o número de usuários ativos, as tendências de uso ao longo do tempo, identificar os principais usuários ativos e analisar os modos de acesso, como o sistema operacional, tipo de dispositivo e navegador utilizados. Essas métricas ajudam a identificar padrões de uso e a planejar melhorias na experiência do usuário.
- **Uso:** O uso do Dataverse envolve a análise das entidades mais utilizadas, tanto as padrão quanto as personalizadas, e das atividades realizadas, como criação, leitura, atualização e exclusão de dados (CRUD). Além disso, é importante monitorar os trabalhos do sistema, plug-ins e o uso de chamadas à API. Essas informações fornecem uma visão detalhada de como os dados estão sendo manipulados e ajudam a identificar possíveis gargalos ou áreas que necessitam de otimização1.
- **Integridade:** A integridade do Dataverse é garantida por meio da análise contínua dos trabalhos do sistema, plug-ins e chamadas à API. É fundamental acompanhar a taxa de aprovação, taxa de transferência, principais falhas e pendências dos trabalhos do sistema. Da mesma forma, a análise dos plug-ins deve incluir a taxa de aprovação, tempo de execução e principais falhas. As chamadas à API também devem ser monitoradas para garantir que estão sendo executadas corretamente e identificar as APIs mais usadas e

suas principais falhas. Essas análises ajudam a manter a plataforma funcionando de maneira eficiente e segura1.

Para os administradores, é recomendável monitorar regularmente as atividades realizadas no banco de dados do Dataverse e garantir a integridade geral da plataforma. Isso inclui verificar constantemente o funcionamento dos trabalhos do sistema, o uso de plug-ins pelos criadores de aplicativos e as chamadas de API realizadas no Dataverse. Além disso, é importante estar atento a novos conectores e garantir que eles sejam classificados adequadamente nas políticas de prevenção contra perda de dados (DLP). Implementar práticas robustas de monitoramento e análise permite que as organizações tomem decisões informadas, ajustem e aprimorem suas soluções para melhor atender às necessidades dos usuários e aos objetivos de negócios.

Em resumo, o monitoramento do uso do Microsoft Dataverse é crucial para garantir a adoção eficaz, o uso otimizado e a integridade dos dados. Administradores devem estar atentos às métricas de adoção, uso e integridade, além de implementar recomendações para manter a plataforma segura e eficiente. Com uma abordagem proativa e bem estruturada, as organizações podem maximizar os benefícios do Dataverse e garantir que suas soluções estejam alinhadas com as melhores práticas de governança e segurança.

e. **Monitore novos conectores**

O extenso ecossistema de conectores SaaS (software como serviço) da Microsoft permite integrar aplicativos, dados e dispositivos na nuvem. Alguns dos conectores mais populares incluem serviços como SharePoint, Office 365, Microsoft Teams e Azure. Novos conectores da Microsoft e de terceiros são frequentemente adicionados, e, como administrador, é fundamental estar atento a esses novos conectores e garantir que eles sejam devidamente classificados nas políticas de prevenção contra perda de dados (DLP).

Para facilitar essa tarefa, o Power Automate oferece modelos que permitem notificações sempre que novos conectores forem adicionados: Para facilitar essa tarefa, o Power Automate oferece modelos que permitem o recebimento de notificações sempre que novos conectores forem adicionados:

- Listar novos modelos de conectores do Microsoft Flow.
- Obter a lista de novos modelos do Power Apps, fluxos e conectores.

Configurar esses fluxos no ambiente correspondente para receber notificações regulares sobre novos conectores. Ao avaliar o impacto de um novo conector, é importante decidir se os dados corporativos poderão ser compartilhados com o novo serviço, movendo o conector para o grupo de dados corporativos dentro das suas políticas de DLP. Dependendo do grupo de dados padrão para novos conectores, estabelecido em cada política de DLP, assim como do seu ambiente e estratégia de DLP no locatário, pode ser necessário atualizar várias políticas e considerar o impacto nos casos de uso e nos criadores de cada ambiente.

12.2 Análise de desempenho e uso

A análise e o desempenho da Power Platform são aspectos importantes para garantir a eficiência e a eficácia das soluções desenvolvidas dentro da plataforma.

a. **Relatórios Personalizados**

A criação de relatórios personalizados é uma prática essencial para monitorar e avaliar o uso e o desempenho dos aplicativos e fluxos de trabalho. Esses relatórios permitem que os administradores e

desenvolvedores obtenham uma visão detalhada sobre como os recursos estão sendo utilizados, identificando padrões de uso, gargalos de desempenho e áreas que necessitam de melhorias.

A personalização dos relatórios possibilita a adaptação das métricas e indicadores às necessidades específicas da organização, proporcionando uma análise mais precisa e relevante.

Os relatórios personalizados podem incluir uma variedade de métricas, como o número de usuários ativos, a frequência de uso dos aplicativos, o tempo de resposta das APIs, a taxa de sucesso dos fluxos de trabalho e a utilização de recursos. Esses dados são fundamentais para entender o comportamento dos usuários e a eficiência das soluções implementadas.

Além disso, os relatórios podem ser configurados para fornecer alertas e notificações em tempo real sobre quaisquer anomalias ou problemas de desempenho, permitindo uma resposta rápida e eficaz.

b. **Insights Acionáveis**

Os insights acionáveis são outro componente vital da análise e desempenho da Power Platform. Eles se referem às informações derivadas dos dados coletados que podem ser transformadas em ações concretas para melhorar o desempenho e a eficiência das soluções.

Por exemplo, ao identificar que um determinado fluxo de trabalho está falhando frequentemente, os administradores podem investigar a causa raiz do problema e implementar correções ou otimizações. Da mesma forma, ao observar que um aplicativo específico está sendo amplamente utilizado, pode-se decidir alocar mais recursos para suportar a demanda crescente ou desenvolver funcionalidades adicionais para atender melhor às necessidades dos usuários.

A obtenção de insights acionáveis requer uma análise contínua e detalhada dos dados, bem como a capacidade de interpretar esses dados de maneira significativa. Ferramentas como o Power BI podem ser integradas à Power Platform para criar dashboards interativos e visualizações que facilitam a interpretação dos dados e a tomada de decisões informadas. Esses dashboards podem ser configurados para exibir métricas-chave e tendências de uso, permitindo que os administradores monitorem o desempenho em tempo real e identifiquem oportunidades de melhoria.

Ao monitorar continuamente o uso e o desempenho dos recursos, os administradores podem tomar decisões informadas e implementar melhorias que beneficiem toda a organização.

12.3 Governança e conformidade

A análise e o desempenho da Power Platform são fundamentais para garantir a eficiência, segurança e conformidade das soluções desenvolvidas dentro da plataforma.

a. **Monitoramento de capacidade**

O monitoramento de capacidade é um aspecto crucial, pois permite que os administradores acompanhem o uso de recursos e a disponibilidade de armazenamento em cada ambiente. A partir da exibição completa de todos os ambientes, é possível detalhar os ambientes individuais para obter informações sobre a entidade que mais utiliza armazenamento e visualizar gráficos de linha do tempo. Verificar regularmente a capacidade disponível, revisar o principal armazenamento usado pelos ambientes e procurar picos inesperados no uso de banco de dados, arquivos e gráficos de log são práticas recomendadas para garantir que novos ambientes possam ser criados conforme necessário.

b. **Monitoramento de conformidade**

O monitoramento de conformidade é igualmente importante para assegurar que os aplicativos e fluxos de trabalho estejam em conformidade com as políticas internas de governança e regulamentações externas.

Utilizar ferramentas como o CoE (Centro de Excelência) Starter Kit pode ajudar a monitorar a criação de aplicativos e fluxos, garantindo que eles atendam às diretrizes organizacionais. Configurar alertas para quando recursos não estiverem em conformidade e realizar auditorias periódicas são práticas recomendadas para manter a conformidade e a segurança dos dados.

Além disso, o CoE Starter Kit oferece dashboards e relatórios no Power BI que fornecem uma visão abrangente do uso da Power Platform na organização, facilitando a identificação de áreas que precisam de atenção.

c. **Automatização de processos de governança**

A automatização de processos de governança é uma estratégia eficaz para garantir a aplicação consistente de políticas e reduzir o esforço manual na administração da Power Platform.

Utilizar fluxos automáticos incluídos no CoE para aplicar políticas de governança, como o arquivamento automático de aplicativos não utilizados ou a notificação de criadores de aplicativos sobre violações de políticas, pode melhorar significativamente a eficiência operacional.

Além disso, a implementação de fluxos de trabalho automatizados para gerenciar a criação de novos ambientes, a atribuição de permissões e a classificação de conectores nas políticas de prevenção contra perda de dados (DLP) ajuda a manter a integridade e a segurança da plataforma.

Com essas práticas, as organizações podem garantir que suas soluções na Power Platform sejam geridas de maneira segura, eficiente e conforme as melhores práticas de governança.

12.4 Rastreamento do acesso do usuário

O rastreamento do acesso do usuário é uma prática essencial para garantir a segurança e a conformidade dentro da Power Platform.

As atividades realizadas no Power Apps e no Power Automate podem ser monitoradas e visualizadas no Centro de Conformidade e Segurança do Office 365. Isso permite rastrear quando aplicativos ou fluxos são criados, editados ou excluídos, além de outras atividades principais. Esses logs de atividades são fundamentais para auditorias e podem ser revisados manualmente ou utilizados via API para automatizar cenários mais complexos.

No Power Automate, as atividades registradas incluem a criação, edição e exclusão de fluxos, além da edição e exclusão de permissões. Também são monitoradas ações como o início e a renovação de avaliações pagas.

Já no Power Apps, as atividades registradas abrangem a criação, edição e publicação de aplicativos, exclusão de aplicativos, restauração de versões anteriores, início de aplicativos, marcação de aplicativos como em destaque ou evidência, e edição e exclusão de permissões de aplicativos.

Para tirar proveito do log de atividades, é necessário ativar o log de auditoria no locatário antes que os dados estejam disponíveis para visualização. Além disso, para manter esses logs por um período maior, é recomendado exportá-los e armazená-los como backup. Como administrador, é importante refletir cuidadosamente sobre o uso dos dados de auditoria, aproveitando o Centro de Conformidade e Segurança do Office

365, além de outros mecanismos de monitoramento. É possível criar políticas de alerta para garantir a integridade geral da plataforma de desenvolvimento de aplicativos voltada para cidadãos.

Com uma abordagem proativa e bem estruturada, o rastreamento do acesso do usuário contribui significativamente para a segurança e a conformidade, permitindo que as organizações monitorem e gerenciem efetivamente as atividades dentro da Power Platform.

12.5 Centralizar toda visão com o Power BI do COE

Como administrador da Microsoft Power Platform, é essencial ter visibilidade clara sobre como a organização utiliza o Power Apps e o Power Automate. Os insights sobre a adoção auxiliam na governança e proteção da plataforma, ajudam a identificar padrões de uso e permitem oferecer suporte aos criadores para acelerar a adoção.

O painel do Power BI, presente no Kit de Início do Centro de Excelência (CoE), fornece uma visão abrangente com visualizações e insights sobre os recursos do seu locatário, como ambientes, aplicativos, fluxos do Power Automate, conectores, referências de conexão, criadores e logs de auditoria.

Esse painel oferece análises detalhadas e dados para monitorar todo o ambiente. A seção Monitor do painel Power BI do CoE permite acessar o inventário básico (ambientes, aplicativos, fluxos, criadores, conectores e registros de auditoria) e monitorar o uso tanto no locatário inteiro quanto em cada ambiente individualmente.

Os seguintes indicadores são propostos para o monitoramento:

a. **Visão Geral – Power Apps, Power Automate e Chatbots**

A página de Visão Geral apresenta uma visão abrangente dos recursos disponíveis no locatário, incluindo: Número total de ambientes (e ambientes criados neste mês); Número total de criadores de ambientes; Número total de conectores personalizados; Número total de aplicativos, criadores de aplicativos e aplicativos criados neste mês; Número total de fluxos, criadores de fluxos e fluxos criados neste mês; e Número total de bots, criadores de bots e bots criados neste mês.

b. **Ambientes**

A página Ambientes exibe a quantidade de ambientes, criadores de ambiente e instâncias do Microsoft Dataverse. Os gráficos disponíveis mostram: Tendência de criação de ambientes ao longo do tempo; Número de recursos por ambiente; Número de ambientes por tipo; Principais criadores de ambientes; e Quantidade de Ambientes Gerenciados.

c. **Ambientes do Teams**

A página Ambientes do Teams apresenta o número de ambientes, criadores de ambientes e recursos do Microsoft Teams nesses ambientes. Os gráficos mostram: Tendência de criação de ambientes; Número de recursos por ambiente.

As tabelas de ambientes fornecem: Nome do ambiente; Link para o ambiente no Centro de administração; Link para o Microsoft Teams conectado; Proprietário; Data do último lançamento de aplicativo no ambiente; Quantidade de aplicativos e fluxos; Um ícone vermelho, indicando a ausência de aplicativos ou fluxos nos ambientes; e Data de criação;

A tabela de aplicativos exibe: Nome do aplicativo; Proprietário; Último lançamento; Data de criação; e Data da última modificação.

d. **Aplicativos**

A página Aplicativos fornece uma visão geral dos aplicativos no ambiente, incluindo: Número total de aplicativos; Número total de aplicativos criados neste mês; Número total de criadores de aplicativos; Número total de aplicativos de tela e baseados em modelo; e Número de aplicativos de produção (um aplicativo de produção é definido como aquele que teve 50 sessões ativas ou sessões ativas de cinco usuários únicos em um mês).

e. **Fluxos da Nuvem**

A página Fluxos de Nuvem oferece uma visão geral dos fluxos de automação de API baseados em nuvem no ambiente, incluindo: Número total de fluxos; Número total de fluxos criados neste mês; Número total de criadores de fluxos; e Número total de fluxos iniciados, suspensos e interrompidos.

Os recursos visuais disponíveis permitem visualizar a tendência de criação de fluxos, principais departamentos ativos, principais ambientes e principais conectores usados em fluxos.

f. **Conectores Personalizados**

Na página Conectores Personalizados, são detalhados os conectores personalizados, incluindo os pontos de extremidade conectados e os recursos que utilizam esses conectores. Além do número total de conectores personalizados e de conectores de teste, a página exibe: Tendência de criação de conectores; Ambientes com o maior número de conectores personalizados; e Fluxos e aplicativos que utilizam conectores personalizados.

g. **Fluxos de Área de Trabalho**

A página Fluxos de Área de Trabalho apresenta uma visão geral dos fluxos de automação robótica de processos (RPA) baseados em interface do usuário no ambiente, incluindo: Número total de fluxos de área de trabalho; Número total de fluxos de área de trabalho criados neste mês; e Número total de criadores de fluxos de área de trabalho.

Os recursos visuais mostram a tendência de criação de fluxos e os principais ambientes com fluxos de área de trabalho. A exibição de lista permite classificar os fluxos por tipo e estado.

h. **Bots**

A página Bots fornece uma visão geral dos bots do Microsoft Copilot Studio no ambiente, incluindo: Número total de bots; Número total de bots criados neste mês; Número total de criadores de bots; e Número total de bots publicados.

Recursos visuais mostram a tendência de criação de bots e os principais ambientes com bots. A exibição de lista permite classificar os bots por criador ou estado.

i. **Modelos do AI Builder**

A página AI Builder Modelos fornece uma visão geral dos Modelos do AI Builder no ambiente, incluindo: Número total de modelos do AI Builder; Número total de modelos do AI Builder criados neste mês; e Número total de criadores de modelos do AI Builder.

Os recursos visuais mostram a tendência de criação de modelos do AI Builder e os principais ambientes com esses modelos. A exibição de lista permite classificar os modelos por criador ou modelo.

j. **Power Pages**

A página Soluções oferece uma visão geral das soluções do Power Platform no ambiente, incluindo: Número total de soluções; Número total de soluções criadas neste mês; e Número total de criadores de soluções.

Os recursos visuais permitem visualizar a tendência de criação de soluções e os principais ambientes com soluções. A exibição de lista permite classificar as soluções por editor, criador ou ambiente.

k. **Fluxos de Processo Empresarial**

A página Fluxos de Processo Empresarial fornece uma visão geral dos fluxos de processo empresarial no ambiente, incluindo: Número total de fluxos de processo empresarial; Número total de fluxos de processo empresarial criados neste mês; e Número total de criadores de fluxos de processo empresarial.

Recursos visuais mostram a tendência de criação de fluxos de processo empresarial e os principais ambientes com esses fluxos. A exibição de lista permite classificar os fluxos por estado, criador e ambiente.

12.6 Política e procedimentos de medição do desempenho da governança

Definir KPIs relevantes como adoção de aplicativos, desempenho, segurança e conformidade é fundamental por várias razões, especialmente ao implementar e gerenciar a Power Platform, pois permite a medição do sucesso, tomada de decisões informadas e alinhamento com metas de negócio. Na seção anterior foi disponibilizadas diversos medidores que podem ser utilizados para estabelecimento de metas, como por exemplo:

a. **Adoção de Aplicativos**
- **KPI**: Número de usuários ativos mensais (MAU) e diários (DAU).
- **Meta**: Aumentar o MAU em 15% ao longo dos próximos 6 meses.

b. **Desempenho**
- **KPI:** Tempo médio de carregamento de páginas e resposta das APIs.
- **Meta:** Manter o tempo de resposta abaixo de 3 segundos para 95% das transações.

c. **Segurança**
- **KPI**: Número de incidentes de segurança relatados.
- **Meta**: Reduzir os incidentes em 25% em relação ao último trimestre.

d. **Conformidade:**
- **KPI**: Percentual de aplicativos que atendem às políticas de conformidade.
- **Meta**: Garantir que 100% dos aplicativos estejam em conformidade com as políticas estabelecidas.

13. Termos

ALM (Application Lifecycle Management): Gestão do ciclo de vida do aplicativo desde sua concepção até sua descontinuação.
Ambiente: Espaço dedicado na Power Platform para armazenamento e gestão de dados e aplicativos.
Aplicativo Canvas: Aplicativo que permite múltiplos coproprietários e é flexível na transferência de propriedade.
Azure DevOps: Plataforma da Microsoft para controle de versão, gerenciamento de projetos e automação de pipelines.
CI/CD (Continuous Integration/Continuous Deployment): Práticas de integração e entrega contínua no desenvolvimento de software.
Dataverse: plataforma de dados da Microsoft Power Platform que permite armazenar e gerenciar dados de maneira estruturada e segura, facilitando a integração com outros serviços e aplicativos.
DLP, ou Data Loss Prevention: estratégia de segurança que visa proteger dados sensíveis contra perda, vazamento ou acesso não autorizado, monitorando e controlando a transferência de informações dentro e fora da organização.
Hotfix: correção rápida e específica aplicada a um software para resolver problemas críticos, como bugs ou falhas de segurança.
Locatário: entidade ou organização que possui uma assinatura do Microsoft Power Platform e gerencia os ambientes e recursos dentro dessa assinatura.
Patch: pequeno programa de computador que pode ser adicionado a um software existente para corrigir problemas, melhorar a funcionalidade ou atualizar o sistema.
RBAC (Role-Based Access Control): Controle de acesso baseado em funções para garantir que os usuários tenham apenas as permissões necessárias.
Tenant: instância única de um serviço em nuvem dedicada a uma organização específica, garantindo isolamento e segurança dos dados e recursos dessa organização.

14. Referências

Documentação da Microsoft sobre Power Platform
Noções básicas de ALM com Microsoft Power Platform
https://learn.microsoft.com/pt-br/power-platform/alm/basics-alm
Visão geral de pipelines no Power Platform
https://learn.microsoft.com/pt-br/power-platform/alm/pipelines
ALM para administradores e criadores
https://learn.microsoft.com/pt-br/power-platform/alm/admins-makers
ALM para desenvolvedores
https://learn.microsoft.com/pt-br/power-platform/alm/alm-for-developers

Microsoft Power Platform adoption best practices
https://learn.microsoft.com/en-us/power-platform/guidance/adoption/methodology
Microsoft Power Platform adoption best practices
https://learn.microsoft.com/en-us/power-platform/guidance/adoption/methodology
Configurar a segurança do usuário em um ambiente
https://learn.microsoft.com/pt-br/power-platform/admin/database-security
Autenticação em fontes de dados
https://learn.microsoft.com/pt-br/power-platform/admin/security/connect-data-sources#authenticating-to-data-sources
Direitos de acesso e privilégios
https://learn.microsoft.com/pt-br/power-platform/admin/security-roles-privileges
Funções e responsabilidades
https://learn.microsoft.com/pt-br/power-platform/guidance/adoption/roles
Microsoft Power Platform adoption best practices
https://learn.microsoft.com/pt-br/power-platform/guidance/adoption/dlp-strategy
https://learn.microsoft.com/pt-br/power-platform/admin/dlp-connector-classification
https://learn.microsoft.com/pt-br/connectors/connector-reference/connector-reference-premium-connectors
Relatório sobre uso de recursos
https://learn.microsoft.com/pt-br/power-platform/guidance/adoption/resource-usage
Monitorar com o painel do Power BI do CoE
https://learn.microsoft.com/pt-br/power-platform/guidance/coe/power-bi-monitor