Apêndice

- Gestão de Riscos
- Gestão dos direitos dos titulares de dados

Gestão de Riscos

Introdução

Objetivo desta seção é oferecer uma abordagem para que as empresas realizem a gestão de risco, de qualquer natureza, no MD2 Quality Manager.

> Risco, segundo a ISO 31000, é o efeito das incertezas nos objetivos.

Identificação dos riscos

Identificar riscos é o primeiro passo para poder gerenciá-los. Segundo a ISO 31000, a identificação de riscos é o processo de busca, reconhecimento e descrição dos riscos. Envolve a identificação das fontes, eventos, suas causas e suas consequências potenciais e pode compreender dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, e as necessidades das partes interessadas.

Uma vez identificado, pode-se então seguir para a análise dos riscos, compreendendo a sua natureza e determinando o nível do risco, os critérios de aceitação e tomando as decisões para o tratamento.

Análise dos riscos

No MD2 Quality Manager é possível analisar os riscos, tanto de processos quanto de tratamento de dados utilizando a metodologia FMEA (Failure Mode and Effect Analysis).

Uma breve história sobre a metodologia:

O FMEA surgiu no fim dos anos 40 a fim de analisar as falhas dos equipamentos do exército americano Na década de 60 a NASA aprimorou e desenvolveu a ferramenta, e foi nessa época que o conhecimento sobre ela foi se disseminando através do setor aeronáutico. Já nos 70 a indústria automobilística passou a utilizá-la de forma ampla, fazendo com que não só as operações na linha de produção a usassem, mas também os seus fornecedores, e todas as outras indústrias que estivessem envolvidas em seu processo.

Hoje, entende-se que o FMEA como uma metodologia sistemática que permite identificar potenciais falhas de um sistema, projeto e/ou processo, com o objetivo de eliminar ou minimizar os riscos associados, antes que tais falhas aconteçam. Atualmente, o FMEA é utilizado em vários tipos de indústrias, hospitais, empresas de variados portes e, inclusive, em análises de processos.

Mas, afinal, o que significa a sigla FMEA? Na verdade, essa sigla é em inglês e significa Failure Mode and Effect Analysis (traduzindo para o português Análise dos efeitos e modos de falha). O FMEA oferece funções distintas como uma ferramenta para prognósticos de problemas e como

procedimento para desenvolvimento e execução de projetos, processos e/ou serviços.

A análise utilizando o FMEA pode ser feita de maneira individual, mas quando aplicada em equipe é mais eficaz, pois a chance de identificação e a prevenção dos potenciais modos de falha são maiores. É importante pontuar que o FMEA permite atuar nos possíveis problemas antes mesmo que eles ocorram, sendo esse mais um motivo para se ter uma equipe qualificada e pronta para realizar as análises de modo de falha.

> Segundo a ISO 31010, a metodologia FMEA é fortemente aplicável para identificação e avaliação de riscos.

Principais tipos de FMEA

O FMEA pode ser aplicado em diversos âmbitos e, hoje, os mais conhecidos deles são o FMEA de produto e o FMEA de processo. A realização das análises e das etapas são as mesmas, o que as difere é o objetivo

- **FMEA de processo:** É direcionado ao desenvolvimento de um processo para que todas as falhas potenciais e suas causas sejam analisadas e tomadas todas as ações preventivas necessárias. O objetivo do FMEA de Processo é evidenciar todas as possíveis falhas ao longo do fluxo produtivo para que sejam identificados todos os riscos que uma tarefa possa apresentar no decorrer do seu processo.
- **FMEA de produto:** Neste caso, são considerados as falhas que podem ocorrer com o produto dentro das especificações do projeto. O objetivo desta análise é evitar falhas no produto decorrente do projeto que está sendo planejado.

Objetivos do FMEA

O objetivo da análise dos efeitos e modos de falha é identificar características do produto, processo ou serviço que são passíveis de apresentar vários tipos de falhas Através de um checklist, é possível identificar essas possíveis falhas antes que elas aconteçam Para fazer esse checklist deve se fazer três perguntas:

- Qual é a probabilidade de a falha acontecer?
- Qual seria a consequência da falha?
- Com qual probabilidade a falha for detectada antes que afete o produto/processo?

Após avaliação quantitativa dessas três perguntas, é calculado o número de prioridade de risco (RPN) para cada causa potencial de falha.

As ações de correção serão priorizadas conforme cada RPN, começando pelo mais alto e/ou pela gravidade mais elevada O foco principal da FMEA é identificar, delimitar e descrever as possíveis não conformidades (modo de falha) de um projeto, processo ou serviço, seus efeitos e causas, criando condições organizacionais para minimizá-los ou eliminá-los, através de ações de prevenção estruturada e realizada no prazo e por profissional especializado.

Metodologia e implementação

É importante lembrar que a metodologia FMEA independe de qual tipo seja a aplicação (produto, processo, etc.), pois os passos a serem feitos serão os mesmos. A análise consiste na formação de um grupo de pessoas que irão identificar produto/ processo/ serviço em função de duas questões, os tipos de falhas que podem acontecer e os efeitos que essas possíveis falhas podem causar.

A seguir, serão apresentadas as 8 etapas para a implementação do FMEA:

Etapa 1: Revisão do processo

A fim de garantir que a equipe que estará realizando o FMEA tenha o mesmo entendimento, é interessante que os processos envolvidos em discussão sejam mapeados, descrevendo o fluxo de tarefas ou fluxo do produto dentro do processo.

Etapa 2: Mapeamento dos potenciais modos de falha

O modo de falha potencial pode ser visto como a maneira que um componente sistema falharia ao cumprir a sua função descrita (seja ela total ou parcial). Portanto, nessa etapa, ocorrerá o brainstorming para levantar os possíveis potenciais de falha. O objetivo é gerar uma lista com possíveis riscos prejudiciais ao produto/ processo.

Etapa 3: Listagem dos possíveis efeitos para cada modo de falha

Entende se como “efeitos de falha” as formas como os modos de falha afetam o desempenho do sistema. Nesse momento, lista-se todos os potenciais riscos para cada etapa do processo, e a equipe identifica quais serão as consequências se esta falha ocorrer.

Etapa 4: Atribuir uma pontuação relativa à gravidade de cada efeito

Gravidade é a apreciação do quão severo é o potencial efeito de falha. Deve se pontuar cada efeito, em uma escala de 10 pontos, sendo 1 o índice menor e 10 o maior. Essa pontuação deve ser estimada levando em consideração os impactos negativos que o efeito pode causar, caso essa falha ocorra.

Nunca	Raramente	Muito Baixa	Baixa	Moderada para baixa	Moderada	Moderada para Alta	Alta	Muito Alta	Sempre
1	2	3	4	5	6	7	8	9	10

Etapa 5: Atribuir uma pontuação relativa à ocorrência de cada efeito

Ocorrência é a probabilidade ou frequência de um evento acontecer durante a vida de um projeto. Nesta etapa serão atribuídas uma pontuação para cada ocorrência, sendo 1 o índice menor e 10 o maior. O melhor método para se determinar a ocorrência é analisando o histórico de falhas, porém, caso o mesmo não exista, a equipe deve estimar a probabilidade de os fatos ocorrerem.

Nunca	Raramente	Muito Baixa	Baixa	Moderada para baixa	Moderada	Moderada para Alta	Alta	Muito Alta	Sempre
1	2	3	4	5	6	7	8	9	10

ETAPA 6: Atribuir uma pontuação relativa para a detecção de cada modo de falha

A pontuação deve ser realizada na capacidade de se identificar a falha ou efeito, antes que a mesma seja perceptível ao cliente. Também é utilizada uma escala de 10 pontos, entretanto, ao contrário das anteriores, sendo 10 o índice de menor detecção e o 1 o índice de maior detecção.

Nunca	Raramente	Muito Baixa	Baixa	Moderada para baixa	Moderada	Moderada para Alta	Alta	Muito Alta	Sempre
10	9	8	7	6	5	4	3	2	1

Etapa 7: Calcular o RPN (grau de prioridade de risco) para cada modo de falha

Calcula se o RPN multiplicando os números da gravidade, ocorrência e detecção para cada item.

> Grau de Prioridade de Risco = Gravidade x Ocorrência x Detecção

Etapa 8: Priorizar os modos de falha para cada ação

Deve se estabelecer uma ordem de priorização através do RPN: quanto maior o grau de prioridade de risco, maior é a prioridade para criar uma ação. Recomenda se também que os modos de falha com 9 ou 10 para gravidade sejam automaticamente priorizados, independentemente de seus RPN.

Exemplo:

FMEA - ANÁLISE DE MODO DE FALHA					
Processo	Potencial Modo de Falha	Gravidade	Ocorrência	Detecção	RPN
Atendimento ao cliente	Ligação para o cliente errado	7	4	5	**140**
	Cobrança indevida	9	4	6	**216**
	Dados cadastrais desatualizados	6	7	3	**126**
	Funcionário indisponível para atendimento	10	1	5	**50**

De acordo com a tabela acima o potencial de modo de falha: Cobrança indevida, deve ser priorizado juntamente com Funcionário indisponível para atendimento para tratativas pois foi o dado que apresentou o maior RPN e a maior gravidade respectivamente.

FMEA e a governança de dados

A governança de dados é uma estrutura com o propósito de coordenar, orientar e definir regras para o uso, coleta e criação dos dados, visando proteger a propriedade intelectual da organização e garantir a segurança no armazenamento, monitoramento e geração de dados no ambiente corporativo.

Quando se tem dados governados, torna-se possível e mais simples a identificação de estratégias, a produtividade, redução de custos, avaliação de índices de crescimento, maior transparência e maior controle e segurança dos dados.

Problemas comuns que surgem quando não há governança de dados são a dificuldade em execução de planos e tarefas, problemas de compliance coleta e utilização de dados com pouca confiabilidade, duplicação de informações, redução de produtividade, entre outras.

> De acordo com o artigo 50 da lei 13 709 18 a Lei Geral de Proteção de Dados Pessoais:
> “Art. 50 Os controladores e operadores, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
> §1 º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular."

É ideal que as organizações estabeleçam boas práticas de governança de dados, e uma forma de se realizar essas boas práticas é realizando a análise de gravidade de riscos através do FMEA

Através da ferramenta FMEA, é possível analisar os riscos dos processos que envolvem esses dados e, assim, transformar a governança em uma função estratégica de negócios.

FMEA no MD2 Quality Manager

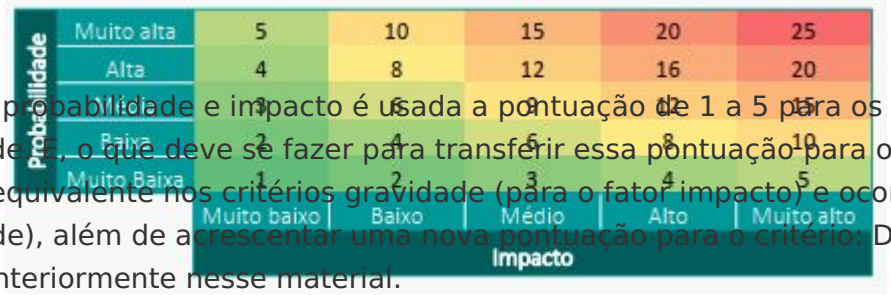
Através do MD2 Quality Manager é possível realizar a o registro e avaliação dos riscos (relacionados aos processos e/ou tratamento de dados), categorizá-los, e pontuá-los de acordo com a metodologia FMEA (utilizando as escalas de pontuação de 1 a 10). Após a listagem de todos os riscos, é possível analisar a prioridade de tratamento através do número de prioridade de risco (RPN).

> Para mais detalhes sobre o cadastro de riscos em processos, consulte o tópico 5 deste manual.

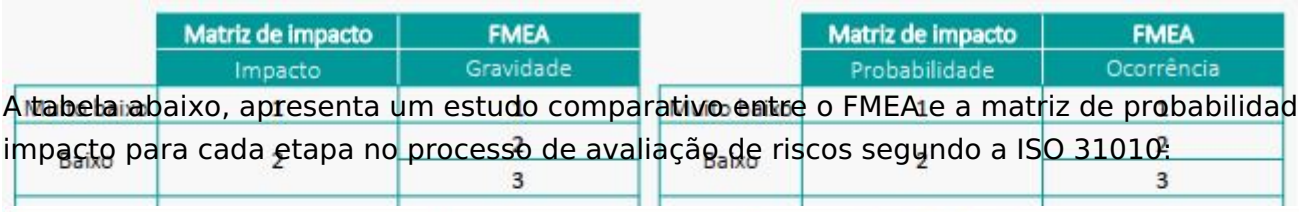
> Para mais detalhes sobre o cadastro de riscos em Tratamento de dados, consulte o tópico 6 deste manual.

Matriz de probabilidade e impacto X FMEA - Proposta de adaptação do uso das metodologias

É possível adaptar o uso da matriz de probabilidade e impacto na metodologia FMEA (e vice-versa), através da equivalência das pontuações. A matriz de impacto, também conhecida como matriz de riscos, é uma ferramenta visual que possibilita focar em quais riscos devem ser priorizados.



A matriz de probabilidade e impacto é usada a pontuação de 1 a 5 para os critérios: Impacto e Probabilidade. E, o que deve se fazer para transferir essa pontuação para o FMEA é verificar a pontuação equivalente nos critérios gravidade (para o fator impacto) e ocorrência (para o fator probabilidade), além de acrescentar uma nova pontuação para o critério: Detecção. conforme foi explicado anteriormente nesse material.



A tabela abaixo, apresenta um estudo comparativo entre o FMEA e a matriz de probabilidade e impacto para cada etapa no processo de avaliação de riscos segundo a ISO 31010:

Ferramentas e técnicas	Processo de avaliação de riscos				
	Identificação de riscos	Análise de riscos			Avaliação de riscos
		Consequência	Probabilidade	Nível de risco	
FMEA	FA	FA	FA	FA	FA
Matriz de probabilidade e impacto	FA	FA	FA	FA	A

A - Aplicável

Tratamento de riscos

A partir da identificação e análise dos riscos, com base na priorização dos riscos serão feitas as tratativas no módulo de ocorrências do MD2 Quality Manager.

> Para mais detalhes sobre o tratamento de riscos, consulte o tópico 8.4 deste manual.

Para realização das tratativas é recomendado que o responsável pela tratativa reúna com uma

equipe multidisciplinar e faça um brainstorming de todas as possíveis causa raízes relacionada ao risco, sendo formalizada e documentada no MD2 Quality Manager utilizando a metodologia de análise de causa e efeito.

Diagrama de causa e efeito

O diagrama de causa e efeito é uma metodologia que ajuda a levantar as causas-raízes de um risco, ou seja, partindo da premissa de que todo risco possui uma causas específicas e e essas causas devem ser analisadas e testadas, uma a uma, a fim de comprovar qual delas está realmente causando o efeito (falha) que se quer eliminar. Eliminado as causas, elimina-se o risco.

> Segundo a ISO 31010, a metodologia de análise de causa e efeito é fortemente aplicável para avaliação de riscos.

Para realizar a análise de causas utilizando o Diagrama de Ishikawa, basta seguir alguns passos:

- Defina o risco a ser analisado;
- Realize um brainstorming para levantar as possíveis causas que possam estar gerando o risco. Para isso, procure responder a seguinte pergunta: "*Por que isto está acontecendo?"*;
- Divida as causas identificadas em **categorias**, por exemplo: máquina, mão de obra, método e materiais ou da forma que for mais coerente com o problema analisado e o contexto da empresa;

Originalmente, foram propostas 6 categorias pelo método, que são: Máquina, Materiais, Mão de obra, Meio-ambiente, Método e Medidas (os 6Ms). Entretanto nem todos os processos ou problemas utilizam-se de todos esses fatores, assim é preciso avaliar quais deles estão presentes ou são importantes para a execução.

> É possível, no MD2 Quality Manager, parametrizar essas categorias. Para mais detalhes sobre configuração e criação de domínios do sistema, consulte o tópico 2 deste manual.

Em sequência, caberá ao responsável pela tratativa, criar e definir um plano de ação para a resolução das causas apontadas. Para construção e elaboração do plano de ação, usamos a metodologia 5W2H. A partir da definição do plano de ação, será preciso executar as atividades propostas de acordo com os prazos estipulados.

5W2H

5W2H é um método de gerenciamento de atividades de um plano de ação. O nome vem de cinco perguntas, em inglês, que começam com a letra "W", e duas questões que começam com a letra "H". Veja, a seguir, quais os significados de cada letra:

- What (o que será feito?);
- When (quando será feito?);
- Where (onde será feito?);

- Why (por que será feito?);
- Who (quem fará?);
- How (como será feito?);
- How much (quanto custará?).

> Para mais detalhes sobre o painel de tarefas, consulte o tópico 7 deste manual.

Concluído o tratamento, é essencial estabelecer o resultado das tratativas assim como, evidenciar e documentar tudo que foi realizado.

Em sequência, são estabelecidas, mapeadas e implementadas todas as melhorias resultantes, tais como: correções, controles, protocolos e barreiras. Em adição, será necessário realizar uma nova avaliação dos riscos, mantendo, caso não solucionado ou diminuindo a pontuação dos critérios de avaliação do risco.

Após realizado o tratamento do risco, ele será classificado como: Risco Ativo, Risco mitigado ou Risco Sanado.

- Risco ativo: risco que foi identificado e analisado, porém, por motivos diversos (risco baixo, impossibilidade de tratativa, custo desproporcional ao benefício, etc.) não foi feito nenhum tipo de tratativa.
- Risco sanado: risco que foi identificado, analisado e após as tratativas e melhorias implementadas, não existe mais a possibilidade de ocorrência.
- Risco mitigado: risco que foi identificado, analisado e após as tratativas e melhorias implementadas, ainda existe a possibilidade de ocorrência.

Gestão dos direitos dos titulares de dados

Introdução

Objetivo desta seção é oferecer uma abordagem para que as empresas realizem a gestão dos direitos dos titulares de dados, no MD2 Quality Manager.

De acordo com a LGPD (Lei Geral de Proteção de Dados Pessoais), todos os cidadãos são titulares de seus dados pessoais, que são individuais e intransferíveis.

> LGPD Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

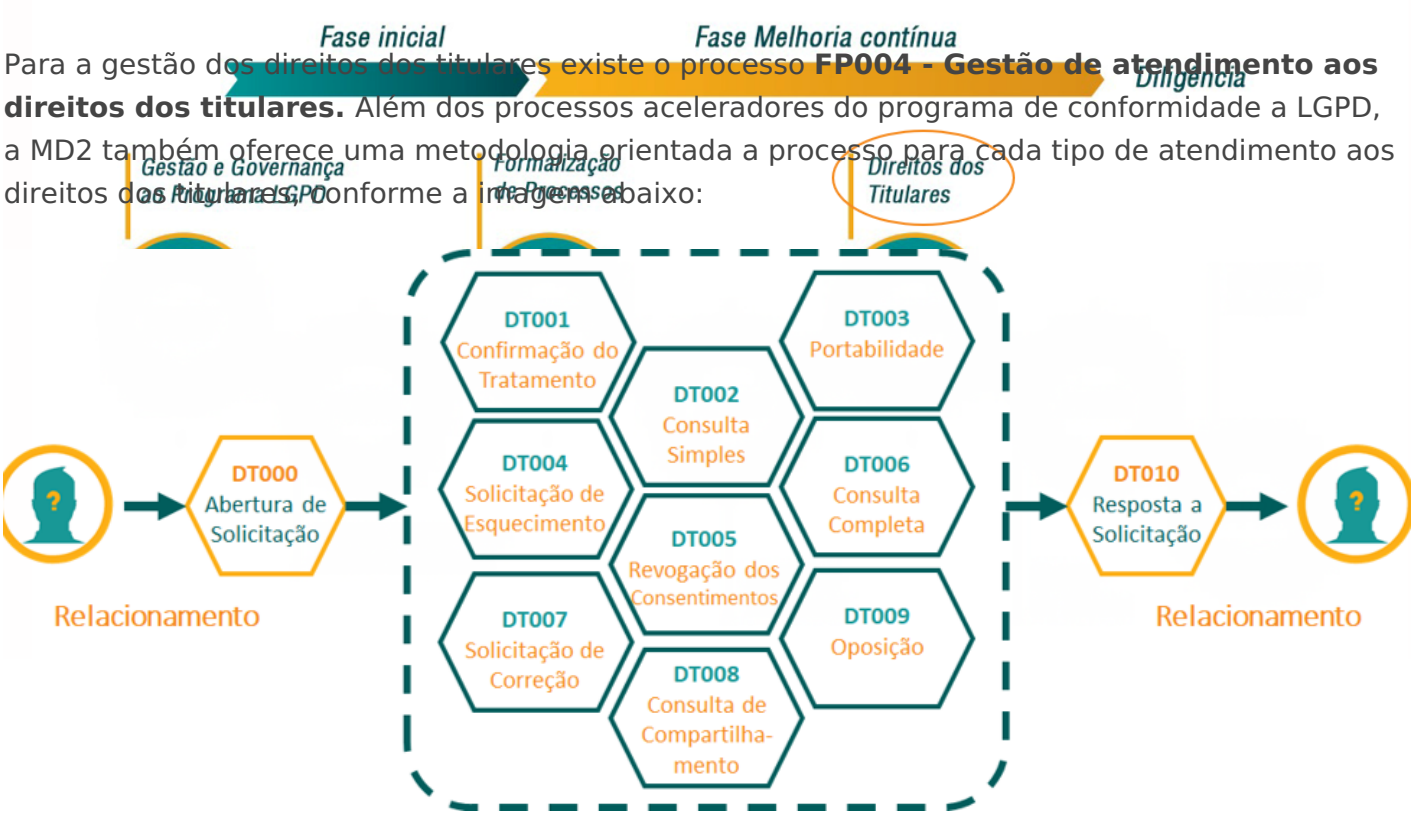
O art. 18 da LGPD, estabelece que a qualquer momento o titular pode solicitar os direitos listados abaixo:

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da Autoridade Nacional, observados os segredos comercial e industrial;
- Eliminação dos dados pessoais tratados com o consentimento do(a) titular, exceto nas hipóteses previstas no art. 16 da Lei;
- Informação das entidades públicas e privadas com as quais o Controlador realizou uso compartilhado de dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre consequências da negativa;
- revogação do consentimento, nos termos do § 5.º do art. 8.º da Lei.

> Titular dos dados, segundo Art. 5º, V, da LGPD, é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento

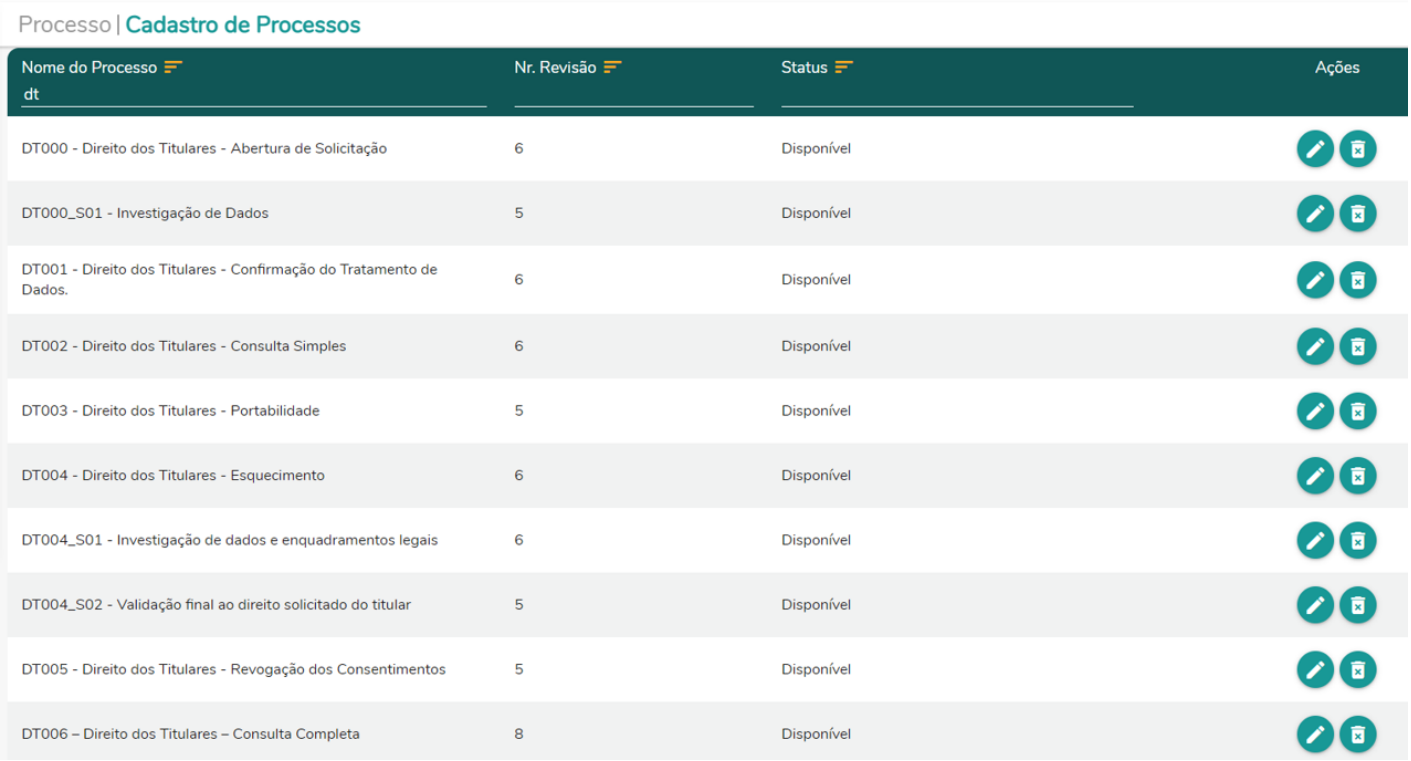
Processos aceleradores

A MD2 consultoria oferece uma metodologia orientada a processo como sugestão ao clientes para gestão do programa de conformidade a LGPD. Os processos aceleradores estão especificados na imagem abaixo:



Para a gestão dos direitos dos titulares existe o processo **FP004 - Gestão de atendimento aos direitos dos titulares.** Além dos processos aceleradores do programa de conformidade a LGPD, a MD2 também oferece uma metodologia orientada a processo para cada tipo de atendimento aos direitos dos titulares LGPD conforme a imagem abaixo:

Os processos aceleradores estão disponíveis no módulo de processos do MD2 Quality Manager. Para mais detalhes sobre o módulo de processos, consulte o tópico 5 deste manual.

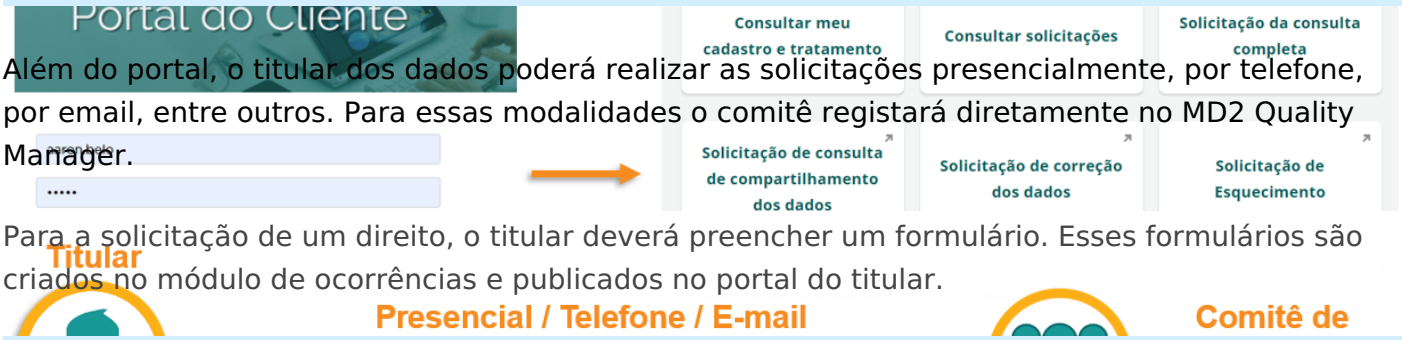


Atendimento aos direitos do titular

Solicitação

O titular poderá realizar sua solicitação diretamente pelo portal do titular, de forma autenticada ou não autenticada. Para isso será necessário que a empresa tenha o portal do titular.

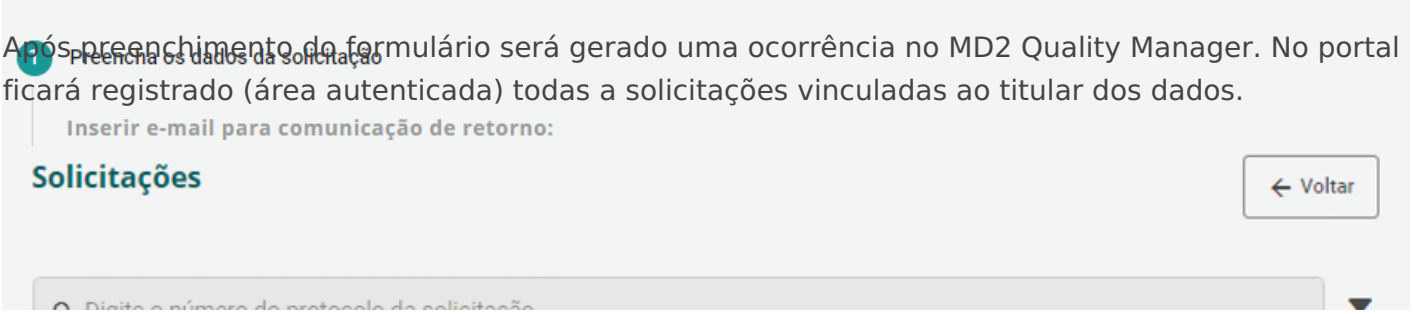
> Para mais detalhes sobre o portal do titular, consulte o tópico 11 deste manual.



Além do portal, o titular dos dados poderá realizar as solicitações presencialmente, por telefone, por email, entre outros. Para essas modalidades o comitê registará diretamente no MD2 Quality Manager.

Para a solicitação de um direito, o titular deverá preencher um formulário. Esses formulários são criados no módulo de ocorrências e publicados no portal do titular.

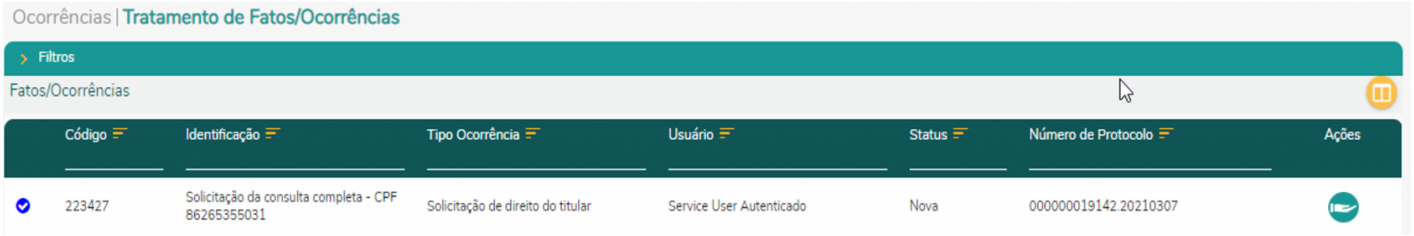
> Para mais detalhes sobre como criar um formulário de ocorrências, consulte o tópico 8.1 deste manual.



Após preenchimento do formulário será gerado uma ocorrência no MD2 Quality Manager. No portal ficará registrado (área autenticada) todas a solicitações vinculadas ao titular dos dados.

Tratativa

Cada ocorrência precisará ser tratada pela equipe de respostas aos direito do titular. O responsável pela tratativa poderá utilizar todos os recursos disponíveis no módulo de ocorrências.

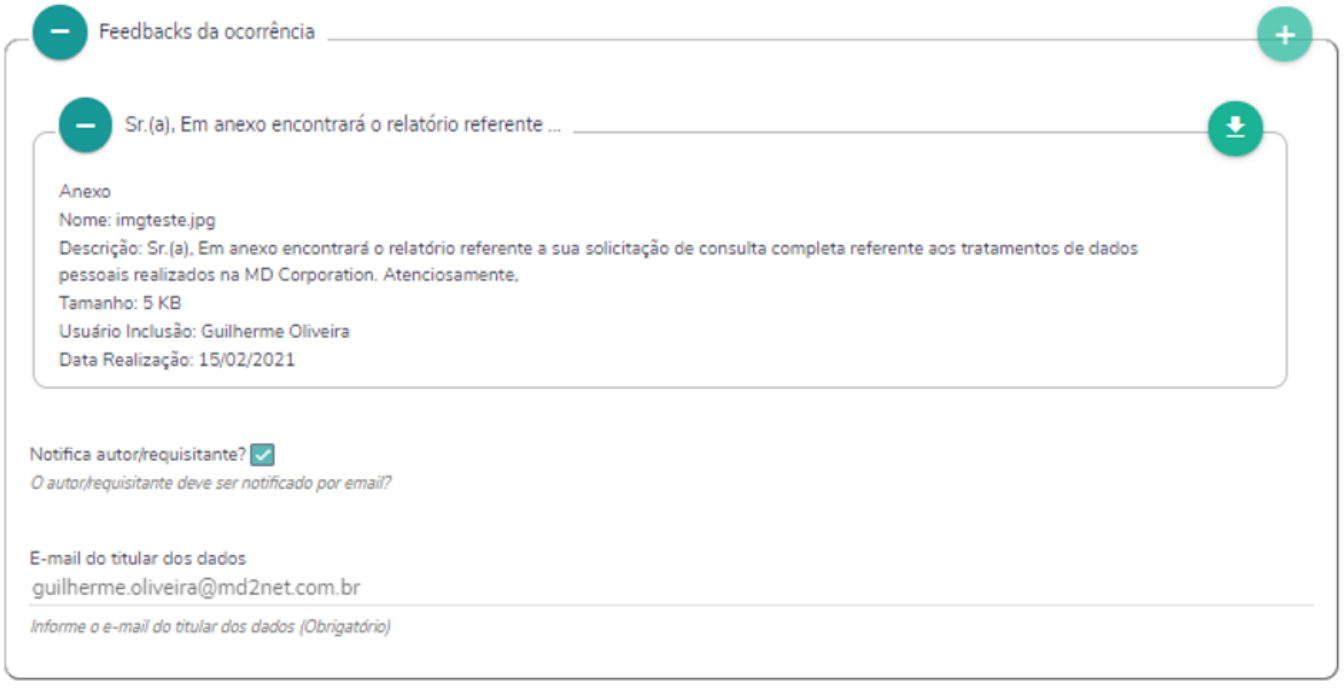


> Para mais detalhes sobre como realizar um tratamento de ocorrência, consulte o tópico 8.4 deste manual.

Realizadas todas as tratativas internas necessárias, através do MD2 Quality Manager será possível enviar um documento de resposta ao titular através do campo feedbacks da ocorrência.

As empresas que possuem o módulo governança MDM, podem utilizar a base unificada para responder as solicitações dos titulares.

> Para mais detalhes sobre o módulo Governança MDM, consulte o tópico 14 deste manual.



> Para os clientes que possuem o MDM é possível gerar relatórios automáticos para alguns direitos do titular. Para mais detalhes consulte o tópico 2.1 deste manual.

O documento de resposta será enviado para o portal do titular (Para os usuários autenticados) ou por email (para os usuários não autenticados).