

nai data privacy

Plataforma de Gestão Estruturada da LGPD

(Funcionalidades)

Índice

Informações gerais 8
Confidencialidade 8
Licença de Uso 8
Objetivo deste manual / mapeamento 9
Abordagem Geral 9
Tópicos a serem abordados 9
Entendimento inicial 9
Sobre o mapeamento 10
Versão do projeto 11
Empresa 12
Sistemas de coleta de dados e Sistemas com propagação de dados 12
Informações não estruturadas 13
Processos 13
Banco de dados 13
Ativos 13
Imagens Biométricas 13
Vulnerabilidades 14
Contratos - Jurídico 14
Riscos 14
Plano de Ação 14
Plano de crise 15
Plano de Treinamento 15
Relatório final 15
Gestão PDCA 15
Formulários Eletrônicos – 17
Dados de introdução dos tópicos mapeados 17
Objetivo 17
Instruções de preenchimento 17
Formulários Eletrônicos – Empresa 18

Objetivo 18
Sumário executivo 18
Instruções de preenchimento 18
Política da Privacidade 19
Responsáveis 19
Instruções de preenchimento: Tabela de Responsáveis 20
Visão Geral 20
Instruções de preenchimento 20
Comunicação 21
Instruções de preenchimento 21
Formulários Eletrônicos – Complementos dos cadastros da Empresa 23
Riscos associados diretamente a empresa 23
Instruções de preenchimento 23
Formulários Eletrônicos – Políticas de segurança 24
Objetivo 24
Políticas de segurança 24
Instruções de preenchimento 24
ITENS DA POLÍTICA DE SEGURANÇA 25
Formulários eletrônicos: Plano de treinamento 26
Objetivo 26
Conteúdo 26
Treinamentos realizados 27
Instruções de preenchimento 27
Análise do DPO para os treinamentos realizados 28
Formulários Eletrônicos – Sistemas de coleta de dados 29
Objetivo 29
Sistemas que fazem coleta de dados 29
Instruções de preenchimento 29
Coleta de dados – Fornecedor de dados comprados 30
Instruções de preenchimento 30

Coleta de dados – Temporalidade 31
Instruções de preenchimento 31
Coleta de dados – Vulnerabilidades 32
Instruções de preenchimento 32
Classificação dos dados coletados 32
Instruções de preenchimento 33
Mapeamento dos riscos 35
Instruções de preenchimento 35
Origem e Finalidade 36
Instruções de preenchimento 36
Sistemas destino – APIs associadas 37
Instruções de preenchimento 37
APIs associadas - Riscos 38
Instruções de preenchimento 38
Formulários Eletrônicos – Sistemas com dados propagados (recebem dados) 39
Sistemas destino – Bases 39
Instruções de preenchimento 39
Sistemas destino – Gerenciamento do acesso 40
Instruções de preenchimento 40
Sistemas destino – Dados do sistema 41
Instruções de preenchimento 41
Riscos 43
Instruções de preenchimento 43
Sistemas destino – APIs associadas 44
Instruções de preenchimento 44
APIs associadas - Riscos 45
Instruções de preenchimento 45
Formulários Eletrônicos – Parceiros Externos 46
Parceiros externos 46
Instruções de preenchimento 46

Informações a compartilhar 47
Informações de preenchimento 48
Riscos 48
Instruções de preenchimento 48
Dados de origem externa 49
Mapeamento básico 49
Instruções de preenchimento 49
Descarte 50
Instruções de preenchimento 50
Riscos 51
Instruções de preenchimento 51
Dados do RH 52
Mapeamento HR 52
Instruções de preenchimento 52
Descartes 53
Instruções de preenchimento 53
Riscos 54
Instruções de preenchimento 54
Dados de terceiros 55
Bases 55
Instruções de preenchimento 55
Descarte 56
Instruções de preenchimento 56
Riscos 56
Instruções de preenchimento 57
Formulários eletrônicos – Processos 58
Objetivo 58
Processos 58
Instruções de preenchimento 58
Etapas do processo 60

Instruções de preenchimento 60
Dados requeridos 61
Instruções de preenchimento 61
Riscos associados ao processo 62
Instruções de preenchimento 62
Formulários eletrônicos – Bancos de dados 63
Objetivo 63
Dados do banco 63
Instruções de preenchimento 63
Instâncias do banco de dados 64
Instruções de preenchimento 64
Acessos internos 64
Instruções de preenchimento 64
Acessos externos 65
Instruções de preenchimento 65
Formulários eletrônicos – Gestão dos ativos 67
Objetivo 67
Ativos 67
Instruções de preenchimento 67
Pessoas com ativos 68
Instruções de preenchimento 68
Instruções de preenchimento 68
Instruções de preenchimento 69
Formulários eletrônicos – Biometria 69
Dados biométricos 69
Instruções de preenchimento 69
Riscos associados 70
Instruções de preenchimento 70
Formulários eletrônicos – Análise dos contratos 71
Contratos 71

Instruções de preenchimento 71
Cláusulas 71
Instruções de preenchimento 71
Instruções de preenchimento 72
Formulários eletrônicos – Vulnerabilidades 73
Instruções de preenchimento 73
Formulários eletrônicos – Plano de Ação 74
Plano de ação – Filtro dos itens cadastrados 74
Instruções de preenchimento 74
Plano de ação – Relação dos itens cadastrados 75
Instruções de preenchimento 75
Plano de Ação – Edição de um item cadastrado 76
Instruções de preenchimento 76

Informações gerais

Confidencialidade

Todas as informações contidas neste documento são de uso estritamente confidencial e não é permitido cópia ou distribuição sem o expresso consentimento da NAI-IT. O infrator estará sujeito às sansões cíveis e criminais.

As informações mapeadas na empresa serão de propriedade da empresa e a equipe de consultoria alocada deverá seguir as normas de confidencialidade firmada, sendo que em nenhum momento, nenhum membro da equipe de consultoria poderá fotografar documentos, escanear documentos ou fazer qualquer tipo de cópia que permita a retirada sem o consentimento formal da empresa.

Licença de Uso

Cada empresa terá sua própria licença de uso. A NAI-IT será a responsável por gerar a licença e mantê-la atualizada.

Mensalmente, através de conexão HTTPS, a NAI-IT fará a revalidação por um novo período, tendo como base para a revalidação a confirmação do pagamento da taxa mensal.

Caso os dados não fiquem disponíveis para acesso, o motivo pode ser a não revalidação ou falha no processo de atualização.

Objetivo deste manual / mapeamento

Este manual tem como objetivo orientar o preenchimento dos formulários eletrônicos afim de conseguir o mapeamento completo das informações da empresa, visando a geração do relatório de análises (RIPD / DPIA) e vulnerabilidades, além de permitir ao DPO o acompanhamento das atividades referentes a segurança da informação.

A utilização de formulários eletrônicos para o registro do mapeamento permite que os dados coletados sejam armazenados em bancos de dados com controle de acesso por usuário / perfil, backup, etc.

Eventuais mudanças em qualquer dos itens permitirá que um novo relatório seja gerado contendo o novo mapeamento.

Abordagem Geral

Tópicos a serem abordados



Entendimento inicial

A LGPD – Lei Geral de Proteção de Dados (Lei 13709/18) tem como base principal a garantia de integridade e acesso aos dados dos indivíduos.

Regulamenta a forma pela qual a empresa poderá captar, armazenar, trabalhar os dados pessoais dos indivíduos e eventualmente compartilhar estes dados captados.

Produz impacto direto na maneira como a empresa poderá utilizar estes dados captados (cadastros em outros sistemas internos, uso pelo CRM, etc.) e como poderá compartilhar estes dados.

Prevê ainda e principalmente, o consentimento formal do indivíduo (com evidência) para uso ou propagação, **independente da forma como o dado foi obtido.**

Prevê, dentre outras coisas, o direito do indivíduo a solicitar a qualquer momento e de uma maneira simples e fácil, seu direito ao esquecimento.

É responsabilidade da empresa gerar evidências quanto ao tratamento que está sendo dados aos dados coletados dos indivíduos, conforme conta no artigo 6º, inciso X "*responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas*".

Conforme consta na LGPD:

Art. 10. Para os fins desta Lei, considera-se: O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I – Apoio e promoção de atividades do controlador; e

II – Proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto a proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo

Sobre o mapeamento

O mapeamento e documentação dos itens previstos neste manual e consequentemente na consultoria proposta visa verificar os riscos e pontos falhos da operação (vulnerabilidades) que precisam ser corrigidos afim de manter o máximo de segurança na proteção dos dados dos titulares dos dados.

Tão importante quanto o mapeamento é a definição do Plano de Ação para o tratamento dos riscos e, mais que isso, a consciência da empresa que precisa estar atenta aos fatos ocorridos e como resolver os problemas de incidentes tendo como base este mapeamento.

As pessoas envolvidas precisam estar atentas a todo momento que a documentação é uma das fases para que a proteção aos dados dos indivíduos esteja garantida, para atender à LGPD ou não.

Este mapeamento e preenchimento dos formulários eletrônicos com a maior acuracidade possível fará com que a empresa contratante tenha possibilidade de demonstrar, quando solicitada, que houve uma preocupação prévia no atendimento da proteção aos dados dos indivíduos e que os procedimentos estão sendo seguidos conforme o previsto.

A equipe do projeto, envolvendo a consultoria contratada e os funcionários da empresa, precisa estar a todo momento interagindo, pois, vários formulários eletrônicos são complementares nos levantamentos das informações e não poderá existir informações diferentes.

Estrutura do mapeamento



Vários podem ser os meios de se realizar ou iniciar a estruturação do mapeamento dos dados. No entanto, se obtivermos o objetivo da LGPD, o “D” significa DADOS. Portanto, a estrutura do mapeamento deve ser iniciada pelo mapeamento dos sistemas que fazem coleta de dados, sejam estes sistemas relativos aos funcionários, clientes, prospects de formulário web, planilhas não estruturadas, o qualquer outro meio.

Ao identificar estes dados coletados e classifica-los será possível definir nos demais formulários eletrônicos a referência estruturada desses dados, ou seja, ao definir um novo tratamento, deverá ser indicado qual o sistema que fez a coleta do dado e qual o dado coletado.

Entendemos que independente do tratamento que estiver sendo mapeado, ou qualquer outro meio que faça uso desse dado coletado, que sua classificação será a mesma, ou seja, se no sistema de coleta de dados for classificado como um dado pessoal sensível, não importa onde ele seja utilizado será sempre um dado pessoal sensível.

Como sugestão no mapeamento estruturado dos dados indicamos definir quais são os sistemas internos que receberão os dados coletados, os tratamentos e processos que também farão uso desses dados.

Pensando no sucesso do mapeamento estruturado indicamos que todos os formulários eletrônicos referentes aos mapeamentos sejam completamente preenchidos e validados.

Versão do projeto

Afim de garantir um modelo de entrada de dados eficiente foi projetado que o mapeamento tenha um controle simples da versão. Desta forma, quando o relatório for impresso será possível identificar qual a versão vigente, ressaltando que as tabelas que tiverem seus dados inseridos não terão versionamento. O controle de versão terá com finalidade a impressão do relatório. Será permitido inserir as informações sobre o que mudou no modelo mapeado que necessitou a geração de uma nova versão. As informações inseridas neste campo (o que mudou) serão apresentadas no topo do relatório final.

Empresa

A Empresa está ligada a um controle de versão do projeto e todas as demais informações que forem inseridas nos formulários eletrônicos, terão relação com a empresa, ou seja, se houver mais de uma empresa para ser mapeada, os relatórios, quando gerados, terão informações específicas de cada uma das empresas.
Os dados a serem informados sobre a empresa fazem referência às responsabilidades, ao comitê de segurança, às políticas (missão, visão, valores), aos entendimentos da alta direção para o 5W2H e ao Plano de Crise em caso de vazamentos ou eventos que não foram previstos.
Como a EMPRESA é base para todos os demais formulários eletrônicos, o primeiro item a ser cadastrado deve ser as informações da empresa, mesmo que num primeiro momento conste apenas a razão social para que os demais formulários possam fazer a referência.

Sistemas de coleta de dados e Sistemas com propagação de dados

Nos formulários eletrônicos referentes aos sistemas utilizados pela empresa serão registradas as informações de cada um dos sistemas que possam ter ou receber (de qualquer fonte de dados) dados de pessoas físicas (funcionários, terceiros, clientes, etc.).
Atrelado aos levantamentos dos sistemas haverá um mapeamento de dois itens importantes:

- Compartilhamento dos dados coletados com os demais sistemas internos.
- Compartilhamento dos dados coletados com parceiros externos que por força do negócio necessitem receber estes dados.

Ainda no quesito de mapeamento de segurança haverá um preenchimento das APIs (programas que permitem acesso aos dados através de requisições de outros sistemas). Este mapeamento

permitirá identificar quais acessos estão sendo realizados, quais dados estão sendo disponibilizados e para quem (qual empresa ou sistema) está sendo liberado.
Atenção especial também está sendo dada às informações que são coletadas junto aos titulares dos dados, com mapeamento, campo a campo, do tipo de dado e tratamento que deve ser dado para garantir a segurança (criptografia, por exemplo), com as classificações de dado sensível, dado de criança / adolescente, etc.

Informações não estruturadas

Formulários eletrônicos específicos para o mapeamento de informações não estruturadas foram criados para permitir catalogar este tipo de coleta de dados.
Por informações não estruturadas entende-se como planilhas eletrônicas, arquivos texto, documento impressos, currículos, etc.

Processos

Nos formulários eletrônicos referentes aos processos mapeados na empresa, serão registradas as informações sobre cada processo, suas respectivas atividades e responsáveis, afim de verificar e deixar registrado cada momento que um dado de uma pessoa física for manipulado. Uma atenção especial no preenchimento dos formulários dos processos diz respeito a obtenção de dados ou documentos para uma determinada finalidade.

Banco de dados

Nos formulários eletrônicos referentes aos bancos de dados em uso pelos sistemas da empresa, serão registradas as informações sobre cada sistema que armazena seus dados nestes bancos, quem é que pode ter acesso direto às tabelas (tanto interno quanto externo), além de verificar se pessoas terceiras (prestadores de serviços) podem acessar via VPN ou outro meio.

Ativos

Nos formulários eletrônicos referentes ao registro dos ativos serão verificados todos os equipamentos que são de propriedade da empresa ou de um determinado indivíduo (funcionário ou terceiro) que possam, de alguma maneira realizar algum tipo de acesso aos sistemas, processos, bancos de dados, etc. da empresa, tanto interno quanto externo.

Imagens Biométricas

Nos formulários eletrônicos referentes ao registro das imagens biométricas serão verificados quais imagens são capturadas, qual o motivo, onde ficarão armazenadas e quem pode ter acesso a estas imagens.

Vulnerabilidades

Nas vulnerabilidades serão informados todos os pontos verificados, através da aplicação de software específico para esta finalidade, que podem gerar pontos de atenção critica quanto ao risco.

O objetivo é que o software de vulnerabilidades fique vigente durante todo o processo de mapeamento e continue após o término das atividades. Robôs inteligentes poderão atuar e alertar os responsáveis em caso de risco verificado.

Contratos - Jurídico

Os mapeamentos para cada um dos itens listados nos formulários eletrônicos farão sempre referência a atenção jurídica que deve ser dada ao item.

Estes mapeamentos gerarão as informações e bases para que o corpo jurídico que estiver acompanhando o mapeamento possa entender as demandas e sugerir e/ou aplicar as mudanças necessárias nos contratos existentes.

O corpo jurídico também analisará os itens considerados e mapeados como de atenção sigilosa (ativos, por exemplo) e definirão os procedimentos e contratos para garantia de comprometimento do indivíduo (funcionário ou terceiro) no cuidado com o equipamento (notebook, celular, tablet, etc.) e no acesso aos sistemas ou planilhas eletrônicas que estes equipamentos permitirão.

Riscos

Todos os formulários eletrônicos, para os itens listados acima, terão relacionamento com o formulário de classificação dos riscos associados.

O preenchimento destas informações permitirá que seja possível avaliar os riscos para cada um dos itens levantados e poder mapear o plano de ação para tratar destes riscos ou pelo menos mitigar os riscos.

Plano de Ação

O Plano de Ação será automaticamente gerado durante o preenchimento dos formulários eletrônicos, para cada um dos riscos que forem cadastrados. Desta forma, o consultor, estando com o mapeamento “quente” já consegue identificar e qualificar quais os riscos que podem acontecer.

Eventualmente poderão ser cadastrados planos de ação específicos, sem estarem obrigatoriamente atrelados a um mapeamento específico.

O DPO ou membros da equipe de consultoria externa ou interna deverão acessar o formulário do plano de ação para completar as informações e poder dar prosseguimento nas análises. Pode ser um dos acessos do DPO para gestão dos dados.

Nesta avaliação o analista do plano de ação poderá optar pela abertura de uma ocorrência para tratamento por gestão de incidentes, baseado no modelo PDCA. Assim, estas ocorrências terão análises e tratamentos mais detalhados quanto a análise da causa raiz, plano de implementação, verificação de eficácia, etc.

Plano de crise

O preenchimento do formulário eletrônico para o plano de crise permite traçar quais ações deverão ser emergencialmente tomadas para casos de vazamento ou acessos indevidos.
Complementar ao Plano de Crise pode ser criado o Plano de contingência para cada crise verificada, ou seja, o modelo permite que sejam criados planos de ações emergenciais para cada situação.

Plano de Treinamento

O preenchimento do formulário eletrônico para o Plano de treinamento tem como finalidade prever os treinamentos e workshops que precisarão ser realizados com as equipes afim de conscientizar os funcionários sobre as responsabilidades e riscos que passarão a existir a partir da entrada em vigência da LGPD e como estes funcionários deverão tratar as informações coletadas e como manusear os documentos eventualmente obtidos com os indivíduos.

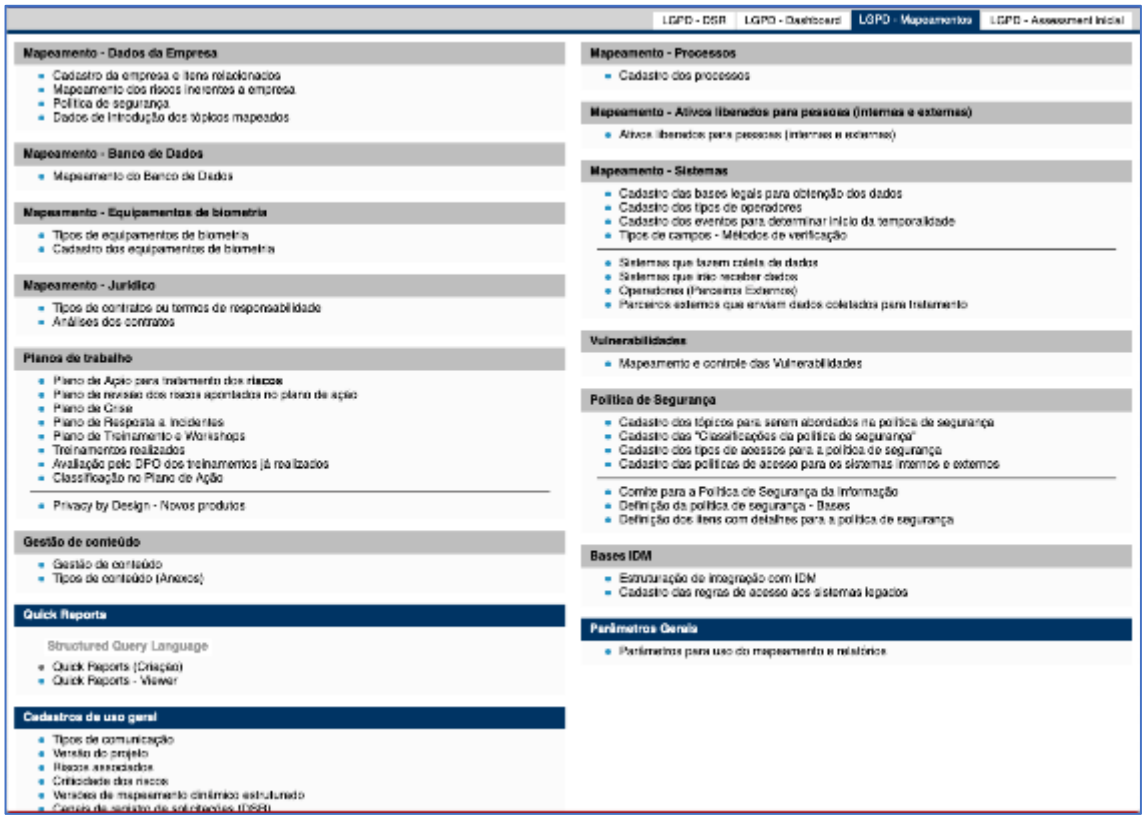
Relatório final

O relatório final permitirá a impressão padronizada dos mapeamentos realizados, afim de disponibilizar quando solicitado por auditorias internas e externas ou pela agência reguladora todo o cuidado e detalhes verificados pela empresa.

Gestão PDCA

A gestão PDCA é um software que pode acompanhar o projeto (mediante contratação adicional) que atende os quesitos relacionados ao PDCA, com abertura de um incidente, avaliação, responsáveis, elaboração do plano de ação e verificação de eficácia. Tudo isso numa estrutura de workflow com responsáveis, formulários eletrônicos e prazos controlados para respostas.

Formulários Eletrônicos – Menu de acessos



A imagem acima demonstra a lista das opções de acesso para o mapeamento estruturado da LGPD.

Cada um dos itens (link) representa um acesso ao formulário eletrônico que permitirá que os dados sejam inseridos.

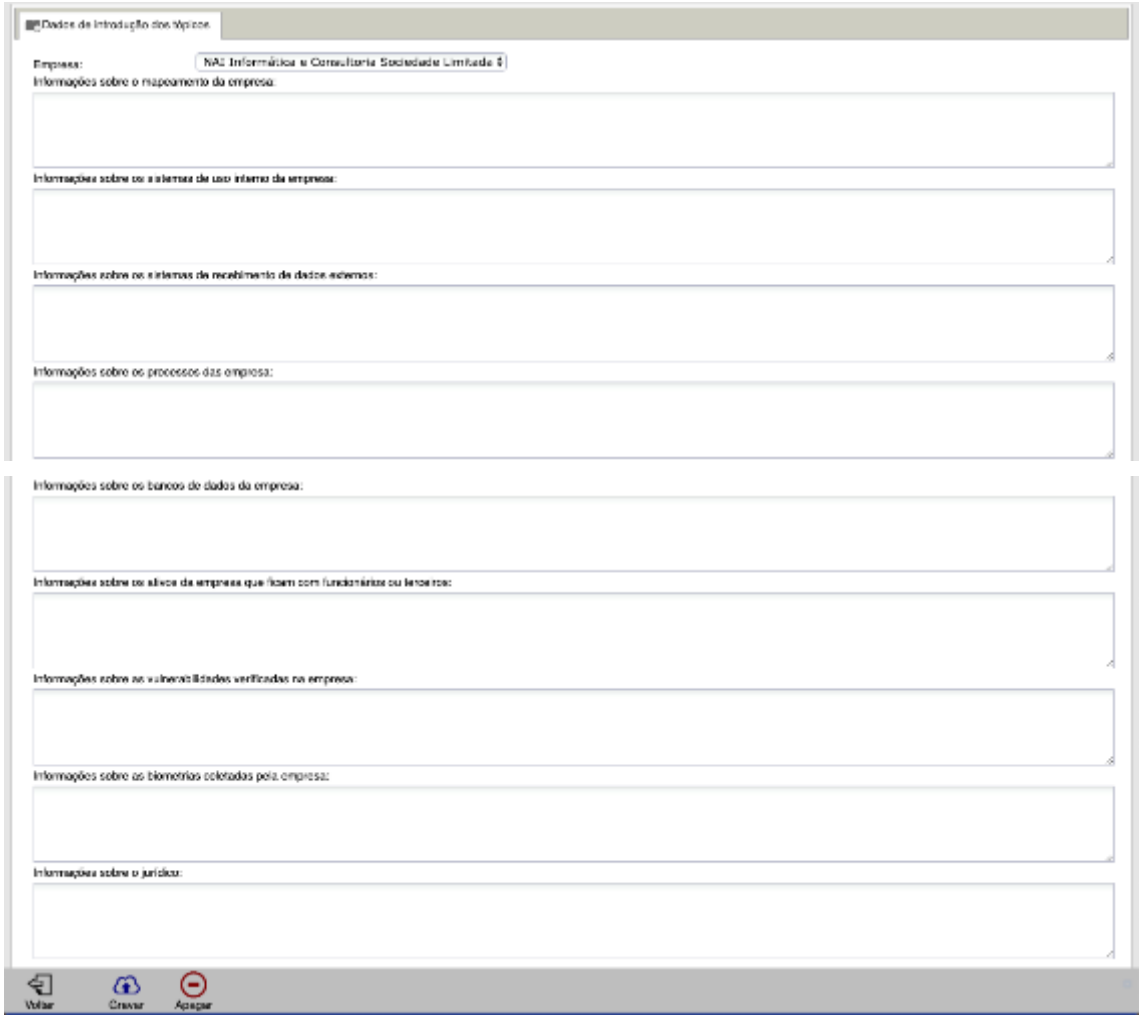
Nesta imagem todos os links estão visíveis e disponíveis, no entanto, de acordo com o perfil de acesso alguns destes links não estarão disponíveis.

Caso alguma informação necessite ser acrescentada em algum link que não aparecer para acesso, o superior deverá ser acionado para atendimento do requisito.

Dados de introdução dos tópicos mapeados

Objetivo

Neste formulário eletrônico devem ser inseridos, para cada um dos itens solicitados, a introdução que será utilizada no documento impresso. Estas informações inseridas não terão impacto na LGPD, mas servirão para orientar quem estiver lendo os documentos sobre o que e como será abordado cada tema.



Instruções de preenchimento

- Para cada um dos itens solicitados deve ser inserido uma introdução contendo o descritivo para ser colocado no documento impresso que retrate o objetivo e demais referências para o tópico abordado.

Empresa

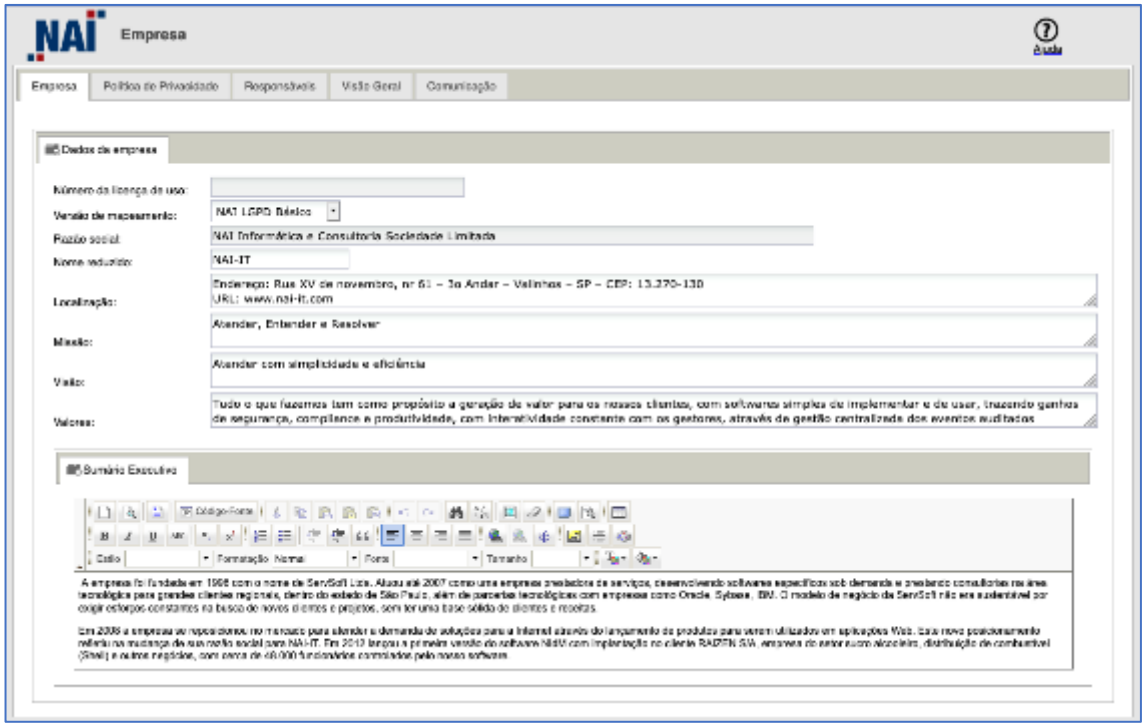
Objetivo

Nos formulários eletrônicos relacionados a empresa, também citada na LGPD como controlador, serão mapeadas as informações que identificarão a empresa.

Esta qualificação prevê principalmente identificar a empresa, seus princípios e valores e quem são os responsáveis por cada um dos principais pontos de atenção no atendimento da LGPD.

Todos os levantamentos das informações a serem inseridas nos formulários eletrônicos serão realizadas em conjunto com a equipe de consultoria e a equipe designada pela empresa para tal finalidade.

Sumário executivo



Instruções de preenchimento

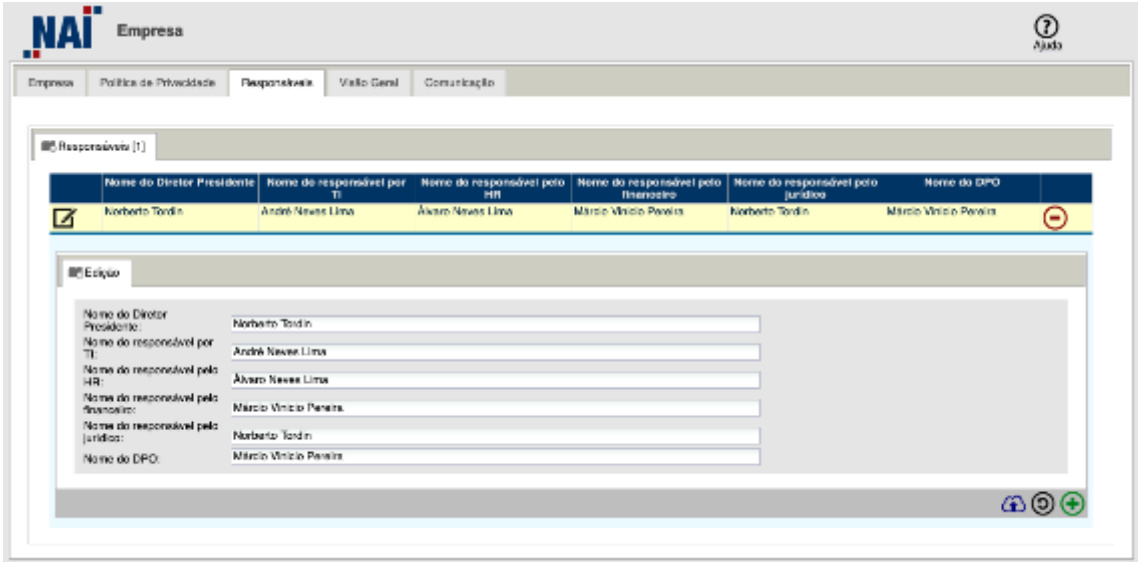
- Número da licença de uso: Esta informação virá previamente preenchida e este campo não será editável.
- Versão de mapeamento: Esta informação virá previamente preenchida e este campo não será editável.
- Razão social: Esta informação virá previamente preenchida e este campo não será editável.
- Localização: Neste campo deverá ser preenchido o endereço completo da empresa.

- Missão: Neste campo deverá ser informado a missão da empresa.
- Visão: Neste campo deverá ser informado a visão da empresa.
- Valores: Neste campo deverá ser informado os valores da empresa.
- Sumário executivo: Neste campo deverá ser preenchido com o sumário executivo da empresa.
    - Por sumário executivo entende-se como um histórico completo da empresa, de uma maneira que permita descrever para uma pessoa que não conhece a empresa, o que ela faz e quais seus principais objetivos. Deve ser um descritivo bem detalhado e objetivo.

Política da Privacidade



Responsáveis

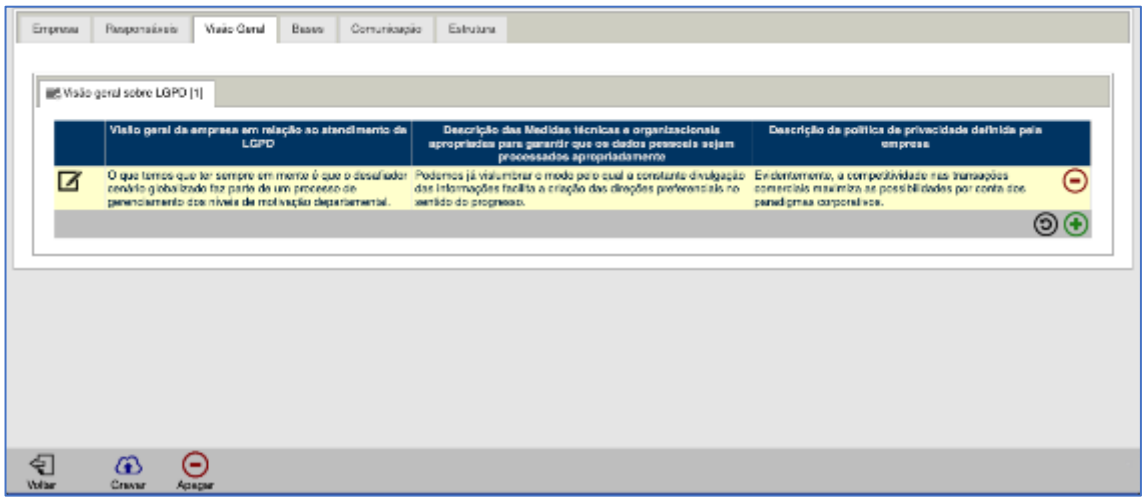


Instruções de preenchimento: Tabela de Responsáveis

Nesta tabela devem ser inseridos os nomes das pessoas que podem ser classificadas como responsáveis por determinados departamentos da empresa. Foram previstos alguns departamentos para definição de responsabilidade com base no que entendemos como necessidade de identificação em caso de vazamento de dados, solicitações não atendidas ou outras demandas que não foram previstas e a equipe não sabe como resolver.

- Nome do diretor presidente: Neste campo deve ser informado o nome do Diretor Presidente da empresa.
- Nome do responsável por TI: Neste campo deve ser informado o nome do responsável por Tecnologia da Informação da empresa.
- Nome do responsável por HR: Neste campo deve ser informado o nome do responsável pelo departamento de Recursos Humanos da empresa.
- Nome do responsável pelo financeiro: Neste campo deve ser informado o nome do responsável pelo departamento Financeiro da empresa.
- Nome do responsável pelo jurídico: Neste campo deve ser informado o nome do responsável pelo departamento Jurídico da empresa
- Nome do DPO: Neste campo deve ser informado o nome do DPO (Data Protection Officer) da empresa. Caso seja terceirizado deverá ser informado o nome da empresa terceira responsável.

Visão Geral



Instruções de preenchimento

Esta tabela definirá qual a visão geral da empresa para o atendimento da LGPD.

Deverá conter um texto detalhando como a alta administração entende o negócio e como pretende dar atenção ao tratamento de privacidade dos dados.

As informações a serem inseridas nos campos abaixo citados devem ser levantadas preferencialmente com os responsáveis pela Segurança da Informação. Verificar se existem procedimento operacionais (POP) documentados para os itens abaixo citados. Caso existam, estes procedimentos operacionais devem ser informados no texto.

- Visão geral da empresa em relação ao atendimento da LGPD: Neste campo deve ser informado como a empresa enxerga a LGPD e qual a atenção que será dada para o atendimento da regulamentação.
- Descrição das medidas técnicas e organizacionais apropriadas para garantir que os dados pessoais sejam processados apropriadamente: Neste campo deve ser informado quais são as medidas técnicas adotadas pela empresa que possa garantir que o tratamento dos dados dos indivíduos será processado apropriadamente, ou seja, quais os comprometimentos oficiais da empresa para garantir segurança aos dados coletados dos indivíduos.
- Descrição da política de privacidade definida pela empresa: Neste campo deve ser informado qual a política de privacidade que a empresa definiu para ser seguida visando o atendimento completo da LGPD. Não se trata de descrever a política, mas sim em como a empresa, no papel dos executivos, entendem que a política de privacidade deve ser atendida.

Comunicação



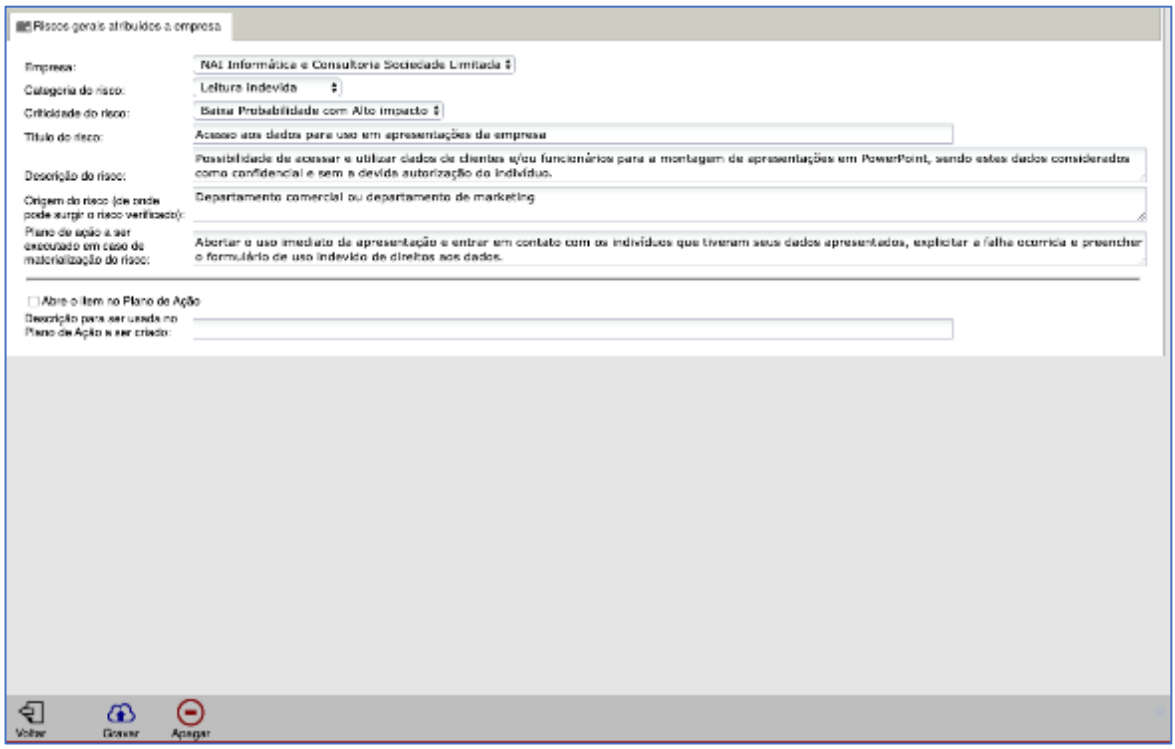
Instruções de preenchimento

Nesta tabela devem ser informados os meios de comunicação com os clientes, como são utilizados, quem é o responsável pela atividade e como deve ser liberado o acesso às informações. Eventualmente ações de marketing, por exemplo, precisam ser disparadas com base nos cadastros internos da empresa e, neste caso, quais os cuidados que devem ser tomados para que, para cada ação mapeada, o indivíduo não se sinta violado.

- Tipo de comunicação: Neste campo deverá ser selecionado um pré cadastro com os tipos de comunicação que a empresa utiliza. Os tipos de comunicação deverão ser previamente cadastrados e se houve necessidade de novos tipos de comunicação, o cadastro deverá ser acessado no Portal LGPD – Mapeamentos, no item: “Cadastros Básicos / Tipos de Comunicação.
- Nome da pessoa responsável: Neste campo deve ser informado o nome da pessoa responsável pelo tipo de comunicação e que responderá pelo item.
- Meio de comunicação: Neste campo deve ser informado qual o meio de comunicação que será utilizado.
- Motivo pelo qual a comunicação com o cliente precisa e será realizada: Neste campo devem ser descritos os motivos pelo qual a comunicação com o cliente precisará ser realizada. Verificar se existem registros do indivíduo autorizado, ou não autorizando, o envio de comunicação. Verificar também caso alguma comunicação com o indivíduo seja para atender alguma regra oficial ou comunicados de inadimplência, por exemplo.
- Maneira pela qual os dados são obtidos para que a comunicação com o cliente seja executada: Neste campo devem ser descritos as maneiras como os dados dos indivíduos foram obtidos. Podem ser dados de cadastro da empresa, ou dados adquiridos de terceiros, etc. Deve-se dar atenção e descrever muito detalhadamente estas informações para que, caso alguma violação de privacidade seja verificada, possa ser possível identificar as origens destes dados.
- Impacto para o consumidor caso o consentimento não seja validado: Neste campo deve-se informar qual será o impacto que o titular dos dados terá caso não tenha havido o consentimento prévio para recebimento deste tipo de comunicação.
    - IMPORTANTE: As informações inseridas neste campo serão utilizadas no processo de transparência e consentimento dos titulares dos dados, para que no envio do formulário de consentimento, o titular possa saber o que acontecerá ser ele não consentir com o recebimento deste tipo de comunicação.
- Requer consentimento do titular: Este campo deve ser selecionado (marcado) se o meio de comunicação com os titulares dos dados necessitar realizar o consentimento prévio.
- Segue regras de OPT-IN: De acordo com o WIKIPEDIA: “*O termo OPT-IN refere-se à expressão da vontade de um usuário de internet ou mobile, afastando-se sua presunção de aceite pelo silêncio. Em detalhe, OPT-IN corresponde ao conjunto de regras segundo as quais as mensagens de marketing ou de caráter comercial só são enviadas para aqueles que expressem, prévia e explicitamente, o seu consentimento. Desta forma uma mesma mensagem é enviada para todos os indivíduos que concordaram ou que manifestaram interesse em receberem informações sobre um produto ou serviço de uma empresa ou organização*”. Portanto, o campo deverá ser selecionado caso seja atendido o requisito de OPT-IN.

Complementos dos cadastros da Empresa

Riscos associados diretamente a empresa



Instruções de preenchimento

- Empresa: Selecionar qual a empresa que terá as informações relacionadas.
- Categoria do risco: Selecionar dentre as opções qual a categoria do risco que está sendo feito o cadastro.
- Criticidade do risco: Selecionar dentre as opções qual a criticidade do risco que está sendo feito o cadastro.
- Título do risco: informar qual o título do risco que está sendo cadastrado.
- Descrição do risco: Informar qual a descrição, com mais detalhes, para o risco que está sendo cadastrado.
- Origem do risco: Informar qual a origem que pode ocasionar a materialização do risco.
- Plano de ação a ser executado...: Descrever qual o Plano de Ação a ser executado em caso de materialização do risco.
- Abrir Item no Plano de Ação: Caso seja necessário um tratamento mais específico para o risco verificado e, desta forma, ter que haver a abertura de um item no Plano de Ação, marcar este item.
- Descrição para ser usada no Plano de Ação a ser criado: Informar qual a descrição do item que deverá ser criado no Plano de Ação.

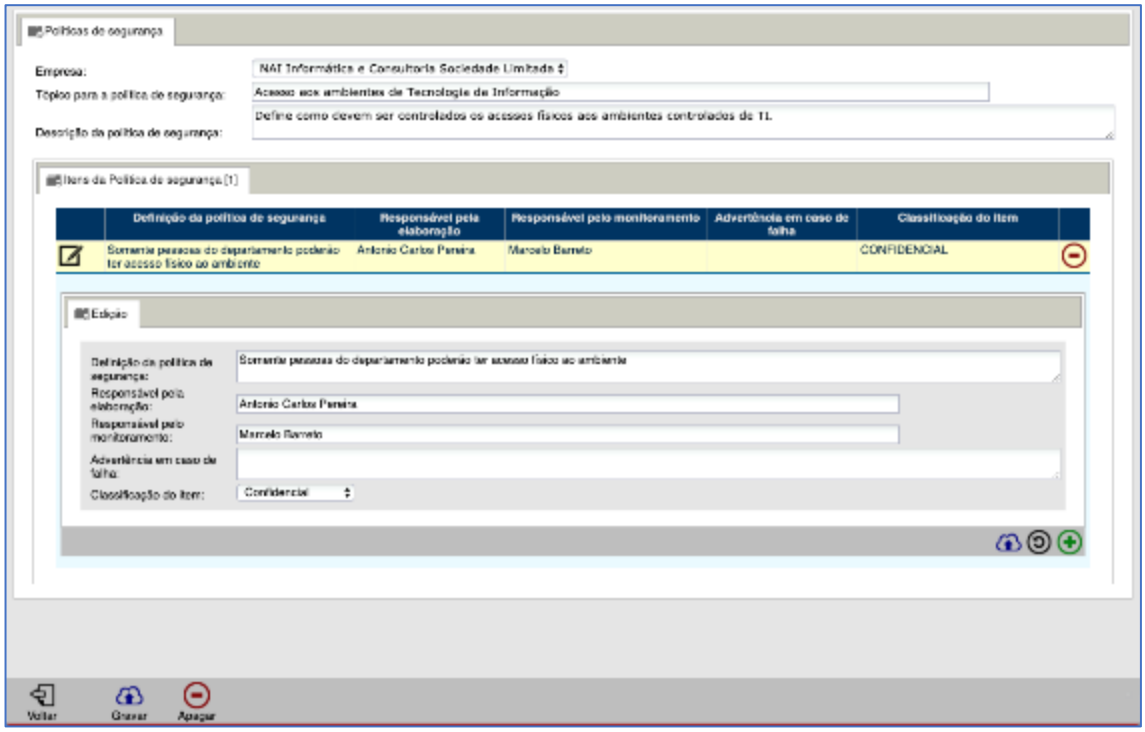
Políticas de segurança

Objetivo

Nesta tabela devem ser definidas e muito bem descritas as políticas de segurança para os diversos ambientes da empresa.

A política de segurança faz parte do mapeamento da LGPD nas definições da empresa (alta direção) sobre como os acessos aos sistemas devem ser previstos. Uma das grandes falhas no processo de acesso aos sistemas está relacionado ao fato de desligamentos de funcionários ou terceiros não terem os logins e senhas removidos dos sistemas, tanto internos quanto acessos externos, o que torna o ambiente vulnerável a acessos indevidos com possibilidade de obtenção indevida dos dados dos indivíduos e até mesmo de instalação de *malwares* no ambiente.

Políticas de segurança



Instruções de preenchimento

- Empresa: Selecionar qual a empresa que terá as informações relacionadas.
- Tópico para a política de segurança: Neste campo deve ser inserido qual o tópico que será abordado na política de segurança.
- Descrição da política de segurança: Neste campo deve ser inserido qual a política que a empresa adota para a gestão dos acessos. Normalmente esta informação está com a equipe de segurança da informação ou com a equipe de TI.

- Caso a empresa não tenha uma política definida, dois caminhos podem ser seguidos:
  - Abrir um item no plano de ação para a definição da política de segurança. Neste caso neste campo deve ser inserido que a empresa não possui política e foi aberto uma atividade no plano de ação para a criação.
  - Se não houver interesse por parte da empresa na definição da política de segurança, informar que não foi verificado o interesse e listar as pessoas que manifestaram esta opinião, de preferência obtendo o aval de alguém da alta direção.

ITENS DA POLÍTICA DE SEGURANÇA

- Definição da política de segurança: Neste item deve ser informado qual o sub título da política de segurança.
- Responsável pela elaboração: Informar quem é o usuário responsável pela elaboração desta política.
- Responsável pelo monitoramento: Informar que é o usuário responsável pelo monitoramento desta política.
- Advertência em caso de falha: Descrever qual a advertência ou alerta que deverá ser acionado em caso de falha nesta política.
- Classificação do item: Selecionar dentre as opções qual a classificação deste item da política de segurança.

Plano de treinamento

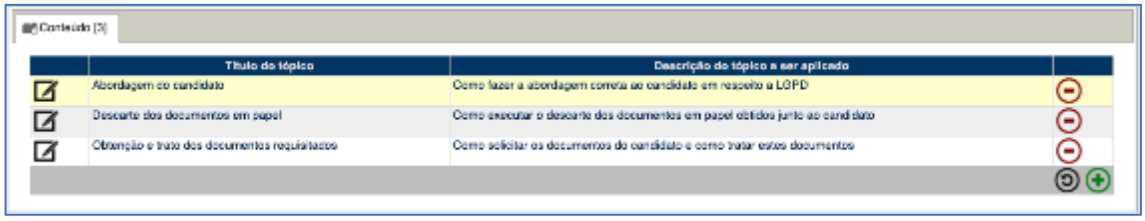


Objetivo

Neste formulário devem ser inseridos os planos de treinamentos e workshops que deverão ser realizados pela empresa para preparação dos funcionários e terceiros no atendimento das definições da LGPD.

- Empresa: Selecionar para qual empresa será mapeado o treinamento.
- Departamento: Indicar para qual departamento que será mapeado o treinamento
- Tópico a ser abordado: Indicar qual o tópico do treinamento a ser abordado.
- Nome do responsável por realizar o treinamento: Indicar o nome do responsável por realizar o treinamento.
- Data limite para treinamento: Indicar qual a data limite para a realização do treinamento.
- Carga horária: Informar qual a carga horária prevista para o treinamento ou workshop.

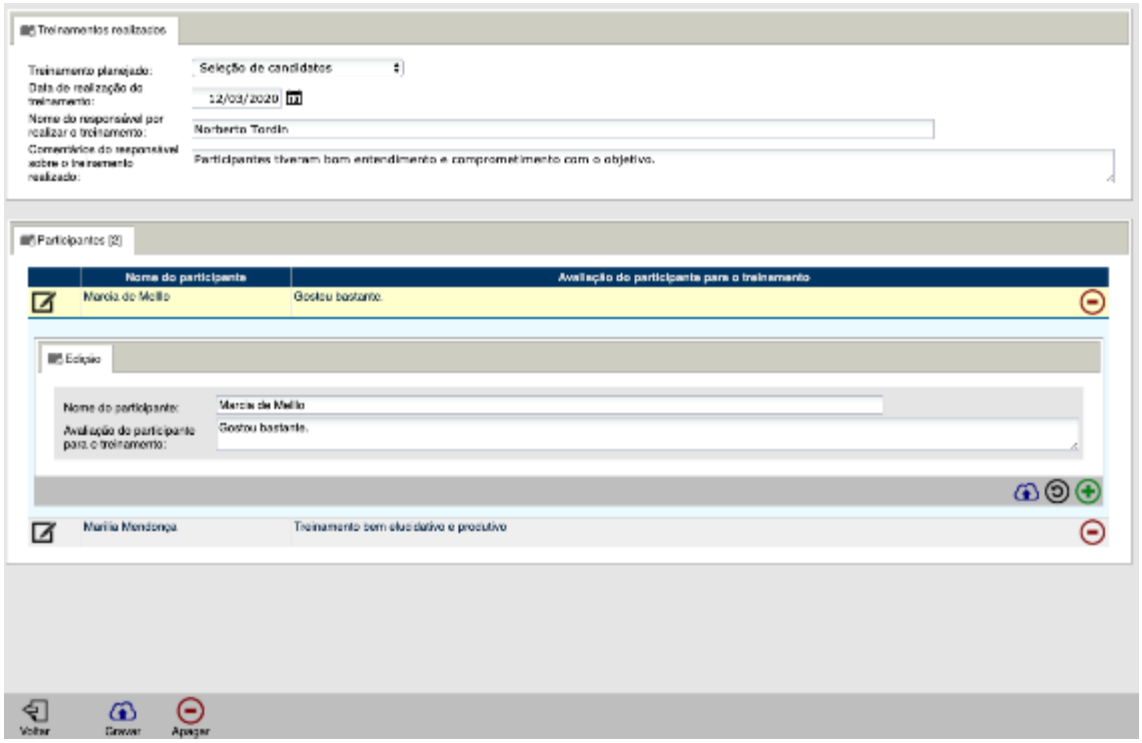
Conteúdo



- Título do tópico: Informar qual o título do tópico do treinamento.

- Descrição do tópico: Descrever qual o conteúdo do tópico do treinamento.

Treinamentos realizados



Instruções de preenchimento

O preenchimento do formulário dos treinamentos realizados deverá ser realizado quando o treinamento previsto tiver sido finalizado e o nível de satisfação dos participantes informado.

Não se trata de um preenchimento obrigatório, mas um complemento das evidências que o treinamento foi realizado.

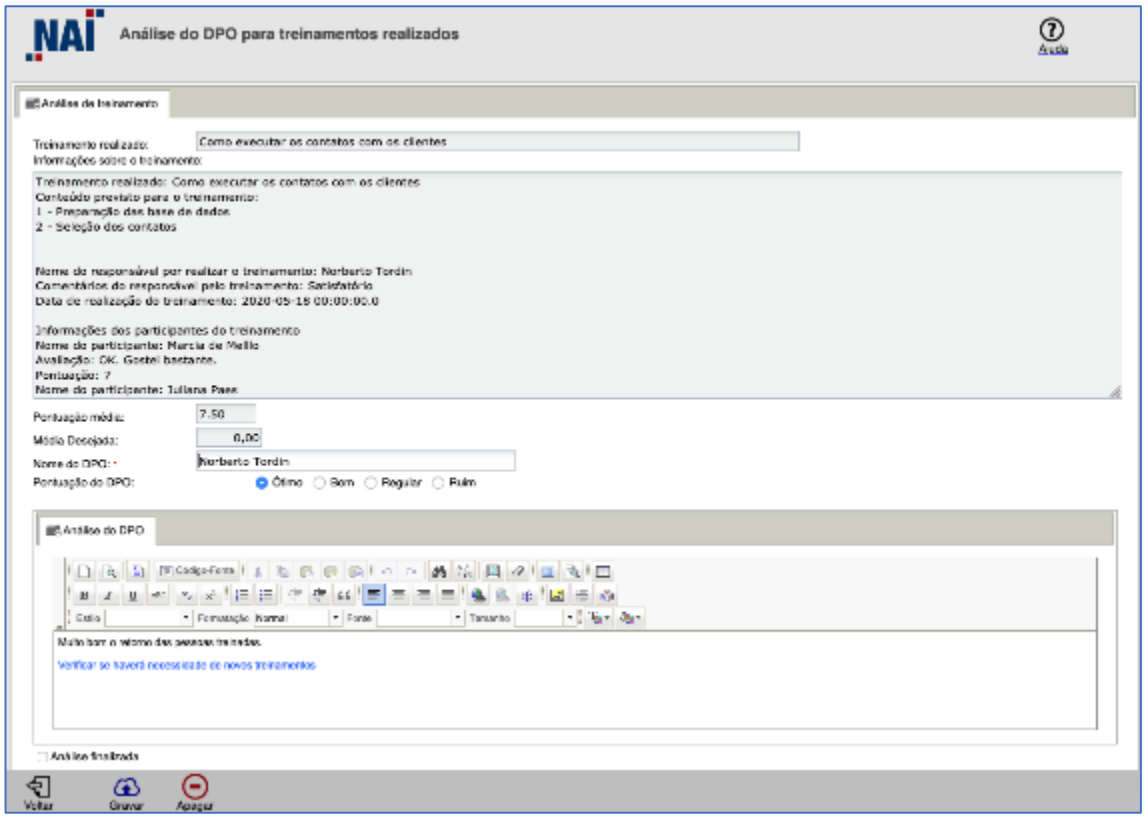
- Treinamento realizado: Selecionar da lista de opções qual o treinamento que foi planejado e neste momento realizado.
- Data de realização do treinamento: Informar a data de realização do treinamento
- Nome do responsável por realizar o treinamento: Informar o nome do responsável que realizou o treinamento.
- Comentários do responsável sobre o treinamento realizado: Informar os comentários do responsável que realizou o treinamento sobre o que ocorreu, se existem sugestões de melhorias, etc.

Participantes:

Inserir nesta tabela o nome dos participantes e qual a avaliação do treinamento realizado.

As informações sobre a participação serão incluídas na ficha do indivíduo do sistema.

Análise do DPO para os treinamentos realizados



Este formulário tem como objetivo permitir ao Encarregado dos Dados (DPO) uma análise para os treinamentos que foram realizados e o feedback do responsável por executar o treinamento e o feedback de cada um dos participantes.

Formulários Eletrônicos – Sistemas de coleta de dados

Objetivo

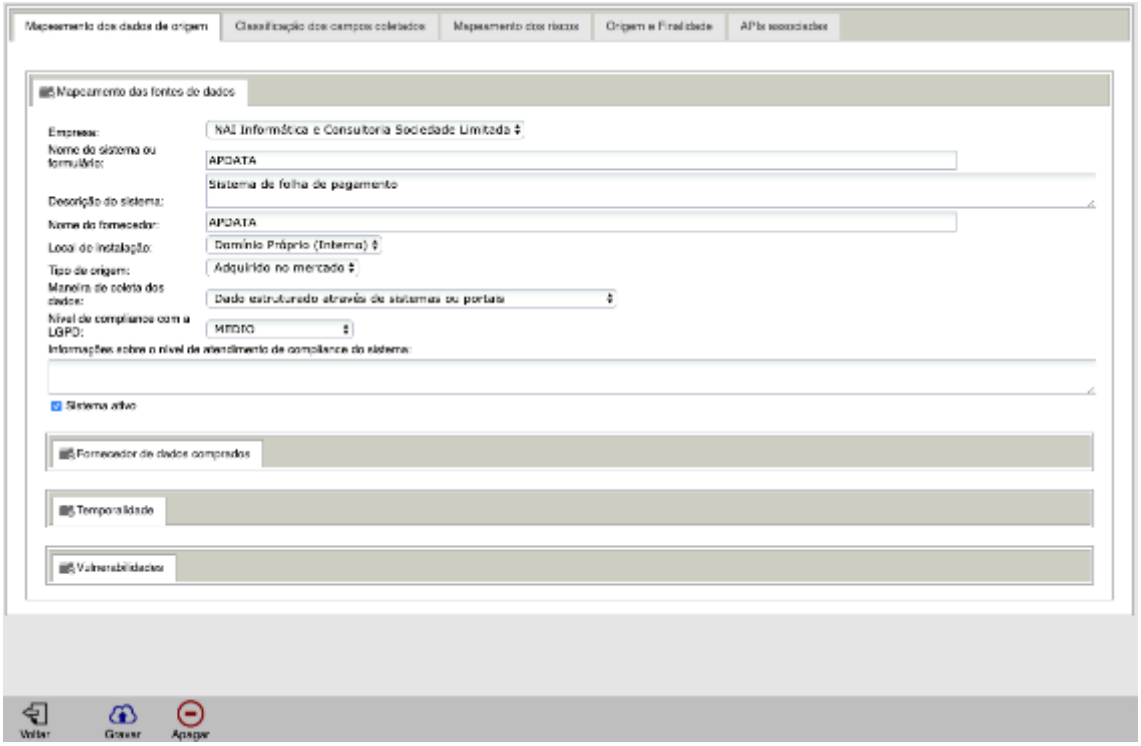
Nos formulários eletrônicos referentes aos sistemas, devem ser mapeados todos os sistemas da empresa que, de alguma maneira, coletem ou recebam dados de indivíduos, sejam funcionários, clientes ou terceiros.

Para cada sistema identificado deverá ser catalogado todos os campos (informações) que façam referência a informações do indivíduo, classificando cada um destes campos de acordo com o tipo de tratamento que deverá ser feito.

Este mapeamento dos campos das tabelas exige a presença de pessoas da empresa que tenham conhecimento e possibilidade de acessar os sistemas e respectivas tabelas nos bancos de dados para passar as informações.

Este mapeamento é um dos principais levantamentos que precisará ser realizado pois será a partir deste trabalho que a identificação dos campos sensíveis tratará.

Sistemas que fazem coleta de dados

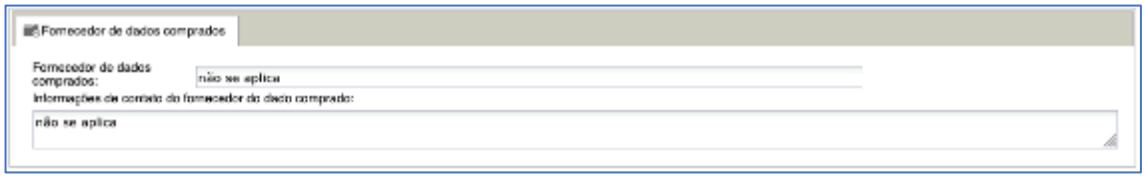


Instruções de preenchimento

- Nome da empresa: Deverá ser selecionada a empresa na lista de opções.

- Nome do sistema: Nome do sistema que será mapeado e que tem, de alguma maneira, dados dos indivíduos.
- Descrição do sistema: Deve ser informado uma descrição do que é o sistema, qual a funcionalidade, e tudo o que mais puder ser fornecido de informações.
- Nome do fornecedor: Nome do fornecedor do sistema.
- Local de instalação: Deverá ser selecionado da lista de opções onde o sistema está instalado.
- Tipo de origem do sistema: Deverá ser selecionado da lista de opções qual o tipo de origem do sistema.
- Maneira de coleta dos dados: Deverá ser selecionado da lista de opções qual a maneira de coleta dos dados.
- Nível de compliance com a LGPD: Selecionar dentre as opções como o sistema se enquadra no conceito de compliance com a LGPD.
- Informações sobre o nível de atendimento de compliance do sistema: Descrever com mais detalhes sobre o nível de compliance do sistema em relação a LGPD.
- Sistema ativo: Esta opção virá sempre selecionada. Caso o sistema seja descontinuado deverá ser desmarcada esta opção.

Coleta de dados – Fornecedor de dados comprados



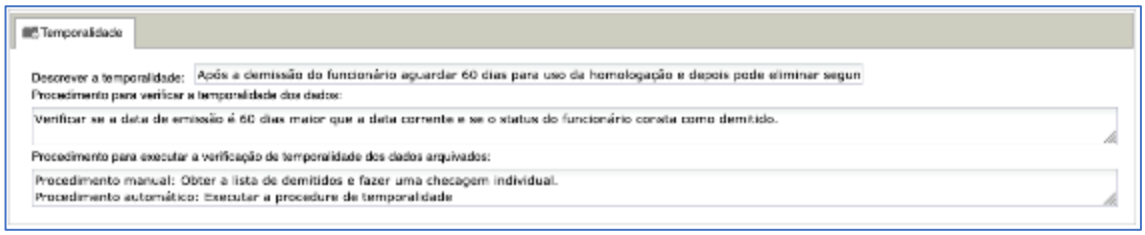
Instruções de preenchimento

Este preenchimento deverá ser realizado caso o sistema acima informado tenha como procedência a compra de dados, ao invés de coleta direta pela empresa.

Por dados comprados entende-se como bancos de dados comprados de terceiros para alguma ação de marketing ou identificação de potenciais clientes.

- Fornecedor de dados comprados: Deverá ser informado a razão social do fornecedor dos dados comprados.
- Informações do contato do fornecedor do dado comprado: Deverá ser informado todas as informações possíveis do contato no fornecedor. Isso é importante de ser muito bem mapeado e preenchido pois será o ponto de contato caso algum problema seja verificado com uso indevido.

Coleta de dados – Temporalidade



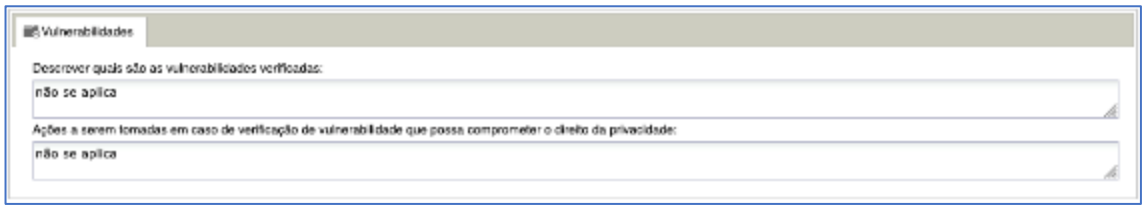
Instruções de preenchimento

A temporalidade deve ser informada para que os gestores tenham condições de identificar os procedimentos operacionais para eliminação dos dados (conforme regras e critérios mapeados) afim de garantir que acessos indevidos obtenham dados de indivíduos que não fazem mais parte da relação da empresa.

Por TEMPORALIDADE entende-se como o tempo que um dado deve ficar armazenado nos sistemas da empresa principalmente para atendimento de requisitos legais. Sugere-se por boas práticas da LGPD que os dados dos indivíduos quando não forem mais necessários para esta finalidade sejam limpos ou “embaralhados” de forma que se alguém realizar acesso não consiga verificar os dados armazenados. Por tratar-se, neste caso de dados comprados, as regras de temporalidade precisam sem muito rígidas e bem definidas.

- Descrever a temporalidade: Descrever como a empresa pretende atender as demandas de temporalidade.
- Procedimento para verificar a temporalidade dos dados: Descrever quais os procedimentos mapeados (ou definir quais serão estes procedimentos) para verificar dentre os dados obtidos como verificar quais dados atingiram o limite da temporalidade para, conforme as regras, serem “eliminados”.
- Procedimento para executar a verificação da temporalidade dos dados arquivados: Descrever quais os procedimentos que devem ser executados (manuais ou automáticos) para executar a gestão da temporalidade dos dados, ou seja, quais procedimentos executar para limpar os dados. Caso estes procedimentos não existam e precisem ser mapeados destacar essa demanda para ser observada no “Plano de Ação”.
    - Abrir o formulário eletrônico do Plano de Ação e registrar esta demanda. Isso deve ser feito no momento da verificação da temporalidade para que quando houver a análise dos itens do plano de ação isso possa ser verificado.

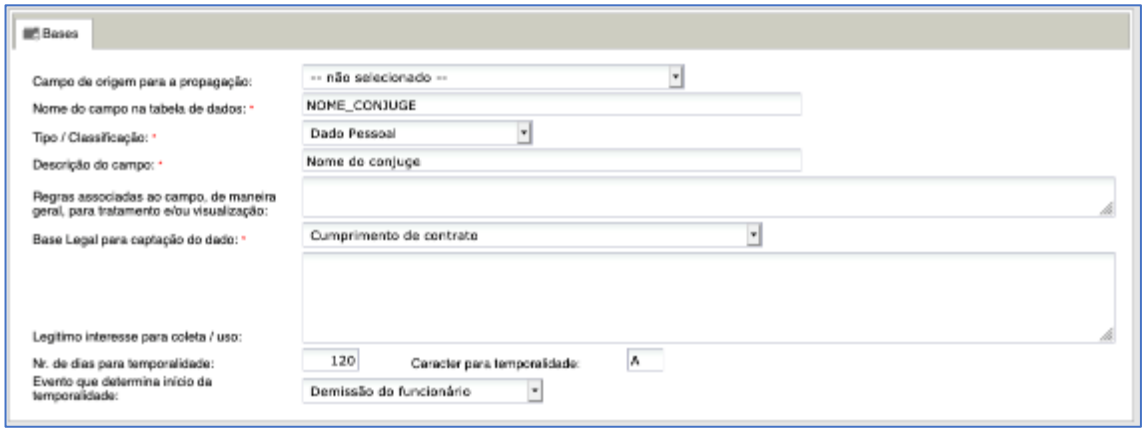
Coleta de dados – Vulnerabilidades

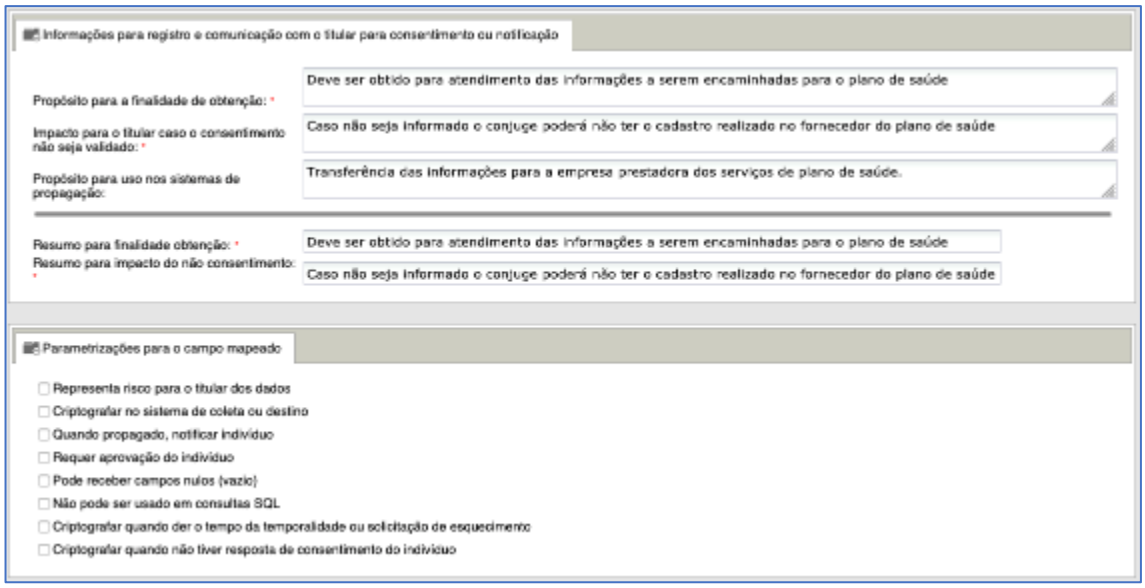


Instruções de preenchimento

- Descrever quais são as vulnerabilidades verificadas: Descrever quais são as vulnerabilidades que este tipo de coleta de dados pode ter.
    - As vulnerabilidades dizem respeito a potenciais riscos de acessos indevidos, arquivos sem controle de acesso, arquivos gravados em computadores pessoais (notebooks, tablets, etc) ou qualquer situação que possa gerar falhas e permitir um risco de acesso indevido aos dados dos indivíduos.
- Ações a serem tomadas em caso de verificação de vulnerabilidade que possa comprometer o direito da privacidade: Descrever quais são as ações que precisam ser executadas para cada um dos casos de vulnerabilidades listadas. Caso algum item demande ações futuras a serem tomadas ou definições de procedimentos operacionais, isso deve ser lançado imediatamente no formulário eletrônico do Plano de Ação.

Classificação dos dados coletados





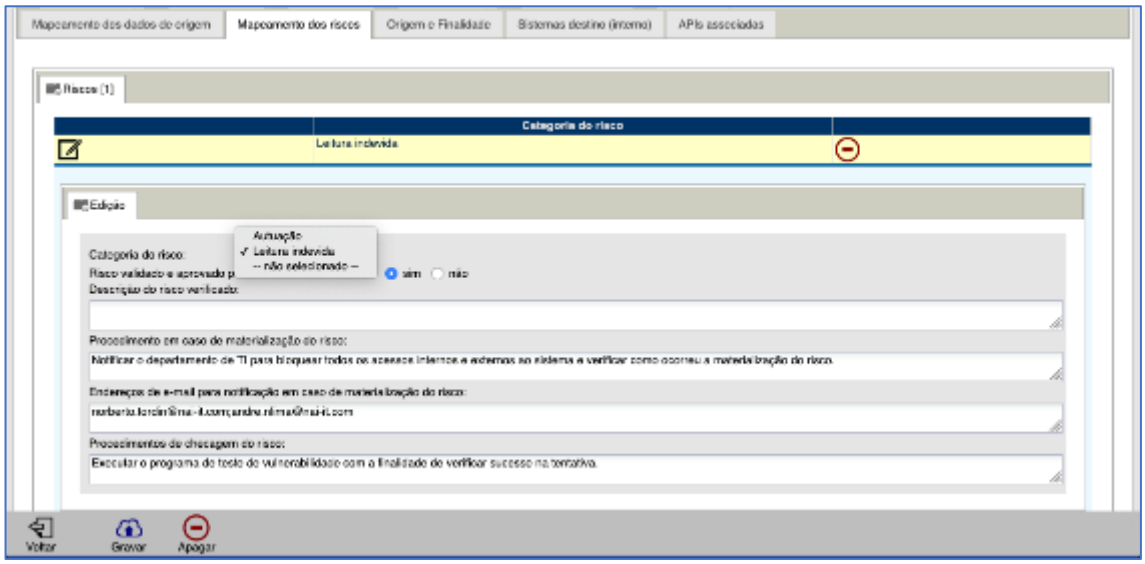
Instruções de preenchimento

A classificação dos dados coletados tem como objetivo identificar e documentar cada dado que será coletado do indivíduo pelo sistema. Esta classificação indicará como a empresa fará o tratamento destes dados e como será interpretado o manuseio destes dados para os diversos itens a serem atendidos pela LGPD.

- Campo de origem para a propagação: Neste cadastro de dados de origem esta informação deve ser desconsiderada.
- Nome do campo na tabela de dados: Informar qual é o nome do campo que consta na tabela do banco de dados. Necessita de apoio da equipe técnica de TI para identificação.
- Tipo / Classificação: Selecionar dentre as opções qual a classificação do campo
- Descrição do campo: Descrever qual é o campo que está sendo classificado.
- Base legal para captação do dado: Selecionar da lista de opções qual a base legal para a captação do dado.
- Legitimo interesse para coleta / uso: Descrever, de acordo com a base legal selecionada, qual o legítimo interesse para a coleta e/ou uso do dado.
- Finalidade para obtenção: Descrever para qual finalidade este campo está sendo coletado.
- Impacto para o titular caso o consentimento não seja validado: Descrever qual o impacto que o titular dos dados terá caso não seja feito o consentimento.
- Propósito para o uso: Descrever qual o propósito para o uso deste campo.
    - IMPORTANTE: As informações inseridas neste campo serão utilizadas para a “comunicação” com o titular dos dados.

- Número de dias para o controle da temporalidade: Informar qual a quantidade de dias que o campo obrigatoriamente terá que ficar armazenado antes da execução do controle da temporalidade.
- Caractere utilizado para a temporalidade: Informar qual o caractere que deverá ser utilizado para a substituição das informações inseridas no campo quando der o tempo da temporalidade.
    - IMPORTANTE: Ao indicar o caractere de substituição do campo para a temporalidade e houver a troca, o dado anterior não será mais recuperado.
- Representa risco para o titular: Marcar como selecionado caso o campo em questão representa algum risco de acesso ou uso indevido risco para o titular dos dados.
- Criptografar no sistema de coleta ou destino: Marcar como selecionado se desejar que o campo em questão seja criptografado após a obtenção.
- Quando propagado, notificar o indivíduo: Marcar como selecionado caso o indivíduo tenha que ser notificado quanto a propagação deste dado coletado para algum outro sistema ou parceiro.
- Requer aprovação (consentimento) do indivíduo: Marcar como selecionado caso o campo em questão, para uso ou propagação para outro sistema ou parceiro demande o consentimento prévio do titular dos dados.
- Pode receber campos nulos (vazios): Marcar como selecionado caso o campo em questão possa receber campos nulos par aos diversos casos de atendimento da LGPD (temporalidade, esquecimento).
- Não pode ser usado em consultas SQL: Marcar como selecionado caso o campo em questão não possa ser utilizado nas consultas SQL, seja de forma direta ou por ferramentas de Business Inteligence.
    - IMPORTANTE: Caberá a empresa cliente definir as regras no banco de dados para controle do acesso.
- Criptografar quando não tiver resposta de consentimento do indivíduo: Marcar como selecionado quando o titular dos dados não responder ao formulário de consentimento de uso deste campo.
    - IMPORTANTE: Dependendo da versão que a empresa cliente estiver utilizando do mapeamento dinâmico estruturado da LGPD poderá haver o procedimento automático para controle deste campo. Caso não tenha, terá que ser criado um item de risco no item mapeado.

Mapeamento dos riscos



Instruções de preenchimento

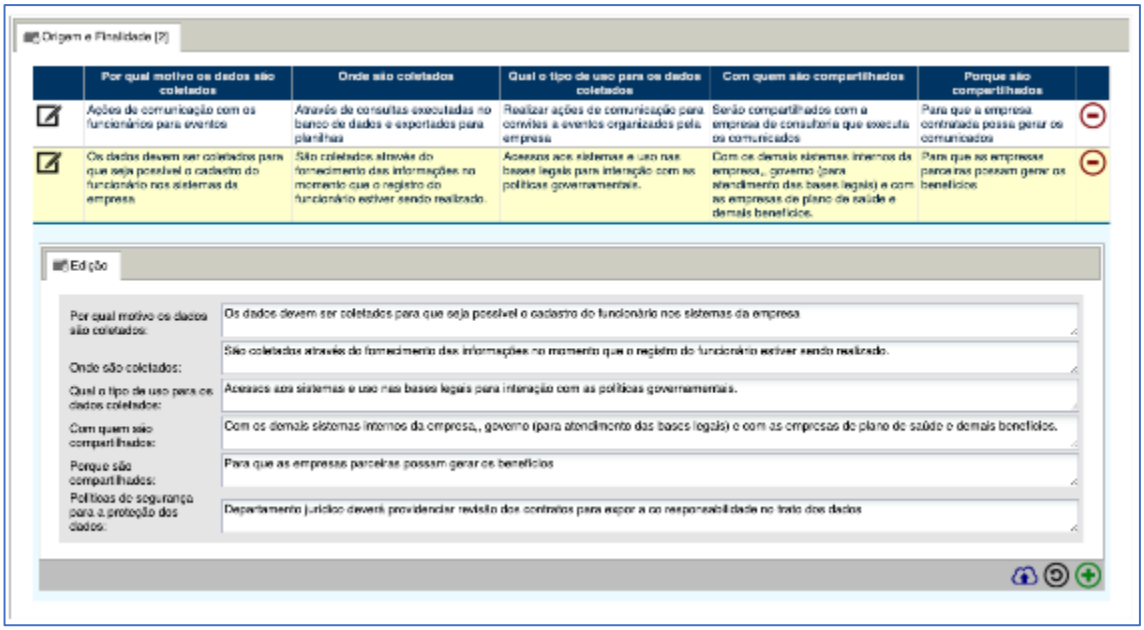
Mapear os riscos significa para a empresa e para a LGPD demonstrar que existe conhecimento dos riscos para o sistema analisado em questão, que a empresa tem ciência dos riscos e que sabe como tratar estes riscos em caso de acesso ou uso indevido.

Caso a empresa não possua esta definição ou conhecimento deve-se abrir um item no Plano de Ação para que os responsáveis identifiquem estes riscos e mapeiem como devem ser tratados.

- Categoria do risco: Selecionar dentre as opções apresentadas qual a categoria do risco que se enquadra o item que está sendo verificado.
- Risco validado e aprovado pelos controladores: (S) Sim – (N) Não
- Descrição do risco verificado: Descrever com detalhes qual o risco que foi verificado.
- Procedimento em caso de materialização do risco: Descrever qual o procedimento a ser adotado caso o risco verificado seja materializado, ou seja, caso o que foi identificado como risco aconteça.
- Endereços de e-mail para notificação em caso de materialização do risco: Cadastrar os endereços de e-mail das pessoas que devem ser notificadas caso o risco seja materializado.
- Procedimentos de checagem do risco: Descrever quais os procedimentos que devem ser executados (e sua temporalidade) para checagem de materialização do risco verificado.
- Abrir item no Plano de Ação: Marcar como selecionado este campo caso tenha que ser aberto um item específico para tratamento do risco no Plano de Ação.
- Descrição a ser utilizado no Plano de Ação: Descrever qual a descrição que será utilizada no processo de abertura automática do item do risco verificado no controle do plano de ação.

- Nome do responsável do plano de ação: Caso seja do conhecimento neste momento, informar qual o nome da pessoa responsável por tratar este item no plano de ação.

Origem e Finalidade



Instruções de preenchimento

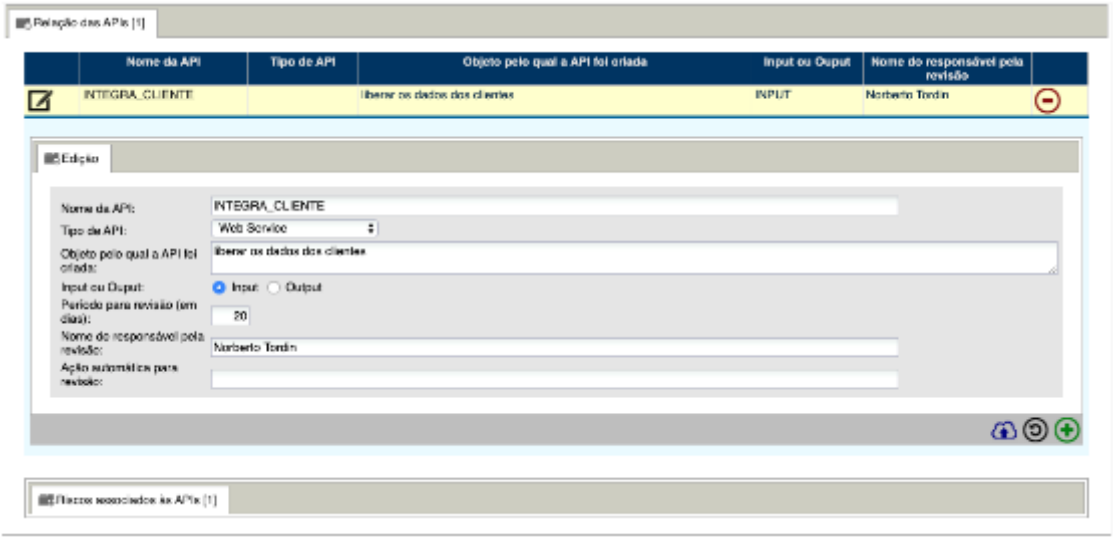
Esta tabela é de preenchimento para as informações básicas dos dados que estão sendo coletados. O objetivo é gerar na documentação as informações de maneira global para depois, nas tabelas de detalhes, informações mais precisas e específicas sobre algum dado mais preciso que demande mais informações e controles.

- Para qual motivo os dados são coletados: Neste campo deve ser descrito o motivo pelo qual os dados são coletados.
- Onde são coletados: Neste campo deve ser informado onde os dados do sistema em questão são coletados. Pode ser através de sistemas de cadastro interno, por planilhas Excel, por recebimento de empresa parceira, etc.
- Onde são coletados: Neste campo deve ser informado onde os dados do sistema em questão são coletados. Supondo que a coleta seja através de planilha Excel, descrever se haverá o tratamento dos dados coletados para a carga nas tabelas dos sistemas. Pode ser, por exemplo, rotinas internas de programas que fazem a leitura dos dados e a carga. Caso o tratamento seja feito por empresa externa ou em local externo, descrever os procedimentos.
- Qual o tipo de uso para os dados coletados: Neste campo descrever para qual finalidade os dados são coletados.
- Com quem são compartilhados: Neste campo deve ser informado com quem os dados coletados devem ser compartilhados. Nesta lista de compartilhamento devem constar os

sistemas internos e sistemas externos, destacando neste caso de ser externo, qual o parceiro que receberá os dados.

- Porque são compartilhados: Neste campo deve ser informado o motivo pelo qual os dados são compartilhados.
- Política de segurança para a proteção dos dados: Descrever qual a política de segurança para que os dados coletados dos titulares sejam protegidos quanto a acessos ou usos indevidos.

Sistemas destino – APIs associadas



Instruções de preenchimento

O mapeamento das APIs (Application Programming Interface) tem como objetivo identificar e registrar as maneiras pela qual um dado coletado poderá ser compartilhado (propagado) para outros sistemas internos e eventualmente externos.

Ao mapear estas APIs será possível identificar o quão seguro está o sistema que faz a coleta de dados está preparado para compliance com a LGPD.

Entendemos que comunicações com outros sistemas através de APIs validadas e homologadas permitem maior controle no acesso aos dados dos titulares e, desta forma, a necessidade de registrar estas informações no contexto do mapeamento dinâmico estruturado.

As informações a serem preenchidas neste formulário deverão ser obtidas com o fornecedor do software.

- Nome da API: Informar o nome da API.
- Tipo de API: Selecionar dentre a lista de opções qual o tipo da API.
- Objeto pelo qual a API foi criada: Descrever qual o motivo de criação e liberação de uso desta API.
- Input ou Output: Selecionar qual o tipo de da API.

- Período para revisão (em dias): Indicar qual o período que a API precisa ser revisada quanto a sua funcionalidade e uso efetivo.
- Nome do responsável pela revisão: Indicar qual o nome do funcionário responsável por fazer as revisões na API.
- Ação automática para revisão: Informar, caso haja, qual a ação automática (robôs, por exemplo) que podem validar a eficácia da API e se, por algum motivo, existe risco.

APIs associadas - Riscos



Instruções de preenchimento

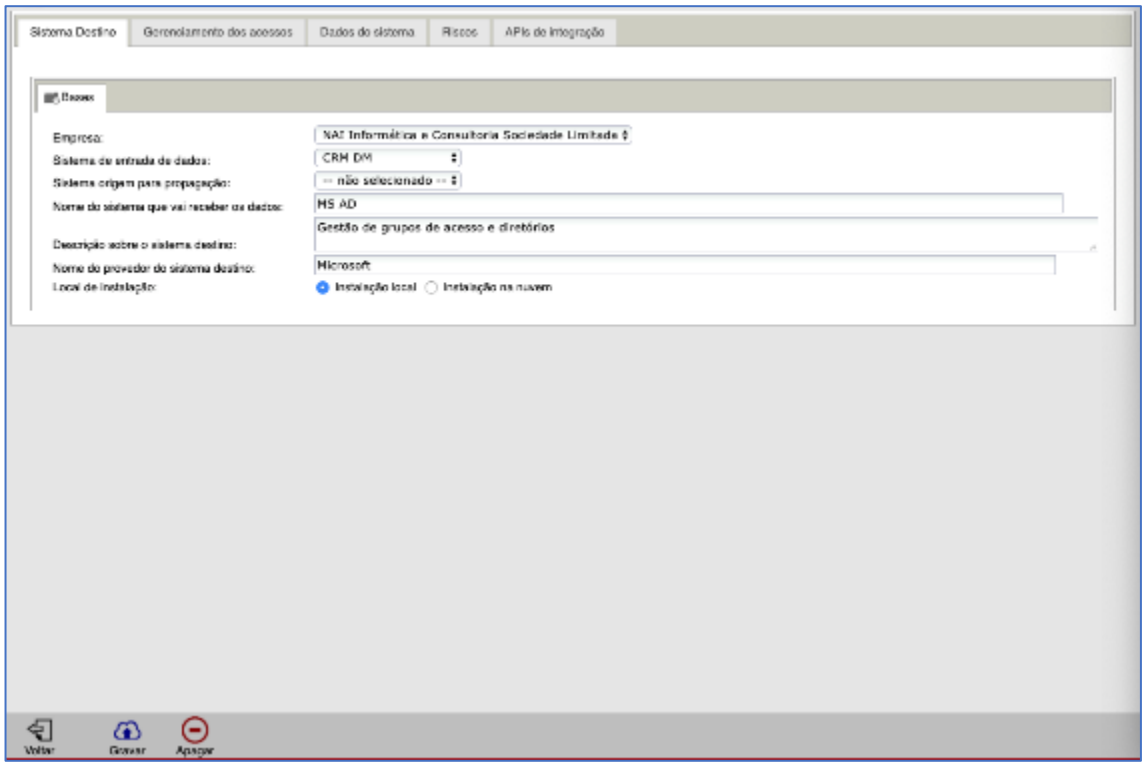
Assim como veremos em vários pontos do mapeamento dinâmico estruturado, para estes mapeamentos, sempre teremos a possibilidade de informar quais os riscos que estão atrelados ao item em questão.

No caso das APIs também devem ser informados quais são estes riscos.

O preenchimento das informações dos riscos é semelhante para todos os mapeamentos.

Formulários Eletrônicos – Sistemas com dados propagados (recebem dados)

Sistemas destino – Bases



Instruções de preenchimento

Neste formulário deverão ser inseridos os dados detalhados referentes aos sistemas que receberão os dados originalmente coletados pelo sistema origem (propagados).

Cada um dos sistemas que receberão os dados deverá ser feito o detalhamento, pois será com base nestas informações que haverá o controle da temporalidade e do direito ao esquecimento. Desta forma, quando alguma regra tiver que ser executada ou verificada, será neste preenchimento que a busca será realizada.

Neste formulário temos um ponto de atenção que precisa ser destacado e bem esclarecido:

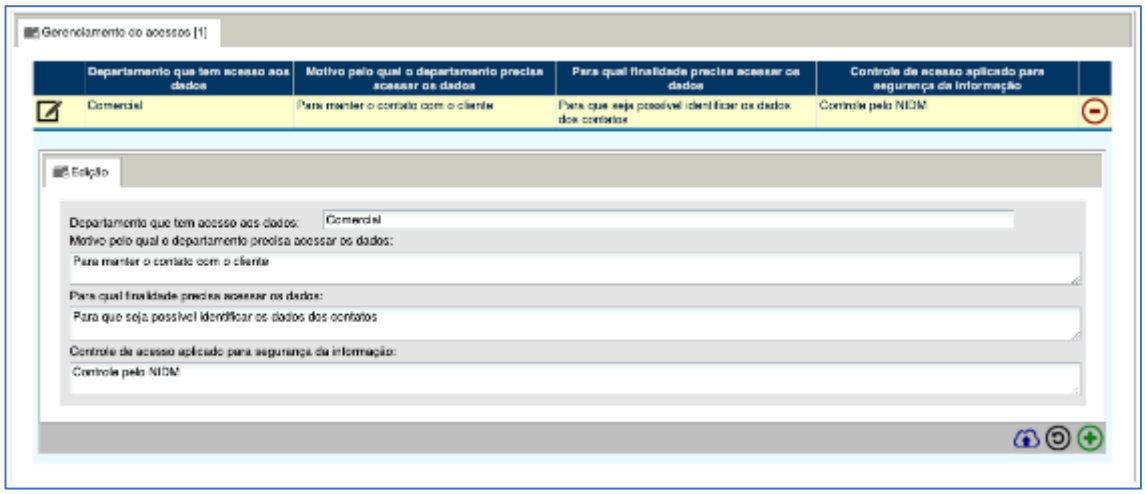
Trata-se a informação das listas de opções para o sistema de entrada de dados e sistema origem para propagação. Somente uma destas caixas de seleção deverá ser utilizada.

Procedimento: Se o sistema que estiver sendo mapeado tiver como origem um sistema de coleta de dados, deve ser preenchido SOMENTE a lista de dados: Sistema de entrada de dados.

Se o sistema de origem for um sistema que não seja de coleta de dados, ou seja, um sistema já mapeado aqui neste formulário e que a propagação ocorrerá a partir deste sistema, deverá ser selecionado na lista de opções de: Sistema origem para propagação. É extremamente importante tomar este cuidado pois a partir destas informações é que será gerado o relatório do Mapa do Fluxo de Dados.

- Empresa: Selecionar na lista de opções qual a empresa que o mapeamento está sendo realizado.
- Sistema de entrada de dados: Selecionar na lista de opções qual o sistema que faz a coleta dos dados para serem propagados.
- Sistema origem para propagação: Selecionar na lista de opções qual o sistema origem para a propagação dos dados.
- Descrição do sistema destino: Descrição detalhada do sistema destino.
- Nome do provedor do sistema destino: Nome da empresa fornecedora do sistema destino.
- Local de instalação: Selecionar se o sistema está instalado no ambiente local ou na nuvem.

Sistemas destino – Gerenciamento do acesso



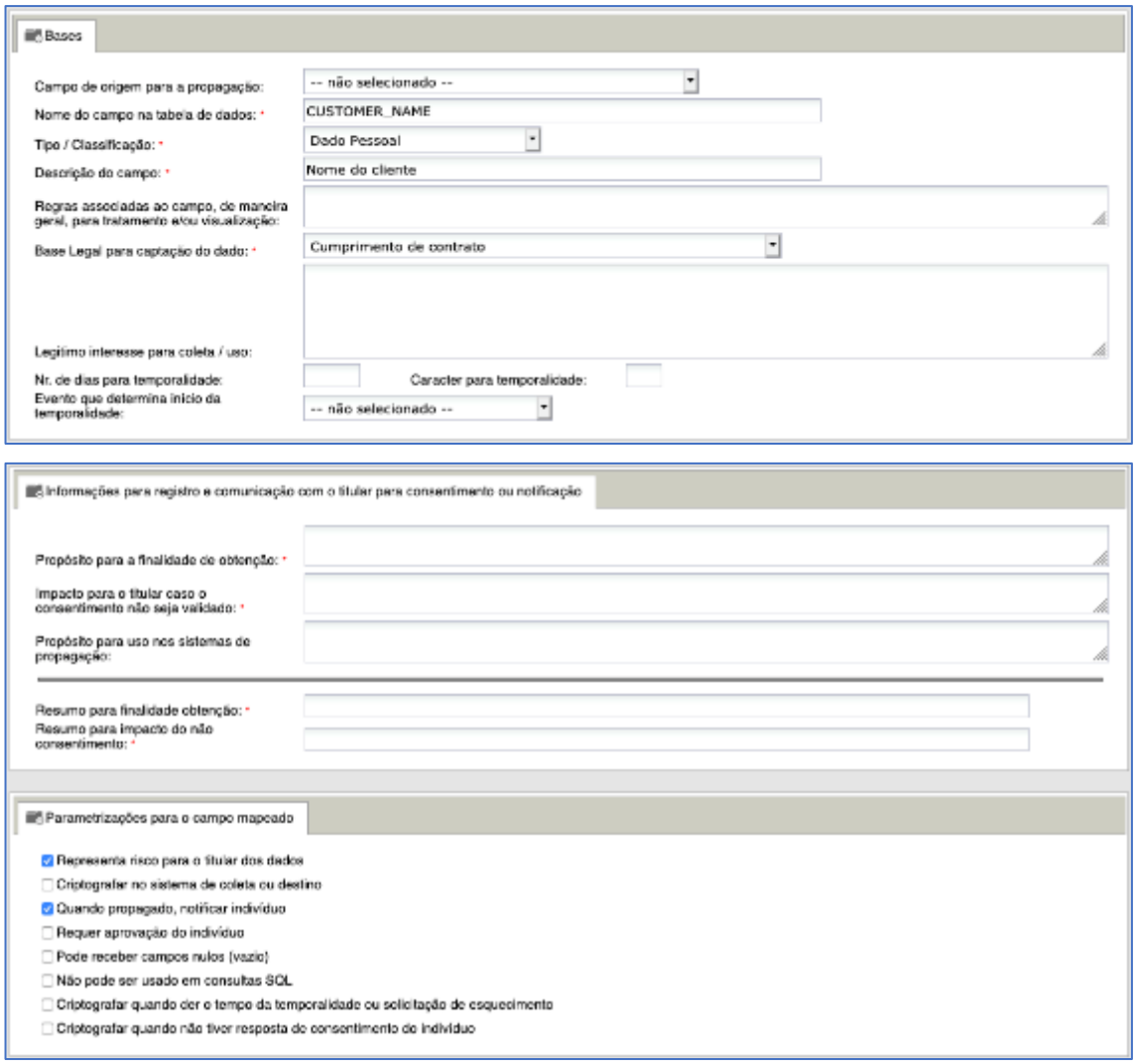
Instruções de preenchimento

Neste sub formulário deverá ser informado todos os departamentos que, de alguma maneira, farão uso deste sistema.

- Departamento que tem acesso aos dados: Informar o nome do departamento.
- Motivo pelo qual o departamento precisa acessar os dados: Descrever qual o motivo que o departamento precisa ter acesso aos dados.
- Para qual finalidade precisa acessar os dados: Descrever qual a finalidade do acesso deste departamento aos dados.

- Controle de acesso aplicado para segurança da informação: Descrever qual o controle de acesso que existe para segurança da informação.

Sistemas destino – Dados do sistema



Instruções de preenchimento

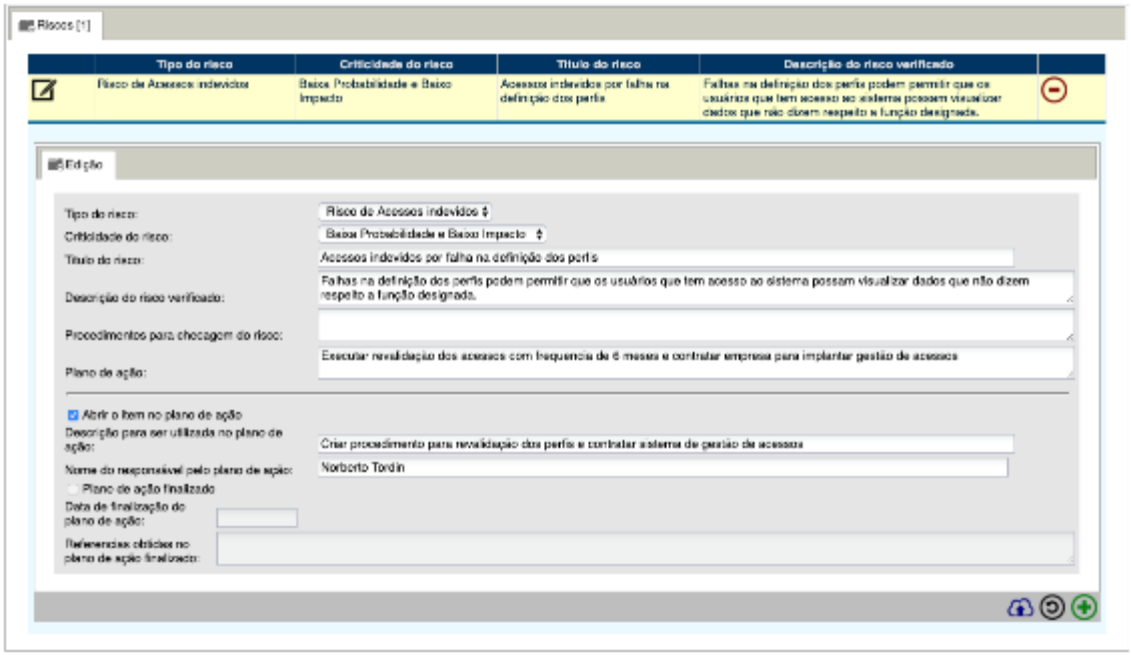
A classificação dos dados coletados tem como objetivo identificar e documentar cada dado que será coletado do indivíduo pelo sistema. Esta classificação indicará como a empresa fara o tratamento destes dados e como será interpretado o manuseio destes dados para os diversos itens a serem atendidos pela LGPD.

- Campo de origem para a propagação: Neste campo deve ser selecionado qual é o campo que foi utilizado na coleta de dados e que será utilizado para o preenchimento do campo em questão. Esta informação permitirá que seja montado o relacionamento entre os campos para o relatório de Mapa de Fluxo de Dados.

- Nome do campo na tabela de dados: Informar qual é o nome do campo que consta na tabela do banco de dados. Necessita de apoio da equipe técnica de TI para identificação.
- Tipo / Classificação: Selecionar dentre as opções qual a classificação do campo
- Descrição do campo: Descrever qual é o campo que está sendo classificado.
- Regras associadas ao campo, de maneira geral, para tratamento e/ou visualização: Descrever quais são as regras que estão associadas ao campo,
- Base legal para captação do dado: Selecionar da lista de opções qual a base legal para a captação do dado.
- Finalidade para obtenção: Descrever para qual finalidade este campo está sendo coletado.
- Impacto para o titular caso o consentimento não seja validado: Descrever qual o impacto que o titular dos dados terá caso não seja feito o consentimento.
- Propósito para o uso: Descrever qual o propósito para o uso deste campo.
    - IMPORTANTE: As informações inseridas neste campo serão utilizadas para a “comunicação” com o titular dos dados.
- Número de dias para o controle da temporalidade: Informar qual a quantidade de dias que o campo obrigatoriamente terá que ficar armazenado antes da execução do controle da temporalidade.
- Caractere utilizado para a temporalidade: Informar qual o caractere que deverá ser utilizado para a substituição das informações inseridas no campo quando der o tempo da temporalidade.
    - IMPORTANTE: Ao indicar o caractere de substituição do campo para a temporalidade e houver a troca, o dado anterior não será mais recuperado.
- Representa risco para o titular: Marcar como selecionado caso o campo em questão representa algum risco de acesso ou uso indevido risco para o titular dos dados.
- Criptografar no sistema de coleta ou destino: Marcar como selecionado se desejar que o campo em questão seja criptografado após a obtenção.
- Quando propagado, notificar o indivíduo: Marcar como selecionado caso o indivíduo tenha que ser notificado quanto a propagação deste dado coletado para algum outro sistema ou parceiro.
- Requer aprovação (consentimento) do indivíduo: Marcar como selecionado caso o campo em questão, para uso ou propagação para outro sistema ou parceiro demande o consentimento prévio do titular dos dados.
- Pode receber campos nulos (vazios): Marcar como selecionado caso o campo em questão possa receber campos nulos par aos diversos casos de atendimento da LGPD (temporalidade, esquecimento).

- Não pode ser usado em consultas SQL: Marcar como selecionado caso o campo em questão não possa ser utilizado nas consultas SQL, seja de forma direta ou por ferramentas de Business Inteligence.
    - IMPORTANTE: Caberá a empresa cliente definir as regras no banco de dados para controle do acesso.
- Criptografar quando não tiver resposta de consentimento do indivíduo: Marcar como selecionado quando o titular dos dados não responder ao formulário de consentimento de uso deste campo.
    - IMPORTANTE: Dependendo da versão que a empresa cliente estiver utilizando do mapeamento dinâmico estruturado da LGPD poderá haver o procedimento automático para controle deste campo. Caso não tenha, terá que ser criado um item de risco no item mapeado.

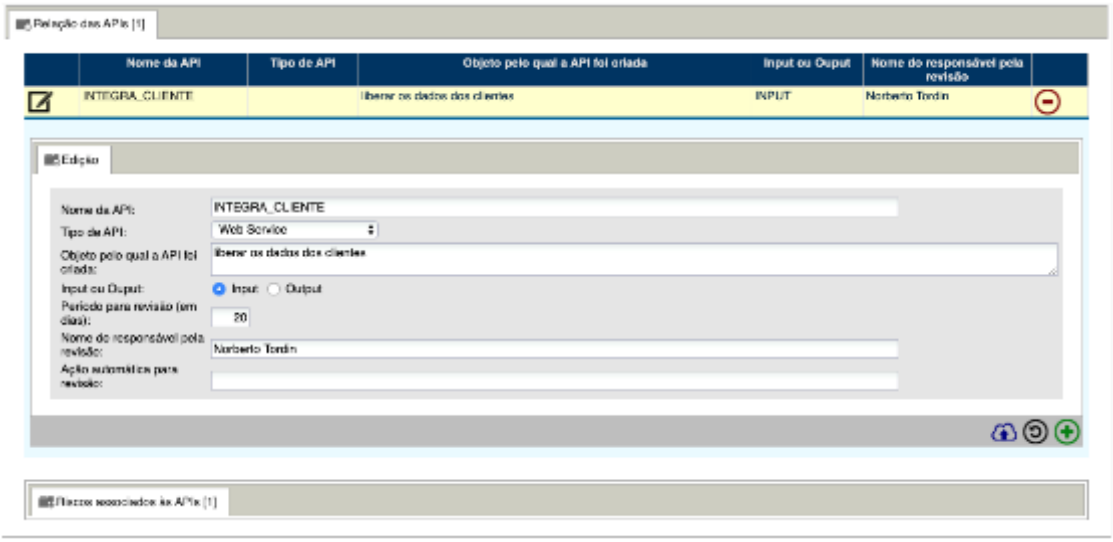
Riscos



Instruções de preenchimento

Seguir as mesmas instruções de preenchimento já descritas neste documento.

Sistemas destino – APIs associadas



Instruções de preenchimento

O mapeamento das APIs (Application Programming Interface) tem como objetivo identificar e registrar as maneiras pela qual um dado coletado poderá ser compartilhado (propagado) para outros sistemas internos e eventualmente externos.

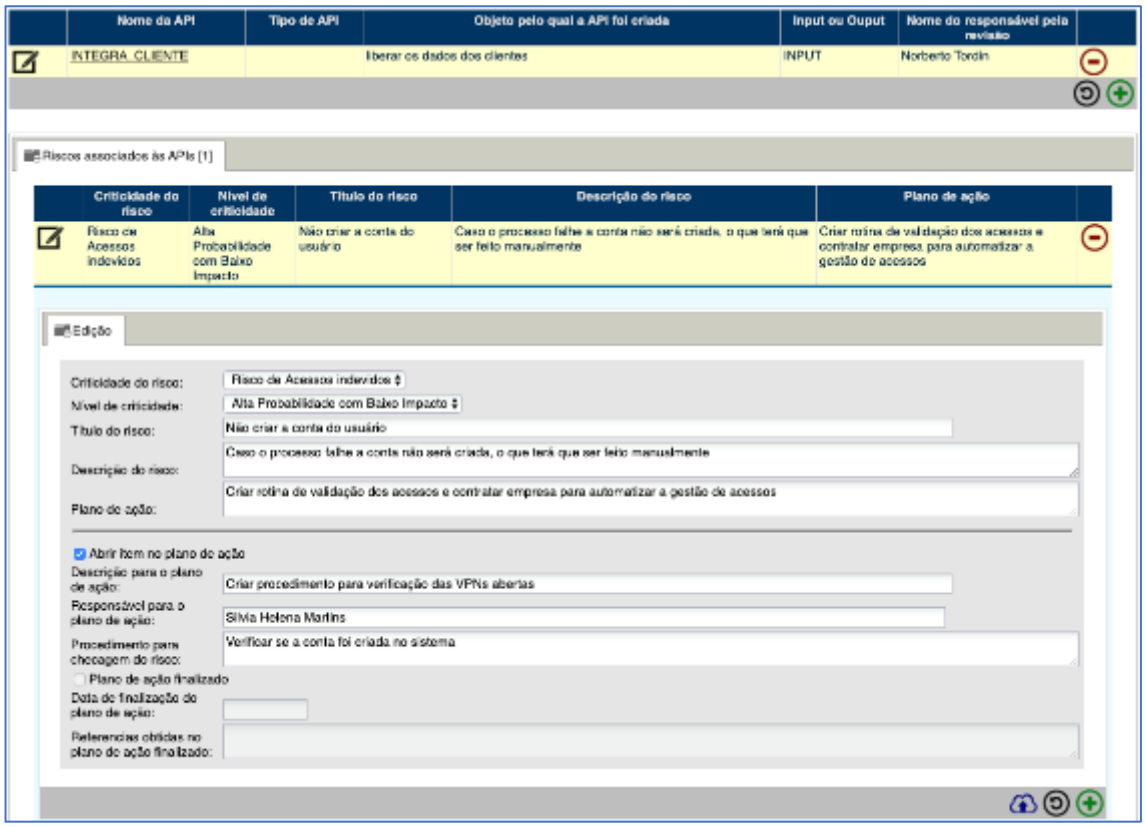
Ao mapear estas APIs será possível identificar o quão seguro está o sistema que faz a coleta de dados está preparado para compliance com a LGPD.

Entendemos que comunicações com outros sistemas através de APIs validadas e homologadas permitem maior controle no acesso aos dados dos titulares e, desta forma, a necessidade de registrar estas informações no contexto do mapeamento dinâmico estruturado.

As informações a serem preenchidas neste formulário deverão ser obtidas com o fornecedor do software.

- Nome da API: Informar o nome da API.
- Tipo de API: Selecionar dentre a lista de opções qual o tipo da API.
- Objeto pelo qual a API foi criada: Descrever qual o motivo de criação e liberação de uso desta API.
- Input ou Output: Selecionar qual o tipo de da API.
- Período para revisão (em dias): Indicar qual o período que a API precisa ser revisada quanto a sua funcionalidade e uso efetivo.
- Nome do responsável pela revisão: Indicar qual o nome do funcionário responsável por fazer as revisões na API.
- Ação automática para revisão: Informar, caso haja, qual a ação automática (robôs, por exemplo) que podem validar a eficácia da API e se, por algum motivo, existe risco.

APIs associadas - Riscos



Instruções de preenchimento

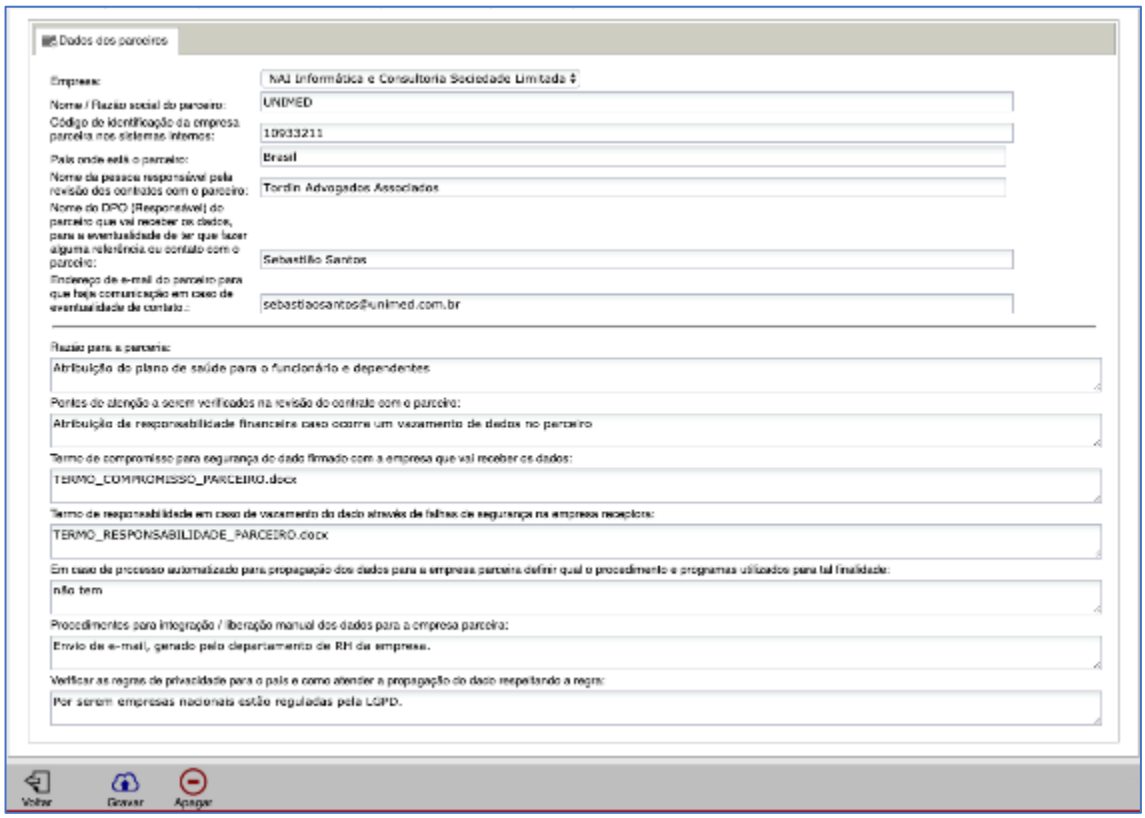
Assim como veremos em vários pontos do mapeamento dinâmico estruturado, para estes mapeamentos, sempre teremos a possibilidade de informar quais os riscos que estão atrelados ao item em questão.

No caso das APIs também devem ser informados quais são estes riscos.

O preenchimento das informações dos riscos é semelhante para todos os mapeamentos.

Formulários Eletrônicos – Parceiros Externos

Parceiros externos



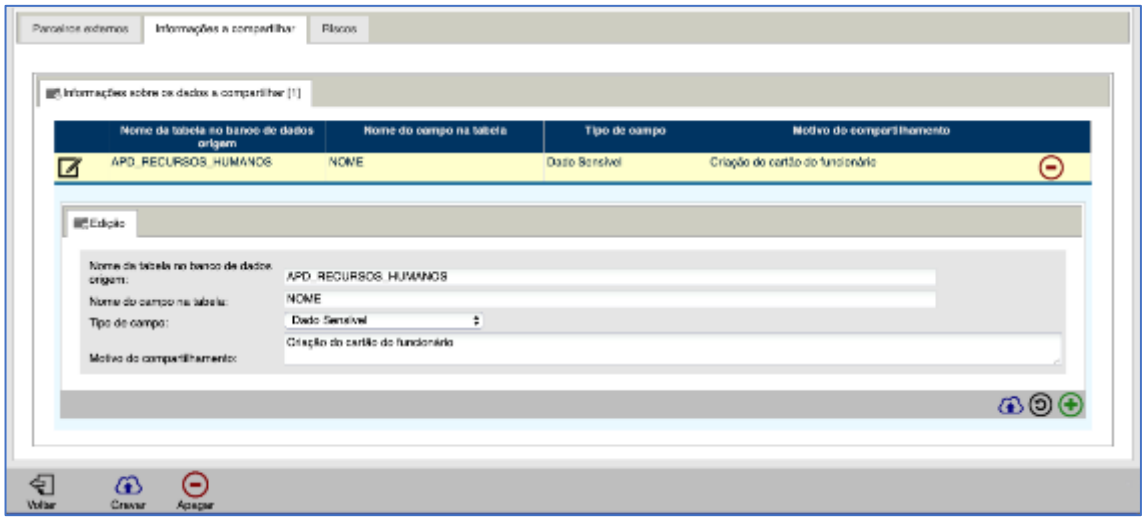
Instruções de preenchimento

Os parceiros externos são empresas que de alguma maneira possuem algum relacionamento com a empresa contratante e necessitam receber algum dado coletado, ou seja, empresas que deverão receber dados dos indivíduos coletados na empresa origem (que está sendo feito o mapeamento).

- Empresa: Selecionar a empresa que está sendo realizado o mapeamento.
- Nome / razão social do parceiro: Descrever o nome / razão social do parceiro que vai receber os dados.
- Código de identificação da empresa parceiros nos sistemas internos: Código de registro da empresa nos cadastros internos da empresa.
- País onde está o parceiro: País onde está sediado o parceiro que vai receber os dados.
- Responsável pela revisão do contrato: Nome do responsável ou empresa pela revisão das cláusulas do contrato com o parceiro.
- Nome do DPO do parceiro que vai receber os dados...: Caso seja possível identificar o nome do DPO do parceiro, informar neste campo.

- Endereço de e-mail do parceiro para que haja comunicação ...: Cadastrar os endereços de e-mail das pessoas do parceiro em caso de haver necessidade de algum contato.
- Razão para a parceira: Descrever qual a razão para que a parceria exista.
- Pontos de atenção a serem verificados na revisão do contrato com o parceiro: Descrever quais os pontos que devem ser verificados na revisão do contrato com o parceiro destacando os cuidados e responsabilidades que devem ser verificadas.
- Termo de compromisso para segurança do dado com a empresa que vai receber os dados: Descrever qual é o termo de compromisso firmado com o parceiro que descreve quais as regras de compartilhamento.
- Termo de responsabilidade em caso de vazamento do dado através de falha de segurança da empresa parceira: Descrever qual o termo de responsabilidade firmado com o parceiro prevendo as responsabilidades em caso de vazamento dos dados dos indivíduos por falha de segurança da empresa parceira.
- Em caso de processo automatizado para propagação dos dados para a empresa parceira definir qual o procedimento e programa utilizados para tal finalidade: Descrever neste campo qual o processo automatizado para a transferência dos dados ao parceiro ou qual o procedimento manual para transferência dos dados.
- Procedimentos para integração / liberação manual dos dados para a empresa parceira: Descrever os procedimentos manual para integração dos dados.
- Verificar as regras de privacidade para o país e como atender a propagação do dado respeitando a regra: Verificar quais são as regras do país destino referente a proteção dos dados do indivíduo, afim de prever como deverão ser feitos os contratos com o parceiro para a garantia da LGPD.

Informações a compartilhar

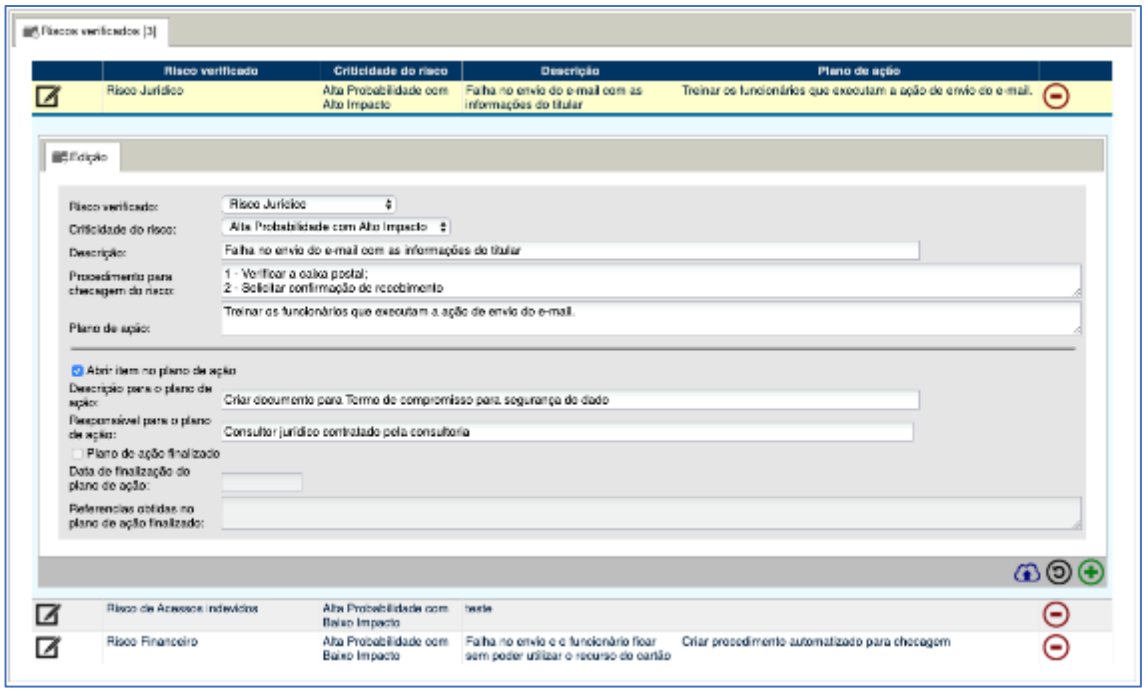


Informações de preenchimento

Nesta tabela devem ser informados quais são os campos que deverão ser compartilhados com o parceiro externo.

- Nome da tabela no banco de dados origem: Informar qual o nome da tabela do banco de dados da empresa que será a origem do dado a compartilhar.
- Nome do campo na tabela: Informar qual o nome do campo que consta na tabela citada acima que será compartilhado com o parceiro externo.
- Tipo de campo: Selecionar dentre a lista de opções qual a classificação do campo.
- Motivo do compartilhamento: Descrever qual o motivo pelo qual o campo precisa ser compartilhado com o parceiro externo.

Riscos



Instruções de preenchimento

Nesta tabela devem ser relacionados quais os riscos verificados para o compartilhamento de dados da empresa com os parceiros de negócios externos.

- Assim como definido para todos os mapeamentos, o procedimento para preenchimento é o mesmo.

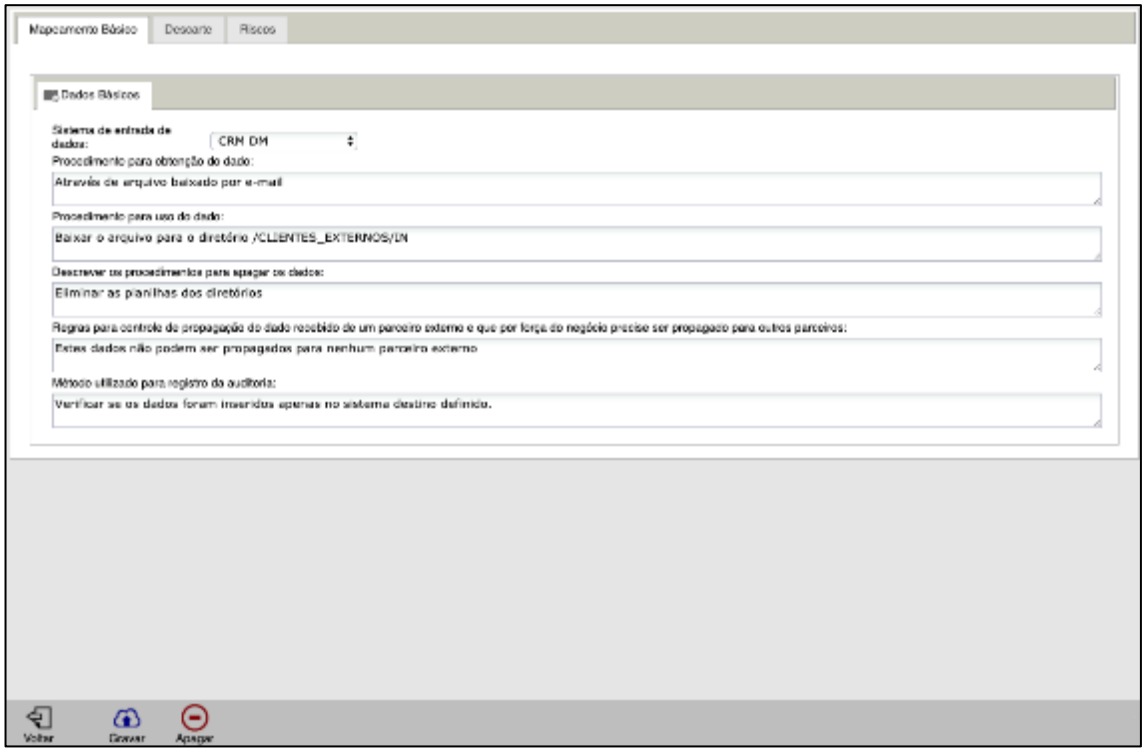
Dados de origem externa

Esta estrutura de cadastro tem por finalidade mapear e documentar os dados de origem externa. Entende-se por dados de origem externa como sendo dados que são recebidos, de alguma maneira, de parceiros externos e que por força do negócio (operação da parceria), a empresa precisa receber estes dados.

Para mapear completamente a estrutura, primeiro será necessário entender quais os procedimentos para obtenção do arquivo com os dados externos. Depois, classificar, para cada campo lido no arquivo recebido, cada um dos campos lidos a tabela destino e nome do campo destino.

Desta forma, sempre que for necessário identificar onde um campo foi inserido, saber quais os tratamentos que serão adotados.

Mapeamento básico



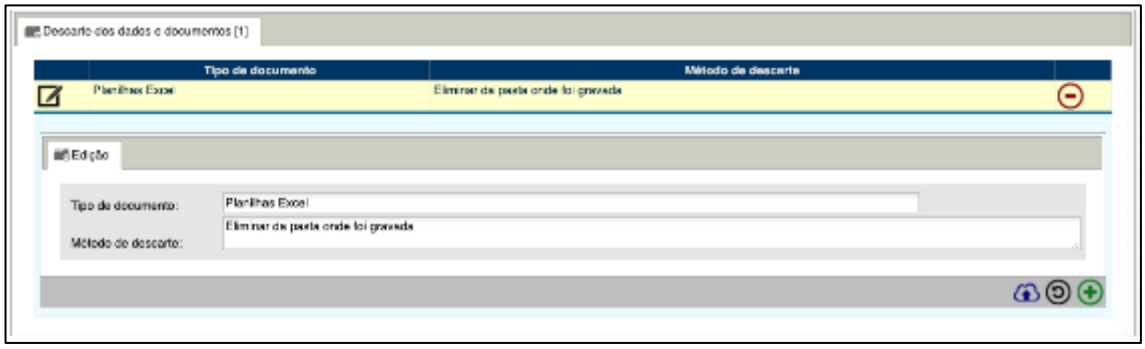
Instruções de preenchimento

Nesta tabela serão armazenados os dados captados de maneira externa. Por dado externo entende-se como os dados originados por parceiros de negócios e que precisam ser compartilhados para uso interno.

- Sistema de entrada de dados: Selecionar da lista qual o sistema de origem.
    - IMPORTANTE: Os itens que constam na lista são somente aqueles que foram previamente mapeados como SISTEMA DE COLETA DE DADOS. Portanto, para preencher este mapeamento é pré requisito que o mapeamento prévio tenha sido realizado.

- Procedimento para obtenção do dado: Descrever qual é o procedimento que a empresa utiliza para que o dado seja obtido.
- Procedimento para uso do dado: Descrever qual o procedimento interno para uso do dado obtido, levando-se em consideração a necessidade de atendimento das regras de privacidade da LGPD.
- Descrever os procedimentos para apagar os dados: Descrever quais os procedimentos para eliminação dos dados após o uso.
- Regras para controle da propagação do dado recebido de um terceiro ...: Descrever qual o procedimento e regras para compartilhar (propagar) os dados recebidos de um parceiro externo com outros parceiros. Ou seja, ao receber um dado externo, onde a coleta não é interna, e precisar compartilhar este dado com outras empresas, qual é a regra e procedimento para garantir o atendimento da LGPD.
- Método utilizado para registro da auditoria: Descrever qual o método utilizado para registrar os eventos de obtenção dos dados externos, de forma a garantir que o atendimento da LGPD seja atendido.

Descarte

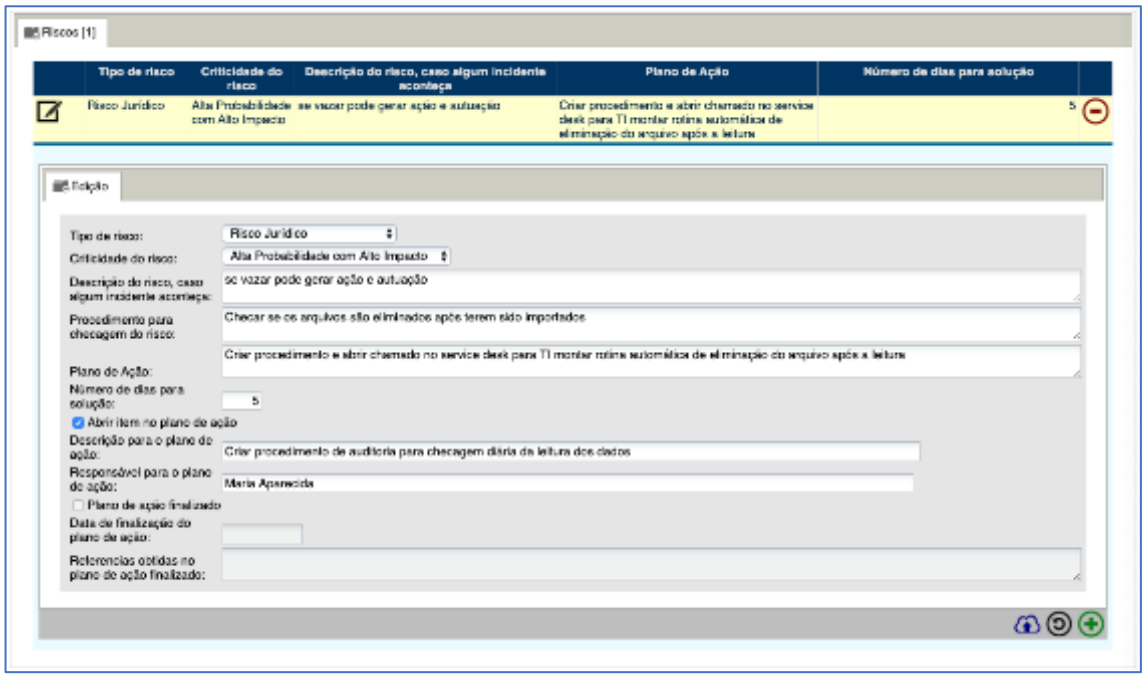


Instruções de preenchimento

Nesta tabela devem ser informados como os dados, após o uso, deverão ser descartados.

- Tipo de documento: Informar qual o tipo de documento que contém os dados.
- Método de descarte: Informar qual o método de descarte a ser seguido para o tipo de documento.

Riscos



Instruções de preenchimento

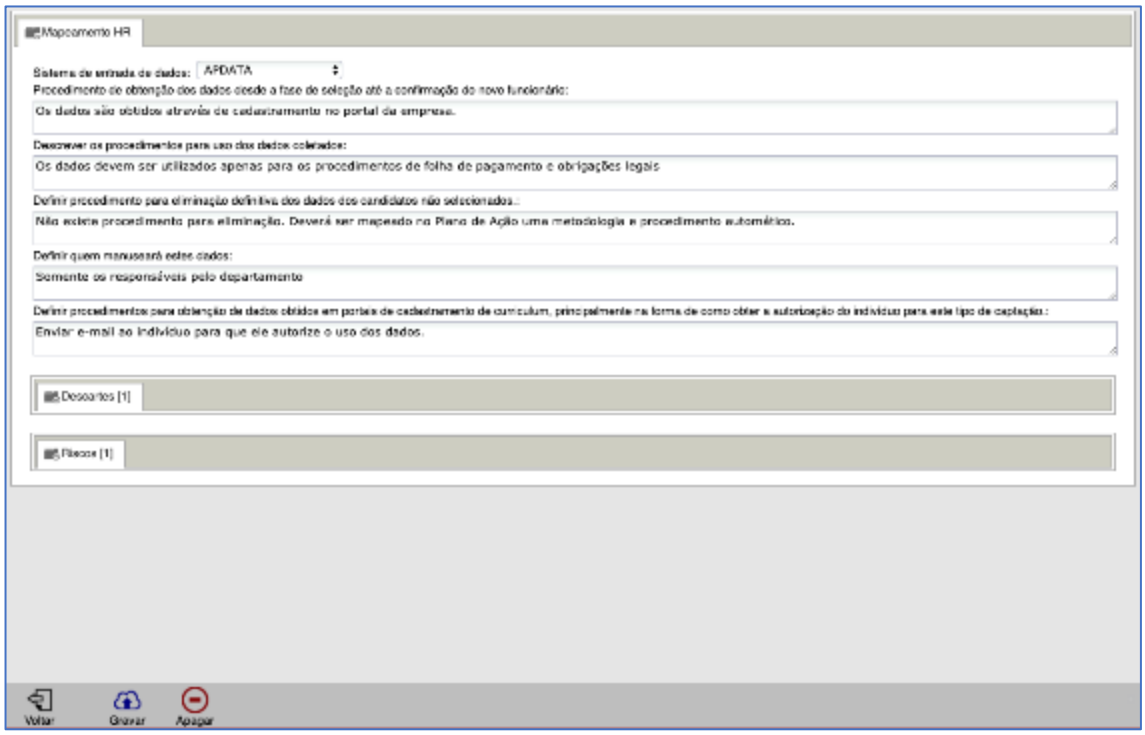
- Seguir o mesmo procedimento de preenchimento já citado neste documento.

Dados do RH

Nesta tabela devem ser inseridos os dados verificados nos sistemas utilizados pelo departamento de Recursos Humanos para a contratação de pessoas.

Todos os sistemas que, de alguma maneira, forem utilizados para a coleta de dados de indivíduos deverão ser mapeados e documentados.

Mapeamento HR

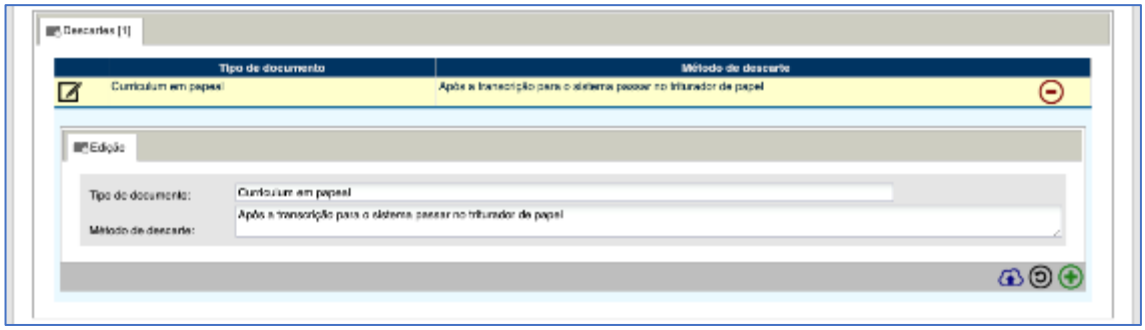


Instruções de preenchimento

- Sistema de entrada de dados: Selecionar qual o sistema de entrada de dados do RH que será documentado.
- Procedimento de obtenção dos dados desde a fase de solicitação até a confirmação do novo funcionário: Descrever como é o procedimento para obter os dados dos candidatos.
- Definir procedimento para eliminação definitiva dos dados dos candidatos não selecionados: Descrever os procedimentos para a eliminação dos dados para os casos daqueles que não foram selecionados. Verificar se o sistema de cadastramento do RH possui alguma rotina que permita expurgar estes dados e, caso positivo, com qual periodicidade e como ficam armazenados. Caso não tenha, verificar e descrever como criar um procedimento operacional. Se necessário abrir um item no Plano de Ação.
- Definir quem manuseará os dados: Descrever quem será o responsável por manusear os dados coletados e se o sistema de RH possui gestão de perfil de acesso para garantir que pessoas indevidas acessem o sistema.

- Definir procedimentos para obtenção de dados obtidos em portais de cadastramento de curriculum, principalmente na forma de como obter a autorização pra este tipo de captação: Descrever os procedimentos para os dados obtidos em portais, como CATHO, por exemplo. Verificar se a empresa possui algum mecanismo de contato com os interessados e como obter o consentimento formal para uso dos dados. Cabe destacar que deve ser dado atenção para o caso do indivíduo ter feito o cadastro nos portais voluntariamente e por este motivo, apesar de subtender que existe uma autorização, isso não se aplica. Precisa ter um procedimento descrito para resolver este problema. Se preciso for, abrir um item no Plano de Ação.

Descartes

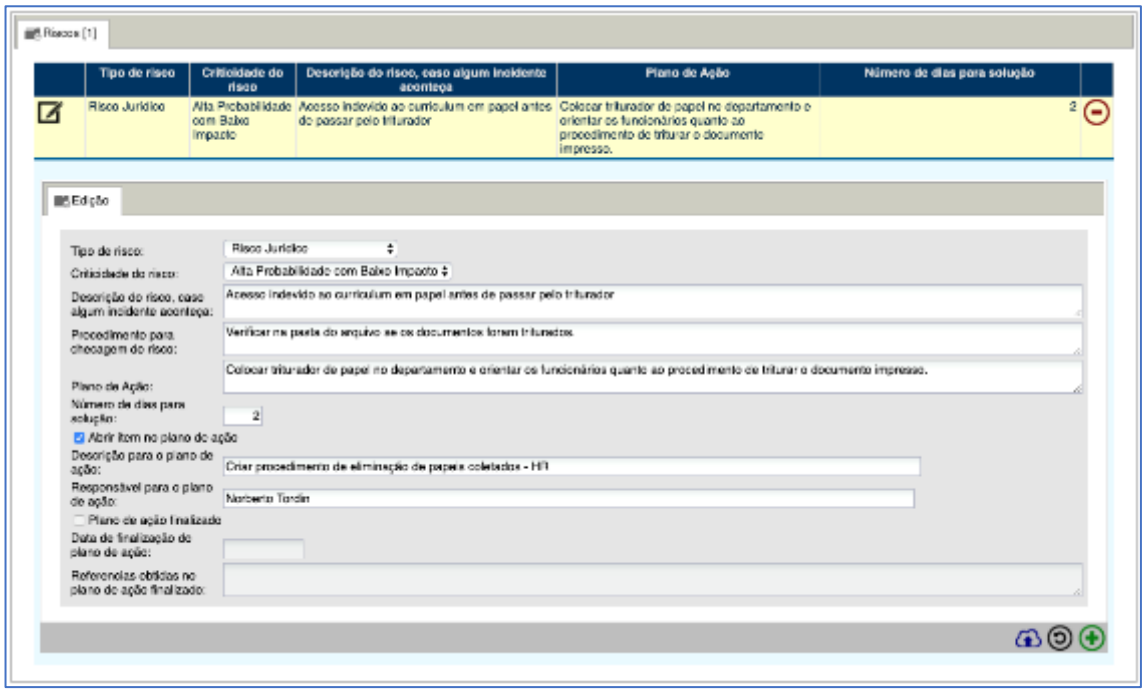


Instruções de preenchimento

Nesta tabela devem ser inseridos os mecanismos que serão utilizados para o descarte dos dados não utilizados (para os candidatos não selecionados) ou até mesmo para os candidatos selecionados, caso necessite de algum tipo de descarte.

- Tipo de documento: Selecionar dentre as opções qual o tipo de documento que foi origem da coleta dos dados.
- Motivo do descarte: Descrever qual o motivo do descarte, para o tipo de movimento selecionado.

Riscos



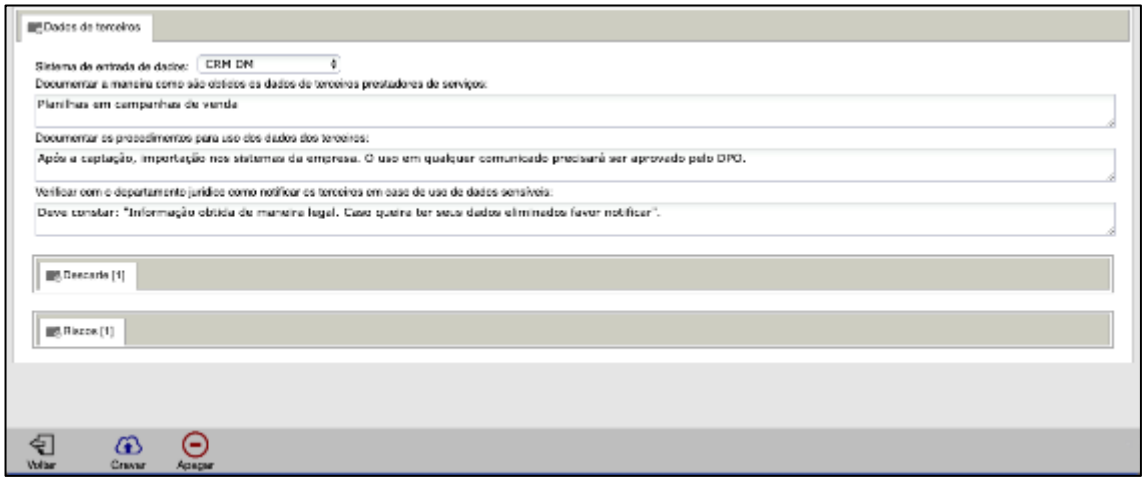
Instruções de preenchimento

- Seguir as mesmas instruções de preenchimento já descrita neste documento.

Dados de terceiros

Nesta tabela devem ser inseridos as informações referentes a dados obtidos com terceiros.
Por Terceiros entende-se como prestadores de serviços que atendem por empresas contratadas, sem serem funcionários da empresa.
Normalmente os terceiros são contratados como PJ de alguma empresa que “fornece” o pessoal. No entanto, normalmente existe um contrato entre a empresa fornecedora e a empresa contratante, sendo que as pessoas que irão realizar a prestação de serviços deverão fornecer seus dados pessoais para os cadastros internos da empresa, afim de liberar os acessos físicos, materiais, computadores, etc.
O que interessa neste mapeamento de terceiros é registrar a maneira como tratar os dados pessoais destes indivíduos.

Bases

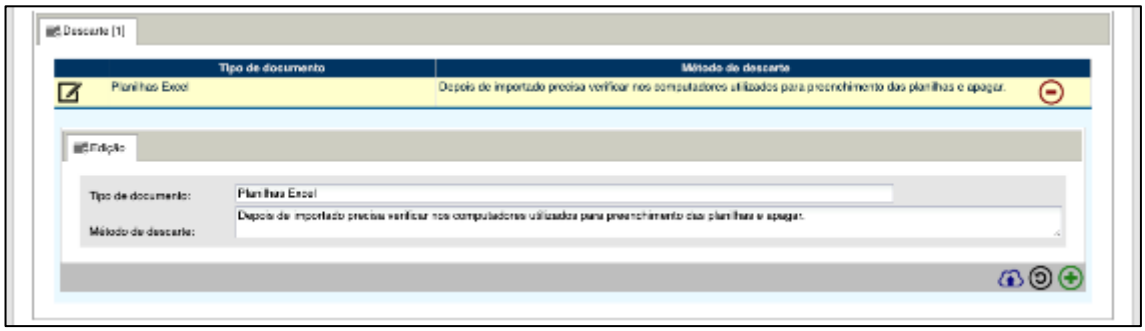


Instruções de preenchimento

- Sistema de entrada de dados: Selecionar, dentre as opções, qual o sistema que registra a entrada de cadastro dos indivíduos terceiros.
- Documentar a maneira como são obtidos os dados de terceiros prestadores de serviços: Descrever a maneira como a empresa obtém os dados dos terceiros, como por exemplo, quais os documentos necessários, onde são guardados, quem tem acesso, etc.
- Documentar os procedimentos para uso dos dados dos terceiros: Descrever a maneira como a empresa usa os dados dos terceiros. Por exemplo, qual a finalidade do uso, porque os dados são coletados, como são eliminados quando o terceiro deixa de prestar os serviços, etc.
- Verificar com o departamento jurídico como notificar os terceiros em caso de uso dos dados sensíveis: Descrever como os documentos jurídicos estão sendo tratados para que os indivíduos terceiros sejam notificados em caso de uso interno ou propagação

destes coletados dados para empresas externas. Se for necessário alguma ação para documentar ou criar algum procedimento abrir um item no Plano de Ação.

Descarte

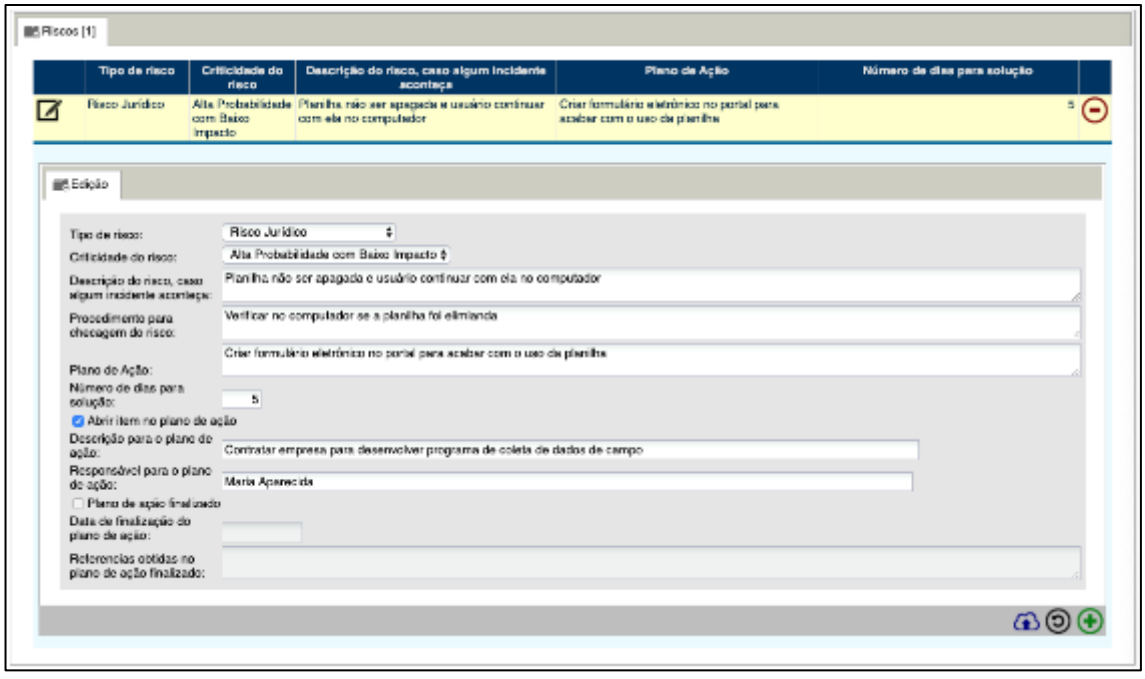


Instruções de preenchimento

Nesta tabela devem ser inseridos os mecanismos que serão utilizados para o descarte dos dados não utilizados (para os candidatos não selecionados) ou até mesmo para os candidatos selecionados, caso necessite de algum tipo de descarte.

- Tipo de documento: Selecionar dentre as opções qual o tipo de documento que foi origem da coleta dos dados.
- Motivo do descarte: Descrever qual o motivo do descarte, para o tipo de movimento selecionado.

Riscos



Instruções de preenchimento

- Seguir o mesmo procedimento de preenchimento já descrito neste documento.

Formulários eletrônicos – Processos

Objetivo

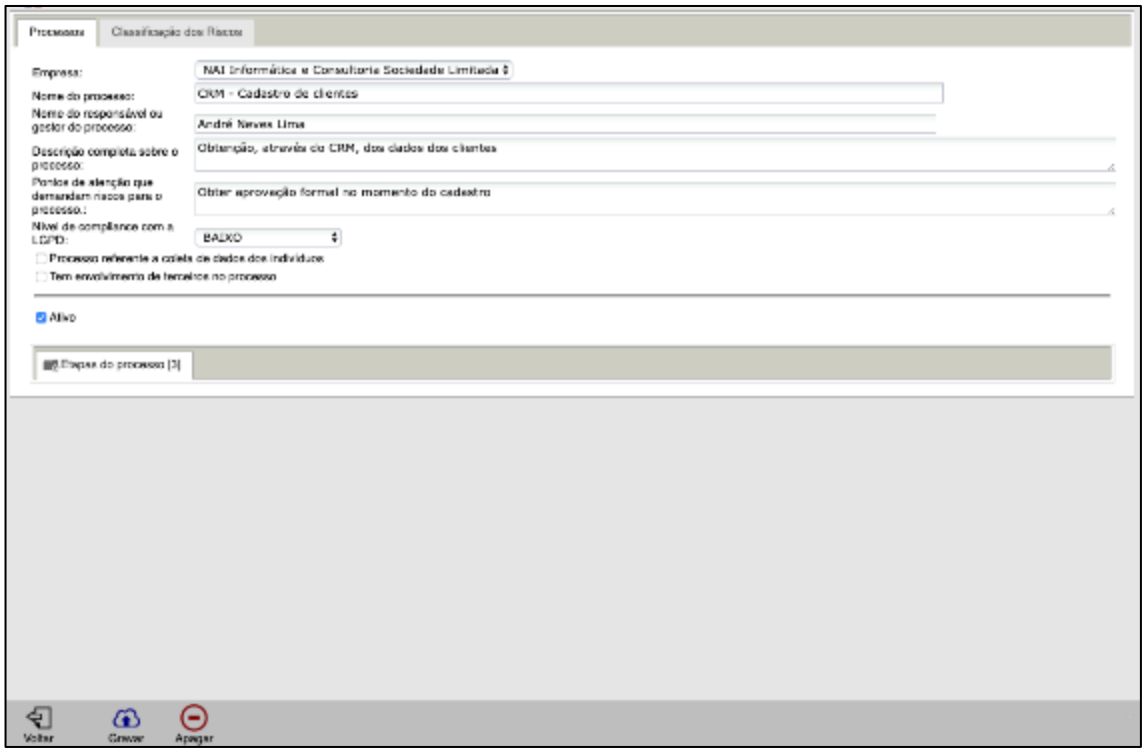
O mapeamento dos processos tem como objetivo analisar todos os processos que fazem qualquer tipo de tratamento ou acesso a dados de indivíduos, sejam estes indivíduos funcionários, terceiros ou clientes.

Tão importante quanto "pensar" nos processos internos para a gestão dos dados está a necessidade de mapear os processos para o atendimento das solicitações dos indivíduos.

O preenchimento dos formulários eletrônicos tem como finalidade analisar cada uma das atividades dos processos que fazem acesso aos dados dos indivíduos e verificar, nestas atividades, quais os pontos críticos que devem ser observados.

Eventualmente pode ser o caso da empresa não ter estes processos mapeados e documentados e, neste caso, uma análise mais detalhada será necessária para entender e validar os processos com os responsáveis. Como o foco não é mapear os processos, o preenchimento dos formulários deverá ser direcionado para registrar as atividades.

Processos



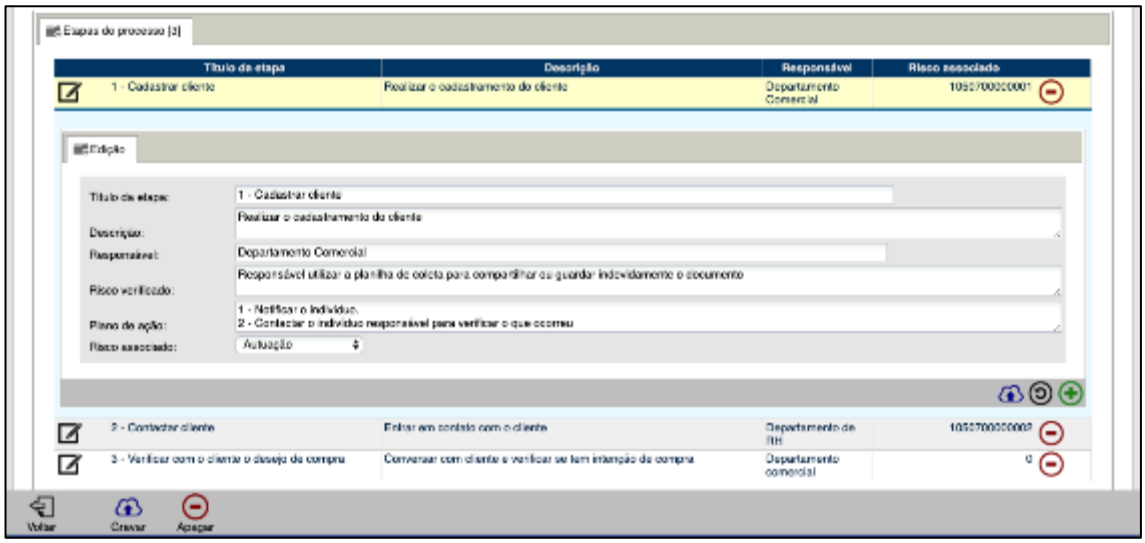
Instruções de preenchimento

- Nome do processo: Neste campo deve ser informado qual é o nome do processo. Normalmente o nome do processo é uma referência a sequência de atividades previstas

no processo. Exemplo: Desenvolvimento de novos produtos; Contratação de funcionários; etc.

- Nome do responsável ou gestor do processo: Informar o nome do funcionário responsável ou gestor pelo processo.
- Descrição completa sobre o processo: Neste campo deve ser descrito com detalhes qual a finalidade do processo, qual o motivo pelo qual o processo foi criado, e tudo mais que puder qualificar o processo de maneira bem clara e subjetiva.
- Pontos de atenção que demandam riscos para o processo: Neste campo deve ser descrito os pontos de atenção que podem representar riscos na execução do processo. Por exemplo, no processo de contratação de funcionários, caso tenha uma atividade de coleta de curriculum e este curriculum vai ficar guardado impresso. Isso representa um risco pois alguém pode ter acesso a estes documentos e copiá-los para alguma outra finalidade que não a prevista no processo.
- Nível de compliance com a LGPD: Selecionar dentre as opções qual o nível de compliance do processo com a LGPD.
- Processo referente a coleta de dados dos indivíduos: Selecionar esta opção caso o processo seja referente a coleta de dados dos indivíduos (funcionários, clientes, terceiros).
- Tem envolvimento de terceiros no processo: Selecionar esta opção caso em alguma atividade do processo tenha envolvimento de pessoas terceiras (com acessos internos ou externos aos dados).
- Ativo: Este campo deve ser sempre marcado para os processos que estivem vigentes. Pode ser que num determinado momento um processo foi extinto e não será mais utilizado. Neste caso esta tabela deverá ser atualizada com a desmarcação deste campo para indicar que as atividades e demais informações inseridas deixaram de ser válidas.

Etapas do processo



Instruções de preenchimento

As etapas do processo devem representar cada interação que envolver ação de determinada pessoa, seja para uma avaliação de um dado, preenchimento de algum dado ou até mesmo interações com outros sistemas.

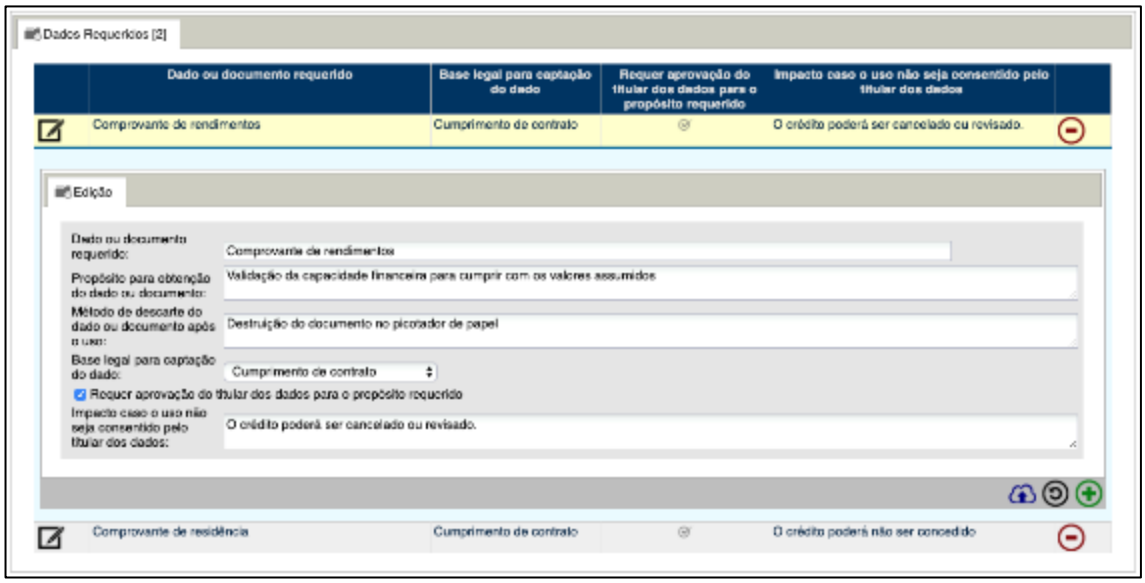
É extremamente importante detalhar bem as atividades do processo, com destaque para as atividades que de alguma maneira manusearem dados dos indivíduos, tanto para simples consulta como para cadastro ou alteração.

Outro ponto de atenção diz respeito a informação dos riscos verificados especificamente na etapa do processo. Para que fique mais coordenado, nas atividades do processo estes riscos devem ser identificados, no entanto não haverá a opção para criação automática do Plano de Ação para o risco. Caso seja necessário abrir um item no plano de ação, o risco deverá ser cadastrado para o processo como um todo.

- Sequência da etapa do processo: Indicar qual a sequência da etapa na execução do processo. Orientamos que seja feito uma sequência com intervalos de 5, pois se precisar inserir uma nova etapa haverá intervalos de números para o encaixe sem a necessidade de renumerar tudo.
- Título da etapa: Neste campo deve ser informado qual o título da etapa do processo. Por exemplo, para um processo de “Contratação de funcionário”, pode ter etapas para: 1) Abrir demanda no portal da empresa; 2) Coletar as informações do portal; 3) Convidar candidatos para entrevista; e assim todas as demais etapas.
- Descrição: Neste campo deve ser informado uma descrição mais detalhada sobre o título da etapa, destacando qual a finalidade, motivo, etc.
- Responsável: Neste campo deve ser informado quem é o responsável por responder pela etapa do processo. Pode ser o nome de um funcionário (neste caso, caso haja troca de pessoas terá que ser ajustado neste campo), ou um cargo.

- Risco verificado: Neste campo deve ser informado, em forma descritiva, qual o risco verificado para a etapa em questão. Para definir este risco pode ser necessário envolver algum funcionário responsável pela segurança da informação.
- Plano de ação: Neste campo deve ser informado qual o plano de ação a ser tomado caso o risco verificado seja materializado.
- Risco associado: Neste campo deve ser selecionado da lista de opções qual o tipo de risco associado.

Dados requeridos



Instruções de preenchimento

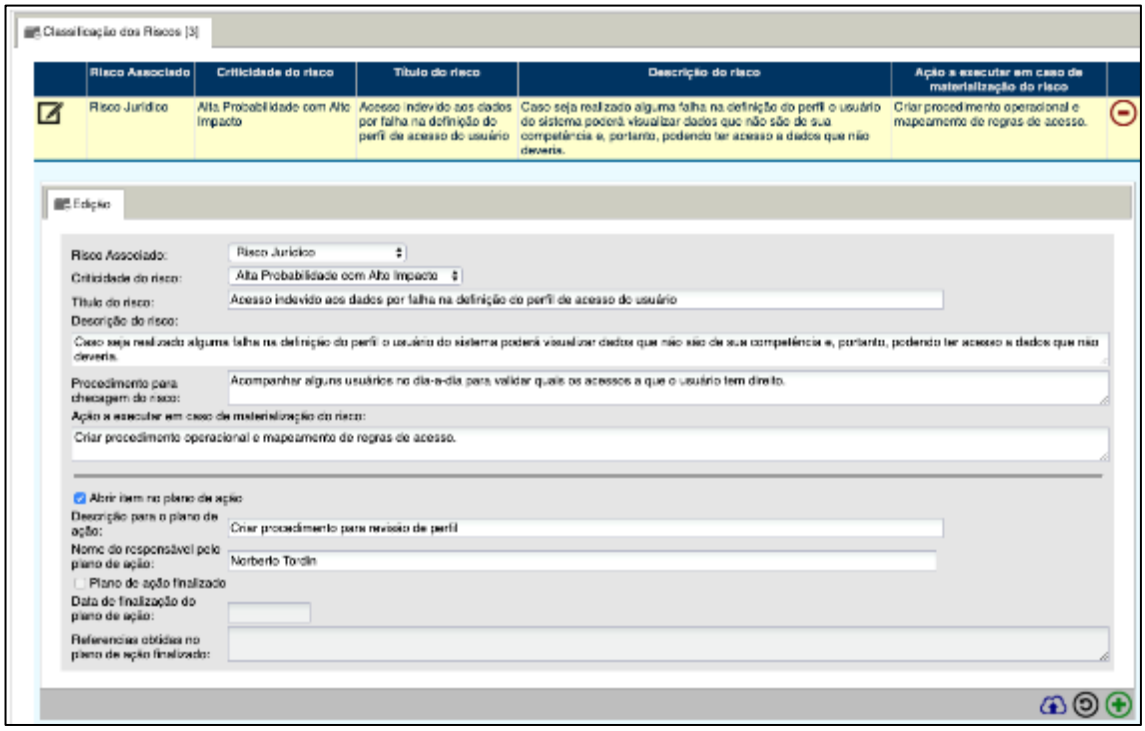
Para cada atividade do processo que estiver sendo mapeado devem ser informados quais os dados ou documentos que são requeridos ao titular dos dados.

É importante destacar que eventualmente os dados requeridos podem ser controlados, assim como os documentos requeridos precisam ser identificados como uso exclusivo para a finalidade a qual de destina.

- Dado ou documento requerido: Descrição do dado requerido ou do documento requerido.
- Propósito para obtenção do dado ou documento: Descrever qual o propósito para a obtenção do dado ou documento.
- Método de descarte do dado ou documento após o uso: Descrever qual o método de eliminação do dado ou documento após o término de uso do documento (temporalidade). Se possível destacar neste texto qual o prazo que o dado ou documento terá que ficar armazenado.
- Base legal para a captação do dado: Selecionar dentre a lista de opções qual a base legal para a captação do dado ou documento.

- Requer aprovação (consentimento) do titular dos dados para o propósito requerido: Selecionar esta opção caso seja necessário solicitar o consentimento formal do titular dos dados.
- Impacto caso o uso não seja consentido pelo titular dos dados: Descrever qual o impacto caso o titular dos dados não formalize o consentimento de uso para a finalidade a qual se destina.

Riscos associados ao processo



Instruções de preenchimento

Seguir as instruções de preenchimento já descritas neste documento.

Formulários eletrônicos – Bancos de dados

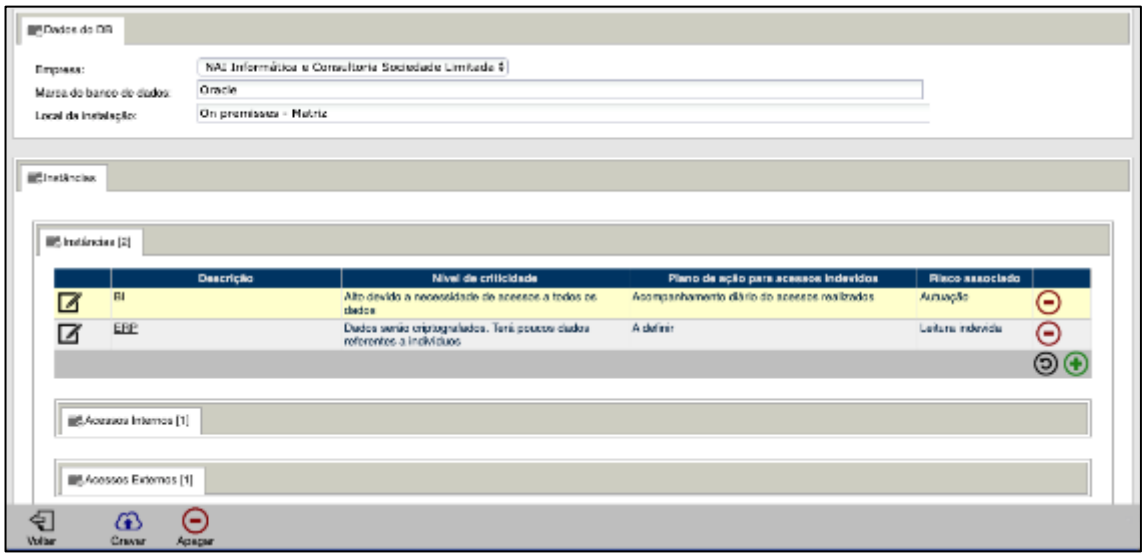
Objetivo

O mapeamento dos bancos de dados tem como objetivo verificar as condições de armazenamento dos bancos de dados utilizados pelos diversos sistemas da empresa.

Cada banco de dados que tiver referência de uso com dados dos indivíduos deverá ser mapeado e documentado conforme as instruções dos formulários eletrônicos.

Este trabalho deve ser desenvolvido em conjunto com a equipe interna da empresa, pelos profissionais que possam acessar as diversas instâncias dos bancos de dados e fornecer as estruturas solicitadas para o preenchimento dos formulários.

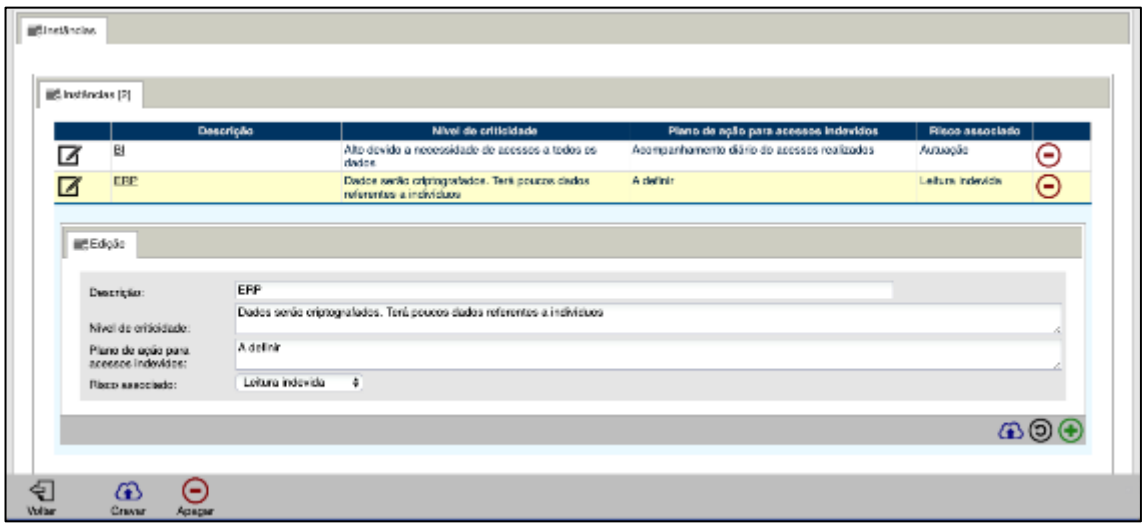
Dados do banco



Instruções de preenchimento

- Empresa: Selecionar dentre a lista de opções qual a empresa que se refere o banco de dados a ser documentado.
- Marca do banco de dados: Informar a marca do banco de dados (Oracle, MS SQL Server, etc).
- Local de instalação: Informar onde está instalado o banco de dados. Pode ser numa instalação local, numa nuvem própria, numa nuvem de terceiros, etc.

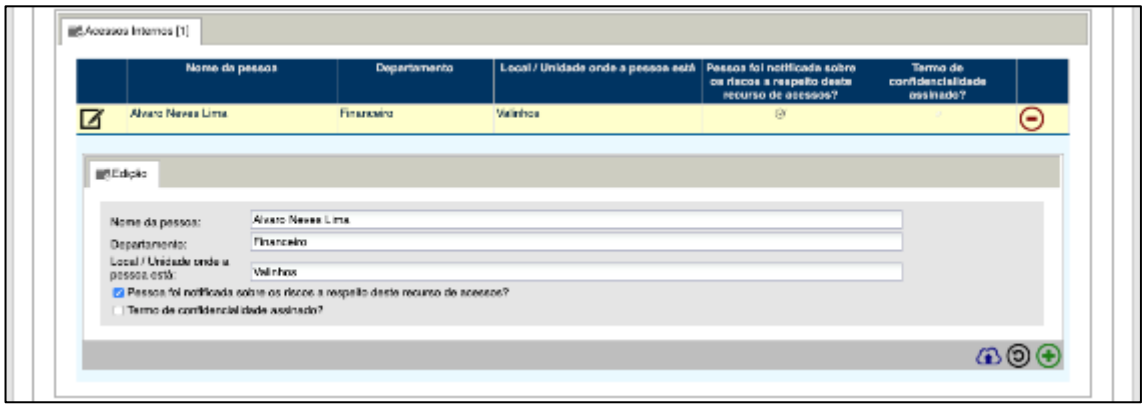
Instâncias do banco de dados



Instruções de preenchimento

- Descrição: Informar o nome da instância que foi criada para o banco de dados.
- Nível de criticidade: Descrever qual a criticidade dos dados inseridos nesta instância.
- Plano de ação para acessos indevidos: Descrever qual o plano de ação a ser executado em caso de acesso indevido ou vazamento de informações.
- Risco associado: Selecionar na lista de opções qual o risco que está associado.

Acessos internos

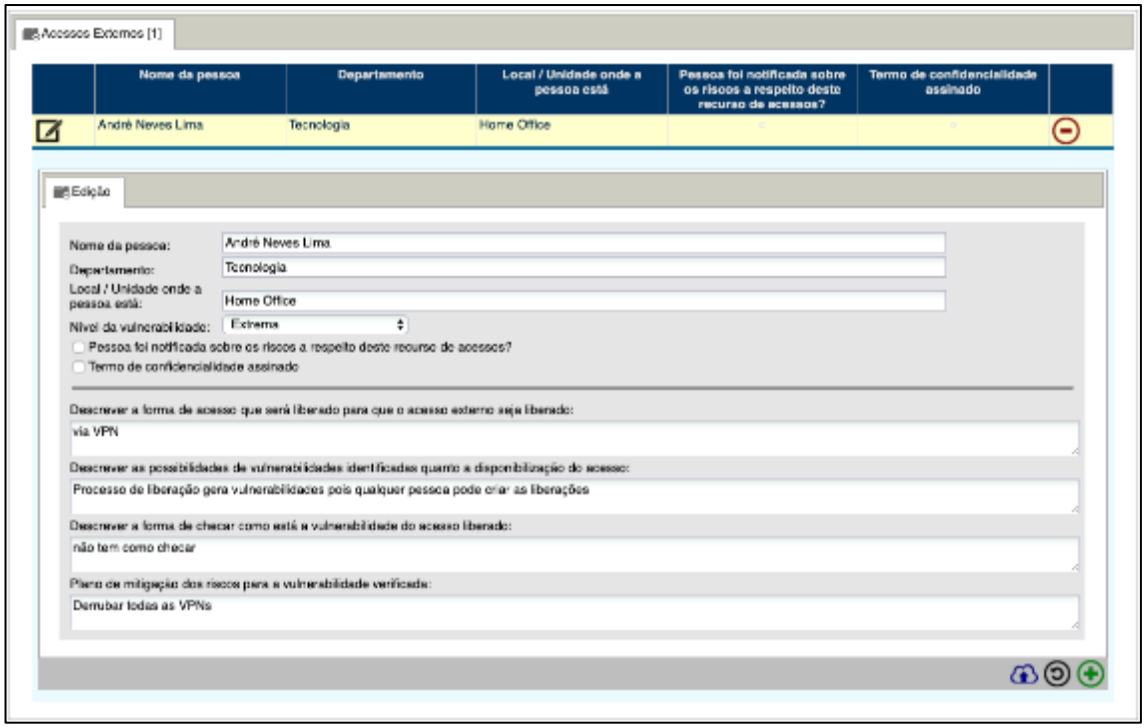


Instruções de preenchimento

Nesta tabela devem ser inseridos os indivíduos **internos** da empresa que possuem acesso direto no banco de dados. Por acesso direto entende-se como sendo as pessoas com privilégio de executar consultas SQL sem que seja por um dos sistemas da empresa, ou que execute este acesso por ferramentas de ETL para exportação dos dados selecionados para um determinado sistema de BI, por exemplo.

- Nome da pessoa: Informar o nome da pessoa que está com direito de acesso direto ao banco de dados.
- Departamento: Informar qual o departamento desta pessoa com acesso direto ao banco de dados.
- Local / Unidade onde a pessoa está: Informar qual o local ou unidade de negócios que a pessoa está
- Pessoa foi notificada sobre os riscos a respeito deste recurso de acesso? Esta opção deve ser marcada quando a pessoa tiver sido notificada sobre os riscos de vazamentos ou acessos indevidos.
- Termo de confidencialidade assinado? Esta opção deve ser marcada quando a pessoa tiver assinado o termo de confidencialidade.

Acessos externos



Instruções de preenchimento

Nesta tabela devem ser inseridos os indivíduos **externos** da empresa (terceiros, por exemplo) que fazem acesso direto ao banco de dados.

- Nome da pessoa: Informar o nome da pessoa que está com direito de acesso direto ao banco de dados.
- Departamento: Informar qual o departamento desta pessoa com acesso direto ao banco de dados.

- Local / Unidade onde a pessoa está: Informar qual o local ou unidade de negócios que a pessoa está
- Pessoa foi notificada sobre os riscos a respeito deste recurso de acesso? Esta opção deve ser marcada quando a pessoa tiver sido notificada sobre os riscos de vazamentos ou acessos indevidos.
- Nível da vulnerabilidade: Selecionar dentre a lista de opções qual o nível de vulnerabilidade verificada.
- Termo de confidencialidade assinado? Esta opção deve ser marcada quando a pessoa tiver assinado o termo de confidencialidade.
- Descrever a forma de acesso que será liberada para que o acesso seja liberado: Descrever como será liberado o acesso externo direto no banco de dados.
- Descrever as possibilidades de vulnerabilidades identificadas quanto a disponibilização do acesso: Descrever quais são as vulnerabilidades que podem ser verificadas com a liberação deste acesso externo.
- Descrever a forma de checar como está a vulnerabilidade do acesso liberado: Descrever como será feito a checagem de verificação do acesso liberado, afim de validar se a vulnerabilidade identificada possui algum risco de materialização.
- Plano de mitigação dos riscos para a vulnerabilidade verificada: Descrever qual o plano de mitigação caso a vulnerabilidade seja materializada.
- Nível da vulnerabilidade: Selecionar da lista de opções qual o nível da vulnerabilidade verificada.

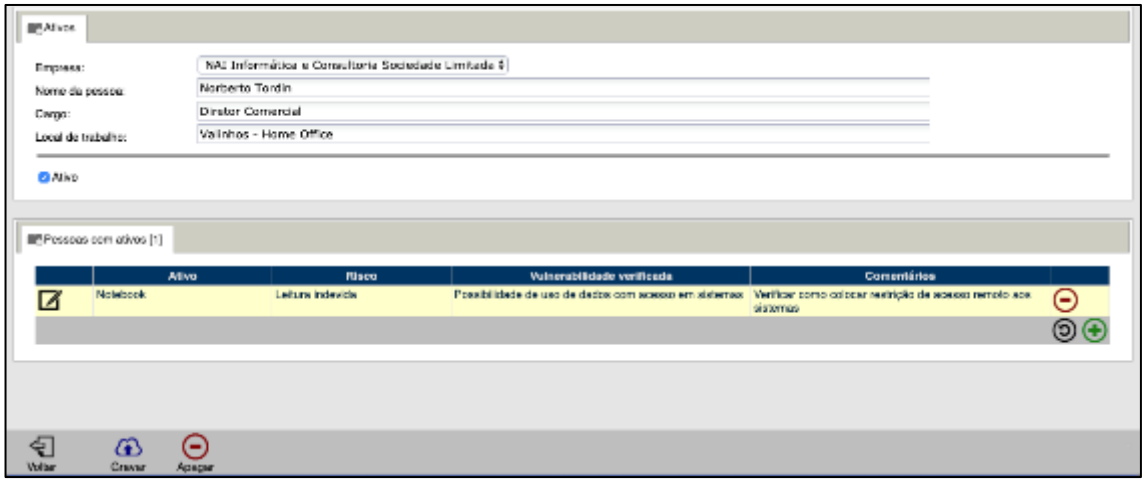
Formulários eletrônicos – Gestão dos ativos

Objetivo

O mapeamento dos ativos da empresa tem como finalidade verificar quais são os funcionários ou terceiros que fazem uso de dispositivos móveis (notebook, celular, tablets, etc) que, de alguma maneira, possam realizar acessos externos aos sistemas e/ou bancos de dados da empresa sem que estejam no ambiente de rede controlado.

Estas verificações devem ser registradas com seus respectivos riscos analisados e, se necessário, haver o treinamento e envolvimento do departamento jurídico para assinatura de Termo de Responsabilidade. Eventualmente, definições de novas políticas de segurança devem ser mapeadas afim de garantir que acessos indevidos gerem falhas no processo e vazamentos de dados dos indivíduos.

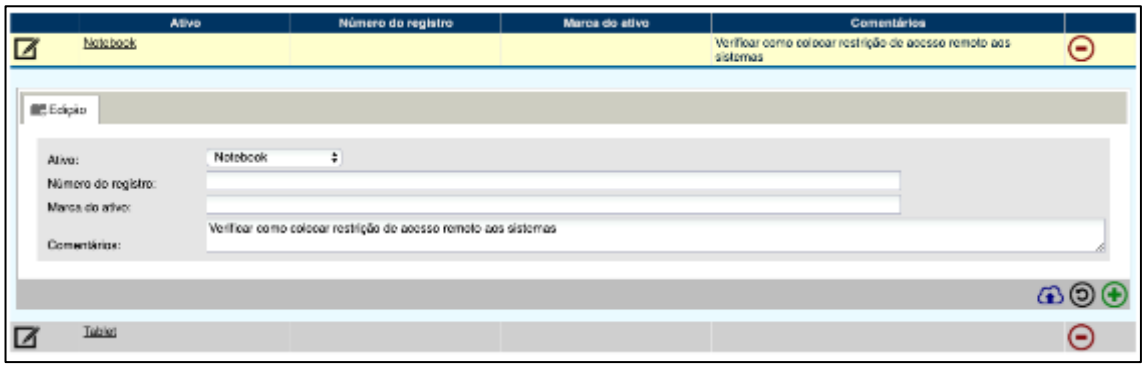
Ativos



Instruções de preenchimento

- Empresa: Selecionar dentre as opções qual a empresa que está sendo feito o mapeamento dos ativos.
- Nome da pessoa: Nome da pessoa que está de posse do ativo.
- Cargo: Cargo da pessoa que está de posse do ativo.
- Local de trabalho: Local de trabalho da pessoa que está de posse do ativo.
- Ativo: Esta opção deve ser marcada enquanto o funcionário ou terceiro estiver utilizando o ativo.

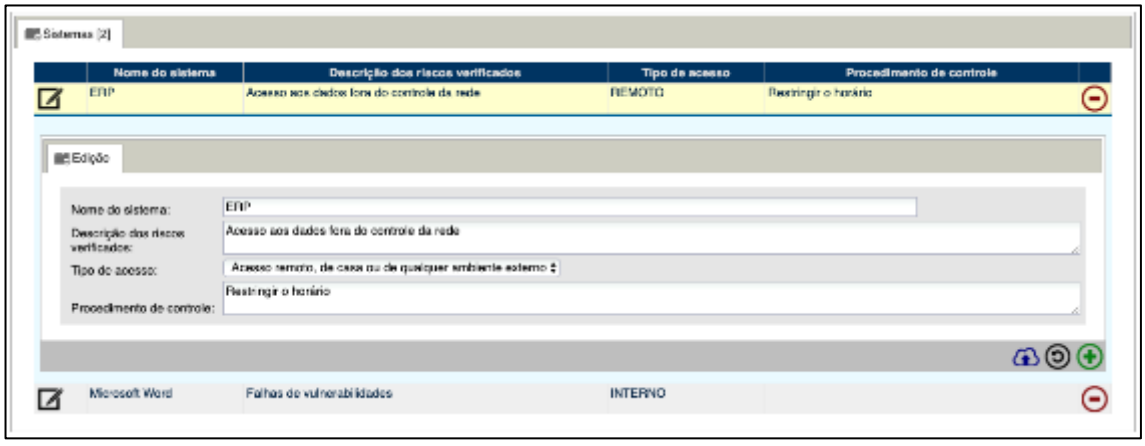
Pessoas com ativos



Instruções de preenchimento

Neste formulário deverão ser inseridos, para a pessoa indicada, quais são os ativos (equipamentos) que foram disponibilizados (notebook, celular, tablet, etc.) que de alguma maneira permitem o uso de sistemas da empresa ou recebam / compartilhem de planilhas que possam conter dados que devem ser cuidados e tratados par atendimento da LGPD.

- Ativo: Selecionar dentre a lista de opções qual o ativo que foi liberado.
- Número do registro: Informar qual o número de registro ou número de série do ativo que foi liberado.
- Marca do Ativo: Informar qual a marca do ativo.
- Comentários: Descrever informações que julgar conveniente sobre o ativo liberado.

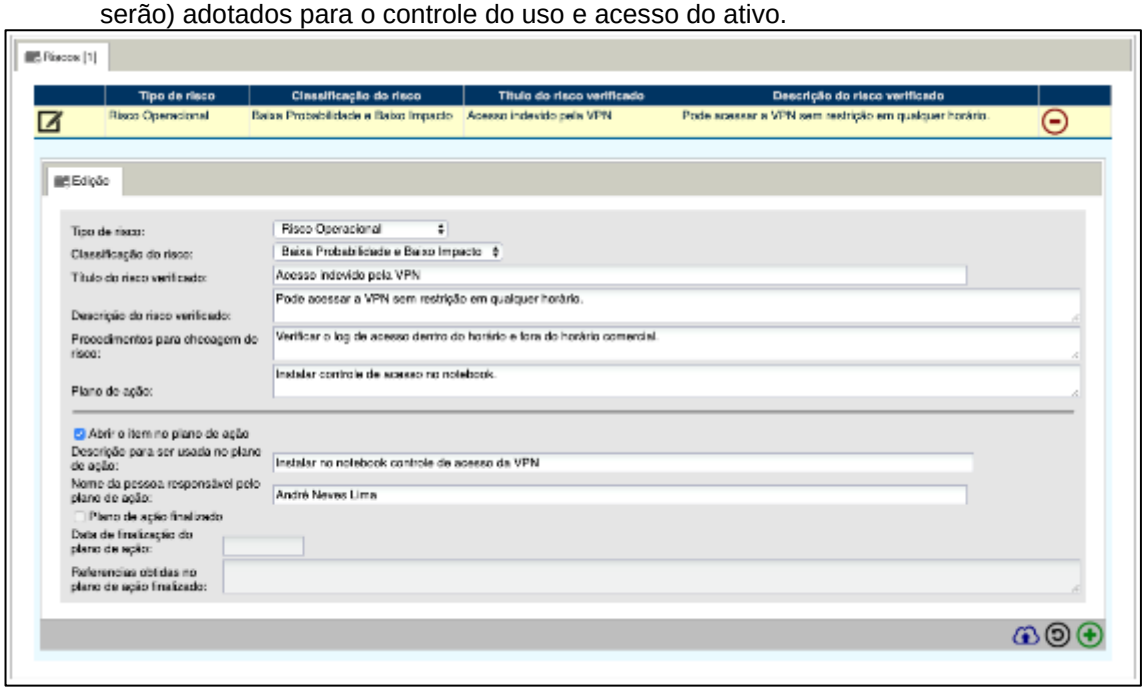


Instruções de preenchimento

Informar a relação dos sistemas que a pessoa para qual o ativo foi fornecido terá possibilidade de acesso.

- Nome do sistema: Informar qual o nome do sistema que a pessoa terá acesso.
- Descrição dos riscos verificados: Descrever se existe algum risco verificado e qual é este risco.
- Tipo de acesso: Selecionar na lista de opções qual o tipo de acesso que será liberado para uso do ativo.

- Procedimento de controle: Descrever quais os procedimentos de controle que são (ou serão) adotados para o controle do uso e acesso do ativo.

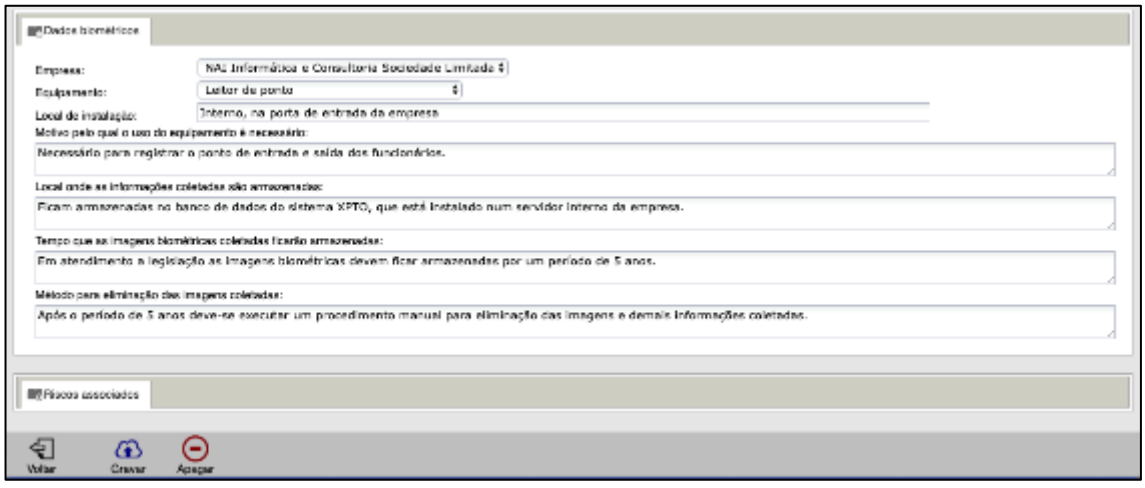


Instruções de preenchimento

Seguir as instruções de preenchimento já descritos neste documento.

Formulários eletrônicos – Biometria

Dados biométricos

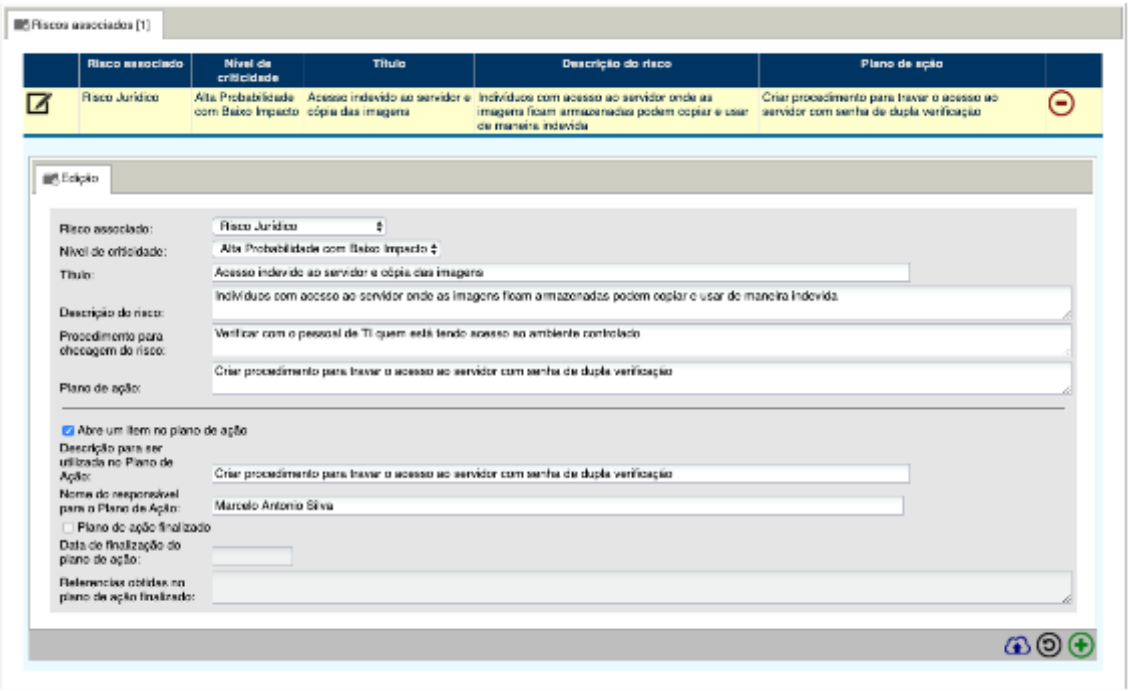


Instruções de preenchimento

- Empresa: Selecionar na lista de opções a empresa para qual o mapeamento está sendo realizado.
- Equipamento: Selecionar na lista de opções qual o equipamento de biometria
- Local de instalação: Descrever onde está instalado o equipamento de biometria.

- Motivo pelo qual o uso do equipamento é necessário: Descrever o motivo que o equipamento de biometria precisa estar instalado e fazendo a captura das informações (imagens, digital, etc).
- Local onde as informações coletadas são armazenadas: Descrever o local onde as informações de biometria coletadas estão sendo armazenadas.
- Tempo que as imagens biométricas ficarão armazenadas: Informa qual o tempo que as imagens biométricas coletadas (para o equipamento em questão) ficarão armazenadas.
- Método de eliminação das imagens coletadas: Descrever qual o método de eliminação das imagens ou digitais coletadas.

Riscos associados



Instruções de preenchimento

Seguir o mesmo procedimento já descrito neste documento.

Formulários eletrônicos – Análise dos contratos

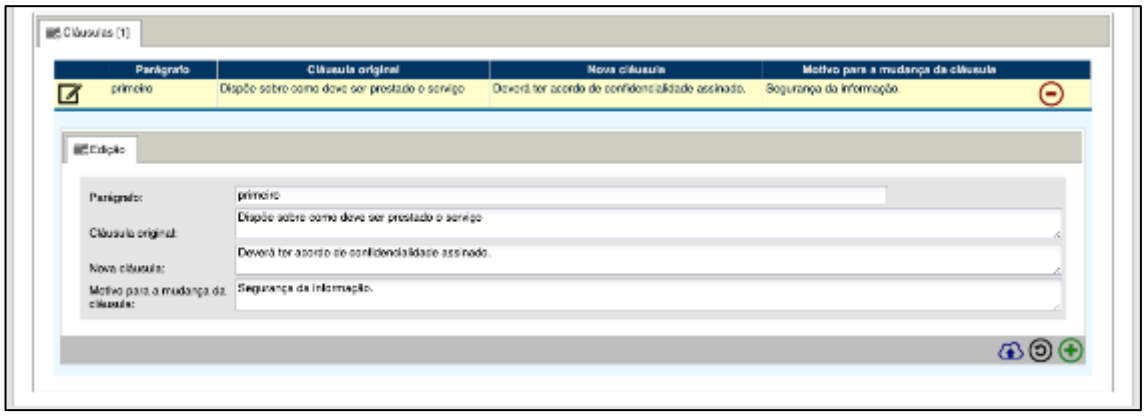
Contratos



Instruções de preenchimento

- Empresa: Selecionar na lista de opções qual a empresa que está sendo feito o mapeamento.
- Título do contrato: Informar qual o título do contrato que está sendo analisado.
- Descrição sobre o contrato: Informar uma descrição sobre o contrato.
- Nome do parceiro: Informar qual o nome do parceiro (outra parte) do contrato
- Tipo de contrato: Selecionar na lista de opções qual o tipo de contrato que está sendo analisado

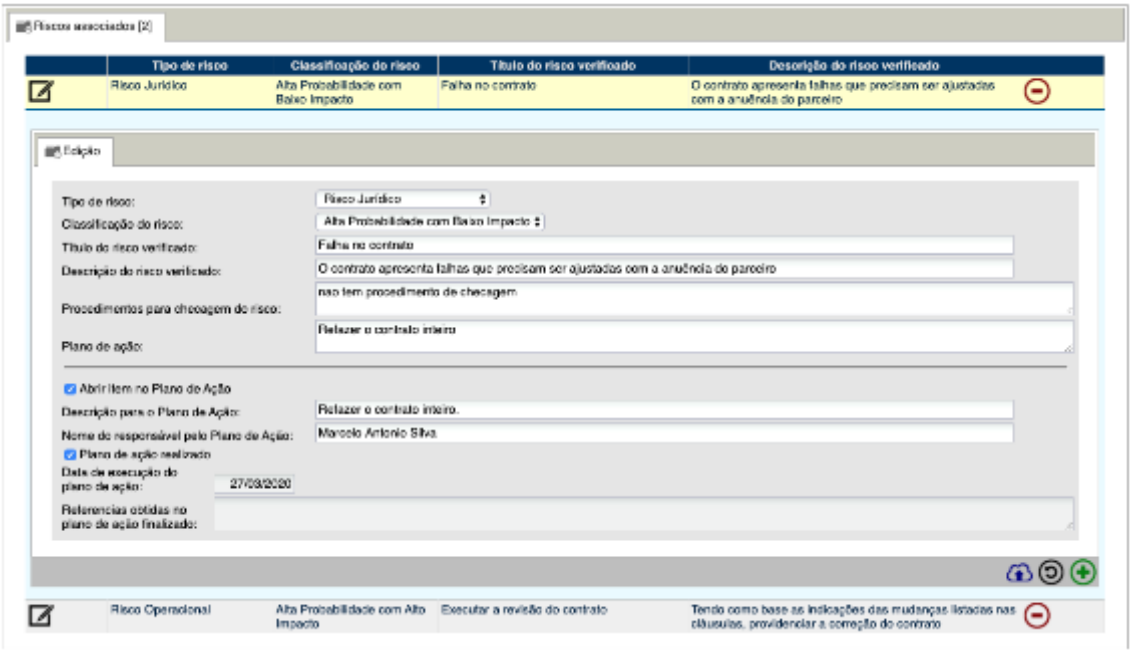
Cláusulas



Instruções de preenchimento

- Parágrafo: Informar qual o parágrafo do contrato que está sendo analisado.
- Cláusula original: Informar qual a cláusula original do parágrafo do contrato.
- Nova cláusula: Informa a nova cláusula para o parágrafo do contrato.

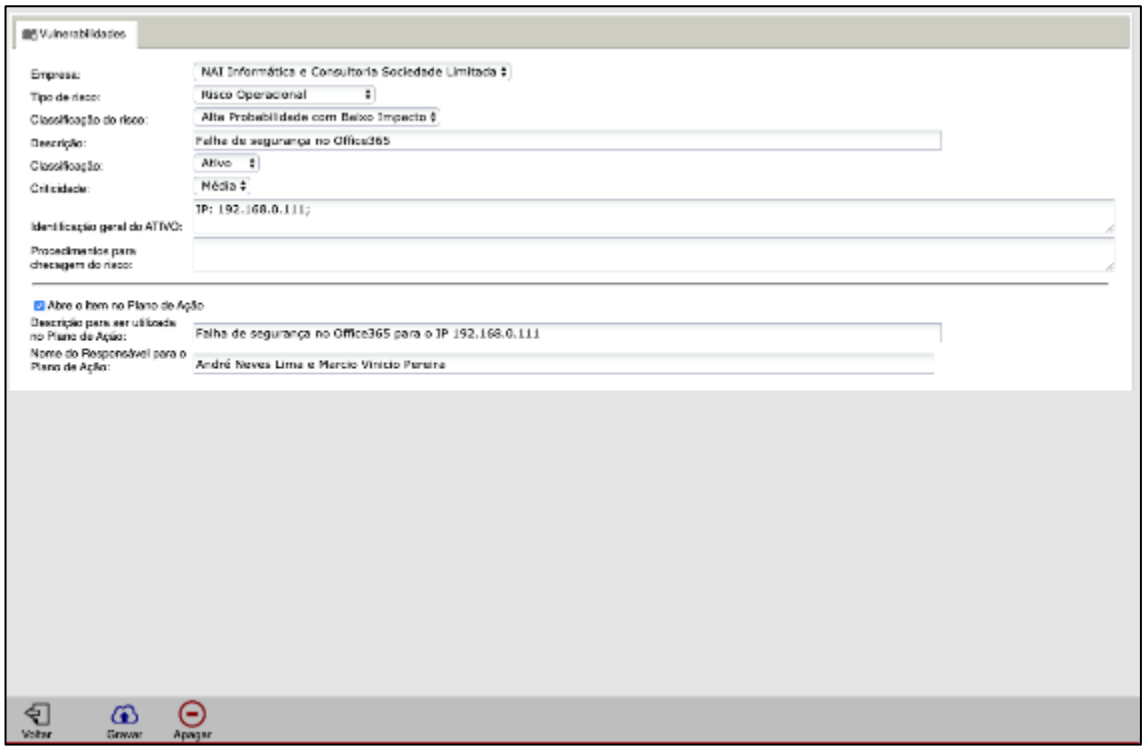
- Motivo para a mudança da cláusula: Descrever qual o motivo para a mudança da cláusula, destacando as informações obtidas na LGPD para que a mudança seja necessária.



Instruções de preenchimento

Seguir as instruções de preenchimento já citadas neste documento.

Formulários eletrônicos – Vulnerabilidades



Instruções de preenchimento

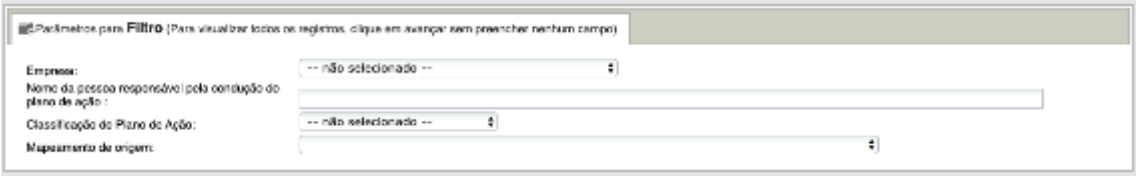
O preenchimento das vulnerabilidades poderá ser feito manualmente ou automaticamente a partir das empresas parceiras que disponibilizarem as APIs de integração automática de criação e manutenção dos itens.

- Empresa: selecionar na lista de opções qual a empresa que está sendo realizado o mapeamento.
- Tipo de risco: Selecionar na lista de opções qual o tipo de risco verificado para a vulnerabilidade.
- Classificação do risco: Selecionar na lista de opções qual a classificação do risco para a vulnerabilidade.
- Descrição: Informar qual a descrição da vulnerabilidade verificada.
- Classificação: Selecionar na lista de opções qual a classificação da vulnerabilidade.
- Criticidade: Selecionar da lista de opções qual a criticidade da vulnerabilidade.
- Identificação geral do ATIVO: Descrever qual a identificação completa do ATIVO que foi verificado a vulnerabilidade.
- Procedimento para checagem do risco: Descrever qual o procedimento para checagem do risco da vulnerabilidade.
- Abre item no Plano de Ação: Selecionar esta opção caso o risco verificado para a vulnerabilidade necessite te um item aberto no Plano de Ação.

- Descrição para ser utilizada no Plano de Ação: Informar qual a descrição a ser utilizada no Plano de Ação.
- Nome do responsável para o Plano de Ação: Informar qual o nome do responsável por tratar do Plano de Ação aberto para a vulnerabilidade.

Formulários eletrônicos – Plano de Ação

Plano de ação – Filtro dos itens cadastrados



Instruções de preenchimento

Uma tela inicial de filtro permite que sejam selecionados, de acordo com a intenção de uso, apenas os itens lançados no plano de ação que atendam aos critérios dos campos destacados para serem usados no filtro.

- Empresa: Filtra apenas os itens do plano de ação para a empresa selecionada.
- Nome da pessoa responsável pela condução do plano de ação: Filtra apenas os itens do plano de ação que foram indicados para tratamento pela pessoa listada.
- Classificação do plano de ação: Filtra apenas os itens do plano de ação para a classificação indicada no plano de ação.
- Mapeamento de origem: Filtra apenas os itens do plano de ação para os mapeamentos de origem (Processos, sistemas de coleta de dados, contratos, ativos, biometria, etc.)

Plano de ação – Relação dos itens cadastrados



		Empresa	Título do risco	Descrição do Plano de ação	Nome da pessoa responsável pela condução do plano de ação	Classificação do Plano de Ação	Mapeamento de origem
★	✎	NAI Informática e Consultoria Sociedade Limitada	Falha de segurança no ERP	Plano de ação verificado: [] Plano de ação a criar: [Falha de segurança no ERP para o IP 192.168.9.120 - mod]	Norberto Tordin - mod	Urgente e Importante	VULNERABILIDADES
	✎	NAI Informática e Consultoria Sociedade Limitada	Vazar informação	Plano de ação verificado: [Criar procedimento para validação] Plano de ação a criar: [Criar procedimento para validação dos acessos criados no MS AD]	André Neves Lima	Importante e Não Urgente	SISTEMAS_DESTINO
	✎	NAI Informática e Consultoria Sociedade Limitada	Falha de segurança no Office365	Plano de ação verificado: [] Plano de ação a criar: [Falha de segurança no Office365 para o IP 192.168.0.111]	André Neves Lima e Marsio Vinício Pereira	Importante e Não Urgente	VULNERABILIDADES
	✎	NAI Informática e Consultoria Sociedade Limitada	Acesso indevido de dados dos titulares	Plano de ação verificado: [Criar procedimento ou validar acesso controlado aos dados] Plano de ação a criar: [Criar procedimento para checagem das pessoas com autorização para recebimento de e-mail]	Norberto Tordin	Urgente e Importante	COMUNICACAO
	✎	NAI Informática e Consultoria Sociedade Limitada	Acesso indevido por ferramentas de BI	Plano de ação verificado: [Criar procedimento para instalar o acesso das ferramentas de BI para não permitir acesso a dados sigilosos] Plano de ação a criar: [Abrir uma senha no service desk para criar regras de controle de acesso e criptografia]	André Neves Lima e Marsio Vinício Pereira	Não Urgente e Não Importante	BANCO_DE_DADOS
	✎	NAI Informática e Consultoria Sociedade Limitada	Não temos o acesso ao servidor, o que impossibilita checar as vulnerabilidades de acesso	Plano de ação verificado: [Criar procedimento de checagem semanal dos acessos] Plano de ação a criar: [Solicitar relatório semanal de vulnerabilidades ao fornecedor]	André Neves Lima	Importante e Não Urgente	BANCO_DE_DADOS
	✎	NAI Informática e Consultoria Sociedade Limitada	Acesso indevido por VPN	Plano de ação verificado: [Criar procedimento para liberar o acesso de VPN fora do horário estipulado] Plano de ação a criar: [TI deve criar regras para validar os horários]	André Neves Lima	Não Urgente e Não Importante	BANCO_DE_DADOS
	✎	NAI Informática e Consultoria Sociedade Limitada	Falha de segurança no uso de equipamentos de terceiros	Plano de ação verificado: [] Plano de ação a criar: [Criar procedimento e regras para definir faixa de IP fixa para acesso]	Norberto Tordin	Urgente e Não Importante	VULNERABILIDADES
	✎	NAI Informática e Consultoria Sociedade Limitada	Usuários com acesso indevido ao sistema	Plano de ação verificado: [Contratar empresa para implementar a automação dos acessos] Plano de ação a criar: [Criar procedimento ou contratar empresa para cuidar da gestão dos acessos]	Paulo Roberto	Urgente e Não Importante	SISTEMAS_COLETA
	✎	NAI Informática e Consultoria Sociedade Limitada	Acesso indevido pela VPN	Plano de ação verificado: [Instalar controle de acesso] Plano de ação a criar: [Instalar no notebook controle de acesso da VPN]	André Neves Lima	Urgente e Importante	

		Empresa	Título do risco	Descrição do Plano de ação	Nome da pessoa responsável pela condução do plano de ação	Classificação do Plano de Ação	Mapeamento de origem
	✎	NAI Informática e	Não criar a conta do usuário	Plano de ação verificado: [Criar rotina de validação dos	Silvia Helena Martins	Importante e Não Urgente	SISTEMAS_COLETA

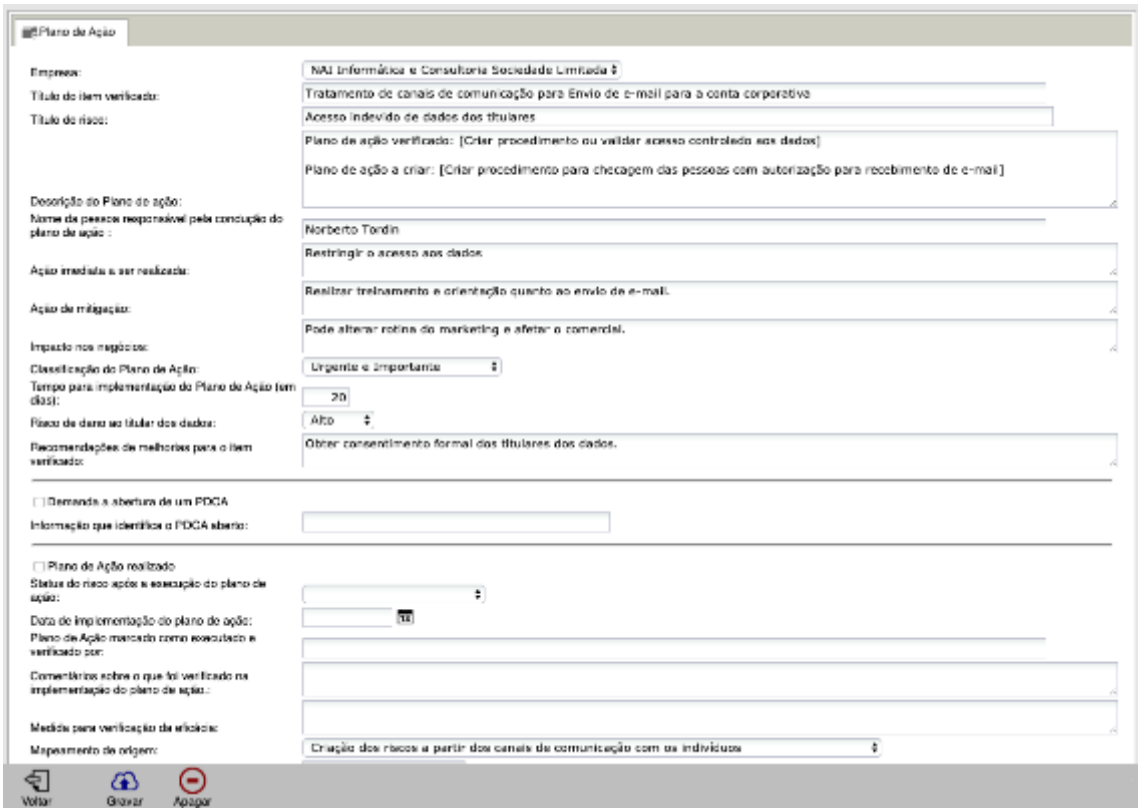
Voltar Atualizar Incluir Principal

Instruções de preenchimento

Após a passagem pela tela de filtro, apenas os itens do plano de ação que atenderem a combinação de itens do filtro serão apresentados.

Para editar um editem, clicar sobre o ícone localizado no lado esquerdo da tela (formulário com lápis).

Plano de Ação – Edição de um item cadastrado



Instruções de preenchimento

Algumas informações virão previamente preenchidas com base nos mapeamentos dos riscos para cada item de formulário eletrônico, conforme apresentado acima neste documento e que permitem a inclusão automática do risco verificado no plano de ação.

As demais informações deverão ser preenchidas:

- Ação imediata a ser realizada: Descrever qual a ação imediata a ser realizada para que o risco cadastrado no plano de ação seja resolvido.
- Ação de mitigação: Descrever qual a ação de mitigação que deverá ser realizada para que o risco cadastrado no plano de ação seja minimizado no impacto.
- Impacto nos negócios: Descrever qual o impacto que o risco cadastrado no plano de ação terá de impacto nos negócios da empresa.
- Classificação do plano de ação: Selecionar na lista de opções qual a classificação do plano de ação.
- Tempo para implementação do plano de ação: Informar qual o tempo desejado para que o plano de ação seja implementado.
- Risco de dano ao titular dos dados: Selecionar na lista de opções qual o risco de dano que o risco cadastrado terá ao titular dos dados.
- Recomendações de melhorias para o item verificado: Descrever quais as recomendações de melhoria para o risco cadastrado no plano de ação.

- Demanda abertura de um PDCA: Caso o profissional que estiver fazendo a análise do plano de ação verifique a necessidade de ampliar o tratamento do plano de ação deverá selecionar esta opção.
    - Ao marcar esta opção automaticamente será aberto uma ocorrência no software para tratamento detalhado do plano de ação. Neste software haverão os controles designados para que sejam definidas as causas raiz (Teorema de Ishikawa), os planos de implementação e verificação de eficácia, para cada causa raiz registrada para tal finalidade.
- Informação que identifica o PDCA aberto: Informação que será inserida no PDCA para relacionamento e integração das informações.
- Plano de ação realizado: esta opção SOMENTE deverá ser marcada quando o plano d ação for finalizado, seja por tratamento nesta tela, seja por ocorrência do PDCA.
- Status do risco após a execução do plano de ação: Deverá ser selecionado na lista de opções qual o status do risco após a execução do plano de ação.
- Data de implementação do plano de ação: Informar qual a data que o plano de ação foi implementado.
- Plano de ação marcado como executado e verificado por: Informar quem foi o responsável pela finalização do plano de ação.
- Medida para verificação de eficácia: Descrever, para os itens que forem necessários, qual a medida para verificação da eficácia.
- Mapeamento de origem: Esta informação virá preenchida dos mapeamentos previamente realizados.
- Data de criação do item: Esta informação virá preenchida dos mapeamentos previamente realizados.