CMPD – COMISSÃO MUNICIPAL DE PROTEÇÃO DE DADOS

WORKSHOP – 20/04/2023

LGPD – LEI GERAL DE PROTEÇÃO DE DADOS

DADO PESSOAL

Informação relacionada a pessoa natural identificada ou identificável. Exemplo: Nome, Endereço, Email, Identidade, CPF, dados de localização.

DADO PESSOAL SENSÍVEL

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

TRATAMENTO

Toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Documentação do Controlador que contém a descrição dos processos de tratamento de dados pessoais, que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Vigente desde o dia 18 de setembro de 2020 a Lei Geral de Proteção de Dados Pessoais (LGPD) estabeleceu um regulamento sobre a forma como as empresas/órgãos públicoss/órgãos públicos devem armazenar e tratar os dados pessoais de seus clientes, o que serve para proteger melhor a privacidade no mundo digital.

Essa lei ganhou legitimidade constitucional em fevereiro de 2022, uma vez que a proteção de dados pessoais se tornou um direito fundamental. Dessa forma, nos últimos anos iniciou-se uma corrida no meio da iniciativa privada para se adequar à nova lei e evitar as sanções penais da LGPD.

COMO FAZER O MAPEAMENTO DE DADOS DA LGPD?

Elaborar um mapeamento de dados ou data flow significa descobrir quais são os dados que a empresas/órgãos públicos coleta, tanto de seus funcionários e parceiros quanto dos clientes,

identificar quais são as pessoas que têm acesso a eles e qual o tratamento que eles recebem uma vez que foram armazenados. É evidente que, sem um mapeamento cuidadoso, o restante do processo de adequação será ineficiente.

Dessa forma, o objetivo do presente artigo consiste justamente em explicitar, em algumas etapas, como se faz um mapeamento de dados em vista da adequação à LGPD. Além disso, aqui também está exposto um quadro acerca dos tipos de dados e da importância de cada um deles.

A INFLUÊNCIA DA LGPD NA GESTÃO DE DADOS

Exemplificando, antes da LGPD, os dados pessoais poderiam ser coletados indiscriminadamente, apenas com um consentimento genérico do titular. Hoje em dia, por outro lado, o consentimento diz respeito à finalidade específica da coleta.

Isso faz com que seja essencial ter um controle sobre cada dado coletado e que a finalidade da coleta dele esteja clara, para que seja deletado o quanto antes após cumprir sua função.

A influência da LGPD, portanto, é a necessidade de criação de um sistema para análise e controle das informações pessoais que determinada empresas/órgãos públicos armazena, o que visa garantir a segurança dos dados e a privacidade de seus titulares.

Sabe-se que o processo de adequação é longo e moroso. No entanto, é possível fracioná-lo em algumas etapas essenciais. Dentre elas destaca-se o mapeamento de dados que é justamente a parte do processo em que se estabelece o controle inicial sobre os dados coletados.

QUAL A IMPORTÂNCIA DO MAPEAMENTO DE DADOS?

A importância do mapeamento de dados consiste em ser um relatório do caminho que todos os dados percorrem uma vez que tenham sido coletados pela empresas/órgãos públicos. Esse processo resultará em um inventário de dados, a partir do qual será possível manter um controle do fluxo dos dados de todos os clientes e parceiros, bem como traçar um plano de ação para a adequação à LGPD.

Ademais, uma vez feito o mapeamento a empresas/órgãos públicos ganhará maior credibilidade e transparência, porquanto poderá fornecer a seus clientes informações sobre todo o tratamento que os dados deles recebem dentro da empresas/órgãos públicos.

QUAIS SÃO OS DADOS PROTEGIDOS PELA LGPD?

A LGPD dispõe sobre o tratamento de dados pessoais, os quais, de acordo com a lei, são classificados em dados pessoais sensíveis ou não-sensíveis.

Assim, considera-se que o dado pessoal seja "uma informação relacionada a pessoa natural identificada ou identificável"; e, por outro lado, que o dado pessoal sensível seja "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural."

A principal diferença entre esses dois tipos de dados é a intensidade de regulamentação que a lei impõe: os dados sensíveis estão mais rígidamente protegidos, de forma que devem ser manejados com o máximo de cuidado possível.

COMO ELABORAR UM MAPEAMENTO DE DADOS?

Em primeiro lugar deve-se reunir um time de pessoas que conheçam toda a estrutura interna, de outra forma o inventário de dados não terá correspondência com a realidade. Outro elemento necessário na equipe será alguém com os conhecimentos técnicos e jurídicos necessários para resolver as inadequações encontradas.

Ademais, mesmo que o inventário de dados possa ser feito em uma planilha e sem ajuda externa.

- Identificação dos dados

Após a estruturação de um time, deve-se analisar as seguintes questões quanto aos dados coletados pela empresas/órgãos públicos:

1. Quais dentre eles são protegidos pela legislação;
2. Quem terá acesso a eles;
3. Onde serão armazenados;
4. Que tipo de proteção digital recebem;
5. Como será feita a destruição desses dados;
6. Como funcionará o fluxo desses dados dentro da empresas/órgãos públicos;
7. Qual a origem dos dados;
8. Com qual finalidade foram coletados.

- Elaboração do fluxograma

Ressalta-se que o inventário de dados resultante deve ser preciso, conter descrições sobre todos os processos aos quais são submetidos os dados e estar constantemente atualizado. Vale lembrar também que o data flow não deve ser pensado apenas em vista dos dados que a empresas/órgãos públicos coletou até hoje, mas também em vista dos dados dos futuros clientes.

- Análise em relação à LGPD

De acordo com o Art. 6 da LGPD, há certas condições específicas sob as quais se deve operar para o tratamento de dados pessoais. À título de exemplo:

1. Os dados coletados devem obedecer à estrita finalidade do propósito informado ao seu titular;
2. O tratamento dos dados é limitado ao mínimo necessário para a realização de suas finalidades;
3. O tratamento deve ser compatível com as finalidades informadas ao titular;

Desse modo, o último passo do mapeamento de dados em vista da adequação à LGPD consiste justamente em procurar as inadequações, ou seja, descobrir quais são os tratamentos dispensáveis, quais os dados armazenados sem propósito, qual o contraste entre a finalidade para que foram coletados e sua real utilização, etc...

DATA DISCOVERY E MAPEAMENTO DE DADOS

Você já ouviu falar em data discovery?

Trata-se de um processo utilizado para melhorar a coleta de dados e otimizar os processos de análise. Em suma, é uma abordagem que permite a apreensão mais eficiente de padrões em meio a grandes volumes de dados, ou seja, é um processo que pode ser articulado em conjunto com o mapeamento e trazer benefícios à sua empresas/órgãos públicos.

Em geral, pode-se dividir o data discovery em três partes: primeiro, a preparação; depois, a análise visual; e, por fim, a análise guiada.

O data discovery consiste em uma busca direcionada para os dados que contenham determinados atributos. Assim, pode-se utilizar esse processo para identificar os dados relacionados à adequação LGPD e facilitar o mapeamento.

Isso porque existem diversas empresas/órgãos públicoss/orgaos publicos/órgãos que, mesmo tendo um processo de tratamento automatizado, por vezes não diferenciam os dados, o que resulta na movimentação desnecessária de informações e um prejuízo para a parte organizacional.

Recomenda-se a utilização de softwares para o data discovery, visto que pode facilitar a adequação à LGPD e a gestão de dados dentro da empresas/órgãos públicos.

O mapeamento de dados exige uma qualificação técnica, por isso recomenda-se o auxílio de uma consultoria jurídica personalizada para o processo.

O que deve ser registrado em um Inventário de Dados Pessoais

Um inventário de dados pessoais deve ser abrangente para garantir a conformidade com a LGPD, discriminando todos os dados pessoais coletados e seu caminho (fluxo) dentro e fora da instituição. No entanto, os registros não precisam ser feitos em um único documento. O inventário pode ser segmentado para discriminar dados pessoais de um único produto/projeto/sistema/titular ou um tipo específico de dados, especialmente em situações complexas. Mas o que deve ser registrado no inventário? Listo, a seguir, alguns dados que são primordiais:

1) Como os dados são coletados?

As instituições precisam identificar como e onde os dados pessoais estão sendo coletados: via formulário online, formulário em papel, fontes de dados externas, dentre outros. É preciso entender quais informações estão sendo coletadas de quais fontes e quais são as obrigações em relação a essa coleta de dados sob o aspecto da LGPD.

2) Quais dados são coletados?

É importante que as instituições tenham uma compreensão completa e clara de todos os dados pessoais que possuem em seu poder. Estes podem ser de clientes, cidadãos, visitantes, funcionários e qualquer pessoa natural que tenha relação com a instituição.

3) Onde os dados são armazenados? Qual é o formato dos dados?

Para que uma instituição tenha um entendimento adequado de suas práticas de privacidade de dados, é necessário saber onde esses dados estão armazenados e em que formato são mantidos. A maioria das instituições armazena informações eletronicamente, mas muitas podem continuar

a ter registros em papel ou os funcionários podem imprimir arquivos contendo dados pessoais para uso próprio. Mesmo os registros eletrônicos precisam de um exame aprofundado, pois podem ser armazenados na nuvem, em servidores locais, computadores locais ou até mesmo em equipamentos de fornecedores terceirizados.

4) Para onde vão os dados?

As instituições precisam saber para onde seus dados estão indo, tanto internamente quanto externamente, parceiros e fornecedores. Também é importante prestar atenção se os dados cruzam fronteiras internacionais, situação em que se deve tomar cuidados adicionais.

5) Para que são usados os dados?

As instituições precisam conhecer suas atividades de tratamento de dados pessoais tanto para fornecer divulgações precisas aos titulares – que têm seus direitos discriminados no art. 18 da LGPD – quanto para cumprir os requisitos de necessidade de registro das operações de tratamento previstos no artigo 37 da LGPD.

É fundamental definir a hipótese de tratamento (arts. 7º e 11), a finalidade e a previsão legal, principalmente se a hipótese de tratamento for para cumprimento de obrigação legal ou regulatória. Nesse caso, a previsão legal deve indicar a Lei, Decreto, normativo ou regulamento que respalda a finalidade e a hipótese de tratamento.

O inventário também permite que as instituições sejam capazes de demonstrar privacidade desde a concepção (*privacy by design*) do produto ou serviço (art. 46, § 2º) e minimização de dados, consagrado pelos princípios da necessidade e adequação, para atendimento à finalidade declarada. Se a instituição identificar a necessidade de ajuste na coleta para atingir o princípio da minimização dos dados pessoais tratados ou mesmo incompatibilidades de adequação à finalidade do tratamento de dados, uma boa prática é sanar imediatamente no serviço/produto/processo essas não conformidades.

6) Por quanto tempo os dados são mantidos?

A retenção de dados é outra área importante da privacidade desde a concepção (*privacy by design*) e minimização de dados. Embora a maioria dos inventários de dados pessoais foque em sua coleta e compartilhamento, uma visão abrangente deve incluir também quando os dados serão eliminados (ou anonimizados), fechando o seu ciclo de vida dentro da instituição.

7) Quais as medidas de segurança e privacidade aplicadas?

A instituição deve identificar as atuais medidas de segurança e técnicas administrativas implementadas, além da descrição dos controles que visam assegurar a confidencialidade, integridade e disponibilidade dos dados pessoais, minimizando os riscos como perda ou vazamento de dados.

O inventário de dados e seu relacionamento com o Relatório de Impacto à Proteção de Dados Pessoais

Ter uma visão geral de todos os inventários de dados pessoais elaborados é fundamental para a instituição, pois facilita a rápida localização de um serviço/processo inventariado, além de permitir um rápido atendimento a uma requisição do titular.

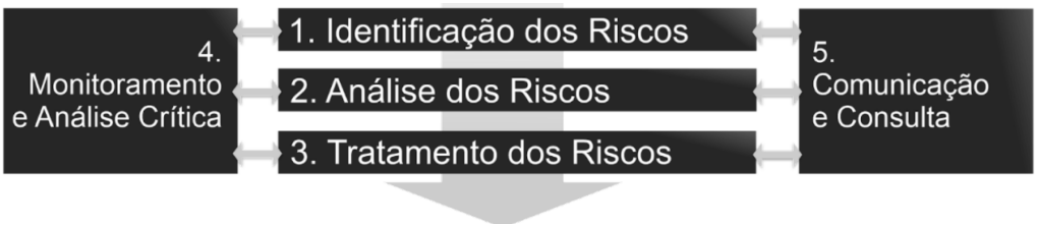
O IDP versa sobre o registro das operações de tratamento dos dados pessoais realizadas pela instituição, dando um retrato exato de como é feito o tratamento para cada serviço/processo/produto. Assim, essas informações se tornam insumos para a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que é um instrumento capital para comprovação da conformidade à LGPD, assim como para que o controlador possa constatar as medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

Mas o inventário de dados não é uma tarefa simples, como vimos. Nesse sentido, a Secretaria de Governo Digital do Ministério da Economia (SGD/ME) criou um guia detalhado, com exemplos e modelos, para orientar a elaboração inventário de dados pessoais, definindo características e um processo para elaboração, que pode ser utilizado como referência para esse árduo trabalho.

Por fim, o inventário é fundamental para que o controlador materialize o princípio da responsabilização e prestação de contas (art. 6º, X), um dos pilares da LGPD. Além de estar em conformidade, as instituições precisam comprovar que os processos em vigor demonstram o comprometimento da organização com a privacidade e proteção dos dados pessoais.

Processo de Gestão de Riscos

O Processo de Gestão de Riscos adotado pela Unicamp, tem como referência os modelos de gestão descritos na ABNT NBR ISO 31000 de 2018 e no Guia PMBOK 6ª Edição. As atividades e ferramentas, descritas nos modelos supracitados, foram adaptadas para garantir melhor aderência às especificidades da Universidade, buscando um nível de gerenciamento de riscos eficiente e com o menor impacto na autonomia gerencial das unidades administrativas, hospitalares, Faculdades, Institutos, Centros e Núcleos.



1. Identificação dos Riscos

A identificação dos riscos tem como objetivo elencar todos os riscos identificados e que possam impactar de forma negativa, na conformidade do processo em relação à Lei Geral de Proteção de Dados (LGPD). A utilização de informações pertinentes e atualizadas são importantes para a eficiência dessa atividade, bem como a identificação dos riscos fora do controle da organização (ABNT, 2018).

1.1. Definir Responsáveis

A definição dos responsáveis consiste na identificação do responsável pelo tratamento do risco. Dessa forma, cada atividade, que presenta o tratamento definido para determinado risco, deve ter obrigatoriamente um único Responsável.

1.2. Realizar Coleta de Dados

Concomitante ao processo *1.1. Definir Responsáveis* será realizada a coleta de informações para definição da lista de riscos. Para essa atividade devem ser utilizadas ferramentas para ampla discussão e que auxiliem na identificação dos riscos para cada processo, tais como as previstas no Guia PMBOK (6ª Edição):

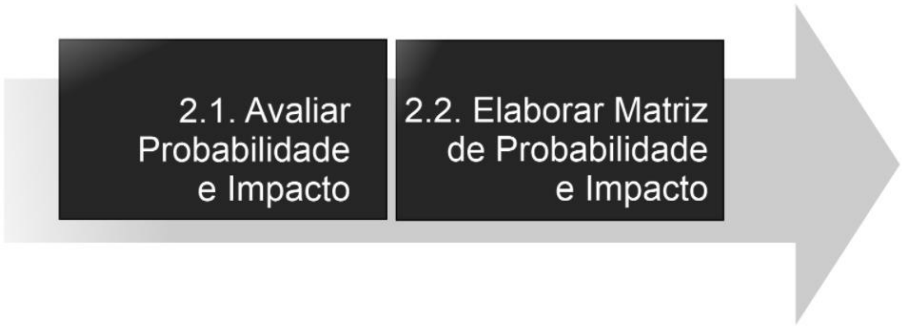
- Brainstorming: Identificar os riscos e suas fontes em reuniões com equipe multidisciplinar de especialistas, contando com a orientação de um facilitador.
- Entrevistas: Identificar os riscos em reuniões com partes interessadas, especialistas ou pessoas com experiência no processo. Garantir um ambiente de confiança e confidencialidade para coleta de informações mais precisas.

As ferramentas descritas acima, devem considerar a seguinte lista de categorias de riscos:

- Acesso não autorizado;
- Modificação não autorizada;
- Perda;
- Roubo;
- Remoção não autorizada;
- Coleta excessiva;
- Informações insuficientes sobre a finalidade do tratamento;
- Tratamento sem consentimento do titular dos dados pessoais;
- Falha em considerar os direitos do titular dos dados pessoais;
- Compartilhar ou distribuir dados pessoais com terceiros; Retenção prolongada de dados pessoais sem necessidade;
- Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular;
- Falha ou erro de processamento;
- Reidentificação de dados peseudonimizados.

2. Análise dos Riscos

A análise dos riscos consiste em aprofundar o nível de compreensão em relação à natureza dos riscos, bem como o nível do impacto nos objetivos dos processos. A utilização de método semiquantitativo adotada, garante amplo entendimento das probabilidades e dos impactos de cada risco com base em uma escala pré definida, deixando a análise mais objetiva e padronizada.



2.1. Avaliar Probabilidade e Impacto

A escala de Probabilidade e Impacto são definidas em 4 níveis, descritos a seguir:

Probabilidade

- Insignificante: Não existem informações que indiquem a ocorrência.
- Limitado: Existem poucos indícios que indiquem a ocorrência;
- Significante: Existem registros históricos de grande repetição ou indício forte que apontam para a possibilidade de ocorrência.
- Máximo: As evidências apontam para a garantia quase certa de ocorrência.

Impacto

- Insignificante: Impacto mínimo no processo;
- Limitado: Impacto discreto sem representar ameaça aos objetivos;
- Significante: Impacto direto nos objetivos com grande dificuldade de recuperação;
- Máximo: Impacto grave que inviabiliza a possibilidade de recuperação.

1.2. Elaborar Matriz de Probabilidade e Impacto

A Matriz de Probabilidade e Impacto será elaborada com base nas informações coletadas em *2.1. Avaliar Probabilidade e Impacto*, considerando a seguinte relação:

Máximo	10	40	80	100
Significante	8	32	64	80
Limitado	4	16	32	40
Insignificante	1	4	8	10
	Insignificante	**Limitado**	**Significante**	**Máximo**

Cada risco deve ser classificado entre RB (Risco Baixo), RM (Risco Médio) e RA (Risco Alto), dessa forma as ações serão planejadas com base no nível de criticidade identificado:

- **RB (Risco Baixo):** Aceitar riscos e manter ações de monitoramento;
- **RM (Risco Médio):** Gerenciar riscos e manter monitoramento das ações de tratamento;
- **RA (Risco Alto):** Exige grande esforço para gerenciamento dos riscos e acompanhamento extensivo das ações de tratamento. Considere a execução constante do processo "4. Monitoramento e Análise Crítica".

3. Tratamento dos Riscos

O tratamento dos riscos é uma atividade para identificação e definição de estratégias e planejamento de ações para lidar com a exposição aos riscos (Guia PMBOK 6ª edição). As ações definidas devem visar o objetivo principal dos processos dentro do contexto da LGPD, buscando a conformidade com a legislação vigente.

3.1 Planejar as Resposta

As ações planejadas devem ser realistas em relação à disponibilidade de recursos humanos, financeiros e de prazo. O responsável pelo processo deve garantir a qualidade das ações definidas, realizando o acompanhamento e as alterações necessárias, sempre que identificadas.

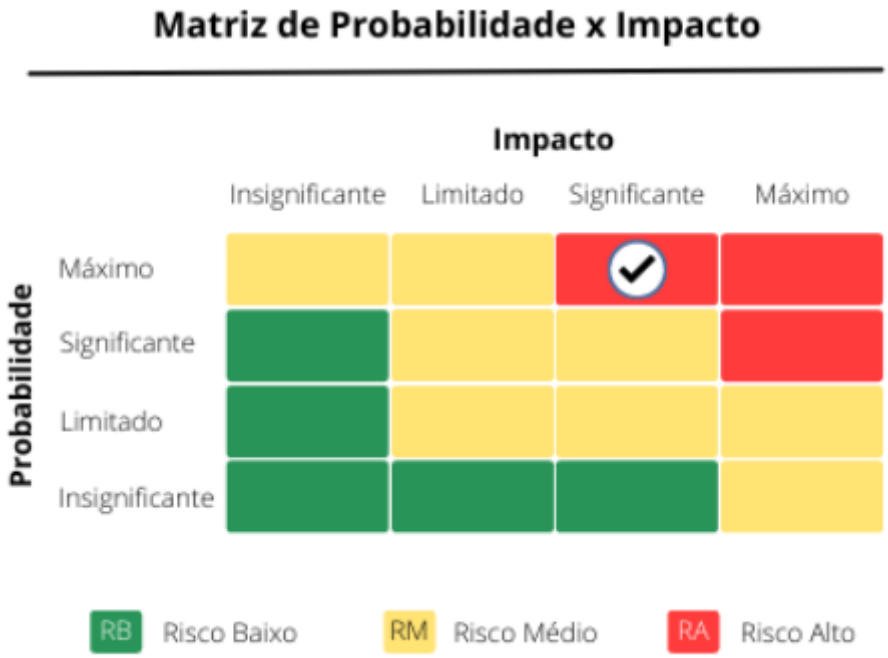
A descrição de cada ação deve ser norteada por uma das 4 categorias, descritas a seguir:

Prevenir: Alterar o processo, deixando de executar a atividade que representa o risco identificado;

Transferir/Compartilhar: Transferir parcialmente ou integralmente o risco para terceiros;

Mitigar/Melhorar: Reduzir o impacto e/ou a probabilidade de ocorrência do risco para níveis aceitáveis;

Aceitar: Definir se a aceitação do risco será de forma passiva, não sendo necessária nenhuma ação, ou ativa, definindo reservas de contingência financeiras, de prazo ou de recursos humanos.



Matriz de Probabilidade x Impacto – Sistema de Gestão de Riscos para LGPD Unicamp

Plano para Tratamento dos Riscos

O conjunto de informações definidas nos processos 1. Identificação dos Riscos, 2. Análise dos Riscos e 3. Tratamento dos riscos resultam no plano para tratamento dos riscos, com o propósito de especificar "como as opções de tratamento escolhidas serão implementadas, de maneira que os arranjos sejam compreendidos pelos envolvidos e o progresso em relação ao plano possa ser monitorado" (ABNT, 2018).

4. Monitoramento e Análise Crítica

O Monitoramento e Análise Crítica tem como objetivo garantir o bom andamento dos planos definidos. Nesta etapa, os responsáveis devem "assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo" (ABNT, 2018). As atividades descritas a seguir podem ocorrer sempre que necessário, concomitantemente ou isoladamente, conforme exigência da situação identificada pelos responsáveis.

4.1. Reavaliar Riscos

Revisar os riscos mapeados para atualizar as informações com novos riscos identificados, atualização de riscos já descritos e exclusão de riscos desatualizados.

4.2. Realizar Auditoria

Examinar o desempenho do processo de gestão de riscos e das ações adotadas para tratamento dos riscos identificados.

4.3. Realizar Análise Crítica

Realizar a análise dos riscos e de seus tratamentos. A equipe responsável, nos diferentes níveis de gestão, deve realizar auto avaliação, na busca contínua por melhorias dos processos de trabalho e nos dados cadastrados.

4.4. Medir Desempenho

Comparar o desempenho técnico do andamento das ações definidas frente ao planejamento realizado nas etapas anteriores.

5. Comunicação e Consulta

O processo de comunicação e consulta é executado de forma permanente com ações, partindo da divulgação dos planos para gestão dos riscos até o resultado final dos tratamentos identificados e executados, para cada risco dos processos. “A comunicação busca promover a conscientização e o entendimento do risco, enquanto a consulta envolve obter retorno e informação, para auxiliar a tomada de decisão” (ABNT, 2018).

5.1. Realizar Ampla Divulgação

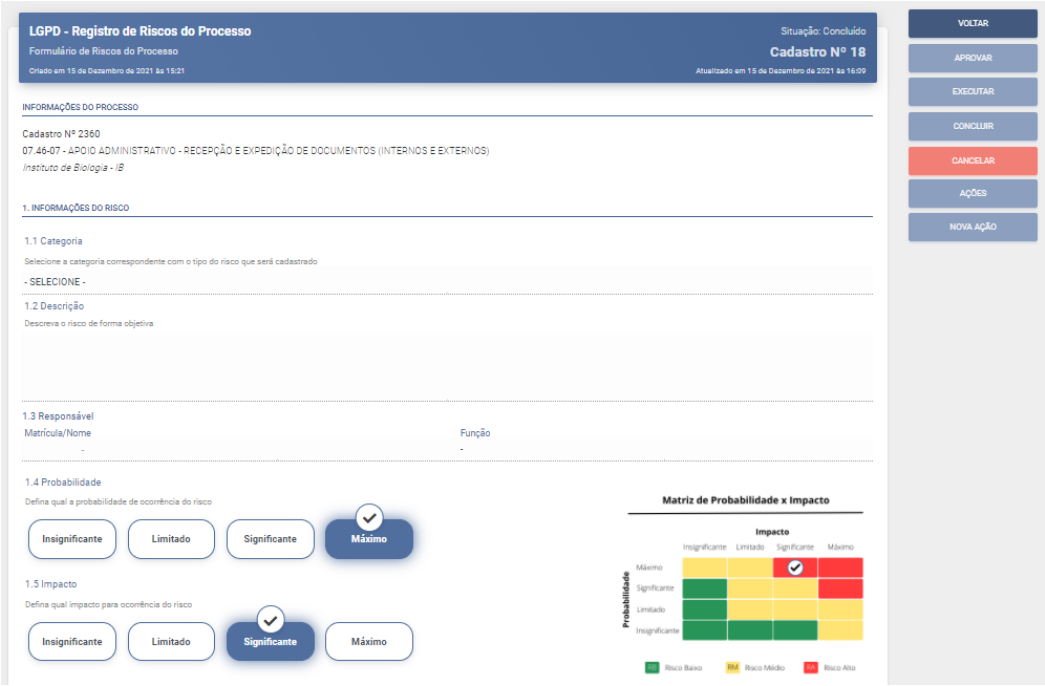
Consiste na criação de documentação para orientação de toda comunidade tais como: Instrução Normativa; Plano de Gestão de Riscos; Política de Gestão de Riscos; Sítio eletrônico informativo; Oficinas de capacitação, entre outros.

5.2. Coletar Retorno dos Interessados

Criar canais de comunicação para coletar informações sobre a eficiência do plano de gestão de riscos na perspectiva da comunidade. A transparência, confidencialidade e a garantia de privacidade dos colaboradores devem ser princípios fundamentais para a execução dessa atividade.

Sistema de Gestão de Riscos
Como suporte às iniciativas para conformidade com a Lei Geral de Proteção de Dados (LGPD), a Universidade faz uso do Sistema de Gestão de Riscos da Unicamp. O sistema tem como princípio fundamental a agilidade para cadastrar e consultar informações necessárias, para a execução do processo de gestão de riscos, contando com canais de comunicação para coleta sobre a experiência de uso, bem como para sugestões de adequação. Os recursos disponibilizados auxiliarão na definição das responsabilidades, cadastros de riscos, cadastrados dos tratamentos dos riscos, geração do Plano para Tratamento dos Riscos e na geração de indicadores para suporte à tomada de decisão para diversos níveis gerenciais.

Conteúdo



Fonte:

https://mittechreview.com.br/7-informacoes-que-nao-podem-faltar-no-inventario-de-dados-pessoais/

https://locusiuris.com.br/mapeamento-de-dados-da-lgpd/

https://privacidade.dados.unicamp.br/