MÉTODO RNP PARA ADEQUAÇÃO À LGPD

VERSÃO 1.0

RNP
ORGANIZAÇÃO SOCIAL DO MCTI
MINISTÉRIO DO TURISMO
MINISTÉRIO DA DEFESA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DAS COMUNICAÇÕES
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES
PÁTRIA AMADA BRASIL GOVERNO FEDERAL

APRESENTAÇÃO

1.0 COMO UTILIZAR O MÉTODO RNP

1.1 MÓDULO CULTURA DE PRIVACIDADE

1.2 MÓDULO PREPARAÇÃO

1.3 MÓDULO MAPEAMENTO DE DADOS E DE RISCOS

1.4 MÓDULO IMPLEMENTAÇÃO E ADEQUAÇÃO

1.5 MÓDULO SEGURANÇA E PROTEÇÃO DOS DADOS

1.6 MÓDULO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

APRESENTAÇÃO

Com a chegada da Lei nº 13.709, de 14 de agosto de 2018, mais conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), e com a necessidade das organizações estarem em conformidade, a Rede Nacional de Ensino e Pesquisa (RNP) desenvolveu um método para apoiá-las em seus projetos de adequação à LGPD, o "Método RNP para adequação à LGPD".

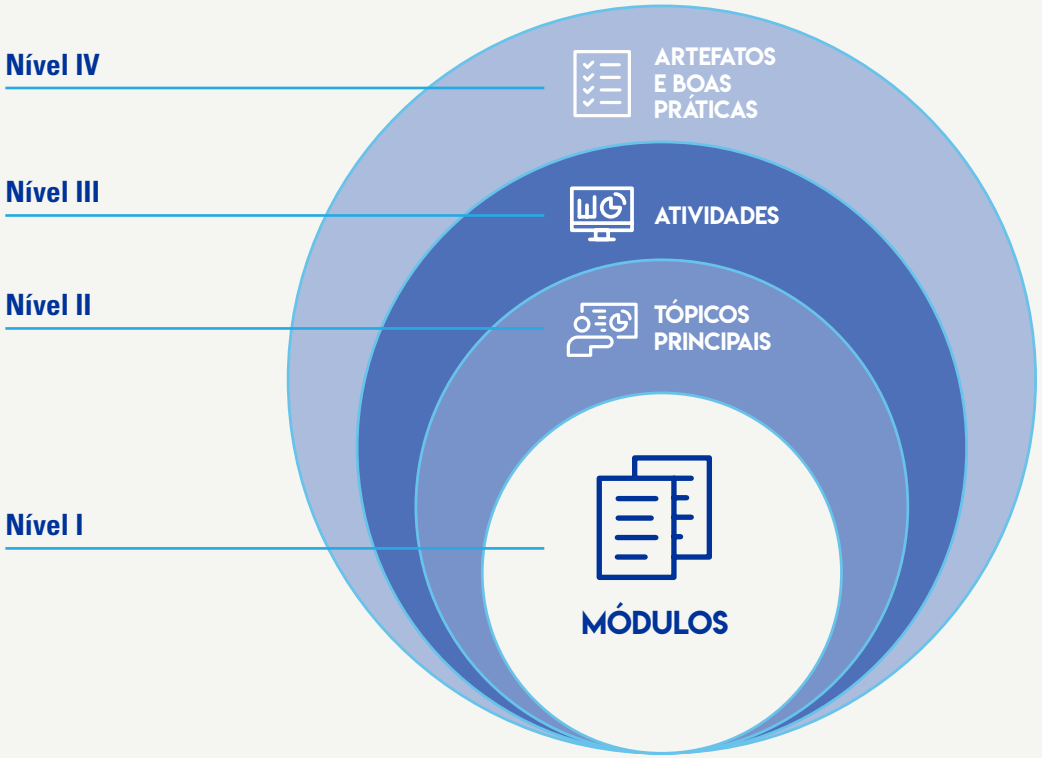
Este método objetiva, ainda, auxiliar as organizações na construção dos seus programas de governança em privacidade.

Durante a construção do **Método RNP** – como será chamado daqui em diante – foi considerada a diversidade das organizações contidas no Sistema RNP. Nesse sentido, este material visa apresentar de forma clara e objetiva, um ciclo de adequação à LGPD, de forma que ele possa ser aplicado, independente da maturidade de cada organização.

O Método RNP foi criado com base em 6 Módulos, onde cada um deles possui detalhamentos compreendidos em 4 diferentes Níveis que englobam as principais demandas para adequação à LGPD.

Nesta primeira versão do documento serão apresentados os Módulos (Nível I) e Tópicos Principais (Nível II) que compõem o Método. Na próxima versão, serão apresentadas as Atividades (Nível III) e as Boas Práticas e Artefatos (Nível IV), completando assim a proposta de adequação à LGPD pelo Método RNP, conforme **Figura 01**.

FIGURA 01:
APRESENTAÇÃO DO MÉTODO



Para um melhor entendimento, vale a pena detalhar que para cada **módulo** apresentado foram identificados os **tópicos principais** que representam e contemplam o conteúdo de adequação à lei. Além disso, para cada tópico, foram identificadas as **atividades** necessárias que as organizações poderão conduzir para estarem em conformidade com a legislação e finalmente, os **artefatos** e **boas práticas** compostos por documentos disponibilizados que poderão facilitar o processo de adequação.

Como explicado, percebe-se que o Método foi concebido para facilitar o entendimento sobre quais caminhos considerar e o que precisa constar em cada etapa para a adequação das organizações à LGPD.

Ressalta-se que o presente documento tem como objetivo apresentar os tópicos-chave que devem ser considerados em um projeto de adequação à LGPD.

COMO UTILIZAR O MÉTODO RNP

O Método RNP possui 4 Níveis que vão detalhando as informações, de acordo com o seu aprofundamento.

Os módulos do Método RNP são **cíclicos**, ou seja, a adequação é **contínua** e **incremental**. Dessa forma, não há uma ordem e nem um sequenciamento quanto às ações de adequação a serem seguidas por cada organização.

Tendo em vista que há organizações em diferentes estágios de adequação, o Método RNP pode ser visto como um direcionamento para o programa ou projeto de adequação à LGPD, considerando as especificidades de cada uma. Por exemplo, para as organizações que já fizeram um mapeamento de dados pessoais, o Módulo de Segurança e Proteção de Dados pode ser o foco principal; para outras, o foco pode ser o desenvolvimento da política de privacidade, que faz parte do Módulo de Implementação e Adequação.

Os 6 Módulos, que serão apresentados a seguir (Figura 02), englobam o conjunto de Tópicos Principais, Atividades, Artefatos e Boas Práticas necessárias para um processo de adequação.

Entretanto, como a própria imagem apresenta, não há a obrigatoriedade de se seguir uma sequência linear, o que torna o método mais flexível e dinâmico para as organizações, **conforme Figura 02**.

FIGURA 02:

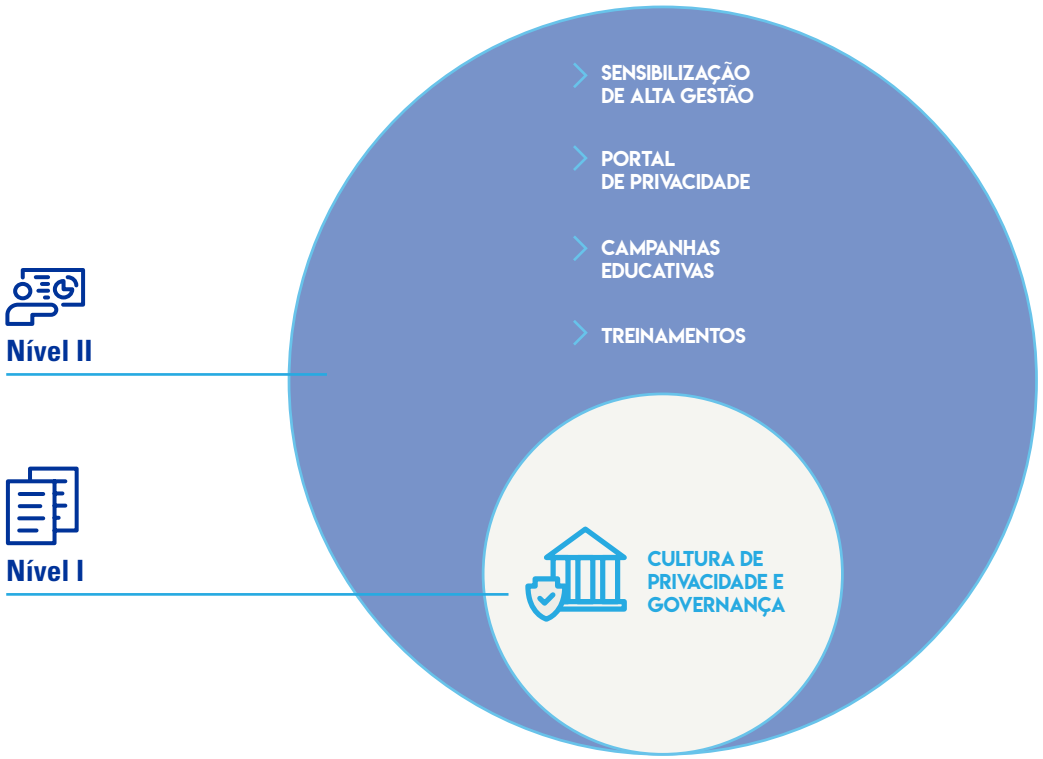
MÉTODO RNP DE ADEQUAÇÃO À LGPD: MÓDULOS

MÓDULO
CULTURA DE PRIVACIDADE

Um dos desafios, se não o maior, é estabelecer com efetividade uma nova cultura organizacional voltada para a proteção de dados pessoais dos titulares, envolvendo ativamente a participação de todos.

Considerar como as pessoas serão impactadas pelo processo de adequação,exigindo em alguns casos mudanças de comportamento, ou ainda definir qual a melhor estratégia organizacional para construir os pilares que sustentarão tais mudanças a curto, médio e longo prazo, são alguns dos pontos relevantes que fazem parte deste módulo. Dessa forma, este módulo refere-se ao conjunto de tópicos principais relacionados às pessoas. Serão apresentados a seguir os tópicos principais que nortearão este importante e desafiador processo.

FIGURA 03:
MÓDULO CULTURA DE PRIVACIDADE



Sensibilização da Alta Gestão

Qualquer processo de mudança de cultura organizacional ou mudança de comportamento, será facilitado se a alta gestão se comprometer com a "causa".

Assim quando ela conhece os princípios da LGPD, da mesma forma que conhece cada área da organização, e reconhece a importância de se desenvolver internamente uma cultura de privacidade e proteção de dados pessoais, e consequentemente compreende a necessidade de se buscar a conformidade com a lei, o processo de adequação tende a fluir melhor, **conforme Figura 04**.

FIGURA 04:

AÇÕES PARA SENSIBILIZAR A ALTA GESTÃO

Portal de Privacidade

O Portal da Privacidade pode ser criado por todas as organizações pois, conforme consta em lei, permite criar um espaço dedicado à comunicação e transparência, possibilitando um relacionamento com os titulares de dados. O objetivo do portal é conter informações sobre como a organização realiza o tratamento de dados pessoais, apontar os compromissos principais e gerais contidos na política de segurança, além de informar os canais de comunicação e procedimentos para o titular exercer seus direitos.

Adicionalmente, o art. 41 da LGPD, afirma que a identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

Para as organizações públicas, o Guia de Boas Práticas do Governo Federal enfatiza, em um dos seus capítulos, a questão da publicidade das informações referentes ao tratamento de dados de um órgão, tornando ainda mais relevante a construção de um portal de privacidade para cumprimento da legislação.

Ressalta-se que, na próxima versão do Método, serão apresentados maiores detalhes sobre como esse Portal de Privacidade poderá ser construído.

Campanhas Educativas

As campanhas educativas têm por objetivo oferecer informações corretas e atualizadas a um grande número de pessoas visando a conscientização e mudança de comportamentos.

Nesse sentido, são sugeridos alguns tópicos para compor as campanhas educativas:

- Informações gerais sobre o que é a LGPD e seus agentes de tratamento de dados
- Bases legais para tratamento dos dados previstos em lei
- Diferenças entre dados pessoais e dados pessoais sensíveis
- Dados pessoais do menor de idade: quais cuidados tomar
- Ciclo de vida dos dados: atenção em todas as fases
- Direitos do titular
- LGPD x LAI (Lei de Acesso à Informação)
- Compartilhamento e transferência de dados
- LGPD e Segurança da Informação
- Governança em Privacidade de Dados Pessoais
- Autoridade Nacional de Proteção de Dados: Qual o seu papel?
- *Privacy by Design*

Vale ressaltar que o Método RNP apresentará em seu Nível IV, a entrega de artefatos e boas práticas, além de modelos de banners educativos que ajudarão as organizações a disseminar informações e promover a conscientização e educação.

Treinamentos

Treinamento é o processo sistemático que pode promover uma mudança de comportamento dos profissionais, estimulando-os a agirem de forma mais correta em prol de um objetivo estabelecido.

Por ser uma prática de curta duração, serão apresentados dois tipos de treinamentos que poderão ocorrer no processo de adequação de uma organização, são eles:

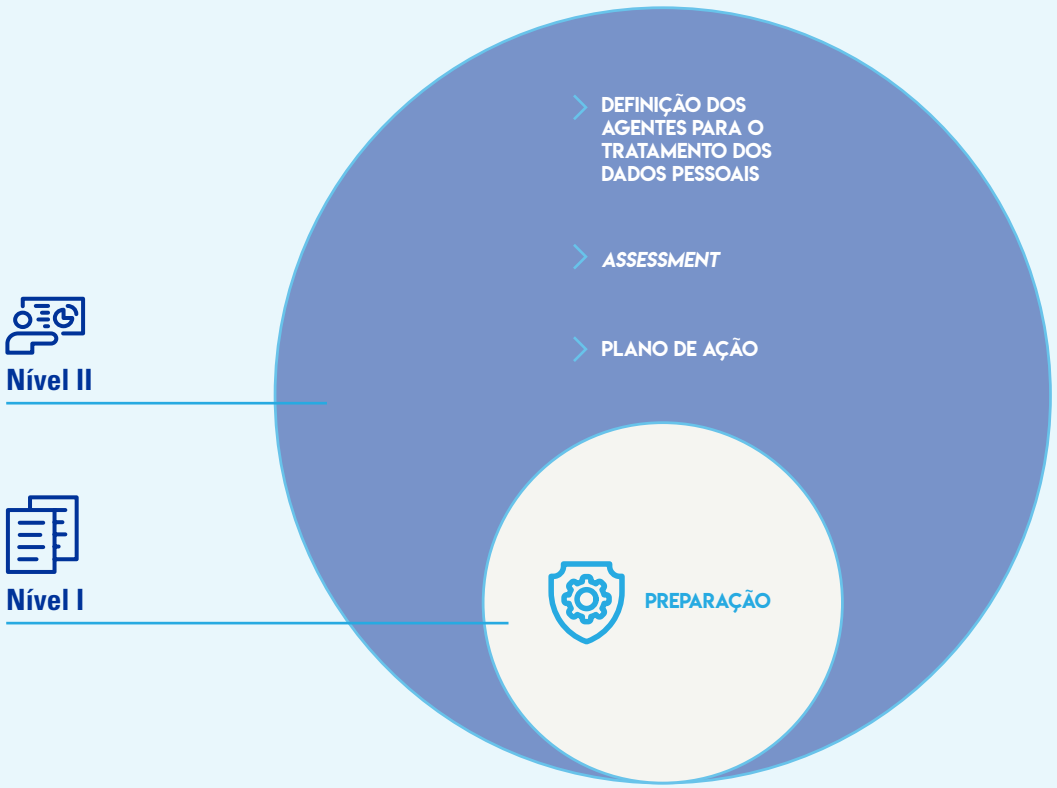
1. **Treinamentos gerais:** que visam à maximização do desempenho profissional quanto ao tratamento dos dados gerando maior conhecimento e consciência para a execução do trabalho.

2. **Treinamentos setoriais:** treinamentos específicos para a realidade de cada unidade de trabalho.

MÓDULO PREPARAÇÃO

Este Módulo compreende um levantamento de informações iniciais para que o processo de adequação aconteça. Nesse sentido, será possível identificar as condições preliminares para aplicação de um projeto, bem como, iniciar a adequação com informações suficientes para redução de erros que geram atrasos ou danos maiores.

FIGURA 05:
MÓDULO PREPARAÇÃO

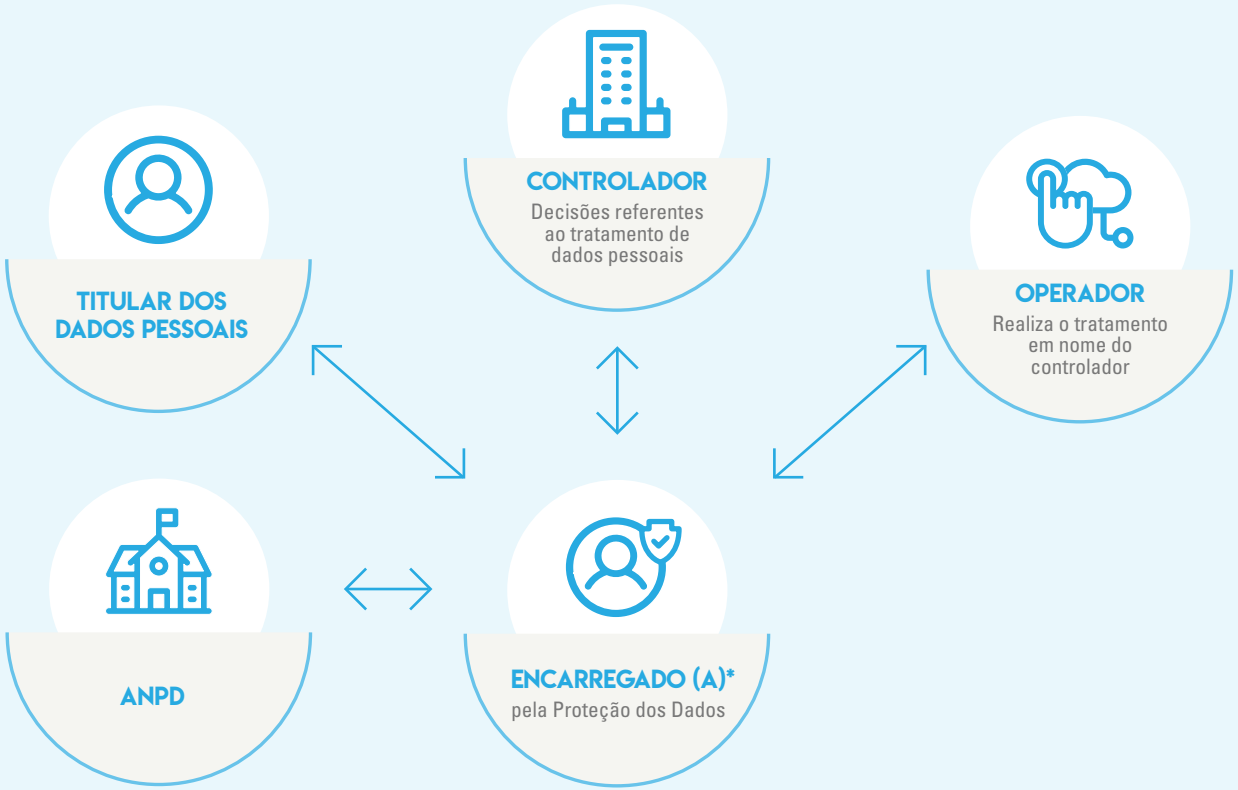


Definição dos Agentes para o Tratamento dos Dados Pessoais

Um dos agentes de tratamento da LGPD é o Encarregado pela Proteção de Dados Pessoais que é a pessoa física indicada pelo controlador para comunicação entre as partes. Além dele, a lei traz outros atores que são fundamentais em um processo de adequação, **conforme Figura 06 a seguir**.

FIGURA 06:

AGENTES DE TRATAMENTO DOS DADOS PESSOAIS



Assessment

O *Assessment* é um recurso indispensável para o entendimento do cenário interno, é por meio dessa atividade que é possível fornecer aos titulares uma análise completa sobre o tratamento dos dados pessoais na organização.

A ideia deste Tópico é promover o levantamento de informações das principais áreas que tratam dados pessoais e que poderão ter ações específicas para a adequação. Além disso, o assessment possibilita a tomada de decisão sobre os melhores instrumentos técnicos, tecnológicos e processuais que poderão ser adotados em cada ambiente avaliado.

Nesse sentido, o fluxo de atividades do *assessment* poderá acontecer da seguinte forma:

FIGURA 07:
FLUXO DO *ASSESSMENT*

Plano de Ação

O Plano de Ação é um documento utilizado para fazer um planejamento do trabalho necessário para atingir um resultado desejado ou, até mesmo, para a resolução de problemas. Para elaboração do Plano de Ação serão apresentadas opções de ferramentas estratégicas que auxiliarão a organização das informações que foram levantadas como também das ações que precisam ser executadas, como:

- Objetivo geral a ser alcançando com o plano de ações
- Data de início e fim previsto para cada ação ou atividade
- Orçamento alocado para cada ação ou atividade
- Responsável pela execução de cada ação
- Objetivos de cada ação ou atividade a ser executada

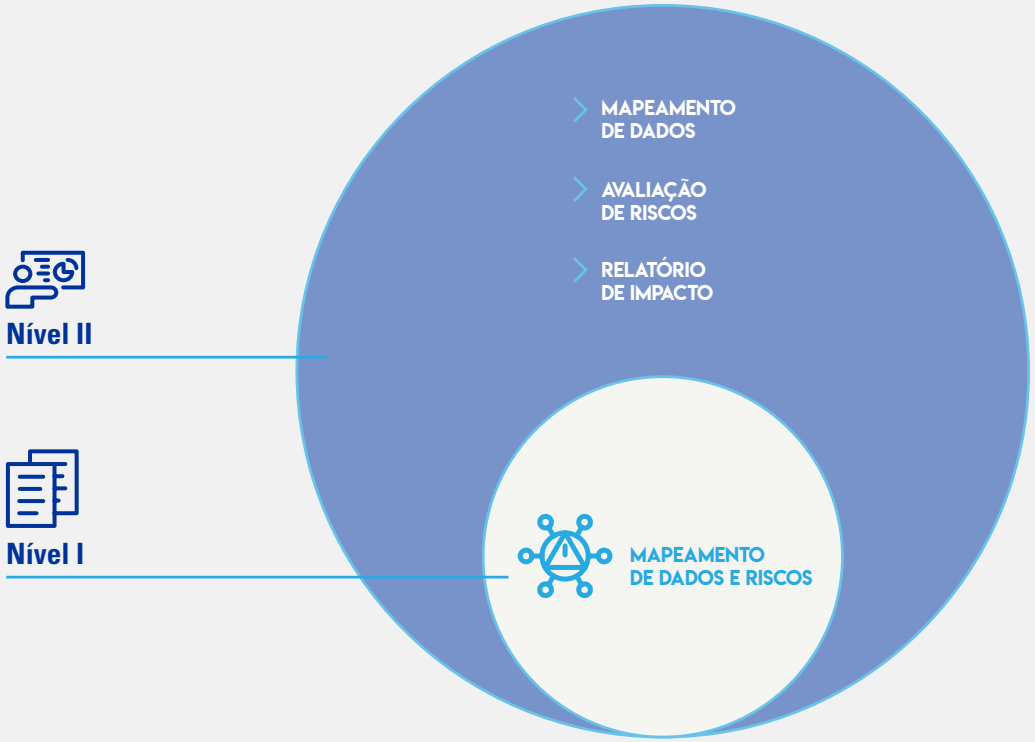
Nesse sentido, o Plano de Ação se torna tanto um documento interno orientativo quanto externo para a prestação de contas para a sociedade e órgãos de controle.

MÓDULO MAPEAMENTO DE DADOS E DE RISCOS

Fazer um mapeamento de dados e de riscos é primordial para que o processo de adequação evolua e consequentemente coloque a organização em conformidade com a LGPD. Neste Módulo serão apresentados três Tópicos que poderão tornar a leitura do cenário da organização ainda mais nítida, bem como, promover condições para analisar e propor as mudanças necessárias para a adequação.

FIGURA 08:

MÓDULO MAPEAMENTO DE DADOS E DE RISCOS



Mapeamento de Dados

O mapeamento é o processo pelo qual é possível conhecer de maneira aprofundada as atividades de tratamento de dados pessoais na organização. Isto é, entender quais dados pessoais são manipulados, por quem e por onde (incluindo sistemas) transitam, são processados e armazenados, identificando, em detalhes, os fluxos existentes dentro e fora da organização.

Também conhecido como *data mapping* ou inventário de dados, trata-se de um documento que contém não só os dados tratados pela organização, mas também a categorização desses dados.

COM ESSE DOCUMENTO, É POSSÍVEL VERIFICAR:

1. Quais dados são pessoais
2. O local onde estão armazenados
3. A forma com que foram coletados
4. Quem acessa e utiliza os dados
5. O tempo de retenção dos dados
6. A forma como os dados são tratados
7. E o lugar de processamento deles

Informações mais detalhadas que apoiem a construção desse documento, farão parte da próxima versão do Método RNP.

Avaliação de Riscos

A avaliação de riscos é um componente central da LGPD. O Artigo 50 da lei estabelece que as organizações devem levar em consideração, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos no tratamento dos dados. Para fazer isso, a organização precisa saber quais são seus riscos e a gravidade da ameaça, e é justamente a avaliação de risco que fornecerá essas informações.

O Método RNP detalhará, em sua próxima versão, como a avaliação de riscos pode ser utilizada para identificar e preencher as lacunas das áreas críticas da organização.

Relatório de Impacto

O relatório de impacto representa um documento fundamental a fim de demonstrar os dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados. Devido a tal importância, o Método RNP apresentará um modelo de relatório, em sua próxima versão, para que as organizações possam ter mais controle sobre o tratamento dos dados pessoais coletados.

MÓDULO IMPLEMENTAÇÃO E ADEQUAÇÃO

Este Módulo tem a finalidade de implementar as adequações sobre os processos, bem como, seus ajustes necessários sobre as questões normativas internas.

FIGURA 09:

MÓDULO IMPLEMENTAÇÃO E ADEQUAÇÃO

Adequação Jurídica

A adequação jurídica diz respeito aos aspectos legais necessários para que a organização esteja em conformidade com a lei. Para isso será apresentado, na próxima versão do Método, um checklist para auxiliar as organizações em seus projetos de adequação.

Políticas de Privacidade e Segurança

O objetivo de uma política de privacidade, além de apresentar uma visão clara de todas as etapas do ciclo de vida dos dados pessoais na organização – incluindo a coleta, utilização, transmissão, distribuição, arquivamento, armazenamento e eliminação – é estabelecer diretrizes que devem ser observadas por todos, podendo ser considerada como principal instrumento de uma estrutura de governança em privacidade.

O Método apresentará modelos de minutas de políticas, normas e termos, na próxima versão, que poderão ser adaptados pelas organizações.

Adequação de Processos e Rotinas de Trabalho

Este tópico contemplará as ações necessárias para a adequação das rotinas e processos de trabalho.

Atendimento aos Titulares

É essencial saber reconhecer se a solicitação feita pelo titular de dados se aplica com base na Lei vigente e quando ela deve ser atendida, bem como ter um plano estruturado para responder às solicitações, reclamações e retificações.

Assim, este tópico aborda as orientações gerais necessárias para o atendimento ao titular além de apresentar ações para uma comunicação efetiva e eficiente entre as partes envolvidas.

Nesse sentido, é fundamental contar com um canal para recebimento de solicitações dos titulares de dados adequado à realidade da organização, considerando os seguintes pontos:

FIGURA 10:

CANAL DE RECEBIMENTO DE SOLICITAÇÕES: O QUE CONSIDERAR

Privacidade no Desenvolvimento

O artigo 46 da LGPD determina que devem ser adotadas medidas técnicas, de segurança e administrativas, que venham garantir a segurança dos dados dos usuários contra acessos não autorizados.

É fundamental que a proteção de dados pessoais e a privacidade dos usuários de qualquer produto ou serviço seja uma premissa em todo e qualquer processo de criação/desenvolvimento, que esta preocupação seja inerente desde a fase de concepção, proteger os dados pessoais ao longo de todo seu ciclo de vida, de ponta a ponta. Este tópico abordará justamente aspectos relevantes associados a esta temática.

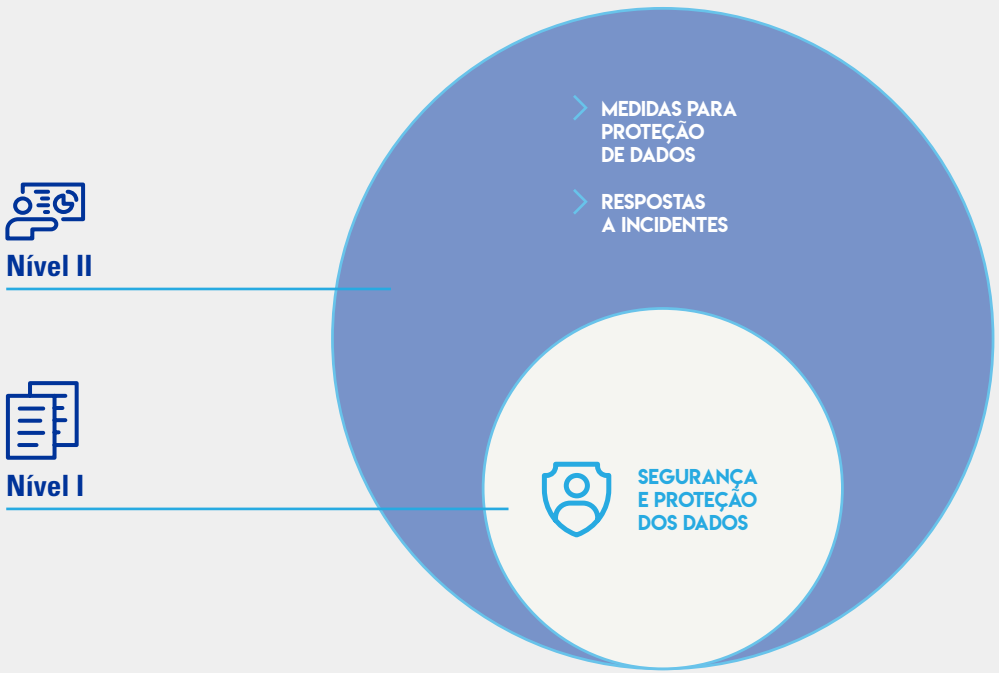
Detalhamentos maiores sobre Privacidade no Desenvolvimento, bem como alguns artefatos (como checklists) que possam auxiliar na adequação deste processo, serão abordados na segunda versão do Método RNP.

MÓDULO SEGURANÇA E PROTEÇÃO DOS DADOS

O art. 46 da LGPD, afirma que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Sendo assim, considera-se fundamental abordar neste módulo dois tópicos muito relevantes que dizem respeito à Proteção dos Dados e ao Tratamento de Incidentes de Segurança, que serão explicados a seguir.

FIGURA 11:
MÓDULO SEGURANÇA E PROTEÇÃO DOS DADOS



Medidas para Proteção de Dados

As medidas para proteger os dados dos titulares e manter a organização em conformidade condiz com análises de aplicabilidades constantes com base nos controles da norma: ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27701.

Detalhamentos maiores sobre o Tópico Medidas para Proteção de Dados bem como alguns artefatos (ex. checklist de segurança para auxiliar as organizações na proteção de dados pessoais), estão previstos na segunda versão do Método RNP.

Respostas a Incidentes

Além da contenção de riscos e tratamento das ameaças, a resposta a incidentes consiste na criação de diversos processos, como por exemplo a comunicação do incidente para os titulares de dados pessoais e para a Autoridade Nacional de Proteção de Dados.

Ressaltando a importância e seguindo o disposto no artigo 48 da LGPD, é obrigação do controlador comunicar à autoridade nacional e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Devendo esta comunicação ser feita em prazo razoável, conforme definição da autoridade nacional, tendo em seu conteúdo, no mínimo:

FIGURA 12:
PONTOS A CONSIDERAR NO COMUNICADO SOBRE INCIDENTES DE SEGURANÇA

- A DESCRIÇÃO DA NATUREZA DOS DADOS PESSOAIS AFETADOS
- AS INFORMAÇÕES SOBRE OS TITULARES ENVOLVIDOS
- A INDICAÇÃO DAS MEDIDAS TÉCNICAS E DE SEGURANÇA UTILIZADAS PARA A PROTEÇÃO DOS DADOS
- OS RISCOS RELACIONADOS AO INCIDENTE
- OS MOTIVOS DA DEMORA, NO CASO DE A COMUNICAÇÃO NÃO TER SIDO IMEDIATA
- AS MEDIDAS QUE FORAM OU QUE ESTÃO SENDO TOMADAS PARA REVERTER OU MITIGAR OS EFEITOS DO PREJUÍZO

Resposta a Incidentes, bem como alguns artefatos que possam auxiliar na adequação deste processo (ex. Modelo de formulário de comunicação de incidentes à ANPD, Modelo de comunicação de incidente ao titular) serão abordados na segunda versão do Método RNP.

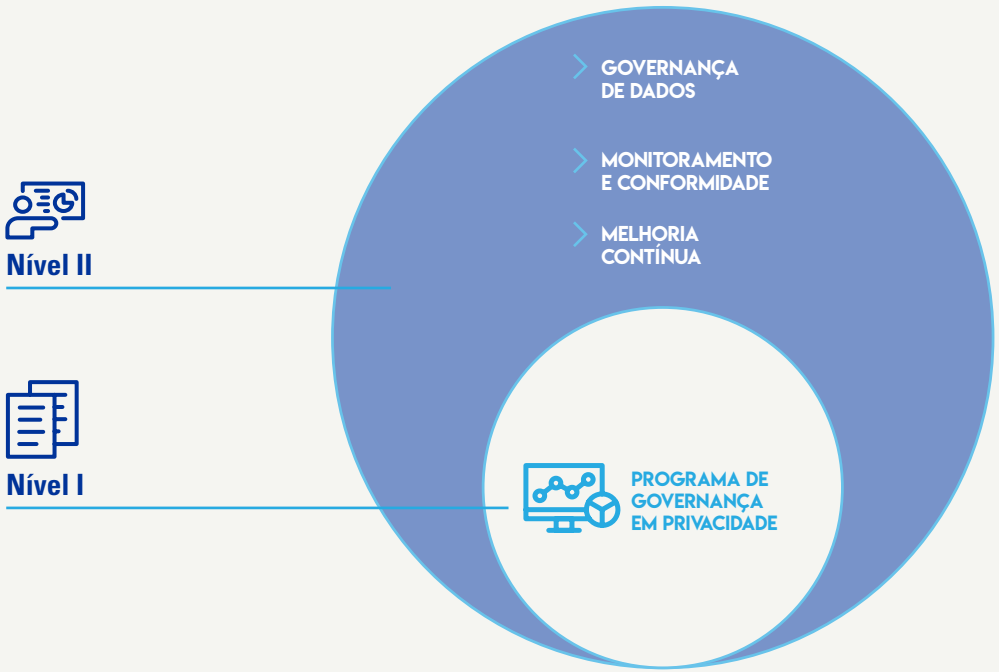
MÓDULO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

A LGPD, em seu art. 50, promove a adoção de boas práticas de governança, formulação de políticas, condução de ações educativas, mitigação de riscos, dentre outros, ressaltando a importância de se implantar um Programa de Governança em Privacidade.

Dessa forma, este módulo apresentará três importantes tópicos que nortearão o estabelecimento e aprimoramento da governança em privacidade dos dados, **conforme Figura 13** a seguir.

FIGURA 13:

MÓDULO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE



Governança de Dados

A Governança de Dados refere-se a um sistema de gestão de dados pessoais, que irá reger todo o ciclo de vida dos dados tratados pela instituição, seja os que já fazem parte de processos e serviços existentes, sejam novos serviços, novos processos, novos dados, ou com novos titulares de dados. Detalhamentos maiores sobre o Tópico Governança de Dados, bem como alguns artefatos como uma minuta de política de governança, estão previstos na segunda versão do Método RNP.

Monitoramento e Conformidade

Além da necessidade de padrões de conformidade e controles que serão apresentados pelo Método RNP, será disponibilizado um fluxo de monitoramento de leis e regulamentos que auxiliará as organizações para estarem em conformidade com a LGPD.

Melhoria Contínua

A prática de melhoria contínua visa tornar os resultados de uma organização, mais eficientes e eficazes, sejam eles em produtos, processos ou serviços relativos ao cumprimento dos normativos internos e identificação de possíveis não conformidades.

Sendo assim, este tópico tem como objetivo avaliar e melhorar de forma permanente os processos, medidas e controles desenvolvidos.

ATENÇÃO

É importante lembrar que o detalhamento dos Níveis III e IV está previsto para a versão 2.0 do Método RNP.