


NORMA DE AVALIAÇÃO DE RISCO

AMCEL - AMAPA FLORESTAL E CELULOSE S.A.

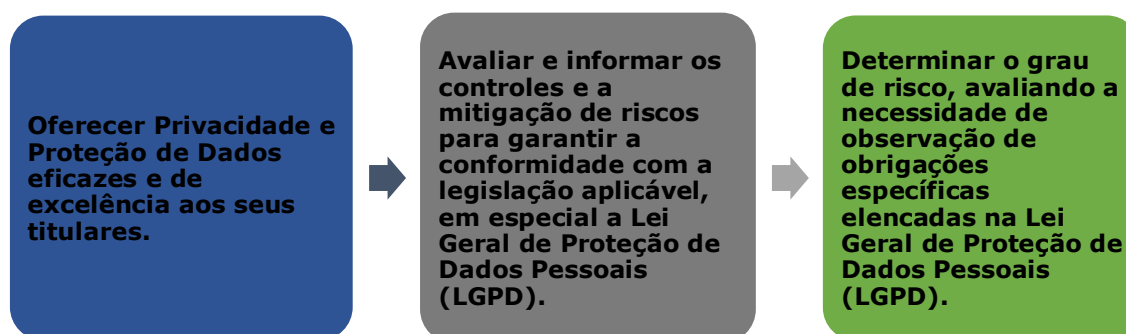
**JUNHO
2021**

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

1. OBJETIVO

Esta Norma de Avaliação de Risco ("Norma") tem como objetivo definir a avaliação do nível de risco, a fim de gerenciar e proteger os Dados Pessoais de acessos não autorizados, assim como de situações acidentais, ilícitas e consequentemente indesejáveis de destruição, perda, alteração, comunicação ou difusão desses ativos de informação, que podem conter dados pessoais de terceiros, dados sensíveis e informações sigilosas que são de responsabilidade efetiva da **AMAPA FLORESTAL E CELULOSE S.A. ("AMCEL")**.

A Avaliação de risco deve ser realizada pelas seguintes razões:




Esta Norma deve ser lida e interpretada de acordo com as demais Políticas de Governança sobre Privacidade e Proteção de Dados desenvolvidas pela **AMCEL**, sendo todas as atribuições e diretrizes aqui definidas aprovadas pela Alta Administração e mandatórias para todos os envolvidos.


Esta Norma aplica-se a todas as unidades da **AMCEL**, e as pessoas nela envolvidas, quais sejam, seus colaboradores, prestadores de serviços, terceiros, parceiros e fornecedores em toda e qualquer operação que envolva o tratamento de Dados Pessoais.

2. DEFINIÇÕES

Para os fins desta Norma, consideram-se as seguintes definições e termos:

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

- **Risco**: Pode ser entendido como a possibilidade, tanto de situações quanto de eventos que venham a ocorrer e que afetem o alcance dos objetivos de negócio. Todas as atividades podem sofrer alguma espécie de risco, a qualquer atividade e pode afetar os ativos, resultados, imagem, reputação, aspectos legais, regulatórios, identidade, confidencialidade ou continuidade dos negócios;
- **Evento**: É o conjunto de circunstâncias que caracteriza a consumação do risco. Na circunstância de risco, os eventos vão além das situações rotineiras, tratando de aspectos de negócios mais amplos, como alteração na estrutura de governança e operacional, influências geopolíticas e sociais e negociações de contratos, entre outros;
- **Incidente**: É o evento indesejável e imprevisto com relação a dados pessoais que tem o potencial de causar transtornos que podem inviabilizar o alcance dos objetivos gerando danos e perdas financeiras, operacionais, legais e de arquivo, entre outros;
- **Severidade**: É a métrica baseada em aspectos como probabilidade e o impacto de eventos ou o tempo necessário para se recuperar dos eventos;
- **Probabilidade**: Indica a possibilidade de ocorrência de um dado evento. Pode ser expressa em termos como: alto, médio, baixo;
- **Impacto**: Resultado ou impacto do risco. Vários possíveis impactos relacionados aos riscos incluem: finanças, operação, imagem e meio ambiente social;
- **Nível de Risco**: Relação entre a probabilidade e impacto, podendo o risco ser classificado em: muito alto, alto, moderado, baixo ou muito baixo;
- **Apetite ao Risco**: O grau de exposição ao risco que a **AMCEL** está disposta a aceitar ou rejeitar na busca de criação de valor e para atingir seus objetivos;
- **Respostas aos Riscos**: A decisão de aceitar, evitar, reduzir e compartilhar o risco. É a decisão que será tomada após a identificação do Risco inerente ou avaliação do

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

ambiente de controle dos Riscos residuais, com objetivo de promover discussões que assegurem a eficiência do ambiente de Controles internos da **AMCEL**;


- **Plano de Ação:** Planejamento e acompanhamento das atividades necessárias para que a resposta ao risco selecionada pela administração seja efetivamente executada para atingir os resultados desejados.

3. PREMISSAS DE AVALIAÇÃO DE RISCO

Esta Norma procura evidenciar diretrizes a fim de nortear a avaliação de riscos relacionados ao tratamento de Dados Pessoais.

Esse processo tem por objetivo que a **AMCEL** esteja segura e alerta sobre atos indesejados que possam acarretar em riscos e incidentes à empresa.

- Adequações práticas: a **AMCEL** adota diversas práticas de governança em privacidade e proteção de dados, através de políticas e normas voltadas às regras e diretrizes que devem nortear o tratamento de Dados Pessoais pela empresa. Assim, há prioridade para que os Titulares dos Dados Pessoais sob o seu controle tenham o tratamento legítimo e legal de tais informações e estejam de acordo com a legislação aplicável;
- Padrões e formalizações: Com um modelo baseado em formalizações e padrões reconhecidos pelo mercado e disseminados entre a estrutura da **AMCEL**, a gestão de riscos relativa ao tratamento de Dados Pessoais é capaz de se adequar a estratégias, iniciativas e estruturas organizacionais, além de atender às exigências setoriais e dos órgãos reguladores e fiscalizadores;
- Reconhecimento e redução de riscos: Estando de acordo com o que foi estabelecido até aqui, e com as demais Políticas e Normas de Privacidade e Proteção de Dados, a **AMCEL** estabelece que todas as avaliações de risco devem incluir a consideração dos benefícios do tratamento, incluindo os benefícios para os indivíduos, para a

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

organização, para terceiros e sociedade, visando a preservação dos benefícios desejados na implementação de quaisquer mitigações para lidar com os riscos identificados. Os benefícios devem ser considerados no início da avaliação de risco uma vez que estão relacionados com a finalidade do tratamento. Os benefícios e propósitos do tratamento devem ser mantidos em mente ao conceber mitigações para evitar a redução desnecessária de os benefícios ou o enfraquecimento dos propósitos;


○ **Infraestrutura:** Para gerenciar os riscos de forma eficiente, a **AMCEL** deve dispor de uma infraestrutura adequada e **AMCEL** de processos, pessoas e tecnologia, estabelecendo mecanismos de comunicação claros e objetivos para tanto;

○ **Avaliação e Reconhecimento de ameaças:** A avaliação de risco deve considerar ameaças potenciais nas atividades de tratamento, como:

- Coleta de dados injustificável ou excessiva;
- uso ou armazenamento de dados imprecisos ou desatualizados;
- uso impróprio ou mau uso de dados, incluindo:
 - Uso de dados além das expectativas razoáveis dos indivíduos;
 - Uso incomum de dados além do razoável, onde qualquer indivíduo médio neste contexto faria objeções;
 - Inferência ou tomada de decisão injustificável, que a organização não pode defender objetivamente.
- dados perdidos ou roubados ou destruição e alteração de dados; e
- acesso injustificável ou não autorizado, transferência, compartilhamento ou publicação de dados.

➤ Deve-se avaliar a probabilidade e gravidade de danos que possam advir do tratamento de risco, como:

- Riscos materiais, tangíveis, físicos ou econômicos aos indivíduos:
 - Perda de liberdade ou movimento, dano ao financeiro e ao poder de ganho.
- Riscos não materiais, intangíveis aos indivíduos:
 - Dano à reputação, perda de autonomia, roubo de identidade.


	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

4. RESPONSABILIDADES

- O **Encarregado pela Proteção de Dados (DPO)** deve atuar de modo a considerar os riscos dos direitos e liberdades fundamentais dos indivíduos no desempenho de suas tarefas, de modo que seja capaz de criar alternativas capazes de suprir quaisquer riscos potenciais.
- O **Comitê Interno de Privacidade e Proteção de Dados** deve auxiliar na identificação e avaliação dos riscos e conduzir os procedimentos de controles rotineiramente a fim de mitigar as vulnerabilidades de suas atividades, em conjunto com o Encarregado, implementar os planos de ação da empresa aprovados pela Alta Administração.

5. PROCESSO E GESTÃO PARA TRATAMENTO DOS RISCOS

- **Primeiro passo - Identificação dos Riscos:**
 - Como primeiro passo, a identificação de riscos deve reconhecer e descrever aos quais eventos que podem causar risco que a empresa está exposta, devendo inclusive, descrever alterações em seus ambientes de negócios;
 - Para tanto, devem ser definidos eventos, causas, consequências e responsáveis por cada risco;
 - Essa identificação dos riscos deve ser realizada com a participação de todos os principais líderes de área e envolvidos nos processos de negócio da empresa, nos seus diferentes níveis, acompanhada pelo Encarregado pela Proteção de Dados Pessoais.
- **Segundo passo - Avaliação dos Riscos:**
 - Como segunda etapa, e já tendo identificado riscos, deve-se realizar análises qualitativas e/ou quantitativas através de processos dinâmicos que objetivam a definição dos atributos de impacto e de probabilidade, para serem utilizados no processo de priorizar os riscos que devem receber o tratamento por primeiro;

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

- Essa avaliação de riscos deve considerar o levantamento e a análise dos controles e ações mitigadoras já existentes.

➤ **Terceiro passo - Tratamento dos Riscos:**

- Posteriormente à avaliação realizada, deve-se prosseguir ao passo de definir o tratamento que será dado aos riscos priorizados e verificar o modo que esses deverão ser monitorados e reportados às diversas partes envolvidas;
- Tratar os riscos consiste em decidir entre evitá-los ou mitigá-los, compartilha-los ou aceitá-los. Devendo estar sempre de acordo com a definição de planos de ação e controles internos;
- A decisão sobre a estratégia adotada para tratar cada risco depende principalmente do Grau de Apetite ao risco da empresa, previamente homologado pela Alta Administração da **AMCEL**.

✓ **Tratamento de riscos de acordo com a Lei Geral de Proteção de Dados**


- De acordo com a Lei Geral de Proteção de Dados, os controladores terão de realizar uma avaliação de risco em vários casos em virtude de requisitos específicos, embora a avaliação de risco não seja explicitamente mencionada nestas disposições.

✓ **Teste de Balanceamento**

- No caso de tratamento de dados pessoais com base no legítimo interesse, para que a **AMCEL** determine se pode seguir o tratamento, deverá se realizar o Teste de Balanceamento com a finalidade de avaliar se seus interesses legítimos são anulados pelos interesses ou direitos e liberdades fundamentais do titular dos dados. Esse teste deve incluir os riscos e potenciais danos, impactos e probabilidades, e incluir uma avaliação de risco.

✓ **Tratamento legítimo**

- A **AMCEL** deve considerar e analisar, entre outros pontos, o impacto e as consequências para os titulares de Dados Pessoais, incluindo riscos e danos que possam sobrevir do tratamento daquelas informações coletadas.

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

✓ **Plano de ação**

- Nessa gestão, o plano de ação envolve o apontamento de ações que sejam necessárias e passíveis de correção para reduzir a exposição aos riscos que sejam residuais, tomando como base o mapeamento das fragilidades indicadas no processo de avaliação do risco.

✓ **Monitoramento dos riscos**


- No processo de monitoramento do risco, deve-se:
- Supervisionar a implantação e manutenção dos planos de ação.
- Verificar o alcance das metas das ações estabelecidas, por meio de atividades gerenciais contínuas e/ou avaliações independentes.
- Garantir que os controles sejam eficazes e eficientes.
- Detectar mudanças no contexto externo e interno, identificando riscos emergentes e analisar as mudanças nos eventos de risco, tendências, sucessos e fracassos e aprender com eles.

✓ **Comunicação dos riscos**

- A comunicação durante todas as etapas aqui descritas na condução do processo de gestão de riscos deve ser acessível e estar disponível a todas as partes interessadas, de modo claro e objetivo, primando pelo respeitando as boas práticas de governança exigidas pela **AMCEL**.

➤ **Redução de riscos:**

- Uma grande variedade de medidas de mitigação de risco pode ser desempenhada pela **AMCEL**, variando desde a pseudonimização, minimização de dados e medidas de segurança. Essas medidas de redução dependem do contexto e devem levar em consideração os riscos envolvidos, o custo de implementação e a eficácia dessas medidas, seu impacto sobre os objetivos, interesses ou benefícios que estão sendo buscados e também as expectativas razoáveis dos titulares, transparência e os elementos de tratamento legítimo.

	NORMA DE AVALIAÇÃO DE RISCO	
	Revisão:	Norma:
Classificação da publicidade: INTERNO	Tipo de documento: NORMA CORPORATIVA	Data de vigência: [xx]

6. REVISÃO

Histórico da última revisão desta Norma:

Elaborado por:	Verificado por:	
Cargo	Cargo	
Nome	Nome	
Aprovado por:		