NORMA DE GESTÃO DE INCIDENTES

AMCEL - AMAPÁ FLORESTAL E CELULOSE S.A.

Junho | 2021

SUMÁRIO

1. INTRODUÇÃO 3
2. OBJETIVO 3
3. APLICAÇÃO E ALCANCE 4
4. RESPONSÁVEL 4
5. LOCALIZAÇÃO DO DOCUMENTO 4
6. TERMOS E DEFINIÇÕES RELATIVAS AO INCIDENTE DE SEGURANÇA DA INFORMAÇÃO 5
7. PAPEIS E RESPONSABILIDADES 6
8. REGRAS GERAIS PARA TRATAMENTO DE INCIDENTES 10
9. ASPECTO DIDÁTICO 13
10. RESUMO HISTÓRICO DAS REVISÕES E CONTROLE DE VERSÕES 15
11. ANEXO I – APROVAÇÃO DO DOCUMENTO 16
12. ANEXO II - REVISÕES 17

1. INTRODUÇÃO

Através de suas governanças internas e gestões que englobam a Privacidade e Proteção de Dados a **AMCEL - AMAPA FLORESTAL E CELULOSE S.A.** estabelece, através desta Norma, os procedimentos relativos à gestão da Segurança da Informação como resposta a ampliar de forma efetiva os valores do comprometimento e segurança à proteção e tratamento dos dados em que qualquer pessoa tenha acesso, direta ou indiretamente.

2. OBJETIVO

2.1 A presente Norma possui o objetivo específico de estabelecer as funções, responsabilidades e medidas a serem adotadas e para assegurar um enfoque consistente e efetivo no gerenciamento dos Incidentes de Segurança que envolvam Dados Pessoais ("Incidente"), incluindo a comunicação interna, as funções de cada equipe, o reconhecimento das fragilidades e eventos que podem causar danos à **AMCEL**.

2.2 pela presente Norma, assegura-se o objetivo do registro e reporte de incidentes e riscos, de modo a garantir, pela tomada de decisão em tempo hábil, minimizar eventuais impactos aos negócios da **AMCEL**, ou riscos e danos aos titulares de dados, sejam clientes e parceiros, principalmente, mas não se restringindo àqueles relativos aos Dados sensíveis, (referentes à saúde ou à vida sexual, dados genéticos ou biométricos) e quaisquer dados que, quando tratados de forma combinada com outras informações, possam permitir inferir informações dessa natureza.

3. APLICAÇÃO E ALCANCE

3.1. Inicialmente, confere-se que a presente Norma é aplicada para qualquer caso de Incidente de Segurança que envolva Dados Pessoais, estando amplamente em consonância com as demais políticas e gestões da **AMCEL**, vigente desde sua apresentação à comunidade.

3.2. Engloba-se, portanto, neste escopo, todos os sócios, diretores, administradores, empregados e demais membros da **AMCEL** ou que possuam relações e possam ter acesso às áreas onde se encontram as informações, equipamentos, arquivos, redes, documentos ou outros dados relativos da **AMCEL.**

4. RESPONSÁVEL

4.1. A revisão da presente Norma ficará a encargo do Comitê Interno de Privacidade e Proteção de Dados e deverá ocorrer anualmente ou em periodicidade menor, quando houver necessidade.

5. LOCALIZAÇÃO DO DOCUMENTO

5.1. Este documento pode ser consultado em sua via digital no diretório ou fisicamente junto ao Departamento de Tecnologia de Informação.

6. TERMOS E DEFINIÇÕES RELATIVAS AO INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

6.1. Inicialmente, cabe destacar que um Incidente de Segurança da Informação envolvendo Dados Pessoais é toda e qualquer violação de segurança que, de forma acidental ou dolosa, enseje ou seja capaz de dar ensejo à destruição, perda, alteração, divulgação ou ao uso ou acesso não autorizados a Dados Pessoais tratados pela **AMCEL**.

6.2 Esses incidentes podem se configurar por diversos modos, explica-se:

Vazamento de Dados Pessoais	Configura-se por ser o Incidente no qual os Dados Pessoais expostos e disponibilizados, *indevidamente,* por meios físicos ou digitais, para um número indeterminado de pessoas, no Brasil ou em qualquer país.
Negação de Serviço **Acesso não autorizado**	Configura-se por ser o Incidente no qual o *acesso (lógico ou físico) a um sistema que armazene Dados Pessoais é prejudicado ou impossibilitado,* de forma que a integridade dos Dados Pessoais (existência e/ou veracidade) pode ser comprometida permanentemente, dada a indisponibilidade do acesso. Configura-se por ser o Incidente no qual o acesso (lógico ou físico) a um sistema que possua Dados Pessoais é tentado ou obtido, sem que se tenha a devida autorização para tal acesso. Portanto, o acesso não autorizado é aquele cuja permissão para conexão, leitura, gravação, autenticação, modificação, eliminação ou criação não tenha sido concedida.

Uso inapropriado	Configura-se por ser o Incidente no qual há a violação das políticas de uso de dados, informações e sistemas da Empresa, incluindo a Política de Segurança da Informação, e demais gestões internas utilizadas para garantir a Privacidade e Proteção de Dados.

6.2. É através dessa gestão de Incidentes, que se garante que seja implementada a gestão da "confiabilidade", composta de três aspectos basilares, quais sejam:

Confiabilidade	Garantir que a informação, quando necessária, esteja acessível apenas aos colaboradores autorizados e/ou processos, e seja devidamente protegida do conhecimento alheio.
Integridade	Garantir que a informação esteja correta, verdadeira e não esteja adulterada, espelhando a realidade.
Disponibilidade	Participar de treinamentos e programas de conscientização para mitigação de Incidentes.

6.3. Desse modo, salienta-se que um Incidente não se caracteriza unicamente pelo vazamento de informações, pela invasão de *crakers* ou pela infecção do sistema por arquivos maliciosos, mas está previsto nas tabelas anteriormente estabelecidas, pode ser um uso inapropriado, por exemplo. Confira a diferença entre incidentes e riscos:

Incidentes	**Riscos**

Assim, todos os eventos que comprometam com os aspectos da confiabilidade da informação serão considerados incidentes. Para tanto, o ideal é que o incidente seja evitado quando ainda é apenas um risco, assim, não é preciso que um incidente se concretize para que ações corretivas sejam tomadas.	Podemos classificar o ***risco como sendo a probabilidade de uma ameaça*** (ex. um arquivo malicioso, um usuário mal-intencionada, um *phishing*, uma descarga elétrica, uma tempestade, etc.), ou atos que visam a tirar proveito de uma vulnerabilidade, (ex. um antivírus desatualizado, arquivos sem controle de acesso, colaboradores sem preparo, um servidor situado em local suscetível a enchentes ou sem nobreak, etc.) e comprometer algum dos aspectos da confiabilidade da informação através de um incidente.

6.4. Portanto, os riscos e incidentes de segurança da informação deverão ser comunicados e tratados de acordo com as diretrizes estabelecidas nesta norma, saiba como, através dos papéis e responsabilidades, abaixo designados:

7. PAPEIS E RESPONSABILIDADES

7.1. Cada uma das áreas da **AMCEL**, sejam as áreas diretamente envolvidas na governança ou não, tem responsabilidades quando da ocorrência ou mera suspeita de um Incidente, conforme descritas a seguir:

7.2. Obrigação de todas as áreas:

- Caberá a todos prezar pela comunicação imediata sobre a ocorrência ou a mera suspeita de um Incidente, ou de um Risco.

- Caberá a todos cumprir rigorosamente as Políticas e gestões vigentes que possam contribuir para a segurança das informações e gestão de incidentes da **AMCEL**, contribuindo para a mitigação de riscos; e

- Caberá a todos participar ativamente de treinamentos e programas de conscientização para mitigação de Incidentes.

7.3. Caberá ao Departamento de Tecnologia da Informação:

7.3.1. Elaborar testes de segurança, realizar avaliações preventivas e reativas, produzir relatórios sobre os indicadores referentes à segurança da rede de computadores da **AMCEL**;

7.3.2. Implementar e receber do Comitê de Proteção de Dados, sugestões de medidas técnicas que visem o monitoramento acerca dos resultados em Relatório Trimestral de Incidentes;

7.3.3. Mapear, tratar, diagnosticar e monitorar os arquivos, programas maliciosos (tais como *malware*), ou eventuais ações de usuários com potencial de gerar incidentes e riscos ao sistema da empresa;

7.3.4. Receber, registrar, classificar e monitorar, em conjunto com o Gestor ou Usuário competente, os comunicados de riscos ou incidentes, visando implementar medidas necessárias para neutralização, restabelecimento de sistemas, recuperação de ativos, a fim de garantir que o risco e incidentes aconteçam;

7.3.5. Informar ao Encarregado todos os riscos atinentes a dados pessoais;

7.3.6. Produzir em conjunto um Relatório de Tratamento do Incidente, do qual constará todos os detalhes do evento, tais como avaliação, possíveis motivos, evidências, classificação quanto à criticidade, ativos comprometidos, extensão dos danos e demais detalhes úteis ao tratamento e registro do incidente;

7.3.7. Extrair o conteúdo didático de incidentes ocorridos na empresa, utilizando o documento em treinamentos a fim de elaborar materiais para conscientização dos Usuários sobre como prevenir e reagir aos incidentes que prejudiquem a Segurança da Informação;

7.3.8. Criar e gerir canal para receber comunicações de riscos ou incidentes associados à segurança da informação e proteção de dados, divulgando amplamente sua existência e forma de utilização aos Usuários;

7.3.9. Criar e divulgar formulário destinado a instruir o processo de comunicação de riscos e incidentes pelos Usuários;

7.3.10. Proceder com auditorias internas para identificação das causas de incidentes, implementando ações corretivas;

7.3.11. Informar aos comunicantes dos riscos ou incidentes sobre o resultado do tratamento.

7.4. <u>Caberá ao Encarregado</u>:

7.4.1. Apoiar o Departamento de Tecnologia da Informação no desempenho de suas atribuições;

7.4.2. Oferecer orientações aos demais colaboradores, terceiros, fornecedores e clientes da **AMCEL**, referentes à prevenção de incidentes;

7.4.3. Comunicar nas reuniões do Comitê de Privacidade de Dados qualquer ocorrência de descumprimento das Políticas de Segurança da Informação por parte dos empregados, a fim de cobrar aplicações de medidas disciplinares.

7.4.4. Comunicar a **Autoridade Nacional de Proteção de Dados - ANPD** e ao titular a respeito da ocorrência de incidentes de segurança que possam acarretar em riscos ou danos relevantes aos titulares. O comunicado deverá conter, no mínimo:

- 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, observados os segredos comercial e industrial;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata; (devendo sempre respeitar o prazo de 02 (dois) dias para seu reporte, e;
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

7.4.5. Receber e atender as comunicações da **Autoridade Nacional de Proteção de Dados - ANPD** referentes a incidentes, desenvolvendo, quando for o caso, em conjunto com o Comitê planos para publicização do incidente e medidas para reverter ou mitigar seus efeitos.

7.5. <u>Caberá aos Gestores de Departamentos:</u>

7.5.1. Realizar a gestão do monitoramento, comunicação e tratamento de riscos e incidentes que afetem sua área;

7.5.2. Fiscalizar colaboradores, terceiros e fornecedores relacionados com seu departamento em relação ao cumprimento de regras de segurança, voltadas à prevenção de riscos e incidentes, prestando orientação e aplicando as sanções, quando detectado descumprimento desta e das demais políticas de segurança.

7.5.3. Comunicar ao DPO e ao Comitê de Privacidade de Dados qualquer ocorrência ou suspeita de violação de dados que vá em desacordo com as políticas de segurança da informação dentro da empresa.

7.6. <u>Caberá aos Usuários</u>:

7.6.1. Observar e cumprir com todas as medidas de segurança previstas nas Políticas e Normas referentes à Segurança da Informação e Proteção de Dados Pessoais da **AMCEL**;

7.6.2. Comunicar imediatamente ao Departamento de Tecnologia da Informação e ao Encarregado pela Proteção de Dados possíveis e quaisquer indícios de risco ou incidente que afetem a segurança da informação e proteção de dados pessoais da **AMCEL**;

7.6.3. Registrar via documentos e comunicar ao Departamento de Tecnologia da Informação e ao Encarregado pela Proteção de Dados sobre pontos vulneráveis de segurança com potencial de acarretar incidentes, bem como sugerir melhorias fundamentadas.

8. REGRAS GERAIS PARA TRATAMENTO DE INCIDENTES

8.1 O tratamento de ameaças e incidentes da **AMCEL** ocorrerá de acordo com o seguinte cronograma:

a) Comunicação: Uma vez identificado o Risco ou o Incidente de Segurança da Informação o comunicante (a primeira pessoa que assim o constatar), deverá no prazo máximo de 24 (vinte e quatro horas), reportar imediatamente ao Departamento de Tecnologia da Informação através

do canal Priv. e Proteção de Dados no website da AMCEL ou através do email eduardo.marques@amcel.com.br

É preferível que nesta comunicação contenha:

- A data e hora em que a suspeita do Incidente ou o Risco foi descoberto;
- O(s) tipo(s) de informações envolvidas;
- A(s) causa(s) do possível Incidente, Risco ou de um Efetivo Incidente;
- O contexto em que ocorreu;
- Informações adicionais que sirvam para facilitar o entendimento do evento, suas causas e consequências.

ATENÇÃO: A COMUNICAÇÃO SOBRE RISCOS OU ATÉ MESMO A SUSPEITA DE UM INCIDENTE DE INFORMAÇÃO É EXTREMAMENTE NECESSÁRIA. ASSIM, CASO O COMUNICANTE CONSTATE TAL SUSPEITA E NÃO O COMUNIQUE, SANÇÕES DISCIPLINARES PODEM OCORRER. AVISE-NOS!

b) **Análise**: Após a comunicação, se seguirá a imediata análise do risco ou incidente pelo Departamento de Tecnologia da Informação, que deverá:

(i) Arquivar a comunicação, caso identifique que não se trata de risco ou incidente relativo à segurança da informação;

(ii) Produzir o Relatório de Tratamento de Incidente, classificando-o de acordo com seu nível de criticidade, nos termos das tabelas abaixo.

volume de Dados Pessoais expostos				
	Alto	**Alta Gravidade**	**Alta Gravidade**	**Alta Gravidade**
	Médio	**Média Gravidade**	**Alta Gravidade**	**Alta Gravidade**
	Baixo	**Baixa Gravidade**	**Média Gravidade**	**Média Gravidade**

Baixa Média Alta

sensibilidade dos Dados Pessoais afetados

GESTÃO CORRETA: OBSERVAR: O VOLUME DE DADOS PESSOAIS EXPOSTOS E A SENSIBILIDADE DESSES DADOS, com apoio das tabelas abaixo:

Criticidade	Descrição
Nível 01: Muito Alto	Comprometimento de diretórios ou sistemas críticos, paralisando um ou mais departamentos; comprometimento da confidencialidade, integridade e/ou disponibilidade de informações estratégicas e dados pessoais.
Nível 02: Alto	Risco ou incidente de comprometimento de diretórios ou sistemas, com a possibilidade de os usuários afetados continuarem a desempenhar sua função, mas sem a garantia da mesma qualidade; alta probabilidade de comprometimento da Confidencialidade, Integridade e/ou Disponibilidade de informações estratégicas e dados pessoais.
Nível 03: Médio	Os usuários conseguem, com certo esforço, realizar com a mesma qualidade as tarefas pelo incidente. É baixa a probabilidade de comprometimento da confidencialidade, integridade e/ou disponibilidade de informações estratégicas e dados pessoais.
Nível 04: Baixo	O risco ou incidente não gera qualquer impacto em diretórios ou sistemas, nem compromete a confidencialidade, integridade e/ou disponibilidade de informações estratégicas e dados pessoais. No entanto, caso não seja tratado o risco ou incidente poderá ter sua criticidade agravada.

VOLUME DE DADOS PESSOAIS EXPOSTOS			**SENSIBILIDADE DOS DADOS PESSOAIS AFETADOS**	
Criticidade	**Descrição**		**Criticidade**	**Descrição**
Alto	volume de Dados Pessoais afetado superior a 10% da base de dados controlada pela Empresa		Alta	Dados Pessoais de crianças ou adolescentes, Dados Pessoais Dados Sensíveis ou que possam gerar discriminação ao titular; dados bancários, de pagamento ou de proteção ao crédito
Médio	volume de Dados Pessoais afetado inferior a 10% e superior a 2% da		Média	Dados Pessoais imediatamente identificáveis (por exemplo, nome, e-mail, CPF), combinados ou não

	base de dados controlada pela Empresa			com informações comportamentais (e.g. histórico de atividades, preferências etc.)
Baixo	volume de Dados Pessoais afetado inferior a 2% da base de dados controlada pela Empresa		Baixa	Dados anonimizados, Dados Pessoais pseudonimizados (desde que a chave de desanonimização também não tenha sido comprometida), Dados Pessoais de difícil identificação (por exemplo o endereço de IP)

c) **Escalação**: Classificado o risco ou incidente, caso envolva dados pessoais, o Departamento de Tecnologia da Informação solicitará apoio por e-mail ao Encarregado e/ou ao gestor e usuários da área afetada, cujo apoio julgue necessário.

- A depender da criticidade, complexidade, extensão dos danos e ativos afetados (conforme analisados pelas tabelas supracitadas), o Departamento de Tecnologia da Informação será envolvido no tratamento o Comitê de Privacidade e Proteção de Dados.

d) **Tratamento**: Após a escalação, o Departamento de Tecnologia da Informação com apoio do Encarregado e demais gestores e Usuários, respeitada a ordem de prioridade de acordo com a classificação de criticidade:

- Alimentará o Relatório de Tratamento de Incidente, documentando o impacto e quais ativos e departamento foram ou serão afetados;
- Implementará ações necessárias para estancar os danos gerados pelo incidente, isolando ambientes, diretórios e sistemas comprometidos;
- Identificará possíveis eventos que podem ter gerado o incidente, coletando e documentando evidências;
- Avaliará possíveis soluções com base em seu conhecimento, normas técnicas, apoio de demais áreas ou empresas terceirizadas, aplicando as ações necessárias para neutralização do incidente, restabelecimento de sistemas, recuperação de ativos, garantindo que o risco de recorrência foi eliminado ou mitigado, se não for possível sua eliminação;
- Quando assim definido pelo Comitê Estratégico de Segurança da Informação e Proteção de Dados, o Encarregado comunicará aos titulares afetados e à **Autoridade Nacional de Proteção de Dados – ANPD** sobre a ocorrência de incidentes envolvendo dados

pessoais, seguindo as determinações do Comitê e em prazo não superior a 02 (dois) dias úteis e seguindo as orientações e modelos disponibilizados pela ANPD;

- Se certificará de que inexistem outros incidentes ou riscos relacionados, abrindo chamados adicionais se for o caso;
- Encerrado o tratamento, devolverá o caso ao Comitê Gestor para validação.

e) **Validação**: Finalizado o tratamento o Departamento de Tecnologia da Informação reportará através do Relatório de Tratamento de Incidentes ao Comitê Interno, que validará se o tratamento aplicado foi suficiente para a completa resolução do incidente; se há a necessidade de coleta de demais dados e evidências para fins didáticos e de auditoria;

f) **Encerramento**: Validado o tratamento, o Departamento de Tecnologia da Informação encerrará o chamado, inserindo todos os dados necessários no Relatório de Tratamento de Incidente e informará ao comunicante sobre o resultado do tratamento.

9. ASPECTO DIDÁTICO

9.1 A fim de reduzir riscos e fortalecer o Sistema de Gestão de Segurança da Informação, o Comitê:

a) Deverá produzir relatório trimestral com informações relacionadas a incidentes de Segurança da Informação, do qual constará um resumo dos Relatórios de Tratamento de Incidente do período, indicadores sobre incidentes, análise da efetividade de tratamentos, recomendações para neutralização ou redução de ameaças, riscos e incidentes. O relatório será apresentado ao Comitê para debate e planejamento de medidas;

b) O relatório trimestral guiará a formulação de um inventário para monitoramento e avaliação dos riscos, o qual deverá ser debatido junto ao Comitê;

c) Produzir e atualizar os materiais didáticos, realizará treinamentos e eventos voltados à Segurança da Informação, tendo por base as informações extraídas dos tratamentos, resguardada a anonimização e sigilo de informações.

10. RESUMO HISTÓRICO DAS REVISÕES E CONTROLE DE VERSÕES

Data da elaboração	Data da revisão atual	Elaborador/Aprovador	Versão
08.06.2021			01/2021

ANEXO I – APROVAÇÃO DO DOCUMENTO

Aprovador	Área	Assinatura	Data

ANEXO II - REVISÕES

Versão / Revisão	**Data**	**Revisor**	**Itens alterados** (adicionar breve descrição da alteração)
1.0			
1.1			
1.2			
1.3			
1.4			
1.5			
1.6			
1.7			