



NORMA DE GESTÃO DE ACESSO

JULHO

2021

Tipo de documento: Norma	Classificação da publicidade: Interno	Versão: 01/2021
Nome do documento: Norma de Gestão de Acesso	Data de vigência:	Código do documento:

1. OBJETIVO

Através desta Política de Gestão de Acesso ("Política"), a **AMCEL - AMAPA FLORESTAL E CELULOSE S.A.**, estabelecerá os critérios de segurança necessários para o controle de acesso às informações e dados armazenados em sistemas, aplicativos ou outros ativos de informação que pertencem à infraestrutura tecnológica da **AMCEL**.

2. ABRANGÊNCIA/VALIDADE

Esta Política se aplica a todos os usuários dos recursos de tecnologia da informação e comunicação, incluindo funcionários, prestadores de serviços ou terceiros que estejam a serviço da **AMCEL** e inicia sua vigência a partir da data de sua emissão, por período indeterminado.

3. CONCEITO DE ACESSO

Por acesso, compreende-se toda e qualquer forma de interação com as informações disponibilizadas e os dados que nela constem, incluindo desde a simples visualização ou consulta até a extração de cópias, alteração, exclusão etc., acesso este, à dados, informações e arquivos contidos em qualquer meio, seja físico ou digital. O conceito de acesso é subdividido em três:

- **Acesso Público:** É todo acesso permitido, sem restrições, a senhas, marcações em lista etc.;
- **Acesso Restrito:** É todo acesso autorizado aos Usuários indicados. O acesso não autorizado pode causar graves danos ao negócio e/ou comprometer a estratégia de negócio da Companhia;
- **Acesso Sigiloso:** É o acesso restrito para um grupo específico de pessoas, podendo ser composto por empregados, clientes e/ou fornecedores. O acesso não autorizado pode causar diversos impactos à **AMCEL**, como de ordem financeira, de imagem e afins. O descumprimento acarretará sanções administrativas, civis e criminais.

Elaboração:	Revisão:	Aprovação:
Data:	Data:	Data:
NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTES DOCUMENTOS TORNA UMA CÓPIA NÃO CONTROLADA		

Tipo de documento: Norma	Classificação da publicidade: Interno	Versão: 01/2021
Nome do documento: Norma de Gestão de Acesso	Data de vigência:	Código do documento:

4. PRINCÍPIO NORTEADOR

O controle de acesso à informação estará norteado sob o Princípio da Necessidade (art. 6º, III, da Lei Geral de Proteção de Dados – LGPD), que determina que o acesso aos dados pessoais e informações de titulares terceiros só poderá e deverá ocorrer quando houver a constatação da efetiva necessidade de se obter acesso àquela informação, sistema ou aplicativo para sua função laboral.

5. RESPONSABILIDADE

O não cumprimento das normas estabelecidas nesta Política, seja isolada ou cumulativamente, poderá ensejar, ao colaborador, de acordo com a infração cometida, as seguintes medidas:

(A) COMUNICAÇÃO DE DESCUMPRIMENTO:

- Será encaminhado ao colaborador, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada.

(B) RESCISÃO DO CONTRATO:

- Em casos de faltas graves e/ou de reiteração da prática, após efetiva comunicação ao colaborador, poderá haver a rescisão do contrato com este, bem como a adoção das medidas legais cabíveis.

6. CRITÉRIOS PARA CONCESSÃO DE ACESSO E LIMITE DA PERMISSÃO

A concessão de acesso será definida tanto de acordo com a necessidade do acesso a dados e informação, quanto pela análise da função desempenhada pelo colaborador. A permissão de acesso será realizada a partir de solicitação do gerente da área, podendo, inclusive, ser determinado tal acesso por um período limitado de tempo.

A concessão de acesso e permissão temporária poderá ocorrer nos casos em que seja necessário ter acesso às informações que antes não havia, por falta de necessidade ou por não precisar

Elaboração:	Revisão:	Aprovação:
Data:	Data:	Data:
NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTES DOCUMENTOS TORNA UMA CÓPIA NÃO CONTROLADA		

Tipo de documento: Norma	Classificação da publicidade: Interno	Versão: 01/2021
Nome do documento: Norma de Gestão de Acesso	Data de vigência:	Código do documento:

utilizar. Desse modo, a permissão de acesso será vigente enquanto for necessário para realizar atividades pontuais que não estão no escopo de atuação do colaborador e que também não será necessário continuar com o acesso no futuro próximo.

Não há limite de tempo para esse acesso, podendo ser tanto de algumas horas quanto dias ou semanas, desde que sempre esteja à luz da necessidade.

7. DIRETRIZES GERAIS

- Somente usuários finais previamente identificados e autorizados podem ter acesso aos ativos de informação da **AMCEL**;
- Todo o acesso aos sistemas, aplicativos ou outros ativos de informação, os usuários deverão digitar seu ID e senha, para que possam ser identificados (identificação) e verificar (autenticação) a identidade do usuário de forma inequívoca, sendo a senha individual e intransferível;
- Para a definição dos critérios a serem usados no controle de acesso, deve-se considerar o seguinte:
 - A natureza do utilizador (isto é, interna e externa, de visitante, consultor etc.);
 - As funções existentes na empresa (por exemplo, diretor, gerente, supervisores, coordenadores, assistentes, estagiário, aprendizes).
- Os critérios de acesso devem ser específicos para cada aplicação, de acordo com as definições de privilégios definidos pelos proprietários das informações;
- A única forma dos usuários acessarem os ativos de informações armazenados em ambientes de produção devem ser por meio de aplicativos;
- As aplicações controlarão o acesso do usuário por meio de mecanismos para garantir que os usuários não tenham acesso com privilégios distintos a outros que não os autorizados pelo proprietário das informações;
- Deve ser definido como limite (01) uma sessão para a mesma aplicação e fonte de dados pelos usuários finais;

Elaboração:	Revisão:	Aprovação:
Data:	Data:	Data:
NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTES DOCUMENTOS TORNA UMA CÓPIA NÃO CONTROLADA		

Tipo de documento: Norma	Classificação da publicidade: Interno	Versão: 01/2021
Nome do documento: Norma de Gestão de Acesso	Data de vigência:	Código do documento:

- Não se deve permitir o acesso anônimo a qualquer recurso dentro da plataforma de tecnologia disponível na **AMCEL**;
- As telas de abertura da aplicação prévia, as telas de solicitações de credenciais, incluindo este último deve mostrar o mínimo de informação sobre o aplicativo que se destina a entrar (ou seja, não exibir informações sobre o sistema operacional). As senhas não devem ser exibidas no procedimento de entrada;
- Os identificadores são automaticamente bloqueados após cinco tentativas fracassadas. Bloqueios automáticos podem ser mais restritivos se as aplicações os garantem com base na importância dos ativos de informação que gerenciam;
- No caso de sistemas multiusuários em que o procedimento de autenticação seja bem sucedido, deve aparecer imediatamente após o acesso, o seguinte:

"Aviso:

*Esses recursos são exclusivos para o uso de pessoal autorizado ou colaboradores da **AMCEL**, suas subsidiárias e coligadas. O uso não autorizado é proibido e sujeito a sanções. Todos os indivíduos que usam este sistema computacional estão sujeitos a que suas atividades sejam monitoradas e gravadas pelo pessoal de sistemas."*

- No caso de sistemas ou aplicações que não permitem apresentar a mensagem acima imediatamente depois de um procedimento de autenticação bem sucedida, os sistemas devem respeitar antes de tentar acessar a rede do texto:

"Atenção:

*Para acessar este sistema necessitará uma autorização prévia, sendo estritamente limitado ao uso especificado na autorização. Acesso não autorizado ou uso indevido do mesmo é estritamente proibida e constitui uma violação da segurança da informação da **AMCEL**. A utilização deste sistema pode ser monitorado. "*

- Todas as tentativas de conexão (sucesso ou falha) deve gerar um registro.

8. ATRIBUIÇÃO A SETORES ESPECÍFICOS

8.1 Atribuições do Departamento de Tecnologia da Informação

Elaboração:	Revisão:	Aprovação:
Data:	Data:	Data:
NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTES DOCUMENTOS TORNA UMA CÓPIA NÃO CONTROLADA		

Tipo de documento: Norma	Classificação da publicidade: Interno	Versão: 01/2021
Nome do documento: Norma de Gestão de Acesso	Data de vigência:	Código do documento:

O Departamento de Tecnologia da Informação (TI) será o responsável pela criação e atualização de acessos, separada por função – cargo e necessidade de acesso. Nessa matriz, constará a definição de cada perfil de acesso, justificativas, diretórios e sistemas acessados por cada perfil, responsáveis e demais detalhes necessários ao gerenciamento de acessos. Além disso, o setor de Tecnologia da Informação terá um diálogo horizontal tanto com os Gestores Internos quanto com o Departamento Pessoal para garantir que as informações de acesso estejam sempre atualizadas.

O setor também será responsável por conceder, alterar e cancelar os acessos de usuários a diretórios e sistemas após o recebimento da solicitação constatando informações para realizar os ajustes das permissões quando verificado que o acesso é excessivo e não condiz com a necessidade do usuário – como pode ocorrer, por exemplo, quando há uma mudança interna de cargo/função e o acesso tenha se tornado desnecessário, conforme descrito nas diretrizes gerais.

8.2 Atribuições dos Gestores dos Setores Internos

Caberá a cada Gestor dos Setores Internos prestar apoio ao Departamento de Tecnologia da Informação durante a definição dos acessos necessários aos colaboradores do seu departamento, garantindo que cada usuário acesse somente as informações de que necessite para o desempenho de sua função.

Além disso, os Gestores deverão solicitar ao Departamento de Tecnologia da Informação, mediante prévia justificativa e por tempo determinado, a liberação de acessos privilegiados aos usuários de seu departamento, em casos específicos e que se julgue necessário a liberação de tal acesso.

8.3 Atribuições ao Departamento Pessoal

Caberá ao Departamento Pessoal comunicar ao Departamento de Tecnologia da Informação sobre a necessidade de concessão, alteração ou cancelamento de acessos de usuários, além

Elaboração:	Revisão:	Aprovação:
Data:	Data:	Data:
NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTES DOCUMENTOS TORNA UMA CÓPIA NÃO CONTROLADA		

Tipo de documento: Norma	Classificação da publicidade: Interno	Versão: 01/2021
Nome do documento: Norma de Gestão de Acesso	Data de vigência:	Código do documento:

de informar, de forma imediata, a alteração de cargo ou o desligamento de empregados, como uma medida de controlar de forma efetiva o acesso aos sistemas de informações.

8.4 Atribuição aos Usuários

O usuário terá o acesso necessário para executar as suas funções laborais, devendo informar ao Departamento de Tecnologia da Informação caso exista a possibilidade de acessar diretórios excedentes ou de outras funções.

Além disso, para ampliar o sigilo e a segurança dos ativos de informação, o Controle de Acesso à Informação também possui a diretriz de que os Usuários não anotem, registrem ou compartilhem logins, senhas, ID's, tokens, etc. Em caso de suspeitas de utilização do seu Usuário por terceiros, este deverá informar, imediatamente, o Departamento de Tecnologia da Informação (TI) para que sejam adotadas as medidas necessárias.

9. REVISÃO

Histórico da última revisão da Norma:

Elaborado por:	Verificado por:
Aprovado por:	

10. LOCALIZAÇÃO DO DOCUMENTO

É possível consultar esta Norma em sua via fisicamente junto à área de Tecnologia de Informação.

Elaboração:	Revisão:	Aprovação:
Data:	Data:	Data:
NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTES DOCUMENTOS TORNA UMA CÓPIA NÃO CONTROLADA		

Tipo de documento: Norma	Classificação da publicidade: Interno	Versão: 01/2021
Nome do documento: Norma de Gestão de Acesso	Data de vigência:	Código do documento:

Elaboração:	Revisão:	Aprovação:
Data:	Data:	Data:
NOTA: A REPRODUÇÃO OU IMPRESSÃO DESTES DOCUMENTOS O TORNA UMA CÓPIA NÃO CONTROLADA		